UNODC

مكتب الأمم المتحدة المعني بالمخدرات والجريمة

استخدام الإنترنت
في أغراض إرهابية

بالتعاون مع

فرقة العمل التابعة للأمم المتحدة المعنية بتنفيذ تدابير مكافحة الإرهاب

مكتب الأمم المتحدة المعني بالمخدرات والجريمة
فيينا

استخدام الإنترنت في أغراض إرهابية

الأمم المتحدة
نيويورك، ٢٠١٣

© الأمم المتحدة، حزيران/يونيه ٢٠١٣. جميع الحقوق محفوظة، في العالم أجمع.

لا تنطوي التسميات المستخدمة في هذا المنشور ولا طريقة عرض المادة التي يتضمّنها على الإعراب عن أيّ رأي كان من جانب الأمانة العامة للأمم المتحدة بشأن المركز القانوني لأيّ بلد أو إقليم أو مدينة أو منطقة أو للسلطات القائمة فيها أو بشأن تعيين حدودها أو تخومها.

والقصد من إيراد عناوين المواقع الشبكية وروابطها الواردة بصيغة صحيحة في هذا المنشور وقت إصداره، هو تيسيرُ الرجوع إليها على القارئ. والأمم المتحدة ليست مسؤولة عن صحّة هذه المعلومات في المستقبل ولا عن مضمون أي موقع خارجي على الشبكة.

هذا المنشور من إنتاج: قسم اللغة الإنكليزية والمنشورات والمكتبة، مكتب الأمم المتحدة في فيينا.

"الإنترنت هي خير مثال يوضِّح كيف يمكن للإرهابيين أن يمارسوا نشاطهم على نحو عابر للحدود حقاً؛ وتصدِّياً لذلك ينبغي للدول أن تفكِّر وتعمل على نحو عابر للحدود أيضاً."

بان كي-مون
الأمين العام للأمم المتحدة

تصدير

المدير التنفيذي
مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة

إنَّ استخـدام الإنترنت في أغراض إرهابية ظاهرة تتفشَّى بسرعة، وتتطلب من الدول الأعضاء أخذ زمام المبادرة للتصدِّي لها بالتنسيق فيما بينها.

ويؤدي مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة (المكتب) دوراً محورياً في تقديم المساعدة للدول الأعضاء، تنفيـذاً للولايـة المسنـدة إليه من أجل تدعيم قـدرة نظم العدالة الجنائيـة الوطنية على تنفيـذ أحكام الصكوك القانونيـة الدوليـة لمكافحة الإرهاب، وذلك وفقاً لمبادئ سيادة القانون والمعايـير الدولية لحقوق الإنسان. ويُذكر، علـى وجه الخصوص، أنَّ الجمعية العامـة أكَّدت من جديد، في قراراها ١٧٨/٦٦ لعام ٢٠١١، الولايةَ المسندة إلى المكتـب لكي يواصل تطوير المعـارف القانونية المتخصِّصة في مجال مكافحة الإرهـاب والمجالات المواضيعية ذات الصلة بولاية المكتب، بما في ذلك استخدام الإنترنت في أغراض إرهابية.

وبالرغـم مـن تزايد الإدراك الدولي للخطـر الذي يشكِّله استخـدام الإرهابيين للإنترنـت في السنوات الأخيرة، فـلا يوجد في الوقـت الراهن صك عالمي يتناول خصِّيصـاً هذا الجانب المتفشِّي من جوانـب الأنشطة الإرهابية. وعـلاوة على ذلك، ليس هناك سـوى عدد محدود من البرامج التدريبية المتخصِّصـة المعنية بالجوانب القانونية والعمليـة للتحقيق في قضايا الإرهاب التي تُستخدم فيها الإنترنت والملاحقة القضائية بشأنها. ويأتي هذا المنشور تكملـةً للمراجع القائمة التي أعدَّها المكتب في مجالات مكافحة الإرهـاب، والجرائم السيبرانية (جرائم الفضاء الحاسوبـي)، وسيادة القانون. كما يتناول أهمية تكوين رصيد معرفي متكامل ومتخصِّص للاستجابة لاحتياجات الـدول الأعضاء من المساعدة التقنية من أجل التصدِّي لهـذا الخطر الذي يتغيَّر باستمرار. وإنَّ المكتب لفي غاية الامتنان لحكومة المملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية لدعمها السخي الذي أتاح نشر هذا العمل.

ويهدف المنشور، الذي يُتوخَّى استخدامُه مرجعاً قائماً بذاته والاستعانة به في دعم مبادرات بناء القدرات التابعة للمكتـب، إلى التوجيه بشـأن الأطر القانونيـة والممارسات القائمة علـى الصعيدين الوطني والـدولي فيما يتعلق بتجريم قضايا الإرهاب التي يُستخدم فيها الإنترنت والتحقيق والملاحقة القضائية بشأنها.

إنَّ الإرهاب، بكل مظاهره، يمسُّنا جميعاً. كما أنَّ استخدام الإنترنت في أغراض إرهابية يتعدَّى الحدود الوطنية، بما قد يترتَّب على ذلك من آثار مضاعفة على الضحايا. ويهدف هذا المنشور، عبر تسليط الضوء على نماذج من تدابـير التصدِّي لهذا التحدِّي الفريد من نوعه وعلى أفضـل الممارسات بهذا الشأن، إلى أمرين هما: أولاً، إذكاء الوعـي بالطرائق التي تمكِّن مـن إساءة استخدام تكنولوجيـا الاتصالات لارتكاب أعمال إرهابيـة؛ ثانياً، تكثيف التعـاون بـين الدول الأعضاء بحيـث يمكن وضع تدابير فعَّالة في مجـال العدالة الجنائية للتصـدِّي لهذا التحدِّي العابر للحدود الوطنية.

يوري فيدوتوف
المدير التنفيذي
مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة

فرقة العمل المعنية بتنفيذ تدابير مكافحة الإرهاب
التابعة للأمين العام

يهدف الفريق العامل المعني بمكافحة استخدام الإنترنت في أغراض إرهابية التابع لفرقة العمل المعنية بتنفيذ تدابير مكافحة الإرهاب إلى تنسيق الأنشطة التي تقوم بها منظومة الأمم المتحدة لدعم استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب، التي اعتمدتها الجمعية العامة في قرارها ٢٨٨/٦٠، والتي عقدت فيها الدول الأعضاء العزم على "تنسيق الجهود المبذولة على الصعيدين الدولي والإقليمي لمكافحة الإرهاب بجميع أشكاله ومظاهره على الإنترنت" وعلى "استخدام الإنترنت كأداة لمكافحة تفشّي الإرهاب، مع التسليم في الوقت نفسه بأنَّ الدول قد تحتاج إلى المساعدة في هذا الصدد". وقد استبان الفريق العامل ثلاثة مواضيع محورية للمناقشة وهي: المسائل القانونية، والمسائل التقنية، والطرائق التي تمكّن المجتمع الدولي من استخدام الإنترنت بمزيد من الفعالية لمكافحة الإرهاب، بكشف زيف الرسالة الإرهابية التي تقول بأنَّ العنف وسيلة مشروعة من وسائل إحداث تغيير سياسي.

ويعود الفضل الكبير في إنجاز هذه الدراسة، التي أعدَّها المكتب في إطار أعمال الفريق العامل، إلى الدول الأعضاء التي أسهمت فيها وقدَّمت لها الدعم. وقد بلغت مناقشةُ التحدِّيات القانونية مرحلةً جديدةً بفضل هذه الدراسة، التي تضيف الكثير إلى رصيد المعارف والخبرات الذي تكوّن لدى الفريق العامل في هذا المجال وتَقاسَمه مع الدول الأعضاء. وتقوم الدراسة، على وجه الخصوص، بتقديم أمثلة مهمة على تشريعات الدول الأعضاء التي تتناول استخدام الإرهابيين لشبكة الإنترنت وتوضِّح، من خلال أمثلة حقيقية على قضايا قانونية، الصعوبات التي تواجهها الدول الأعضاء في تجريم هذه الأعمال والملاحقة القضائية بشأنها.

وإنَّ الفريق العامل لعلى ثقة من أنَّ هذا التقرير سوف يساعد على الوقوف على المجالات التشريعية التي يمكن للأمم المتحدة أن تساعد فيها الدول الأعضاء على تنفيذ الاستراتيجية العالمية لمكافحة الإرهاب من أجل التصدِّي لاستخدام الإنترنت في أغراض إرهابية.

ريتشارد باريت
منسِّق فريق الدعم التحليلي ورصد الجزاءات
المشارِك في رئاسة الفريق العامل المعني بمكافحة استخدام الإنترنت في أغراض إرهابية
التابع لفرقة العمل المعنية بتنفيذ تدابير مكافحة الإرهاب

حكومة المملكة المتحدة

لقـد اضطلعت المملكة المتحدة بدور ريادي في سنِّ تشريعـات لمكافحة استخدام الإنترنت في أغراض إرهابية على مدار العقد الماضي؛ وقد حقَّقنا نجاحاً ذا شأن في التصدِّي للأنشطة الإرهابية عبر الإنترنت داخل حدود البلاد، فيما نبذل قصارى جهدنا للحفاظ على الحريات وما جلبته الإنترنت من مزايا لمواطنينا.

بيـد أننـا ندرك أنَّ هذا الخطر يتعدَّى الحدود الوطنية بطبيعته. ولـن يتأتَّى للمجتمع الدولي أن يأمل في التصدِّي الفعَّال لاستخدام الإنترنت في أغراض إرهابية إلاَّ بالعمل سوياً.

ومن ثمَّ فإنَّ الحكومة البريطانية ترحِّب بالفرصة التي سنحت لها لمساندة مكتب الأمم المتحدة المعني بالمخدِّرات والجريمـة في إعداد المنشور الـذي بين أيديكم. ونأمل أن يتحوَّل هذا المنشور بسرعـة إلى أداة مفيدة يستعين بها المشرّعـون، والمسؤولـون عن إنفاذ القانون، والممارسـون في مجال العدالة الجنائية، علـى استحداث وتنفيذ أطر قانونيـة مـن شأنها أن تعرقل أنشطة الإرهابيـين على الإنترنت بفعالية، فيكون بذلـك، في حال بلوغ هذا الهدف، إسهاماً قيِّماً في جعل مجتمعاتنا—الحقيقية منها والافتراضية—أماكن أكثر أماناً.

سايمن شيركليف
رئيس قسم مكافحة الإرهاب (العمليات)
وزارة الخارجية البريطانية

سو هيمينغ
رئيسة شعبة الجرائم الخاصة ومكافحة الإرهاب
النيابة العامة البريطانية

المحتويات

الصفحة

تصدير v

المدير التنفيذي، مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة v

فرقة العمل المعنية بتنفيذ تدابير مكافحة الإرهاب التابعة للأمين العام vi

حكومة المملكة المتحدة..... vii

الخلفية ١

أولاً- استخدام الإنترنت في أغراض إرهابية..... ٣

ألف- مقدِّمة..... ٣٣

باء- طرائق استخدام الإنترنت في أغراض إرهابية..... ٣٣

جيم- استخدامات الإنترنت في مكافحة الأنشطة الإرهابية ١٢

دال- الاعتبارات المتعلقة بسيادة القانون ١٣

ثانياً- السياق الدولي ١٥

ألف- مقدِّمة..... ١٥

باء- قرارات الأمم المتحدة بشأن مكافحة الإرهاب ١٦

جيم- الصكوك القانونية العالمية بشأن مكافحة الإرهاب ١٧

دال- القانون الدولي لحقوق الإنسان ١٩

هاء- الصكوك القانونية الإقليمية ودون الإقليمية بشأن مكافحة الإرهاب..... ٢٠

واو- التشريعات النموذجية..... ٢٣

ثالثاً- أطر السياسات العامة والتشريعات..... ٢٧

ألف- مقدِّمة..... ٢٧

باء- السياسات العامة ٢٧

جيم- التشريعات..... ٣١

رابعاً- التحقيقات وجمع المعلومات الاستخبارية..... ٥٣

ألف- أدوات ارتكاب جرائم الإرهاب باستخدام الإنترنت ٥٣

باء- التحقيقات في جرائم الإرهاب المرتكبة باستخدام الإنترنت ٦٠

الصفحة

جيم- حفظ بيانات التحليل الجنائي واسترجاعها ٦٤

دال- التأكّد من صحة الأدلة الرقمية ٦٧

هاء- وحدات عمليات الجرائم السيبرانية ٦٨

واو- جمع المعلومات الاستخبارية ٧٠

زاي- التدريب ٧٢

خامساً- التعاون الدولي ٧٣

ألف- مقدِّمة ٧٣

باء- الصكوك والترتيبات المتعلقة بالتعاون الدولي ٧٣

جيم- الأطر التشريعية الوطنية ٨٢

دال- التدابير غير التشريعية ٨٣

هاء- التعاون الرسمي مقابل التعاون غير الرسمي ٨٩

واو- التحديات والقضايا المطروحة ٩١

سادساً- الملاحقة القضائية ١٠١

ألف- مقدِّمة ١٠١

باء- اتِّباع نهج قائم على سيادة القانون في الملاحقات الجنائية ١٠١

جيم- دور أعضاء النيابة العامة في قضايا الإرهاب ١٠٢

دال- مرحلة التحقيقات ١٠٣

هاء- التعاون الدولي ١٠٦

واو- مرحلة الاتهام ١٠٦

زاي- مرحلة المحاكمة: المسائل المتعلقة بالأدلة ١٠٧

حاء- مسائل أخرى ١٢٠

سابعاً- التعاون مع القطاع الخاص ١٢٣

ألف- دور جهات القطاع الخاص المعنية ١٢٣

باء- الشراكة بين القطاعين العام والخاص ١٣٠

ثامناً- الخلاصة ١٣٣

ألف- استخدام الإنترنت في أغراض إرهابية ١٣٣

باء- السياق الدولي ١٣٣

جيم- أطر السياسات العامة والتشريعات ١٣٤

الصفحة

دال- التحقيقات وجمع المعلومات الاستخبارية ١٣٦
هاء- التعاون الدولي ١٣٦
واو- الملاحقة القضائية..... ١٣٩
زاي- التعاون مع القطاع الخاص..... ١٤١

المرفق

قائمة بأسماء المساهمين في هذا المنشور ١٤٣

الخلفية

التكنولوجيا هي أحد العوامل الاستراتيجية التي تمكِّن التنظيمات الإرهابية وأنصارها من استخدام الإنترنت استخداما متزايدا في مجموعة واسعة ومتنوعة من الأغراض، تشمل التجنيد، والتمويل، والدعاية، والتدريب، والتحريض على ارتكاب أعمال إرهابية، وجمع المعلومات ونشرها لأغراض إرهابية. ولئن كانت العديد من فوائد شبكة الإنترنت بديهية، فإنَّها قد تُستخدم أيضاً لتيسير الاتصال داخل التنظيمات الإرهابية، لا لإرسال معلومات حول الأعمال الإرهابية المزمع القيام بها فحسب، بل لتقديم الدعم المادي لتنفيذ هذه الأعمال أيضا، مما يتطلب معرفة تقنية معيَّنة تمكّن من التحقيق في هذه الجرائم بفعالية.

ومن بين المبادئ المقبولة عموماً أنه ينبغي أن تتاح لمن يشتبه في كونهم إرهابيين، بالرغم مما يُنسب إليهم من أعمال شنيعة، الضمانات الإجرائية ذاتها التي يكفلها القانون الجنائي لغيرهم من المشتبه فيهم. والدفاع عن حقوق الإنسان قيمةٌ من القيم الأساسية للأمم المتحدة وحجر الزاوية في نهج مكافحة الإرهاب بالاستناد إلى سيادة القانون. ومن ثم فإنَّ هذا المنشور يسلِّط الضوء على أهمية احترام مبادئ حقوق الإنسان والحريات الأساسية على الدوام، ولا سيما في سياق وضع الصكوك القانونية المتعلقة بمكافحة الإرهاب وتنفيذ هذه الصكوك.

ويشارك مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة (المكتب)، بصفته كياناً رئيسياً من كيانات الأمم المتحدة المعنية بتقديم المساعدة القانونية في مجال مكافحة الإرهاب والمساعدة التقنية ذات الصلة، مشاركة فاعلة في أنشطة فرقة العمل المعنية بتنفيذ تدابير مكافحة الإرهاب، بما يضمن تنفيذَ عمله في مجال مكافحة الإرهاب في سياق أوسع نطاقا وهو الجهود المبذولة على صعيد منظومة الأمم المتحدة واتّساقَه مع تلك الجهود. وفي كانون الثاني/يناير ٢٠١٠، بدأ الفريق العامل المعني بمكافحة استخدام الإنترنت في أغراض إرهابية التابع لفرقة العمل في عقد سلسلة من المؤتمرات بمشاركة ممثلين عن الحكومات، والمنظمات الدولية والإقليمية، ومجامع الفكر، والأوساط الأكاديمية، والقطاع الخاص، لدراسة استخدام الإنترنت في أغراض إرهابية والوسائل التي يمكن استعمالها للتصدي له. وكان الهدف من وراء مبادرة الفريق العامل تقديم لمحة عامة للدول الأعضاء عن طبيعة هذا التحدي في الوقت الراهن واقتراح مبادئ توجيهية للسياسات العامة، ومشاريع وإرشادات عملية فيما يخص جوانب هذا التحدي القانونية والتقنية والجوانب المتعلقة بالخطاب المضاد. وقد عُقدت مؤتمرات الفريق العامل في برلين في كانون الثاني/يناير ٢٠١٠، وفي سياتل بالولايات المتحدة الأمريكية في شباط/فبراير ٢٠١٠ وفي الرياض في كانون الثاني/يناير ٢٠١١.

واضطلع فرع منع الإرهاب التابع للمكتب، في إطار أداء الولاية المسندة إليه في "تطوير المعارف القانونية المتخصصة في مجال مكافحة الإرهاب ... وتقديم المساعدة لمن يطلب[ها] من الدول الأعضاء ... لتعزيز قدرة نظم العدالة الجنائية على مواجهة الإرهاب، بما في ذلك ... استخدام شبكة الإنترنت لأغراض إرهابية"،[1] بالإسهام في مشروع الفريق العامل عبر وضع هذه الأداة للمساعدة التقنية بشأن استخدام الإنترنت في أغراض

[1] قرار الجمعية العامة ١٧٨/٦٦.

إرهابية، وذلك بالتعاون مع الفرع المعني بالجريمة المنظمة والاتجار غير المشروع التابع للمكتب وبدعم من حكومة المملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية. ويستند هذا المنشور، الذي يصدره المكتب، إلى ما خلصت إليه مؤتمرات الفريق العامل، وبالأخص المؤتمر المنعقد في برلين في كانون الثاني/يناير ٢٠١٠ بشأن جوانب الإرهاب القانونية الخاصة بالإنترنت.

وعقد المكتب، في إطار إعداد هذا المنشور، اجتماعين لفريق من الخبراء في فيينا، في تشرين الأول/أكتوبر ٢٠١١ وشباط/فبراير ٢٠١٢، لإتاحة الفرصة لممارسين متخصصين في مجال مكافحة الإرهاب من مجموعة متنوعة جغرافياً من الدول الأعضاء للالتقاء وتبادل الخبرات فيما يتعلق باستخدام الإنترنت في أغراض إرهابية. وقد شارك في هذين الاجتماعين خبراء من ٢٥ دولة عضواً، منهم مجموعة من كبار المدعين العامين والمسؤولين عن إنفاذ القانون والأكاديميين، فضلا عن ممثلين عن عدة منظمات حكومية دولية. وقد اعتُمد في هذا المنشور اعتماداً كبيراً على المناقشات والخبرات التي جرى تبادلها أثناء هذين الاجتماعين، وهو يهدف إلى تقديم إرشادات عملية للدول الأعضاء تيسيراً للتحقيق والملاحقة القضائية بمزيد من الفعالية بشأن قضايا الإرهاب التي تُستخدم فيها الإنترنت.

أولاً- استخدام الإنترنت في أغراض إرهابية

ألف- مقدِّمة

١- ثبتت جدوى الإنترنت منذ أواخر الثمانينات باعتبارها وسيلة اتصال شديدة الحيوية، لها القدرة على الوصول إلى جمهور ما فتئ يزداد في كل أنحاء العالم. وقد أدى استحداث تكنولوجيات تتطور باستمرار إلى خلق شبكة ذات نطاق انتشار شامل بحق للعالم أجمع، تقلّ العوائق أمام الدخول إليها نسبيا. وقد جعلت تكنولوجيا الإنترنت من السهل على الفرد أن يتواصل عبر الحدود، بسرعة وفعالية ومع إمكانية عدم الكشف عن هويته إلى حدّ ما، مع عدد يكاد يكون غير محدود من الأشخاص. ولتكنولوجيا الإنترنت فوائد عديدة، بدءاً من سهولة تبادل المعلومات والأفكار التي تتيحها بشكل منقطع النظير، وهذا حقّ من حقوق الإنسان الأساسية المعترف بها.[٢] غير أنَّه لا بد من الإقرار بأنَّ نفس التكنولوجيا التي تتيح هذا النوع من التواصل يمكن أن تُستغل أيضاً لأغراض إرهابية. ويطرح استخدام الإنترنت في أغراض إرهابية تحدياتٍ كما يتيح فرصاً في مجال مكافحة الإرهاب.

باء- طرائق استخدام الإنترنت في أغراض إرهابية

٢- اعتُمد في هذا المنشور نهج وظيفي فيما يخص تصنيف الطرائق التي كثيراً ما تُستخدم بها الإنترنت للتشجيع على القيام بأعمال إرهابية ودعمها. وقد أفضى هذا النهج إلى تحديد ست فئات تتداخل في بعض الأحيان وهي: الدعاية (بما يشمل التجنيد، والدفع باتجاه التطرف، والتحريض على الإرهاب)، والتمويل، والتدريب، والتخطيط (بما يشمل التخطيط عبر الاتصالات السرية والمعلومات المستمدة من مصادر علنية)، والتنفيذ، والهجمات السيبرانية. ويتطرق المنشور كل فئة من هذه الفئات بمزيد من التفصيل فيما يلي.

١- *الدعاية*

٣- يستخدم الإرهابيون الإنترنت أكثر ما يستخدمونه لبثّ دعايتهم. وعادة ما تتخذ الدعاية شكل اتصالات عبر وسائط متعددة تحمل تعاليم إيديولوجية أو إرشادات عملية، أو تقدم شروحاً للأنشطة الإرهابية أو تسوق المبررات لها أو تشجع على القيام بها. ومن بين ما يمكن أن تتضمنه هذه الاتصالات الرسائلُ الافتراضية، والعروض الإيضاحية، والمجلات، والأطروحات، وملفات صوتية ومرئية، وألعاب الفيديو التي تصممها التنظيمات الإرهابية أو يصممها المتعاطفون معها. بيد أنَّ اعتبار مادة ما بمثابة دعاية إرهابية، بدلا من اعتبارها من قبيل المناصرة المشروعة لوجهة نظر ما، غالباً ما يدخل في باب الاستنساب. وعلاوة على ذلك، فإنَّ بث الدعاية ليس، على وجه العموم، نشاطاً محظوراً في حدّ ذاته. فأحد المبادئ الأساسية للقانون الدولي هو حماية حقوق الإنسان الأساسية، التي تشمل الحق في حرية التعبير (انظر المناقشة الواردة في الباب أولا-دال أدناه)، وهو

[٢] انظر، على سبيل المثال، العهد الدولي الخاص بالحقوق المدنية والسياسية (مرفق قرار الجمعية العامة ٢٢٠٠ ألف (د-٢١)، (الفقرة ٢ من المادة ١٩.

ما يكفل للفرد الحق في أن يشاطر الآخرين رأيه أو أن يوزّع مواد ذات محتوىً قد يعتبره غيره مُشينا، إلا في حالات محدودة معينة. ومن بين الاستثناءات المقبولة عموماً فيما يتعلق بهذا الحق الحظرُ المفروض على توزيع مواد معينة ذات محتوى جنسي صريح يرتأى حظرها خدمةً للصالح العام من أجل حماية بعض الفئات الضعيفة. وهناك استثناءات أخرى تستوجب جميعا النص عليها في القانون وتبيان أسباب لزومها، وقد تشمل الاتصالات التي تضرّ ضرراً واضحاً بحماية الأمن القومي، والاتصالات التي يجتمع فيها عنصرا التحريض عن قصد على ارتكاب أعمال عنف ضد أفراد بعينهم أو مجموعات معينة من الأفراد، واحتمال نجاح هذا التحريض.[٢]

٤- والتشجيع على العنف أمرٌ شائع في الدعاية للإرهاب. ويزيد نطاق الانتشار الواسع للمواد التي توزَّع عبر الإنترنت من أعداد المتأثرين بمحتوى هذه المواد بأضعاف مضاعفة. وعلاوة على ذلك، فإنَّ القدرة على توزيع المواد عبر الإنترنت تقلّل من الاعتماد على قنوات الاتصال التقليدية، مثل دوائر الإعلام، التي قد تتخذ خطوات للتحقّق من مصداقية المعلومات الواردة إليها على نحو مستقل أو تقوم بتعديل أو حذف الجوانب التي تعتبرها استفزازية إلى حدّ الإفراط. كما قد تشتمل الدعاية على الإنترنت على محتويات من قبيل مشاهد فيديو لأعمال إرهابية عنيفة أو ألعاب فيديو تصممها تنظيمات إرهابية للتحريض على القيام بأعمال إرهابية وتشجيع المستخدم على تمثيل دور إرهابي افتراضي.

٥- كما أنَّ الترويج للخطاب المتطرف الذي يشجّع على أعمال العنف توجّهٌ شائع لدى مجموعة متزايدة من منصات الإنترنت التي تنشر محتويات يعدّها المستخدِمون أنفسهم. وقد أصبحت الإنترنت وسيلة لعرض الكثير من المحتويات التي كانت توزَّع في السابق على جمهور محدود نسبياً، من شخص إلى شخص أو عن طريق وسائط مادية مثل الأقراص المدمجة وأقراص الفيديو الرقمية. وقد توزَّع هذه المحتويات باستخدام مجموعة كبيرة ومتنوعة من الأدوات، كالمواقع المخصّصة لمواضيع معيّنة، أو بعض غرف الدردشة والمنتديات المحددة الأهداف، والمجلات الإلكترونية، ومنصات التواصل الاجتماعي مثل تويتر وفيسبوك، والمواقع ذات الشعبية لعرض صور الفيديو وتبادل الملفات، مثل يوتيوب ورابيدشير. كذلك فإنَّ استخدام خدمات الفهرسة، مثل محرّكات البحث على الإنترنت، يجعل من كشف المحتويات ذات الصلة بالإرهاب والحصول عليها أمراً أكثر سهولة.

٦- إنَّ أكبر خطر تشكّله الدعاية الإرهابية يتعلق بالطريقة التي تُستخدم بها والقصد الذي تُبثّ من أجله. فالدعاية الإرهابية التي توزَّع عبر الإنترنت تشمل مجموعة واسعة من الأهداف وتُوجَّه إلى مختلف أنواع الجماهير. فقد تُصمَّم الدعاية خصّيصاً من أجل المؤيدين المحتملين أو الفعليين لتنظيم من التنظيمات أو لأحد المعتقدات المتطرفة المشتركة، أو من أجل معارضي هذا التنظيم أو المعتقد، أو من أجل الضحايا المباشرين أو غير المباشرين لأعمال إرهابية، أو من أجل المجتمع الدولي أو جزء منه، في جملة مجموعات أخرى. وقد تركِّز الدعاية التي تستهدف المؤيدين المحتملين أو الفعليين على التجنيد، والدفع باتجاه التطرف، والتحريض على الإرهاب، عبر رسائل تعبّر عن مشاعر الفخر والاعتزاز بتحقيق الأهداف المرسومة والتفاني من أجل تحقيق هدف متطرف. كما يمكن أن تُستخدم هذه الدعاية لإثبات النجاح في تنفيذ هجمات إرهابية لمن قدَّم دعماً مالياً لمنفذي هذه الأعمال. وقد تشمل الأهداف الأخرى للدعاية الإرهابية التأثير على نفسية الفرد لإضعاف إيمانه ببعض القيم الاجتماعية الجماعية، أو لبث شعور بالقلق الزائد أو الخوف أو الذعر في مجتمع من المجتمعات أو شريحة منه. وقد يتأتى

[٢] المرجع نفسه، الفقرة ٣ من المادة ١٩.

ذلـك عبر نشر معلومات مضلِّلة، أو شائعات، أو تهديدات باستخـدام العنف، أو صور لأعمال عنف تثير المشاعر. وقد يشمل الجمهور المستهدف أولئك الذين يشاهدون المواد الدعائية مباشرة، فضلا عن من يتأثرون بالإشاعات التـي قـد تنتشر بسبب هذه المواد. وفيما يخص المجتمع الدولي بشكل عام، فإن الهدف من الدعاية غالباً ما يكون إعطاء الانطباع بأنَّ القائمين عليها يسعون لتحقيق غايات سياسية نبيلة.[٤]

(أ) التجنيد

٧- يمكـن استخدام شبكة الإنترنت لا باعتبارها وسيلة لنشر الخطـاب المتطرف ومقاطع الفيديو التي تندرج ضمنـه فحسب، بـل أيضاً لإقامة علاقات بمـن يتجاوبون مع الدعايـة والتماس الدعم منهـم. وتُقبِل التنظيمات الإرهابيـة إقبـالا متزايدا على استخـدام مواد الدعاية التي تُـوزَّع عبر منصّات مثل المواقـع المحمية بكلمات سرّ وروابـط مجموعـات الدردشة التي يخضع الدخول إليها لقيود باعتبارها وسيلـة للتجنيد السري.[٥] ويتيح انتشار شبكة الإنترنت الواسع للتنظيمات الإرهابية والمتعاطفين معها إمكانيةَ التجنيد على نطاق عالمي. وتُنسِج منتديات الإنترنـت التـي يخضع الدخـول إليها لقيود المجـالَ أمام المجنَّدين ليتعرّفـوا على التنظيمـات الإرهابية ويقدّموا دعمهم لها وينخرطوا مباشرة في أعمال تهدف إلى تحقيق أهداف إرهابية.[٦] كما أنَّ استخدام حواجز تكنولوجية أمـام دخول منصات التجنيـد يزيد من تعقيد عملية تعقّب الأنشطة المتصلة بالإرهـاب من قِبل العاملين بأجهزة الاستخبارات وإنفاذ القانون.

٨- وكثيراً ما تعدّ مواد الدعاية الإرهابية خصّيصاً لتلقى قبولاً لدى الفئات الضعيفة والمهمَّشة في المجتمع. ومن الشّائـع استغـلالُ إحساس الفرد بالحيف أو الإقصاء أو المهانة لتجنيـده والدفع به باتجاه التطرف.[٧] وقد تُكيَّف الدعاية بحسب العوامل الديموغرافية، مثل السن أو نوع الجنس، وكذلك الظروف الاجتماعية أو الاقتصادية.

٩- وقـد تكون شبكة الإنترنت وسيلـة فعّالة للغاية لتجنيد القُصَّر، الذين يمثلون نسبة كبيرة من مستخدميها. وقـد تتّخذ الدعايـة المنشورة عبر الإنترنت بغرض تجنيد القُصَّر شكل رسـوم متحرّكة، أو مقاطع فيديو لموسيقى ذات شعبية، أو ألعاب الكمبيوتر. ومن الأساليب المتّبعة في استهداف القُصَّر من قبل المواقع الشبكية التي تديرها تنظيمـات إرهابية أو أتباعها إقحامُ رسائل تشجع علـى الأعمال الإرهابية، كالهجمات الانتحارية، وتشيد بها، في رسـوم متحركة وقصص للأطفال. وبالمثل، صمّمت بعض التنظيمات الإرهابية ألعاب فيديو على الإنترنت بغرض استخدامهـا أدوات للتجنيـد والتدريب. وقد تـروِّج هذه الألعاب لاستخدام العنف ضد دولـة أو شخصية سياسية بـارزة، مع مكافأة اللاعب على نجاحه في تنفيذ هـذه الأعمال الافتراضية. وقد تُتاح هذه الألعاب بلغات متعددة، حتى تلقى قبولا لدى جمهور واسع.[٨]

---

(٤) Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, D.C., United States Institute of Peace Press, 2006), pp. 37-38.

(٥) Scott Gerwehr and Sarah Daly, "Al-Qaida: terrorist selection and recruitment"، المنشـور في: *The McGraw-Hill Homeland Security Handbook,* David Kamien, ed. (New York, McGraw-Hill, 2006), p. 83.

(٦) Dorothy E. Denning, "Terror's web: how the Internet is transforming terrorism"، المنشـور في: *Handbook of Internet Crime,* Yvonne Jewkes and Majid Yar, eds. (Cullompton, United Kingdom, Willan Publishing, (2010)), pp. 194-213.

(٧) European Commission, Expert Group on Violent Radicalisation, "Radicalisation processes leading to acts of terrorism" (٢٠٠٨). انظر الرابط التالي: www.clingendael.nl/publications/2008/20080500_cscp_report_vries.pdf.

(٨) Gabriel Weimann, "Online terrorists prey on the vulnerable", *YaleGlobal Online,* 5 March 2008. انظر الرابط التالي: http://yaleglobal.yale.edu/content/online-terrorists-prey-vulnerable.

(ب) التحريض

١٠- لئن كانت الدعاية في حد ذاتها غير محظورة على وجه العموم، فإنَّ العديد من الدول الأعضاء تعتبر استخدام الإرهابيين للدعاية من أجل التحريض على أعمال إرهابية أمراً مخالفاً للقانون. فشبكة الإنترنت تتيح عدداً وفيراً من المواد والفرص لتحميل وتحرير وتوزيع محتويات يمكن اعتبارها تمجيداً لأعمال إرهابية أو تحريضاً على ارتكاب هذه الأعمال بما يخالف القانون. بيد أنَّه تجدر الإشارة إلى أن بعض الآليات الحكومية الدولية والآليات المعنية بحقوق الإنسان قد أعربت عن تشكّكها في كون مفهوم "تمجيد" الإرهاب محدَّداً ودقيقاً بما يكفي ليكون بمثابة سند لفرض عقوبات جنائية تفي بمتطلبات مبدأ الشرعية ومع ما هو مسموح به من قيود على الحق في حرية التعبير، على النحو المنصوص عليه في المادتين ١٥ و١٩ من العهد الدولي الخاص بالحقوق المدنية والسياسية.[٩]،[١٠]

١١- ومن المهم التأكيد على التمييز بين الدعاية لمجرّد الدعاية والمواد التي يُقصد بها التحريض على ارتكاب أعمال إرهابية. ففي العديد من الدول الأعضاء، يجب إثبات وجود رُكنيْ القصد اللازم والصلة السببية المباشرة بين الدعاية المزعومة وبين عمل إرهابي خُطِّط له أو نُفِّذ بالفعل، حتى يمكن إقرار المسؤولية الجنائية عن جريمة التحريض على الإرهاب. وعلى سبيل المثال، أشار خبير فرنسي، في إسهام له في اجتماعي فريق الخبراء، إلى أنَّ نشر مواد حول كيفية استعمال المتفجرات لا يعتبر انتهاكاً للقانون الفرنسي ما لم تتضمن الرسالة معلومات تفيد بأن القصد من نشر هذه المواد هو تحقيق غرض إرهابي.

١٢- ويُعتبر كلٌّ من منع التحريض على الإرهاب وردع ذلك التحريض لحماية الأمن القومي والنظام العام مسوِّغين مشروعين لتقييد حرية التعبير، على النحو المنصوص عليه في الفقرة ٣ من المادة ١٩ من العهد الدولي الخاص بالحقوق المدنية والسياسية. كما أنَّ هذين المسوّغين يتفقان مع الفقرة ٢ من المادة ٢٠ من العهد، التي تقتضي أن تحظر الدول أية دعوة إلى الكراهية القومية أو العنصرية أو الدينية تشكِّل تحريضاً على التمييز أو العداوة أو العنف. إلا أنَّ أي القيود على ممارسة الحق في حرية التعبير، في ضوء الأهمية الجوهرية لهذا الحق، لا بد أن تكون ضرورية ومتناسبة مع الخطر الذي يشكّله على حدّ سواء. كما أنَّ الحق في حرية التعبير يرتبط بحقوق هامة أخرى، بما فيها الحق في حرية الفكر والضمير والدين والمعتقد والرأي.[١١]

(ج) الدفع باتجاه التطرف

١٣- يمكن النظر إلى التجنيد والدفع باتجاه التطرف والتحريض على الإرهاب باعتبارها حلقات في سلسلة متصلة. ويشير تعبير "الدفع باتجاه التطرف" في المقام الأول إلى عملية التلقين التي غالباً ما تصاحب تحوّل المجنّدين إلى أفراد عازمين على انتهاج مسلك عنيف استناداً إلى أفكار متطرفة. وكثيراً ما تُستخدم الدعاية في عملية الدفع باتجاه التطرف، سواء الدعاية المنقولة من شخص إلى شخص أو عبر الإنترنت، على مدار فترة

[٩] قرار الجمعية العامة ٢٢٠٠ ألف (د-٢١)، المرفق.

[١٠] انظر التقريرين التاليين الصادرين عن المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب: A/65/258 (الفقرة ٤٦) وA/61/267 (الفقرة ٧)؛ وانظر أيضاً الإضافة المعنونة "الإعلان المشترك بمناسبة الذكرى السنوية العاشرة: التحديات العشر الرئيسية لحرية التعبير في العقد المقبل" إلى تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، (A/HRC/14/23/Add.2).

[١١] مفوضية الأمم المتحدة لحقوق الإنسان، "حقوق الإنسان والإرهاب ومكافحة الإرهاب"، صحيفة الوقائع رقم ٣٢ (جنيف، ٢٠٠٨)، ثالثا، جاء.

زمنيـة. ويتفاوت طول الفـترة الزمنية المطلوبة ومدى فعالية الدعاية وغيرها مـن وسائل الإقناع المستخدمة وفقاً لظروف الأفراد والعلاقات فيما بينهم.

٢- *التمويل*

١٤- يمكـن للتنظيمات الإرهابية وأنصارها أن يستخدموا الإنترنت أيضـاً لتمويل الأعمال الإرهابية. ويمكن أن تصنَّـف الطرائـق التي يستخدمها الإرهابيـون لطلب الأموال والموارد وجمعها عبر الإنترنـت إلى أربع فئات عامة هـي: الطلب المباشر، والتجارة الإلكترونية، واستغـلال أدوات الدفع عبر الانترنت، واستغلال المنظمات الخيرية. ويشير الطلب المباشر إلى استخدام المواقع الشبكية، ومجموعات الدردشة، ورسائل البريد الإلكتروني الجماعية، والاتصـالات الموجَّهـة للأنصار لطلـب تبرعات منهم. كما يمكـن أن تستخدم المواقع الشبكيـة باعتبارها متاجر إلكترونية تبيع الكتب وتسجيلات صوتية ومرئية وغيرها من المواد للأنصار. وتسهِّل خدمات الدفع عبر الإنترنت، المتاحة عبر المواقع الشبكية المخصّصة أو عبر منصّات الاتصالات، تحويلَ الأموال إلكترونياً بين الأطراف المعنية. وكثـيراً ما تحوَّل الأموال عن طريق التحويلات البرقية الإلكترونية، أو بطاقات الائتمان، أو خدمات الدفع البديلة مثل "باي بال" أو "سكايب".

١٥- كذلـك من الممكن استغلال خدمات الدفع عبر الإنترنت بأساليب احتيالية مثل انتحال الشخصية، وسرقة بطاقـات الائتمـان، والاحتيال في التحويلات البرقية الإلكترونية، والاحتيـال في معاملات الأوراق المالية، وجرائم الملكيـة الفكريـة، والاحتيـال في المزادات. ومن الأمثلـة على استخـدام مكاسب غير مشروعـة في تمويل الأعمال الإرهابيـة قضيةُ المملكة المتحدة ضد يونس التسولي (انظر الفقرة ١١٤ أدناه). ففي هذه القضية، غُسلت الأرباح التـي جُنيـت من بطاقات ائتمان مسروقـة بأساليب عديدة، بما في ذلك التحويل بـين حسابات دفع عبر الإنترنت تابعـة لخدمـة إي-غولد، حيث نُقلت الأموال عبر عـدة بلدان قبل أن تصل إلى وجهتهـا المقصودة. وقد استخدم التسولي الأموال المغسولة لتسجيل ١٨٠ من المواقع التي تستضيف مقاطع فيديو دعائية لتنظيم القاعدة من جهة، ولتوفـير المعدات اللازمة لأنشطـة إرهابية في عدة بلدان من جهة أخرى. واستُخـدم في هذه العملية زهاء ١ ٤٠٠ من بطاقات الائتمان للحصول على ما يقارب ١,٦ مليون جنيه إسترليني من الأموال غير المشروعة بغرض تمويل أنشطة إرهابية.[١٢]

١٦- كمـا يمكن تحويل وجهة الدعم المالي الموجَّه إلى منظمات مشروعـة ظاهرياً، مثل المؤسسات الخيرية، إلى أغراضـ غير مشروعة. ومن المعروف أنَّ بعض التنظيمات الإرهابيـة تنشئ شركات صورية، تحت غطاء مشاريع خيرية، لطلب التبرعات عبر الإنترنت. وقد تدّعي هذه المنظمات أنها تقوم بدعم أهداف إنسانية في حين تُستخدم التبرعات في الواقع لتمويل أعمال إرهابية. وتشمل الأمثلة على المنظمات التي تدعي في العلن أنَّها منظمات خيرية فيما تُستخدم لأغراض إرهابية عدداً من المؤسسات التي تحمل أسماء لا توحي بأغراضها الحقيقية مثل: مؤسسة الإحسـان الدوليـة، ومؤسسة الغوث العالميـة، ومؤسسة الأرض المقدسـة للإغاثة والتنميـة، وجميعها استخدمت أساليـب احتياليـة لتمويل تنظيمات إرهابيـة في الشرق الأوسط. كما أنَّ الإرهابيين قـد يخترقون فروعاً لمنظمات خيرية، فيستخدمونها غطاءً للترويج لأفكار التنظيمات الإرهابية أو تقديم دعم مادي لجماعات المقاتلين.[١٣]

[١٢] مذكِّرة مكتوبة قدَّمها الخبير البريطاني.

[١٣] Maura Conway, "Terrorist 'use' of the Internet and fighting back", *Information & Security*, vol. 19 (2006), pp. 12-14.

٣- *التدريب*

١٧- في السنوات الأخيرة، أصبحت التنظيمات الإرهابية تستخدم الإنترنت استخداما متزايدا بوصفه ساحة تدريب بديلة للإرهابيين. وهناك مجموعة متزايدة من الوسائط التي توفِّر منصات لنشر أدلة عملية في صورة كتيبات إلكترونية، ومقاطع صوت وفيديو، ومعلومات، ونصائح. وتتيح هذه المنصات أيضاً تعليمات مفصّلة، غالباً ما تتخذ شكل وسائط متعددة بلغات متعدّدة يسهل الاطّلاع عليها، حول موضوعات مثل كيفية الانضمام إلى تنظيمات إرهابية، وكيفية صُنع المتفجرات، أو الأسلحة النارية، أو غيرها من الأسلحة أو المواد الخطرة، وكيفية التخطيط للهجمات الإرهابية وتنفيذها. وهكذا تكون هذه المنصات بمثابة معسكر تدريبي افتراضي. كذلك فإنَّ هذه المنصات تُستخدم لأمور في جملتها تبادل أساليب أو تقنيات أو معلومات عمليّة محدّدة بغرض ارتكاب عمل إرهابي.

١٨- ومن بين الأمثلة على ما سبق مجلةٌ إلكترونية بعنوان "*إنسباير*"، يُزعم أنَّ تنظيم القاعدة في شبه الجزيرة العربية هو الذي يصدِرها، وغرضها المعلن هو تمكين المسلمين من التدرُّب على الجهاد في منازلهم. وتحتوي المجلة على كمية كبيرة من المواد الإيديولوجية الرامية إلى تشجيع الإرهاب، بما في ذلك تصريحات منسوبة إلى أسامة بن لادن، والشيخ أيمن الظواهري، وغيرهما من الشخصيات المعروفة من تنظيم القاعدة. وقد تضمّن عدد خريف عام ٢٠١٠ تعليمات عمليّة حول كيفية تهيئة سيارة رباعية الدفع لتنفيذ هجوم على أفراد الجمهور، وكيف يمكن لفرد واحد أن يشن هجوماً عشوائياً عن طريق إطلاق النار من سلاح ناري من أعلى برج. بل إنَّ المجلة قد اقترحت مدينة لتكون هدفا لهجوم من هذا القبيل، وذلك لزيادة احتمالات قتل أحد أعضاء الحكومة.[١٤]

١٩- وتشمل المواد التعليمية المتاحة على الإنترنت أدوات لتيسير أنشطة مناهضة الاستخبارات والاختراق الحاسوبي ولتحسين أمن الاتصالات غير المشروعة والأنشطة غير المشروعة على الإنترنت عبر استخدام ما هو متاح من أدوات التشفير وتقنيات إخفاء الهوية. وتساعد الطبيعة التفاعلية لمنصات الإنترنت على خلق شعور بالانتماء إلى جماعة واحدة بين أفرادٍ من مواقع جغرافية وخلفيات مختلفة، بما يشجّع قيام شبكات لتبادل المواد التعليمية والتكتيكية.

٤- *التخطيط*

٢٠- أشار العديد من الممارسين في مجال العدالة الجنائية إلى أنَّ جميع قضايا الإرهاب التي خضعت للملاحقة القضائية تقريباً قد استخدُمت فيها تكنولوجيا الإنترنت. ويُذكر، على وجه الخصوص، أنّ التخطيط لعمل إرهابي عادة ما ينطوي على اتصال عن بُعد ما بين عدة أطراف. ويتضح من قضية حديثة في فرنسا، هي قضية *النائب العام ضد هيشر*،[١٥] كيف يمكن أن تستخدم مختلف أشكال تكنولوجيا الإنترنت لتسهيل التحضير لأعمال إرهابية، بوسائل منها إجراء اتصالات مكثفة داخل التنظيمات التي تروِّج للتطرف العنيف وفيما بينها، وكذلك عبر الحدود.

[١٤] مذكرة مكتوبة قدَّمها الخبير البريطاني.

[١٥] حكم صادر بتاريخ ٤ أيار/مايو ٢٠١٢ عن محكمة باريس الابتدائية في القضية رقم ٠٩٢٦٦٣٩٠٣٦ (الغرفة الرابعة عشرة/٢)، باريس.

النائب العام ضد هيشر

في أيار/مايو ٢٠١٢، حكمت محكمة فرنسية على عدلان هيشر، وهو مواطن فرنسي من أصل جزائري، بالسجن خمس سنوات لاشتراكه في مؤامرة إجرامية للتحضير لعمل إرهابي (بموجب المادة ٤٢١-١ وما بعدها من القانون الجنائي الفرنسي)، فيما يتصل بأعمال وقعت في فرنسا في عامي ٢٠٠٨ و٢٠٠٩.

وقد بدأ التحقيق الذي أسفر عن إدانة هيشر، وهو عالم في فيزياء الجزيئات، في أوائل عام ٢٠٠٨ بسبب رسالة بالبريد الإلكتروني تتضمن محتوى جهاديا، أُرسلت إلى موقع رئيس الجمهورية الفرنسية وجرى تعقّبها وصولا إلى عضو في تنظيم القاعدة في بلاد المغرب الإسلامي.

وقد مكَّن أمرُ التحفظ الصادر في كانون الثاني/يناير ٢٠٠٩ السلطاتِ من الوقوف على مراسلات بالبريد الإلكتروني بين عضو تنظيم القاعدة من ناحية وبين الجبهة الإعلاميةِ الإسلامية العالمية ومركز الرافدين ضمن مجموعة من الجهات الأخرى من ناحية ثانية، ومركز الرافدين هو موقع هدفه المعلن استضافة ونشر مستندات تنظيم القاعدة وتسجيلاته بالصوت الصورة وتصريحات أمراء الحرب ومنفذي الهجمات الانتحارية، ومواد تخص جماعات إسلامية متطرفة أخرى. وكانت مراسلات البريد الإلكتروني مشفرة باستخدام البرنامج المخصّص لهذا الغرض والمسمى "أسرار المجاهدين"، والذي يشتمل على تشفير بنظام ٢٥٦-بت، ومفاتيح تشفير متغيرة للشفرات الخفية، ومفاتيح تشفير بنظام آر إس إيه ٢٠٤٨-بت، ونظام مشفَّر للمراسلات الفورية لمنتديات الدردشة.

وقد قُدِّمت أثناء المحاكمة عشرات من رسائل البريد الإلكتروني بعد فكّ تشفيرها، وادَّعت النيابة العامة بأنَّ محتوى هذه الرسائل يبيِّن أنَّ هيشر قد أدَّى بفاعلية أعمالا، من ضمنها ما يلي، دعماً للشبكة الجهادية، وبالأخص باسم مركز الرافدين:

- ترجمة مواد جهادية التوجه، وتشفيرها، وضغطها، وحمايتها بكلمة سر، بما في ذلك مستندات ومقاطع فيديو، وتحميلها بعد ذلك على الإنترنت وبثها عبر الشبكة
- توزيع برنامج التشفير "أسرار المجاهدين" لتيسير الاتصالات السرية عبر الإنترنت
- التآمر مع عضو في تنظيم القاعدة في بلاد المغرب الإسلامي لتنظيم أنشطة جهادية التوجه ولتنسيق هذه الأنشطة، بما يشمل على سبيل التمثيل لا الحصر: توفير الدعم المالي للأغراض الجهادية، وتوزيع معلومات جهادية التوجه، ودعم تكوين خلية عاملة في أوروبا، وتحديداً في فرنسا، للتحضير لهجمات إرهابية محتملة
- إدارة موقع "الرباط" الشبكي ذي التوجه الجهادي
- اتخاذ خطوات ملموسة لتوفير الدعم المالي لتنظيم القاعدة في بلاد المغرب الإسلامي، بوسائل منها الشروع في استخدام باي بال وغيره من نظم الدفع الافتراضية.

وفي المحاكمة، ادَّعت النيابة العامة بأنَّ هذه الاتصالات تثبت أن هيشر كان على علم تام بأنه كان يتعامل مع عضو في تنظيم القاعدة في بلاد المغرب الإسلامي، وأنه تصرّف طوعاً وعن بيّنة بوصفه وسيطاً بين مقاتلين جهاديين وبين الجبهة الإعلامية الإسلامية العالمية. وفي ختام المحاكمة، رأت المحكمة أن "هيشر بات ... نصيراً يقدِّم الدعم اللوجستي والإعلامي لهذا التنظيم الإرهابي الذي يُعَدُّ 'الجهاد الإعلامي' أمراً بالغ الأهمية بالنسبة له".

كما رأت المحكمة أنَّ "عدلان هيشر يكون، بموافقته على تأسيس خلية عاملة مرتبطة بتنظيم القاعدة في بلاد المغرب الإسلامي في أوروبا، أو حتى في فرنسا، وعلى تحديد أهداف أو فئات من الأهداف التي سيجري ضربها، قد اشترك في جماعة [تنظيم القاعدة في بلاد المغرب الإسلامي] أنشئت خصيصاً للتحضير لأعمال إرهابية".

وبنـاء علـى ذلك فقد وجدت المحكمة أدلة كافيـة، وفقاً لما يقتضيه القانون الفرنسـي، لبيان أنَّ هيشر لم يقدم دعماً فكرياً فحسب، بل دعماً لوجستياً مباشراً لمخطط إرهابي واضح. وقرار المحكمة قابل للاستئناف.

المصدران: حكم صادر بتاريخ ٥ أيار/مايو ٢٠١٢ عن محكمة باريس الابتدائية، وكذلك: Tung, Liam, *Jihadists get world-class encryption kit* (29 January 2008)، انظر الرابط التالي:
www.zdnet.com.au/jihadists-get-world-class-encryption-kit-339285480.htm.

٢١- كذلـك مـن الممكن اتخاذ خطوات عبر شبكة الإنترنت لتحديد هـدف محتمل لهجوم إرهابي وللوقوف على أكـثر الوسائـل فعالية لتحقيق غرض إرهابي. وقد تتراوح هذه الخطـوات التحضيرية بين الحصول على تعليمات حـول الأساليب الموصى بها لتنفيذ الهجوم وجمع المعلومـات حول هدف مقترح من مصادر علنية ومن غيرها من المصـادر. فالإمكانيـة التي تتيحها شبكة الإنترنت لتقريب المسافات وتجاوز الحـدود، والكم الهائل من المعلومات المتاحة للجمهور في الفضاء السيبراني، تجعل من هذه الشبكة أداة رئيسية في التخطيط للأعمال الإرهابية.

(أ) الاتصالات السرّية التحضيرية

٢٢- إنَّ الوظيفة الأولى للإنترنت هي تيسير الاتصال. والإرهابيون باتوا على قدر كبير من الحنكة في استغلالهم لتكنولوجيـات الاتصالات للاتصال ببعضهـم البعض دون الكشف عن هوياتهم عنـد التخطيط لأعمال إرهابية. فقـد يستخـدم الإرهابيون حساب بريد إلكتروني بسيط لإيداع رسائـل في "صندوق بريد" إلكتروني أو افتراضي. ويُقصـد بذلك كتابةُ رسائـل دون إرسالها، بحيث لا تخلِّف وراءها إلا الحد الأدنى مـن الآثار الإلكترونية، ويمكن الاطّـلاع عليهـا في أي جهاز متصل بالإنترنـت في جميع أنحاء العالم من قبل أفراد متعدديـن يعرفون كلمة السر الخاصة بهذا الحساب.

٢٣- كمـا أنَّ هناك العديد مـن التقنيات الأكثر تطوراً التي تزيد من صعوبة الكشـف عن هوية صاحب الرسالة الأصلية المنقولة عبر الإنترنت أو عن هوية متلقّيها أو محتواها. فأدوات التّشفير وبرمجيات إخفاء الهوية متوافرة علـى الإنترنت ويمكن تنزيلها بسهولة. وتتيح هذه الأدوات أمورا في جملتها إخفاء عنوان بروتوكول الإنترنت الذي يميّـز كل جهـاز يُستخـدم للدخول إلى الإنترنـت عن غيره ويحدِّد موقعـه، أو إعادة توجيـه الرسائل المنقولة عبر الإنترنـت عـن طريق خادوم واحد أو أكـثر إلى ولايات قضائية أقل مستوى من حيث إنفـاذ القانون ضد الأنشطة الإرهابيـة، أو تشفـير بيانات حركة المعلومات الخاصة بالمواقع التي جـرى الدخول إليها، أو جميع هذه الإجراءات معاً. ويمكن أيضاً استخدام الستيغانوغرافي، أي إخفاء رسائل في صور.

(ب) المعلومات المتاحة لعموم الناس

٢٤- في كثير من الأحيان، يقوم كل من المنظمات والأفراد بنشر كميات كبيرة من المعلومات على شبكة الإنترنت. وفيمـا يتعلق بالمنظمات، قد يرجـع ذلك جزئياً لرغبتها في الترويج لأنشطتها وتيسـير تواصلها مع الجمهور. كما أنَّ بعضـ المعلومـات الحساسة التي يمكن أن يستخدمها الإرهابيون في أغراض غير مشروعة تتوفر عبر محركات البحـث علـى الإنترنت، والتي قد تفهرس معلومات غير مشمولة بالحمايـة الكافية وتسترجعها من ملايين المواقع الشبكيـة. وعلاوة على ذلك، فـإنَّ الحصول عبر الإنترنت على معلومات لوجستيـة مفصّلة، كلقطات آنية منقولة عبر تلفزيون بدارة مغلقة، وتطبيقات مثل غوغل إيرث، وهي خدمات مُعدَّة ليستخدمها الأفراد لأغراض مشروعة وتُستخدم بالفعل لهذه الأغراض في المقام الأول، يمكن أن يساء استخدامه من قبل من يسعون إلى الاستفادة من

حرية الحصول على صور وخرائط ومعلومات ساتلية عالية الاستبانة عن التضاريس والمباني، لاستطلاع الأهداف المحتملة عن بعد عبر جهاز حاسوب.

٢٥- كذلك فإنَّ الأفراد بدورهم ينشرون، طوعاً أو عن غير قصد، كميات غير مسبوقة من المعلومات الحساسة على شبكة الإنترنت، ولا سيما في عصر وسائط التواصل الاجتماعي الواسعة الانتشار، مثل فيسبوك، وتويتر، ويوتيوب، وفليكر، ومنصات التدوين. ولئن كان قصد هؤلاء الأفراد من نشر هذه المعلومات قد يكون إطلاع جمهورهم على أخبارهم أو غيرها من المستجدات لأغراض إعلامية أو اجتماعية، فقد يُختلس شيء من هذه المعلومات ويُستخدم في أنشطة إجرامية.

٥- *التنفيذ*

٢٦- قد تُوظَّف عناصر من الفئات المذكورة أعلاه في سياق استخدام شبكة الإنترنت لتنفيذ أعمال إرهابية. فعلى سبيل المثال، يمكن أن تُبثّ عن طريق الإنترنت تهديدات صريحة باستخدام العنف، بما في ذلك التهديد باستخدام السلاح، لإشاعة القلق أو الخوف أو الذعر بين أفراد مجتمع من المجتمعات أو فئة منه. وفي العديد من الدول الأعضاء قد يعتبر توجيه تهديدات من هذا القبيل، ولو لم تُنفَّذ، بمثابة جريمة. فالتشريعات الصينية المحلية، على سبيل المثال، تجرِّم القيامَ بتلفيق تهديد أو نشره مع العلم بكونه ملفّقاً أو بكلا الفعلين معاً، فيما يتعلق باستخدام القنابل، أو المواد البيولوجية أو الكيميائية أو المشعة أو غيرها من الأسلحة، عندما يُرتكب ذلك بقصد "الإخلال الجسيم بالنظام العام".[١٦] ويمكن أيضا أن يتم التواصل عبر الإنترنت مع الضحايا المحتملين أو لتنسيق تنفيذ أعمال إرهابية مادية. فعلى سبيل المثال، استُخدمت شبكة الإنترنت على نطاق واسع في التنسيق ما بين المشاركين في هجمات ١١ أيلول/سبتمبر ٢٠٠١ على الولايات المتحدة.

٢٧- وقد يكون استخدام شبكة الإنترنت في تنفيذ الأعمال الإرهابية في أغراض من بينها الحصول على مزايا لوجستية، أو الحد من احتمالات الكشف عن هذه الأعمال، أو إخفاء هوية الأطراف المسؤولة. كما يمكن أن تُستخدم الإنترنت لتسهيل الحصول على المواد الضرورية لتنفيذ الهجوم. فقد يعمد الإرهابيون إلى شراء كل مكوّن وخدمة من المكوّنات أو الخدمات اللازمة لارتكاب أعمال إرهابية عنيفة عن طريق التجارة الإلكترونية. وقد تُستخدم بطاقات الائتمان المختلسة أو غيرها من أشكال الدفع الإلكترونية الاحتيالية لتمويل هذه المشتريات.

٦- *الهجمات السيبرانية*

٢٨- يُقصد بالهجمات السيبرانية، على العموم، استغلالُ الشبكات الحاسوبية عن عمد باعتبارها وسيلة لشن هجوم. وتهدف هذه الهجمات عادة إلى تعطيل النظم التي تستهدفها. وتتضمن تلك الأهداف نظم الحاسوب والخواديم وبنيتها التحتية الأساسية، وذلك عبر استخدام الاختراق الحاسوبي، أو التقنيات المتقدمة للتهديد المستمر، أو فيروسات الحاسوب، أو البرمجيات الضارة،[١٧] أو الإغراق،[١٨] أو غيرها من وسائل الدخول غير

[١٦] مذكرة مكتوبة قدَّمها الخبير الصيني.

[١٧] وفقاً للفقرة *(ن)* من المادة ١ من عُدّة التشريع في مجال الجرائم السيبرانية الصادرة عن الاتحاد الدولي للاتصالات، فإنَّه يمكن تعريف البرمجيات الضارة بأنها برمجيات تُدرج في برمجيات حاسوبية أو نظام حاسوبي، في الخفاء عادة، بقصد الإضرار بسرية هذه البرمجيات أو البيانات أو النظام، أو سلامتها، أو توفُّرها للجمهور.

[١٨] يُقصد بـ"الإغراق" استهدافُ الخواديم المركزية الخاصة بالتوثُّق من الهوية لمنظمة ما بتقديم العديد من طلبات التوثُّق في وقت واحد، بهدف تحميل الخواديم عبئاً يفوق طاقتها، مما يؤدي إلى ما يُسمَّى بحجب الخدمة الموزَّع، أي حرمان المستخدمين المشروعين من الحصول على الخدمة التي تتيحها هذه الخواديم.

المصـرَّح بـه أو ذي الأهداف الضارة. وقد تحمل الهجمات السيبرانية سمات عمل إرهابي، بما في ذلك الرغبة في زرع الخـوف دعمـاً لأهداف سياسية أو اجتماعية. ومن بين الأمثلة على الهجمـات السيبرانية ما وقع في إسرائيل في كانـون الثاني/ينايـر ٢٠١٢، من استهداف لعدة مواقع شبكية إسرائيلية ذات قيمة رمزية، مثل موقعَي سوق تل أبيب للأوراق المالية وشركة الطيران الوطنية، وكشف غير مصرّح به عن تفاصيل البطاقات الائتمانية والحسابات البنكيـة للآلاف مـن مواطني إسرائيل.[١٩] ولئن كان قدر كبير من الاهتمام قـد انصبّ في السنوات الأخيرة على الخطـر الـذي تشكِّلـه الهجمات السيبرانية التـي يشنها إرهابيون، فـإن هذا الموضوع لا ينـدرج ضمن نطاق هذا المنشور، ومن ثم فلن يكون موضوعاً للتحليل هاهنا.

جيم- استخدامات الإنترنت في مكافحة الأنشطة الإرهابية

٢٩- لئـن استحـدث الإرهابيـون العديـد مـن الطرائـق لاستخدام الإنترنـت في أغراض غير مشروعـة، فإنَّ استخدامهم لشبكة الإنترنت يتيح كذلك فرصاً لجمع المعلومات الاستخبارية وغير ذلك من الأنشطة الهادفة لمنع الأعمـال الإرهابيـة ومكافحتها، فضلا عن جمع الأدلة من أجل الملاحقـة القضائية عن هذه الأعمال. فقدرٌ كبير مما نعرف عن طريقة عمل التنظيمات الإرهابية وأنشطتها وأحياناً أهدافها يُستمدّ من اتصالات المواقع الشبكية ومنتديـات الدردشة وغيرها من الاتصـالات عبر الإنترنت. وعلاوة على ذلك، فإنَّ زيـادة استخدام الإنترنت في أغراض إرهابية يتيح زيـادة مقابلة في توافر البيانات الإلكترونية التي يمكن جمعهـا وتحليلها لأغراض مكافحة الإرهـاب. وتقـوم جهات إنفاذ القانـون والمخابرات وغيرهـا من السلطـات باستحداث أدوات تتطـور باستمرار للمبـادرة إلى منـع الأنشطـة الإرهابية التي تستخدم فيها شبكـة الإنترنت وكشف هذه الأنشطـة وردعها. كما أنَّ استخدام أساليب التحري التقليدية، مثل الموارد المخصصة للترجمة بغرض كشف التهديدات الإرهابية المحتملة في وقت مناسب، آخذٌ في الازدياد بدوره.

٣٠- وتتيـح المناقشات التي تجري على الإنترنت فرصةً لطرح وجهات النظر المعارضة أو الدخول في نقاش بناء، وهو ما قد يؤدي إلى ثني أنصار محتملين للتنظيمات الإرهابية عن الانخراط في أعمالها. ومن الممكن طرح أفكار مضادة تقوم على أساس راسخ من الحقائق عبر منتديات النقاش والصور وشرائط الفيديو على الإنترنت. كذلك فمن الممكن، ضماناً لفعالية الأفكار المطروحة، إظهارُ التعاطف إزاء القضايا الدفينة التي تساهم في الدفع باتجاه التطـرف، مثـل الظروف السياسية والاجتماعية، وتسليط الضوء على بدائـل لتحقيق النتائج المرجوة دون اللجوء للوسائل العنيفة.[٢٠] كما يمكن بث رسائل استراتيجية تحتوي على أفكار مضادة للدعاية الإرهابية عبر الإنترنت بلغات متعددة للوصول إلى جمهور عريض ومتنوع جغرافياً.

٣١- ويقـدِّم مركـز الاتصـالات الاستراتيجية لمكافحـة الإرهاب، التابع لـوزارة الخارجيـة في الولايات المتحدة الأمريكيـة، مثالا على مبادرة مشتركة بين الوكالات أطلقت مؤخراً، بهدف الحد من التحول إلى التطرف والعنف بدافـع مـن التطرف عبر الكشـف في الوقت المناسب عن أمـور في جملتها الدعاية المتطرفة علـى شبكة الإنترنت

[١٩] انظـر: Isabel Kershner, "Cyberattack exposes 20,000 Israeli credit card numbers and details about users", *New York Times*, 6 January 2012، وكذلك: "2 Israeli web sites crippled as cyberwar escalates", *New York Times*, 16 January 2012.

[٢٠] الفريـق العامـل المعنـي بمكافحة استخدام الإنترنت في أغراض إرهابية التابع لفرقة العمل المعنية بتنفيـذ تدابير مكافحة الإرهاب، "ملخَّص ورشـة العمل المعنية بالتركيز على استخـدام الإنترنت لمكافحة التطرف والعنف ومتابعة نتائجهـا وتوصياتها"، المنعقدة في الرياض في الفترة ما بين ٢٤ و٢٦ كانون الثاني/يناير ٢٠١١. انظر الرابط التالي: www.un.org/en/terrorism/ctitf/pdfs/ctitf_riyadh_conference_summary_recommendations.pdf.

والـرد السريع عليها بخطاب مضاد محـدد الهدف عبر مجموعة واسعة من تكنولوجيات الاتصالات، بما في ذلك الأدوات الرقميـة.[٢١] فعلـى سبيل المثال، ذُكـر، في أيار/مايو ٢٠١٢، أنَّ المركز قـد ردَّ، في غضون ٤٨ ساعة، على لافتـات إعلانية تروِّج للعنف بدافع التطرف، نشرها تنظيم القاعدة في شبه الجزيرة العربية على مختلف المواقع الشبكيـة، بإعلانـات مضادة علـى المواقع نفسها، تتضمَّن نسخـة معدّلة من الرسالة نفسهـا، فحواها أن ضحايا أنشطـة هذا التنظيـم الإرهابي كانوا من المواطنين اليمنيين. وقد نُفذت هـذه الحملة بالتعاون بين وزارة خارجية الولايات المتحدة ودوائر المخابرات والجيش. كما أنَّ المركز يستخدم منصات إعلامية مثل فيسبوك ويوتيوب لبثّ رسائله المحتوية على خطابات مضادة.[٢٢]،[٢٣]

دال- الاعتبارات المتعلقة بسيادة القانون

٣٢- إنَّ احـترام حقـوق الإنسـان وسيادة القانـون جزء لا يتجزأ مـن جهود مكافحة الإرهـاب. ولا بد من إيلاء عنايـة كافية لاحترام المعايير الدولية لحقـوق الإنسان في جميع مراحل مبادرات مكافحة الإرهاب، بدءاً من جمع المعلومات الاستخبارية بغرض منع الإرهاب، وانتهاءً بالتأكد من مراعاة الأصول القانونية أثناء الملاحقة القضائية للمشتبه بهم، الأمر الذي يتطلب استحداث تشريعات وممارسات وطنية لمكافحة الإرهاب تعزز من حقوق الإنسان الأساسية ومن سيادة القانون وتحمي كليهما.[٢٤]

٣٣- وللـدول حـق وعليها واجب في أن تتخـذ تدابير فعالة لمكافحة الأثـر المدمّر للإرهاب علـى حقوق الإنسان، ولا سيمـا حقـوق الأفراد في الحياة والحرية والسلامة الجسدية، وحقوق الـدول في سلامة أراضيها وأمنها. ويعدُّ وضـع تدابـير فعالة لمكافحة الإرهـاب وحماية حقوق الإنسان هدفـين متكاملين ومتعاضديـن ومن ثم فلا بد من السعـي لتحقيقهما سويـاً.[٢٥] فقد يكون لمبادرات مكافحـة الإرهاب المتعلقة باستخـدام الإنترنت تأثير على تمتع الأفـراد بعدد من الحقوق، بما في ذلك الحق في حرية التعبير، وفي حرية تكوين الجمعيات، وفي الخصوصية، وفي المحاكمـة العادلة. ولئن كان تحليل مسائل حقوق الإنسان تحليلا شاملا يتجاوز نطاق هذا المنشور، فإنَّه من المهم أن يسلَّط الضوء على المواضيع الرئيسية التي تستدعي النظر فيها.

٣٤- كمـا أُشير آنفاً في الباب الفرعي بـاء-١ *(ب)*، قد تُفرض قيود على حرية التعبير في إطار حظر التحريض علـى الإرهاب. فحريـة التعبير ليست حقاً مطلقاً ويُمكـن تقييدها، شريطة استيفاء معايـير دقيقة التفسير فيما يخصـ شرعيـة التقييـد، وضرورته، وكونـه متناسباً مع سبب التقييـد، وتوخي عدم التمييـز، في تطبيقه، إذا ما استُخدمـت هـذه الحريـة للتحريض على التمييـز أو العداء أو العنف. ومـن بين الصعوبـات الرئيسية في قضايا

---

[٢١] Executive Order 13584 of 9 September 2011, "Developing an Integrated Strategic Counterterrorism Communications Initiative and Establishing a Temporary Organization to Support Certain Government-wide Communications Activities Directed Abroad", *Federal Register,* vol. 76, No. 179, 15 September 2011.

[٢٢] "United States State Department fights al-Qaeda in cyberspace", *Al Jazeera* (25 May 2012). انظر الرابط التالي: http://blogs.aljazeera.com/americas/2012/05/25/us-state-department-fights-al-qaeda-cyberspace.

[٢٣] "U.S. uses Yemeni web sites to counter al-Qaeda propaganda", *The Washington Post* (24 May 2012). انظر الرابط التالي: www.washingtonpost.com/world/national-security/us-hacks-web-sites-of-al-qaeda-affiliate-in-yemen/2012/05/23/gJQAGnOxlU_story.html.

[٢٤] مفوضية الأمم المتحدة لحقوق الإنسان، صحيفة الوقائع رقم ٣٢، ثالثاً، حاء.

[٢٥] المرجع نفسه، أولا، جيم.

تمجيد الإرهاب أو التحريض عليه تحديدُ الخط الفاصل بين ما هو مقبول وما هو غير مقبول، إذ إن هذا يتفاوت تفاوتاً كبيراً بين بلد وآخر باختلاف الخلفيات التاريخية الثقافية والقانونية.[٢٦] كذلك فإنَّ الحق في حرية تكوين الجمعيات حق مشروط قد يخضع لقيود واستثناءات تُفسَّر في حدود ضيقة.

٣٥- وقد تشمل مكافحة استخدام الإنترنت في أغراض إرهابية وضعَ المشتبه بهم تحت المراقبة وجمع معلومات عنهم. وينبغي إيلاء الاعتبار الواجب لعدم تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخّل في خصوصياته،[٢٧] بما يشمل الحق في خصوصية المعلومات المتعلقة بهوية الفرد إضافة إلى المعلومات المتعلقة بحياته الخاصة. ويجب أن تكون القوانين المحلية مفصّلة تفصيلاً كافياً فيما يتعلق بأمور في جملتها الظروف المحدَّدة التي يجوز فيها أن يُسمح بهذا التدخّل. كما يجب أن توضع ضمانات مناسبة للحيلولة دون إساءة استخدام أدوات المراقبة السرّية. وعلاوة على ذلك، فيجب أن تُوفر الحمايةُ اللازمة لأي بيانات شخصية يتم جمعها، منعاً من الاطّلاع عليها أو إفشائها أو استخدامها على نحو تعسفي أو غير قانوني.[٢٨]

٣٦- ويُعد ضمان الحقوق المتعلقة بالإجراءات القانونية الواجبة أمراً بالغ الأهمية للتأكد من أن تدابير مكافحة الإرهاب فعّالة وتحترم سيادة القانون. وتشمل إجراءاتُ حماية حقوق الإنسان لجميع المتهمين بارتكاب جرائم، بما فيها جرائم الإرهاب، حقَّ الشخص في افتراض براءته حتى الحكم بإدانته، والحق في المحاكمة وفق الضمانات الواجبة وفي غضون فترة معقولة ومن قبل هيئة قضائية مختصة ومستقلة ونزيهة، والحق في مراجعة الإدانة أو الحكم من قبل هيئة قضائية أعلى درجةً ومستوفية للمعايير ذاتها.[٢٩]

٣٧- ولتحليل أكثر تفصيلا للمسائل التي سلِّط عليها الضوء في هذا الباب وغيرها من الاعتبارات ذات الصلة، يرجى الرجوع، على سبيل المثال، إلى صحيفة الوقائع رقم ٣٢ الصادرة عن مفوضية الأمم المتحدة لحقوق الإنسان بشأن "حقوق الإنسان والإرهاب ومكافحة الإرهاب"، وتقرير مفوضة الأمم المتحدة السامية لحقوق الإنسان عن حماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب (A/HRC/16/50)، والتقريرين التاليين للمقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب: عشرة مجالات للممارسات الفضلى في مكافحة الإرهاب (A/HRC/16/51)، وتجميع الممارسات الجيدة المتعلقة بالأطر والتدابير القانونية والمؤسسية التي تضمن احترام حقوق الإنسان من جانب وكالات الاستخبارات في سياق مكافحة الإرهاب، بما في ذلك ما يتعلق بالرقابة على هذه الوكالات (A/HRC/14/46).

---

[٢٦] منظمة الأمن والتعاون في أوروبا، مكتب المؤسسات الديمقراطية وحقوق الإنسان، البابان الثالث والرابع في مذكرة معلومات أساسية بعنوان "Human rights considerations in combating incitement to terrorism and related offences" (الاعتبارات المتعلقة بحقوق الإنسان في جهود مكافحة التحريض على الإرهاب والجرائم المتصلة به)، أعدّت لحلقة عمل تخصصية حول منع الإرهاب عن طريق مكافحة التحريض وما يتصل به من أنشطة إرهابية، انعقدت يومي ١٩ و٢٠ تشرين الأولَ/أكتوبر ٢٠٠٦.

[٢٧] انظر المادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية.

[٢٨] "حقوق الإنسان والإرهاب ومكافحة الإرهاب"، ثالثاً، ياء.

[٢٩] المرجع نفسه، ثالثاً، واو.

ثانياً- السياق الدولي

ألف- مقدِّمة

٣٨- إنَّ استخدام الإنترنت في أغراض إرهابية ظاهرة عابرة للحدود الوطنية، تتطلب اتخاذ تدابير متكاملة للتصدي لها، تكون هي أيضا ذات طابع عابر للحدود فيما بين نظم العدالة الجنائية الوطنية. وتؤدي الأمم المتحدة دوراً محورياً في هذا الصدد، بتيسيرها للمناقشة ولتبادل الممارسات الجيدة فيما بين الدول الأعضاء، إلى جانب التوصل إلى توافق في الآراء حول النُّهج المشتركة لمكافحة استخدام الإنترنت في أغراض إرهابية.

٣٩- ويرِد الإطار القانوني الدولي الواجب التطبيق المتعلق بمكافحة الإرهاب في طائفة من المصادر، من بينها قرارات الجمعية العامة ومجلس الأمن، والمعاهدات، والسوابق القضائية، والقانوني الدولي العرفي. وقد تفرض قرارات مجلس الأمن التزامات قانونية على الدول الأعضاء، أو تتيح لها مصادر للالتزامات السياسية أو معايير مستجدة للقانون الدولي تندرج في إطار القانون غير الملزم. وتعتبر قرارات المجلس التي تُعتمد بموجب الفصل السابع من ميثاق الأمم المتحدة ملزمة لجميع الدول الأعضاء. وقد اعتمدت الجمعية العامة بدورها عدداً من القرارات المتعلقة بالإرهاب التي تشكِّل مصادر مفيدة للقانون غير الملزم ولها أهمية سياسية كبرى ولو لم تكن ملزمة قانوناً.[٣٠]

٤٠- كذلك تُفرض التزامات قانونية على الدول بموجب الصكوك الثنائية أو المتعددة الأطراف التي تتناول الإرهاب. وتُعتبر الصكوك القانونية صكوكاً "عالمية" إذا كان التصديق عليها أو الانضمام إليها مفتوحاً أمام جميع الدول الأعضاء في الأمم المتحدة. وفي المقابل، فإنّ الاتفاقات التي تضعها التجمعات الإقليمية أو غيرها من التجمعات الدولية قد لا تكون مفتوحة إلا لمجموعة محدودة من الموقِّعين المحتملين، وتكون هذه الالتزامات المستندة إلى معاهدات ملزمة للدول التي تختار أن تكون طرفاً في الاتفاقات المنشئة لها دون غيرها من الدول.

٤١- ويقع واجب تقديم منفذي الأعمال الإرهابية للعدالة على كاهل السلطات المحلية في المقام الأول، إذ لا يكون للمحاكم الدولية عادة اختصاص النظر في هذه الأعمال.[٣١] وتؤدي قرارات الأمم المتحدة، والصكوك القانونية العالمية، والاتفاقات الإقليمية، والقوانين النموذجية لمكافحة الإرهاب، دوراً رئيسياً في إرساء معايير مشتركة مقبولة لدى ولايات قضائية متعددة.

---

[٣٠] انظر مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة، أسئلة يكثر طرحها بشأن جوانب مكافحة الإرهاب ذات الصلة بالقانون الدولي (٢٠٠٩). انظر الرابط التالي: www.unodc.org/documents/terrorism/Publications/FAQ/AR_V0981186.pdf.

[٣١] المحكمة الخاصة بلبنان، التي أنشئت بموجب قرار مجلس الأمن ١٧٥٧ (٢٠٠٧)، هي المحكمة الدولية الوحيدة التي لها اختصاص النظر المحدود في جرائم الإرهاب في الوقت الراهن.

باء- قرارات الأمم المتحدة بشأن مكافحة الإرهاب

٤٢- اعتمدت الجمعية العامة بالإجماع الاستراتيجية العالمية لمكافحة الإرهاب[٣٢] في عام ٢٠٠٦، الأمر الذي يُعدُّ علامة فارقة في مجال المبادرات المتعددة الأطراف لمكافحة الإرهاب. وبموجب هذه الاستراتيجية، قررت الدول الأعضاء ما يلي، ضمن جملة أمور أخرى:

(أ) إدانة الإرهاب بجميع أشكاله ومظاهره إدانة مستمرة وقاطعة وقوية، أياً كان مرتكبوه، وحيثما ارتكب، وأياً كانت أغراضه، على أساس أنَّه يعد واحداً من أشد الأخطار التي تهدد السلام والأمن الدوليين.

(ب) اتخاذ إجراءات عاجلة لمنع ومكافحة الإرهاب بجميع أشكاله ومظاهره؛

(ج) التسليم بأن التعاون الدولي وأي تدابير [تضطلع الدول الأعضاء] بها من أجل منع الإرهاب ومكافحته يجب أن تتماشى مع الالتزامات المنوطة [بها] بموجب القانون الدولي، بما في ذلك ميثاق الأمم المتحدة والاتفاقيات والبروتوكولات الدولية ذات الصلة، وبخاصة قانون حقوق الإنسان وقانون اللاجئين والقانون الإنساني الدولي؛

(د) العمل إلى جانب الأمم المتحدة، مع إيلاء الاعتبار الواجب لطابع السرية واحترام حقوق الإنسان والامتثال للالتزامات الأخرى المنصوص عليها في القانون الدولي، على استكشاف طرق وسبل القيام بما يلي: "*(أ) تنسيق الجهود المبذولة على الصعيدين الدولي والإقليمي لمكافحة الإرهاب بجميع أشكاله ومظاهره على الإنترنت؛ (ب) استخدام الإنترنت كأداة لمكافحة تفشي الإرهاب، مع التسليم في الوقت نفسه بأن الدول قد تحتاج إلى المساعدة في هذا الصدد*" [التوكيد مضاف].

٤٣- ومن بين قرارات مجلس الأمن التي اعتُمدت في السنوات الأخيرة، هنالك عدة قرارات تقتضي من الدول التعاونَ الكامل على محاربة الإرهاب بجميع أشكاله. ويشار، على وجه التحديد، إلى أن القرارين ١٣٧٣ (٢٠٠١) و١٥٦٦ (٢٠٠٤)، اللذين اعتُمدا بموجب الفصل السابع من ميثاق الأمم المتحدة، يُلزمان الدول الأعضاء كافة باتخاذ إجراءات تشريعية وغير تشريعية لمكافحة الإرهاب، بوسائل منها زيادة التعاون مع الحكومات الأخرى في التحري عن الضالعين في الأعمال الإرهابية، والكشف عنهم، واعتقالهم، وتسليمهم، وملاحقتهم قضائياً. كما يهيب هذان القراران بالدول أن تنفِّذ الاتفاقيات والبروتوكولات الدولية المتعلقة بالإرهاب.

٤٤- ومن بين قرارات مجلس الأمن الرئيسية الأخرى فيما يتعلق بالأنشطة الإرهابية التي يمكن القيام بها بالاستعانة بالإنترنت القرارُ ١٦٢٤ (٢٠٠٥)، الذي يتناول التحريض على الأعمال الإرهابية وتمجيدها. ففي الفقرة الرابعة من ديباجة هذا القرار، يدين المجلس "بأشد العبارات التحريض على الأعمال الإرهابية و[يستنكر] المحاولات الرامية إلى تبرير أو تمجيد (اختلاق أعذار) للأعمال الإرهابية التي قد تحرض على ارتكاب مزيد من تلك الأعمال". وفي الفقرة ١ من منطوق القرار، يدعو المجلس جميع الدول إلى أن تعتمد من التدابير ما قد يكون لازماً ومناسباً، وأن تحظر بنص القانون، وفقا لالتزاماتها بموجب القانون الدولي، التحريض على ارتكاب عمل أو أعمال إرهابية وأن تمنع هذا التحريض.

[٣٢] قرار الجمعية العامة ٦٠/٢٨٨.

٤٥- وقد أكدَّت تقارير وقرارات صادرة عن الأمم المتحدة مؤخراً تأكيدا خاصا على أهمية مكافحة استخدام الإنترنت في أغراض إرهابية باعتبارها جزءا رئيسيا من أي استراتيجية شاملة لمكافحة الإرهاب. ففي تقرير الأمين العام المقدَّم للجمعية العامة عن عام ٢٠٠٦، والذي حمل عنوان "الاتحاد في مواجهة الإرهاب: توصيات لاستراتيجية عالمية لمكافحة الإرهاب"[٣٣] أفاد الأمين العام صراحة بأنَّ: "القدرة على إيجاد الأموال ونقلها، وعلى حيازة الأسلحة وتجنيد الكوادر وتدريبها وعلى الاتصال، خاصة باستخدام الإنترنت، هي كلها عناصر أساسية بالنسبة للإرهابيين".[٣٤] واستطرد الأمين العام مؤكداً على أنَّ الإنترنت قد باتت أداة تتسارع وتيرة توسّع الإرهابيين في استخدامها في تجنيد الأفراد ونشر المعلومات والدعاية، الأمر الذي لا بد من مواجهته بعمل منسّق بين الدول الأعضاء، مع احترام حقوق الإنسان والتقيد بالالتزامات الأخرى التي يفرضها القانون الدولي.[٣٥]

٤٦- وقد أعرب مجلس الأمن في قراره ١٩٦٣ (٢٠١٠) عن "القلق إزاء ازدياد استخدام الإرهابيين في مجتمع معولم للتكنولوجيا الجديدة للمعلومات والاتصالات، وبخاصة الإنترنت، لأغراض التجنيد والتحريض، إضافة إلى تمويل أنشطتهم وتخطيطها وإعدادها". كما سلَّم المجلس بأهمية التعاون بين الدول الأعضاء لمنع الإرهابيين من استغلال التكنولوجيا والاتصالات والموارد.

جيم- الصكوك القانونية العالمية بشأن مكافحة الإرهاب

٤٧- يعمل المجتمع الدولي منذ عام ١٩٦٣ على وضع صكوك قانونية عالمية لمنع الأعمال الإرهابية، برعاية الأمم المتحدة ووكالاتها المتخصصة، وخصوصاً منظمة الطيران المدني الدولي والمنظمة البحرية الدولية والوكالة الدولية للطاقة الذرية. وتمثِّل الصكوك العالمية لمكافحة الإرهاب عنصراً رئيسياً في النظام العالمي لمواجهة الإرهاب وإطاراً هاماً للتعاون الدولي على مكافحة الإرهاب. وتتناول أحكام هذه الصكوك القانونية العالمية أعمالا تتراوح بين اختطاف الطائرات إلى ممارسة الإرهاب النووي من جانب الأفراد والجماعات،[٣٦] وتلزم الدول التي تعتمده بتجريم معظم الأعمال الإرهابية التي يمكن تصورها في المجالات التي تشملها الاتفاقيات. ومع ذلك، فإنَّ هذه الصكوك القانونية العالمية ليست ملزِمة إلا للموقِّعين عليها،[٣٧] الذين يعتبرون مسؤولين أيضاً عن إنفاذ أحكام هذه الصكوك عبر نظم العدالة الجنائية المحلية.

٤٨- ونتيجةً للاهتمام المنصب على مكافحة الإرهاب في أعقاب اعتماد مجلس الأمن لقراره ١٣٧٣ (٢٠٠١)، الذي طلب فيه من الدول الأعضاء الانضمام إلى الصكوك القانونية العالمية لمكافحة الإرهاب، فقد زادت نسبة

---

[٣٣] A/60/825.

[٣٤] المرجع نفسه، الفقرة ٣٨.

[٣٥] المرجع نفسه، الفقرتان ٥٨ و٦٠.

[٣٦] تتضمن الأعمال الإرهابية الأخرى التي تتناولها هذه الصكوك أعمال التخريب الموجّهة ضد الطيران، وأعمال العنف في المطارات، والأعمال الموجّهة ضد سلامة الملاحة البحرية، والأعمال الموجّهة ضد سلامة المنصات الثابتة القائمة في الجرف القاري، والجرائم المرتكبة ضد الأشخاص المتمتعين بحماية دولية (مثل اختطاف الدبلوماسيين)، والاستيلاء على مواد نووية وحيازتها بطرائق غير مشروعة، وأخذ الرهائن، والهجمات الإرهابية بالقنابل، وتمويل ودعم ارتكاب الأعمال الإرهابية والمنظمات الإرهابية.

[٣٧] للحصول على قائمة بحالة التصديق الراهنة على هذه الصكوك العالمية، يُرجى مراجعة الرابط التالي: www.unodc.org/tldb/universal_instruments_NEW.html.

الانضمـام لهذه الصكوك زيـادة كبيرة. وحتى حزيران/يونيه ٢٠١١، كان ثلثا الـدول الأعضاء قد صدَّق على ١٠ صكوك على الأقل من بين ١٦ صكاً عالمياً لمكافحة الإرهاب أو انضم إليها.[٣٨]

٤٩- ولا توجـد في الوقـت الراهن معاهدة شاملة للأمم المتحدة بشأن الإرهاب تنطبق على قائمة جامعة لمظاهر الإرهـاب كافـة. وبالمثل، فإنَّ المجتمع الدولي لم يتفق بعد على تعريـف ملزم دولياً لمصطلح "الإرهاب"،[٣٩] وهو ما يرجع في جزء كبير منه إلى صعوبة وضع تصنيف قانوني مقبول عالمياً لأعمال العنف التي يرتكبها كل من الدول، والجماعات المسلحة مثل حركات التحرير أو حركات تقرير المصير، أو الأفراد.

٥٠- وتشارك الدول الأعضاء منذ عام ٢٠٠٠ في مفاوضات تتعلق بإبرام اتفاقية شاملة لمكافحة الإرهاب، تشتمل في نهاية المطاف على تعريف للإرهاب. لكن، وفي مواجهة صعوبة الوصول إلى توافق في الآراء بشأن تعريف واحد مقبـول عالميـاً لما قد يُعتبر إرهابـاً، فقد تحقق التقدم عوضاً عـن ذلك عبر الصكوك القانونيـة العالمية القائمة، التي وُضعت لتتناول جوانب محددة من الموضوع. وتركِّز هذه الصكوك على تجريم "أعمال إرهابية" بعينها دونما تعريف للإرهاب بمفهومه الأوسع.

٥١- ولا تعرِّف الصكوكُ العالمية الجرائمَ الإرهابية باعتبارها جرائم تخضع للقانون الدولي، وإنما تنشئ التزاماً علـى الـدول الأطراف في الاتفاقات بتجريم الفعل المخالف للقانون المذكـور في إطار قانونها الداخلي، وأن تمارس ولايتهـا القضائية علـى الجناة بمقتضى الشـروط المحددة في الاتفاقـات، وأن تتيح آليات للتعـاون الدولي تمكِّن الدول الأطراف إما من محاكمة المتهمين بارتكاب الجرائم أو تسليمهم. وحتى اكتمال المفاوضات الجارية بنجاح بشـأن تعريـف عالمي للإرهاب أو اتفاقيـة شاملة لمكافحته، فإنَّ مـن شأن الاتفاقات الثنائيـة والمتعددة الأطراف أن تهيـئ الأسـاس اللازم لوضع معايـير موحدَّة لمكافحة استخدام الإنترنت في أغراض إرهابية، من أجل تعزيز التعاون الدولي.

٥٢- كذلـك لم تُعتمـد اتفاقيـة عالميـة مخصصة لمنـع وإحباط استخـدام الإنترنـت في أغراض إرهابية. وفي كانـون الأول/ديسمـبر ٢٠١٠، اعتمدت الجمعية العامـة القرار ٦٥/٢٣٠، الذي أقرت فيه إعـلان سلفادور بشأن الاستراتيجيـات الشاملـة لمواجهـة التحديات العالمية: نظـم منع الجريمـة والعدالة الجنائيـة وتطورها في عالم متغـير،[٤٠] وطلبت إلى لجنـة منع الجريمة والعدالة الجنائية أن تنشئ، بما يتفـق وإعلان سلفادور، فريق خبراء حكوميـاً دولياً مفتـوح العضوية من أجل إجراء دراسة شاملة لمشكلة الجرائـم الإلكترونية والتدابير التي تتخذها الـدول الأعضـاء والمجتمـع الدولي والقطـاع الخاص للتصدي لها، بمـا في ذلك تبادل المعلومات عـن التشريعات

[٣٨] انظر الرابط التالي: www.un.org/en/sc/ctc/laws.html.

[٣٩] ومـع ذلـك فمـن الجدير بالذكر أنَّ المحكمة الخاصة بلبنان قـد رأت في قرار أصدرته مؤخراً أنَّه ثمة أدلـة كافية لإثبات وجود تعريف لجريمة الإرهاب بموجب القانون الدولي العرفي. انظر: قرار تمهيدي حول القانون الواجب التطبيق: الإرهاب، والمؤامرة، والقتل، والفعل، واجتماع الجرائم، القضية رقم: STL-11-01/I المحكمة الخاصة بلبنان (١٦ شباط/فبراير ٢٠١١). انظر الرابط التالي:
http://www.stl-tsl.org/en/the-cases/stl-11-01/rule-176bis/filings/orders-and-decisions/appeals-chamber/f0010

[٤٠] اعتمـده مؤتمر الأمم المتحدة الثـاني عشر لمنع الجريمة والعدالة الجنائية الذي عقد في سلفادور بالبرازيل، في الفترة من ١٢ إلى ١٩ نيسان/أبريـل ٢٠١٠، والـذي تنـاول، ضمن جملة أمور، الحاجة لأن تنظر الـدول الأعضاء في أساليب مكافحة الأشـكال الجديدة للجريمة، مثل الجرائم السيبرانية.

الوطنيــة وأفضل الممارسات والمساعــدة التقنية والتعاون الدولي. وسوف تيسِّر هــذه الدراسة، التي أطلقها مكتب الأمم المتحــدة المعني بالمخدِّرات والجريمة في شباط/فبرايــر ٢٠١٢، تقييمَ آثار استخدام تكنولوجيات المعلومات المستجــدة في تنفيذ الأنشطة الإجرامية، بما فيها ما يخص بعض استخدامات الإنترنت في أغراض إرهابية، مثل التحريض على الإرهاب عبر الحاسوب وجرائم تمويل الإرهاب.

دال- القانون الدولي لحقوق الإنسان

٥٣- تشــكِّل الالتزامــات المتعلقة بحقوق الإنسان جــزءاً لا يتجزأ من الإطار القانوني الــدولي لمكافحة الإرهاب، وذلك من خلال الالتزام الواقع على الدول بأن تمنع الهجمات الإرهابية التي يُحتمل أن تؤدي إلى الانتقاص كثيراً مــن حقوق الإنســان، وكذلك من خلال الالتزام بضمان احترام حقوق الإنسان في جميع تدابير مكافحة الإرهاب. وقد أعادت الدول الأعضاء التأكيد على هذه الالتزامات، في استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب، ولا سيمــا بإقرارهــا بأنَّ "اتخــاذ تدابير فعَّالة لمكافحة الإرهــاب وحماية حقوق الإنسان هدفــان لا يتعارضان، بل متكاملان ويعزّز كل منهما الآخر".

٥٤- ومــن بين الصكوك العالميــة الرئيسية لحقوق الإنسان التي اعتُمدت برعايــة الأمم المتحدة الإعلانُ العالمي لحقــوق الإنســان،[٤١] والعهــد الــدولي الخاص بالحقــوق المدنيــة والسياسيــة، والعهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية،[٤٢] والبروتوكولات المنطبقة.

٥٥- كذلــك فإنَّ عدّة منظمات إقليمية قد وضعت بدورهــا اتفاقيات لضمان حقوق الإنسان. وتشمل الأمثلة على ذلــك الاتفاقيــة الأوروبية لحماية حقوق الإنسان والحريات الأساسيــة[٤٣] (١٩٥٠)، والاتفاقية الأمريكية لحقوق الإنســان[٤٤] (١٩٦٩)، والميثاق الأفريقي لحقوق الإنسان والشعوب[٤٥] (١٩٨١)، وميثاق الاتحاد الأوروبي للحقوق الأساسية[٤٦] (٢٠٠٠).

٥٦- وعلى الرغم من أن التحليل الشامل للمسائل المتعلقة بقانون حقوق الإنسان لا يندرج في نطاق هذا المنشور، فســوف يتم تناول الاعتبارات المتعلقة بسيادة القانــون والصكوك القانونية المنطبقة مع الإشارة إلى تدابير معينة لمكافحة الإرهاب حيثما استوجب السياق ذلك.[٤٧]

---

[٤١] قرار الجمعية العامة ٢١٧ ألف-ثالثاً.

[٤٢] قرار الجمعية العامة ٢٢٠٠ ألف (د-٢١)، المرفق.

[٤٣] مجلس أوروبا، مجموعة *المعاهدات الأوروبية*، الرقم ٥.

[٤٤] الأمم المتحدة، مجموعة *المعاهدات*، المجلد ١١٤٤، الرقم ١٧٩٥٥.

[٤٥] المرجع نفسه، المجلد ١٥٢٠، الرقم ٢٦٣٦٣.

[٤٦] *Official Journal of the European Communities*, C 364, 18 December 2000.

[٤٧] انظر أيضاً مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة، أسئلة يكثر طرحها بشأن جوانب مكافحة الإرهاب ذات الصلة بالقانون الدولي، الباب ٥.

هاء- الصكوك القانونية الإقليمية ودون الإقليمية بشأن مكافحة الإرهاب

٥٧- بالإضافة إلى الصكوك العالمية لمكافحة الإرهاب، هناك العديد من الصكوك الإقليمية ودون الإقليمية التي تتيح معايير موضوعية وإجرائية قيِّمة لتجريم الأعمال الإرهابية التي يُمكن أن تُرتكب بالاستعانة بالإنترنت. وتتنوع هذه الصكوك، التي تستكمل الصكوك العالمية لمكافحة الإرهاب، من حيث نطاقها ودرجة قابليتها للإنفاذ.

١- *مجلس أوروبا*

٥٨- في عام ٢٠٠١، وضع مجلس أوروبا الاتفاقية المتعلقة بجرائم الفضاء الحاسوبي،[٤٨] التي هي الصك الوحيد المتعدد الأطراف والملزم قانوناً في الوقت الراهن الذي يتناول النشاط الإجرامي الذي يُمارس عن طريق الإنترنت. وتسعى الاتفاقية إلى التنسيق بين القوانين الوطنية المتعلقة بالجرائم السيبرانية، لتحسين الإجراءات المحلية للكشف عن هذه الجرائم، والتحقيق فيها، وملاحقتها قضائياً، ولوضع ترتيبات من أجل تعاون دولي سريع وجدير بالثقة في هذه المسائل.[٤٩] وتضع الاتفاقية معياراً أدنى مشتركاً للجرائم المحلية المتعلقة بالحاسوب[٥٠] وتنص على تجريم تسع من هذه الجرائم، بما في ذلك الجرائم المتعلقة بالدخول غير المصرح به إلى نظم الحاسوب أو برامجه أو بياناته، أو التلاعب غير القانوني بها؛ والاحتيال والتزوير عن طريق الحاسوب، والشروع في ارتكاب هذه الأعمال أو المساعدة أو التحريض عليها.[٥١]

٥٩- كما تتضمن الاتفاقية أحكاماً إجرائية هامة يُمكن أن تسهّل عملية التحقيق وجمع الأدلة فيما يتصل بالأعمال الإرهابية التي تُستخدم فيها الإنترنت. وتنطبق هذه الأحكام على أي جريمة تُرتكب عن طريق الحاسوب وعلى جمع الأدلة ذات الشكل الإلكتروني، وتخضع للضمانات المنطبقة المنصوص عليها في القانون المحلي.[٥٢]

٦٠- فعلى سبيل المثال، تقتضي اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي أن تعتمد أطرافها تشريعات تُلزم مقدّمي خدمات الإنترنت بحفظ بيانات معيَّنة تُخزَّن على خواديمها لمدة تصل إلى ٩٠ يوماً[٥٣] (قابلة للتجديد)، إذا طلب منهم ذلك مسؤولو إنفاذ القانون أثناء سير تحقيق أو إجراء جنائي، حتى يتأتّى اتخاذ الخطوات القانونية المناسبة لإلزامهم بالكشف عن هذه البيانات.[٥٤] ويُعدُّ هذا الإجراء المستعجل لحفظ

---

[٤٨] مجلس أوروبا، مجموعة *المعاهدات الأوروبية*، الرقم ١٨٥. (انظر أيضاً الرابط التالي: www.coe.int/cybercrime).

[٤٩] المرجع نفسه، الديباجة.

[٥٠] تقرير توضيحي لاتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي، الفقرة ٣٣، متاح على الرابط التالي: http://conventions.coe.int/Treaty/EN/Reports/Html/185-Arabic.pdf.

[٥١] المرجع نفسه، المواد ٢-٨ و١١.

[٥٢] المرجع نفسه، الفقرة ٢ *(ب)* و*(ج)* من المادة ١٤، والمادة ١٥. وتشمل هذه الضمانات حماية حقوق الإنسان وحرياته، بما في ذلك الحقوق الناشئة عن الالتزامات المتعهد بها بموجب الاتفاقية الأوروبية بشأن حماية حقوق الإنسان والحريات الأساسية، والعهد الدولي الخاص بالحقوق المدنية والسياسية، وغيرهما من الصكوك الدولية المنطبقة لحقوق الإنسان، والرقابة القضائية أو غيرها من أشكال الرقابة المستقلة.

[٥٣] تفرض الاتفاقية حداً أدنى مدته ٦٠ يوماً فيما يخص أوامر الحفظ التي تصدر بناءً على طلب للمساعدة القانونية المتبادلة. (اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي، المادة ٢٩).

[٥٤] اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي، المادة ١٦.

البيانات المخزَّنة أمراً بالغ الأهمية نظراً للطبيعة المؤقتة للبيانات الإلكترونية ولأنَّ الإجراءات التقليدية للمساعدة القانونية المتبادلة غالباً ما تستغرق وقتا طويلا في القضايا العابرة للحدود الوطنية.[٥٥] كما أنَّ لإصدار أمر الحفظ، أو غيره من التدابير المماثلة، العديد من الفوائد مقارنة بإجراءات التفتيش والضبط التقليدية، إذ إنَّ مقدمي خدمات الإنترنت قد يكونون أقدر على تقديم الأدلة المطلوبة بسرعة. وبالإضافة إلى ذلك، فأمر الحفظ قد يكون أقل إضراراً بالأعمال المشروعة لمقدِّمي خدمات الإنترنت، لأن احتمال إضراره بسمعتهم أقل،[٥٦] وهو ما قد يسهل التعاون القائم. ويكفل إجراء التفتيش والضبط الخاص بالبيانات المخزَّنة، والمنشأ بموجب المادة ١٩ من الاتفاقية، أشكالا من الحماية لهذه البيانات مماثلة لتلك التي عادة ما تُكفل للأدلة الملموسة[٥٧] بموجب التشريعات المحلية المعنية.[٥٨]

٦١- كذلك فإنَّ اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي تقتضي أن تطبِّق أطرافها تشريعات فيما يخص تقديم بيانات المشتركين المخزَّنة.[٥٩] وقد تكون لهذه المعلومات أهمية بالغة أثناء مرحلة التحري للكشف عن هوية شخص ارتكب عملا إرهابياً باستخدام الإنترنت، بما قد يشمل معلومات عن مكان وجود هذا الشخص، وكذلك ما استُعمل في ارتكاب هذا الفعل من خدمات اتصال أخرى. كما أنَّ الاتفاقية تقتضي أن تقيم الدول الموقِّعة معايير دنيا لإتاحة الجمع الآني لبيانات عن حركة المعلومات[٦٠] المرتبطة باتصالات بعينها، ولاعتراض بيانات المحتوى المتعلقة بالجرائم الخطيرة التي ينص عليها القانون المحلي.[٦١]

٦٢- ويمكن تطبيق اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي مقترنةً بصكوك مكافحة الإرهاب، مثل اتفاقية مجلس أوروبا المتعلقة بمنع الإرهاب،[٦٢] لإتاحة سند قانوني للتعاون على مكافحة استخدام الإنترنت في أغراض إرهابية. وتقضي اتفاقية مجلس أوروبا المتعلقة بمنع الإرهاب بأن تجرِّم أطرافُها في قوانينها المحلية بعض الأعمال التي قد تؤدي إلى ارتكاب جرائم إرهابية، مثل التحريض العلني والتجنيد والتدريب، وجميعها يُمكن أن تُرتكب عن طريق الإنترنت. كما أنَّ الاتفاقية تقضي باتخاذ تدابير تعاون دولي ووطني لمنع الإرهاب، بما في ذلك التدابير المتعلقة بالتحقيقات. فعلى سبيل المثال، تنص المادة ٢٢ من الاتفاقية على تقاسم المعلومات مع طرف آخر دون طلب منه، فيما يتعلق بالتحقيقات أو الإجراءات، في الحدود التي يفرضها القانون المحلي، ومن أجل المصلحة المشتركة في التصدي للأعمال الإجرامية (تقاسم المعلومات التلقائي).

---

[٥٥] تقرير توضيحي لاتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي، الفقرة ١٥٧.

[٥٦] المرجع نفسه، الفقرة ١٥٥.

[٥٧] مثل الوسيلة المستخدمة لتخزين البيانات.

[٥٨] تقرير توضيحي لاتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي، الفقرة ١٨٤.

[٥٩] انظر اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي، المادة ١٨. إذ تُعرَّف "بيانات المشتركين" بحيث تتضمن أية معلومات، باستثناء بيانات حركة المعلومات وبيانات المحتوى، تتعلق بهوية المستخدم، أو عنوانه البريدي أو الجغرافي، أو رقم الهاتف أو الأرقام الأخرى للحصول على الخدمة، أو المعلومات الخاصة بالفواتير والسداد، أو غيرها من المعلومات التي تخص الموقع أو المكان الذي توجد فيه معدات الاتصال، المتوفرة بناءً على اتفاق الخدمة مع مقدِّم خدمات الإنترنت.

[٦٠] تبعاً للفقرة *(د)* من المادة ١ من اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي، فإنَّ "البيانات المتعلقة بحركة المعلومات" تتضمن أية معلومات تشير إلى مصدر الرسالة ووجهتها ومسارها وتوقيتها وتاريخها وحجمها ومدتها ونوع الخدمة الأصلية.

[٦١] تبعاً للمادتين ٢٠ و٢١، على التوالي، من اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي.

[٦٢] مجلس أوروبا، مجموعة المعاهدات الأوروبية، الرقم ١٩٦. انظر أيضاً الرابط التالي:
.http://conventions.coe.int/Treaty/en/treaties/html/196.htm

٦٣- وكلٌ من اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي واتفاقية مجلس أوروبا المتعلقة بمنع الإرهاب مفتوحٌ للتصديق أو الانضمام أمام جميع الدول الأعضاء في مجلس أوروبا،[٦٣] وأمام الدول غير الأعضاء التي شاركت في وضع هاتين الاتفاقيتين، وأمام غيرها من الدول غير الأعضاء التي تُوجَّه لها الدعوة، بموافقة كل الدول التي تتمتع بالعضوية في الاتفاقية المعنية وقت توجيه الدعوة.[٦٤] ومن الجدير بالذكر أنَّ العديد من البلدان التي لم تنضم رسمياً إلى اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي، قد استخدمت أحكامها، رغم ذلك، باعتبارها مبادئ توجيهية في صياغة تشريعاتها الوطنية للجرائم السيبرانية (انظر أيضاً الباب واو أدناه بشأن التشريعات النموذجية).

٦٤- كما وضع مجلس أوروبا البروتوكول الإضافي لاتفاقية الجريمة الإلكترونية بشأن تجريم الأفعال ذات الطبيعة العنصرية وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر.[٦٥] وقد يسهّل هذا البروتوكول الإضافي الملاحقة القضائية بشأن الأعمال الإرهابية المرتكبة عن طريق الإنترنت بقصد التحريض على العنف على أساس العرق، أو اللون، أو النسب، أو الأصل القومي أو العرقي، أو الدين.[٦٦] والبروتوكول الإضافي مفتوح أمام كل الدول المتعاقدة في اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي.[٦٧]

٢- *الاتحاد الأوروبي*

٦٥- في عام ٢٠٠٢، اعتمد مجلس الاتحاد الأوروبي القرار الإطاري (2002/475/JHA) الصادر في ١٣ حزيران/يونيه ٢٠٠٢ بشأن مكافحة الإرهاب، والذي يوحِّد تعريف الجرائم الإرهابية في جميع الدول الأعضاء في الاتحاد الأوروبي[٦٨] عبر طرح تعريف محدَّد ومشترك لمفهوم "الإرهاب"، ويؤسس قواعد للولاية القضائية لضمان إمكانية ملاحقة الجرائم الإرهابية قضائياً بفعالية، ويبيِّن تدابير محدَّدة فيما يخص ضحايا الجرائم الإرهابية. وفي إطار التصدي لخطر الإرهاب المتزايد، بما يشمل استخدام تكنولوجيات جديدة مثل الإنترنت، عُدِّل القرار الإطاري (2002/475/JHA) في عام ٢٠٠٨[٦٩] ليتضمَّن على وجه التحديد أحكاماً بشأن التحريض العلني على ارتكاب جرائم إرهابية، والتجنيد والتدريب بغرض الإرهاب. في ذلك القرار، أتى مجلس الاتحاد الأوروبي أيضاً على ذكر قرار مجلس الأمن رقم ١٦٢٤ (٢٠٠٥)، الذي دعا فيه المجلس الدول أن تحظر بنص القانون التحريض على ارتكاب عمل إرهابي أو أعمال إرهابية وأن تمنع ذلك التصرف.

---

[٦٣] في تاريخ صدور هذا المنشور، كانت الدول الـ٤٧ الأعضاء في مجلس أوروبا هي: الاتحاد الروسي، أذربيجان، أرمينيا، إسبانيا، إستونيا، ألبانيا، ألمانيا، أندورا، أوكرانيا، إيرلندا، آيسلندا، إيطاليا، البرتغال، بلجيكا، بلغاريا، البوسنة والهرسك، بولندا، تركيا، الجبل الأسود، الجمهورية التشيكية، جمهورية مقدونيا اليوغوسلافية السابقة، جمهورية مولدوفا، جورجيا، الدانمرك، رومانيا، سان مارينو، سلوفاكيا، سلوفينيا، السويد، سويسرا، صربيا، فرنسا، فنلندا، قبرص، كرواتيا، لاتفيا، لكسمبرغ، ليتوانيا، ليختنشتاين، مالطة، المملكة المتحدة، موناكو، النرويج، النمسا، هنغاريا، هولندا، اليونان.

[٦٤] انظر اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي، المادة ٣٦، واتفاقية مجلس أوروبا المتعلقة بمنع الإرهاب، المادتان ٢٣ و٢٤.

[٦٥] مجلس أوروبا، مجموعة *المعاهدات الأوروبية*، الرقم ١٨٩.

[٦٦] المرجع نفسه، المادة ٢.

[٦٧] المرجع نفسه، المادة ١١.

[٦٨] في تاريخ صدور هذا المنشور، كانت الدول الـ٢٧ الأعضاء في الاتحاد الأوروبي هي: إسبانيا، إستونيا، ألمانيا، إيرلندا، إيطاليا، البرتغال، بلجيكا، بلغاريا، بولندا، الجمهورية التشيكية، الدانمرك، رومانيا، سلوفاكيا، سلوفينيا، السويد، فرنسا، فنلندا، قبرص، لاتفيا، لكسمبرغ، ليتوانيا، مالطة، المملكة المتحدة، النمسا، هنغاريا، هولندا، اليونان.

[٦٩] قرار مجلس الاتحاد الأوروبي الإطاري (2008/919/JHA) الصادر في ٢٨ تشرين الثاني/نوفمبر ٢٠٠٨ بتعديل القرار الإطاري (2002/475/JHA) بشأن مكافحة الإرهاب.

٦٦- ويوفِّر القرار الإطاري (2008/919/JHA) سنداً للملاحقة القضائية بشأن نشر الدعاية الإرهابية والدراية الفنية اللازمة لصنع القنابل عبر الإنترنت، إذا كان هذا النشر متعمّدا ومستوفيا لشروط الجرائم المذكورة. وتستند تعديلات القرار الإطاري (2002/475/JHA)، فيما يتعلق بالتحريض العلني والتجنيد والتدريب، إلى أحكام مشابهة في اتفاقية مجلس أوروبا المتعلقة بمنع الإرهاب.[٧٠] وقد استحدث القرار الإطاري (2008/919/JHA) جرائم جديدة فيما يتعلق بالسلوكيات التي قد تؤدي إلى أعمال إرهابية، بغض النظر عن الوسائل أو الأدوات التكنولوجية التي تُرتكب هذه الجرائم عبرها. وكما هو الحال في اتفاقية مجلس أوروبا المتعلقة بمنع الإرهاب، تشمل أحكام القرار الإطاري (2008/919/JHA) الأنشطة التي تُمارس عن طريق الإنترنت وإن كانت غير مخصصة لها حصراً.

٣- *صكوك قانونية إضافية*

٦٧- من بين الصكوك القانونية الإضافية الملزمة التي اعتمدتها منظمات إقليمية أو دون إقليمية والتي قد تتضمن أحكاماً ذات صلة بمكافحة استخدام الإنترنت في أغراض إرهابية ما يلي:

- الاتفاقية الإقليمية لرابطة جنوب آسيا للتعاون الإقليمي لقمع الإرهاب (١٩٨٧)
- الاتفاقية العربية لمكافحة الإرهاب (١٩٩٨)
- معاهدة التعاون بين الدول الأعضاء في رابطة الدول المستقلة لمكافحة الإرهاب (١٩٩٩)
- معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي (١٩٩٩)
- اتفاقية منظمة الوحدة الأفريقية لمنع الإرهاب ومكافحته (١٩٩٩)
- اتفاقية البلدان الأمريكية لمناهضة الإرهاب (٢٠٠٢)
- اتفاقية رابطة أمم جنوب شرق آسيا بشأن مكافحة الإرهاب (٢٠٠٧)
- التوجيه الصادر عن الجماعة الاقتصادية لدول غرب أفريقيا بشأن مكافحة الجرائم السيبرانية (٢٠٠٩).

واو- التشريعات النموذجية

٦٨- على الرغم من أن التشريعات النموذجية لا تنشئ التزامات ملزمة قانوناً وإنما تتيح مبادئ توجيهية استرشادية، فإنها تؤدي دوراً هاماً في تحقيق التجانس بين المعايير القانونية في مختلف الدول. وعلى العكس من الاتفاقيات الدولية، التي قد تتطلب مفاوضات مكثفة لوضع احتياجات مجموعة متنوعة من الموقِّعين المحتملين بعين الاعتبار، فإنَّ أحكام القوانين النموذجية تمدّ الدول بميزة الاستفادة من أحكام قانونية تأسيسية مُحكمة باعتبارها نقطة انطلاق لوضع التشريعات المحلية. ومن بين المزايا الرئيسية لاستخدام الأحكام النموذجية أساساً

[٧٠] مجلس الوزراء، "تعديل القرار الإطاري المتعلق بمكافحة الإرهاب" بيان صحفي صادر في ١٨ نيسان/أبريل ٢٠٠٨.

للتشريعات الوطنية تيسيرُ التعاون الدولي، بوسائل منها التخفيف من المنازعات الناجمة عن الخطأ في تفسير الأحكام في مختلف النظم القانونية (على سبيل المثال، بين الولايات القضائية الخاضعة لنظام القانون العام والخاضعة منها لنظام القانون المدني) وفيما يتعلق بمتطلبات ازدواجية التجريم.[٧١] (انظر المناقشة الواردة في الباب خامساً-واو-٥ أدناه.)

١- *الكومنولث*

٦٩- صيغ قانون الكومنولث النموذجي بشأن الحواسيب والجرائم المتصلة بها (٢٠٠٢) على أساس اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي.[٧٢] ويهدف القانون النموذجي إلى الاستفادة من أوجه التشابه في النظم القانونية للدول الأعضاء في الكومنولث[٧٣] لتعزيز التجانس في كل من الجوانب الموضوعية والجوانب الإجرائية لمكافحة الجرائم السيبرانية ولتعزيز التعاون الدولي. وقانون الكومنولث النموذجي متسقٌ مع المعايير التي حددتها اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي.

٢- *رابطة الدول المستقلة*

٧٠- كذلك فقد اعتمدت الدول الأعضاء في رابطة الدول المستقلة قوانين ومبادئ توجيهية تشريعية نموذجية تهدف إلى تحقيق التجانس فيما بين نظم التشريع الوطنية، آخذةً في الاعتبار الخبرات الدولية في مجال مكافحة الإرهاب. ووُضعت هذه الأحكام النموذجية استنادا إلى المعايير القانونية الدولية مع تطويعها لتلائم احتياجات الدول الأعضاء في رابطة الدول المستقلة.[٧٤] فعلى سبيل المثال، تنص المادة ١٣ من القانون النموذجي بشأن إطار التنظيم الرقابي لشبكة الإنترنت[٧٥] على أحكام نموذجية فيما يخص مكافحة استخدام الإنترنت لأغراض غير قانونية.

٣- *الاتحاد الدولي للاتصالات*

٧١- الاتحاد الدولي للاتصالات وكالة متخصصة من وكالات الأمم المتحدة تؤدي دوراً رياديا في المسائل المتعلقة بالجرائم السيبرانية. وقد وضع الاتحاد عُدّة التشريع في مجال الجرائم السيبرانية (٢٠١٠) لتعزيز التجانس فيما بين التشريعات الوطنية بشأن هذه الجرائم وقواعدها الإجرائية، بما في ذلك ما يتعلق بأعمال الإرهاب

---

[٧١] لا يكون تسليم المطلوبين ممكنا، تبعاً لمبدأ ازدواجية التجريم، إلاّ في الحالات التي يكون فيها الفعل الذي يستند طلب التسليم إليه فعلا يُعاقب عليه في كل من الدولة الطالبة والدولة متلقية الطلب.

[٧٢] لمزيد من المعلومات، انظر: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.

[٧٣] في تاريخ صدور هذا المنشور، كانت الدول الـ٥٣ الأعضاء في الكومنولث هي: أستراليا، أنتيغوا وبربودا، أوغندا، بابوا غينيا الجديدة، باكستان، بربادوس، بروني دار السلام، بليز، بنغلاديش، بوتسوانا، ترينيداد وتوباغو، توفالو، تونغا، جامايكا، جزر البهاما، جزر سليمان، جمهورية تنزانيا المتحدة، جنوب أفريقيا، دومينيكا، رواندا، زامبيا، ساموا، سانت فنسنت وجزر غرينادين، سانت كيتس ونيفيس، سانت لوسيا، سري لانكا، سنغافورة، سوازيلند، سيراليون، سيشيل، غامبيا، غانا، غرينادا، غيانا، فانواتو، قبرص، الكاميرون، كندا، كيريباتي، كينيا، ليسوتو، مالطة، ماليزيا، ملاوي، ملديف، المملكة المتحدة، موريشيوس، موزامبيق، ناميبيا، ناورو، نيجيريا، نيوزيلندا، الهند.

[٧٤] في تاريخ صدور هذا المنشور، كانت الدول الـ١١ الأعضاء في كومنولث الدول المستقلة هي: الاتحاد الروسي، أذربيجان، أرمينيا، أوزبكستان، أوكرانيا، بيلاروس، تركمانستان، جمهورية مولدوفا، طاجيكستان، قيرغيزستان، كازاخستان.

[٧٥] مرفق القرار رقم ٣٦-٩ الصادر عن الجمعية البرلمانية للدول الأعضاء في رابطة الدول المستقلة، الذي اعتُمد في ١٦ أيار/مايو ٢٠١١.

المرتكبَة عبر استخدام الإنترنت. وقد وُضعت العُدَّة التشريعية على أساس تحليل شامل لاتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي وتشريعات الدول المتقدمة بشأن الجرائم السيبرانية.[٧٦] ولئن كانت عُدّة الاتحاد التشريعية تتناول في المقام الأول المسائل المتعلقة بالأمن السيبراني، فإنها تقدِّم أحكاماً نموذجية لتجريم بعض الأعمال الإرهابية التي تُستخدم فيها الإنترنت، مثل الدخول غير المصرح به إلى برامج أو بيانات حاسوبية لأغراض إرهابية أو نقل برمجيات ضارة بقصد دعم الإرهاب.[٧٧]

[٧٦] الاتحاد الدولي للاتصالات، عُدّة التشريع في مجال الجرائم السيبرانية (٢٠١٠)، الفقرة ٢-٢.

[٧٧] المرجع نفسه، المادتان ٣ *(و)* و٦ *(ح)*.

ثالثاً- أطر السياسات العامة والتشريعات

ألف- مقدِّمة

٧٢- بالإضافة إلى استخدام الإنترنت للتخطيط للأعمال الإرهابية وتمويلها، فإنَّ الإرهابيين يستخدمونها أيضاً لتجنيد أعضاء جدد وتدريبهم، والاتصال فيما بينهم، والتحري عن الأهداف المحتملة أو استطلاعها، ونشر الدعاية، وتحريض آخرين على القيام بأعمال إرهابية.

٧٣- ويتناول هذا الفصل المسائل المتعلقة بوضع سياسات عامة وتشريعات في مجال العدالة الجنائية تهدف إلى مواجهة هذه المخاطر بهدف الوقوف، عن طريق تقديم أمثلة وتجارب وطنية من بعض الدول الممثَّلة في اجتماعات فريق الخبراء، على التحديات والنُّهج الشائعة التي يمكن إما أن تعوق أو تعزز التحقيق والملاحقة القضائية الفعّالين بشأن قضايا الإرهاب التي تنطوي على جانب من جوانب استخدام الإنترنت.

باء- السياسات العامة

٧٤- على الدول أن تضع سياسات عامة وأطراً تشريعية واضحة على الصعيد الوطني ليتسنى اتخاذ تدابير فعَّالة في مجال العدالة الجنائية لمواجهة المخاطر التي يشكِّلها استخدام الإرهابيين لشبكة الإنترنت. وبصورة عامة، تركِّز هذه السياسات العامة والقوانين على ما يلي:

(أ) تجريم الأعمال غير القانونية التي يقوم بها الإرهابيون على الإنترنت أو الخدمات المتعلقة بها؛

(ب) تزويد جهات إنفاذ القانون المسؤولة عن التحقيقات المتعلقة بالإرهاب بصلاحيات التحقيق اللازمة؛

(ج) التنظيم الرقابي للخدمات المتعلقة بشبكة الإنترنت (مثل مقدِّمي خدمات الإنترنت) ومراقبة المحتويات على الشبكة؛

(د) تيسير التعاون الدولي؛

(هـ) استحداث إجراءات قضائية أو استدلالية متخصصة؛

(و) الحفاظ على المعايير الدولية لحقوق الإنسان.

النُّهُج المتَّبعة في تقرير السياسات العامة

٧٥- حدَّد الفريق العامل المعني بمكافحة استخدام الإنترنت في أغراض إرهابية التابع لفرقة العمل المعنية بتنفيذ تدابير مكافحة الإرهاب، في منشوره الصادر في عام ٢٠١١ تحت عنوان "*مكافحة استخدام الإنترنت في أغراض إرهابية: الجوانب القانونية والتقنية*"،[٧٨] ثلاثة نُهُج استراتيجية عامة يُمكن للدول أن تتصدى للأنشطة الإرهابية على الإنترنت من خلالها باستخدام ما يلي:

[٧٨] انظر الأمم المتحدة، فرقة العمل المعنية بتنفيذ تدابير مكافحة الإرهاب، الفريق العامل المعني بمكافحة استخدام الإنترنت في أغراض إرهابية، *Countering the Use of the Internet for Terrorist Purposes: Legal and Technical Aspects* (نيويورك، ٢٠١١).

(أ) تشريعات عامة عن الجرائم السيبرانية؛

(ب) تشريعات عامة عن مكافحة الإرهاب (أي غير مخصصة للإنترنت)؛

(ج) تشريعات مخصصة للإنترنت عن مكافحة الإرهاب.

٧٦- ويُلاحَظ أنَّه يُمكن الاستعانة في النهج *(أ)*، إضافة إلى التشريعات العامة المتعلقة بالجرائم السيبرانية، بجرائم أخرى غير مكتملة، مثل التحريض والتواطؤ الإجرامي، عند تناول قضايا الإرهاب التي تنطوي على جانب من جوانب استخدام الإنترنت، ولا سيما عندما يتعلق الأمر بالأعمال المزعومة التي تهدف إلى التحريض على أعمال إرهابية.

٧٧- ويُعتبر نظام التصنيف الواسع الذي يعتمده الفريق العامل إطاراً مفاهيمياً مفيداً لتوجيه عمل مقرِّري السياسات العامة والمشرِّعين عند النظر في نُهج السياسات العامة والنُّهج التشريعية المناسبة في الدول التي ينتمون إليها.

٧٨- وثمة مرجع مفيدٌ آخر لمقرِّري السياسات العامة والمشرّعين، في مجال "*مكافحة استخدام الإنترنت في أغراض إرهابية*"،[٧٩] ألا وهو عُدّة التشريع في مجال الجرائم السيبرانية، التي وُضعت برعاية الاتحاد الدولي للاتصالات. فهي، بالإضافة إلى احتوائها على أحكام جنائية نموذجية أخرى، تشتمل على العديد من الجرائم المتعلقة خصيصاً بالإرهاب، بما في ذلك الفقرة *(و)* من المادة ٣، التي تتناول الدخول غير المصرَّح به إلى برامج حاسوبية أو الحصول على برامج حاسوبية بغرض التحضير لارتكاب أعمال إرهابية، أو التآمر على ذلك، أو التخطيط له، أو تسهيله، أو المساعدة فيه.

٧٩- ولدى الحكومات، في ضوء الإطار الواسع الذي تتيحه الصكوك العالمية لمكافحة الإرهاب وما يتصل بها من معايير دولية لحقوق الإنسان، قدر كبير من المرونة في اختيار النهج الذي تُفضله، فلا مفر من أن تختلف النُّهُج باختلاف الدول. ولا يعدو هذا الفصل أن يسلِّط الضوء على أمثلة للنُّهج التي اعتمدتها بعض الدول، وهو ما قد يكون مُعيناً لمقرري السياسات العامة والمشرعين.

٨٠- وفي الوقت الراهن، ليس هناك إلا قليلٌ من الدول التي وضعت تشريعات لمكافحة الإرهاب تستهدف خصيصاً استخدام الإرهابيين للإنترنت، ومن بين تلك الدول المملكةُ المتحدة، حيث سنَّت الحكومة، في أعقاب تفجيرات عام ٢٠٠٥ في لندن، قانون الإرهاب لسنة ٢٠٠٦ الذي يتضمن الجزء الأول منه أحكاماً تتناول خصيصاً الأنشطة التي تستند إلى الإنترنت والتي يُرجَّح أن تشجِّع على ارتكاب أعمال إرهابية أو تساعد في ذلك. ويستكمل القانون المذكور قانون إساءة استخدام الحاسوب لسنة ١٩٩٠، الذي يتناول الجرائم الحاسوبية والجرائم السيبرانية عموما.

٨١- وفي عام ٢٠٠٧، أقرَّت الإمارات العربية المتحدة قوانين اتحادية بشأن الجرائم السيبرانية تجرِّم أفعالا أخرى إلى جانب الاختراق الحاسوبي وغيره من الأنشطة المتعلقة بالإنترنت، هي إنشاء موقع شبكي أو نشر معلومات لجماعات إرهابية تحت مسميات تمويهية بقصد تسهيل الاتصال بقياداتها، أو ترويج أفكارها،

[٧٩] المرجع نفسه، الفقرة ٢٠.

أو تمويل أنشطتها، أو نشر معلومات عن كيفية صنع المتفجرات أو غيرها من المواد لاستخدامها في هجمات إرهابية.[٨٠]

٨٢- وفي عام ٢٠٠٨، طبَّقت حكومة المملكة العربية السعودية قوانين جديدة في شأن التكنولوجيا، بما يشمل قانوناً يعتبر امتلاك موقع شبكي يناصر الإرهاب أو يدعمه جريمةً يعاقَب عليها بالغرامة والسجن لمدة تصل إلى ١٠ سنوات.[٨١]

٨٣- وفي عام ٢٠٠٨ أيضاً، سنَّت حكومة باكستان قانون منع الجرائم الإلكترونية لسنة ٢٠٠٨، الذي نص على أحكام محددة في شأن الجرائم المرتبطة بالإرهاب السيبراني. إلا أنَّ هذا القانون لم يعد نافذاً.[٨٢]

٨٤- وأخيراً فقد شهد العام نفسه قيام حكومة الهند بتعديل قانون تكنولوجيا المعلومات لسنة ٢٠٠٠، لكي ينصَّ على جرائم "الإرهاب السيبراني" (المادة ٦٦ واو) وغيرها من المسائل المتعلقة بالإنترنت.

٨٥- والمستوى الدولي، مع بعض الاستثناءات، وفي غياب أي صك عالمي يفرض التزاماً صريحاً بسنِّ تشريعات تستهدف خصيصاً الأنشطة الإرهابية على الإنترنت، اختارت معظم الحكومات مع ذلك أن تتعامل مع هذه المخاطر باتباع نهج مختلط، مستعينةً بمزيج من القوانين الجنائية العامة إلى جانب تشريعات الجرائم السيبرانية وتشريعات مكافحة الإرهاب. ففي بعض البلدان، على سبيل المثال، تركِّز القوانين الجنائية على الأفعال الإجرامية الموضوعية دون التفرقة بينها من حيث الوسيلة التي تُستخدم لارتكابها. وبموجب هذا النهج، تُعتبر شبكة الإنترنت مجرد أداة يستخدمها الإرهابيون لارتكاب جريمة موضوعية غالباً ما تكون واردة في أحكام قانون العقوبات الوطني.

٨٦- وهذا هو النهج المتَّبع في الصين، حيث يتضمن القانون الجنائي لجمهورية الصين الشعبية مادة تتناول تجريم كل الأنشطة غير القانونية التي تُستخدم فيها الإنترنت. فالمادة ٢٨٧ من القانون الجنائي تجعل من استخدام الحاسوب لارتكاب فعل مجرَّم جريمةً يلاحَق مرتكبها قضائياً ويعاقَب وفقاً للأحكام المنصوص عليها في ذلك القانون. وعليه، فإنّ الإنترنت تُعتبر بمثابة وسيلة أو أداة يُمكن أن يُرتكب العمل الإجرامي من خلالها، لا ركنا مستقلا من أركان الجريمة، ومن ثم فهي مجرَّمة ضمن الأحكام الموضوعية للقانون الجنائي.

٨٧- وفي سياق الإرهاب، ثمة أحكام في الصين تجرِّم مختلف أشكال الأنشطة الإرهابية، بما في ذلك المادة ١٢٠ من القانون الجنائي، التي تجرِّم الأنشطة المتعلقة بإنشاء التنظيمات الإرهابية وقيادتها والاشتراك فيها. ويشمل هذا الحكم الواسع النطاق مجموعة متنوعة وكبيرة من الأنشطة المتعلقة بالإرهاب، بما في ذلك الأنشطة التي تُمارس على الإنترنت.

---

[٨٠] قانون اتحادي رقم (٢) لسنة ٢٠٠٦ في شأن *مكافحة جرائم تقنية المعلومات، الجريدة الرسمية لدولة الإمارات العربية المتحدة*، العدد ٤٤٢، السنة السادسة والثلاثون، محرم ١٤٢٧هـ/كانون الثاني/يناير ٢٠٠٦م. انظر الرابط التالي: www.moft.gov.ae/images/dcontent/rules/27.pdf.

[٨١] David Westley, "Saudi tightens grip on Internet use", *Arabian Business*, 26 January 2008.

[٨٢] "Pakistan lacks laws to combat cyber terrorism", *The New New Internet*، انظر الرابط التالي: www.thenewnewInternet.com/2010/09/01/pakistan-lacks-laws-to-combat-cyber-terrorism.

٨٨- وفي جمهورية كوريا، يمكن تطبيق نوعين من القوانين الجنائية على الأعمال الإرهابية التي تُستخدم فيها الإنترنت بطريقة ما. النوع الأول هو القانون الجنائي العام، أمَّا الآخر فهو قانون جنائي خاص، وُضع عام ١٩٨٦، بشأن الأعمال الإجرامية المتعلقة بالمعلومات أو الاتصالات. وتتناول المادة ٩٠ من القانون الجنائي التحضير لهذه الأعمال فضلا عن التآمر أو التحريض أو الدعاية، وتنص على أنَّ أي شخص يقوم بالتحضير لارتكاب جريمة منصوص عليها في المادة ٨٧ من القانون الجنائي (أعمال الشغب، أو التمرد، أو الاضطرابات) أو المادة ٨٨ (القتل في إطار الأفعال المنصوص عليها في المادة ٨٧)، أو بالتآمر لهذا الغرض، يُعاقب بالسجن لثلاث سنوات أو أكثر. وتنص المادة ١٠١ من القانون الجنائي على أن أي شخص يقوم بالتحضير لارتكاب جريمة منصوص عليها في المواد من ٩٢ إلى ٩٩ من القانون الجنائي، أو بالتآمر لهذا الغرض، يكون مذنباً ويُعاقب بالسجن لسنتين أو أكثر. وتتعلق المادة ١١٤ من القانون الجنائي بإنشاء الجماعات الإجرامية. وبموجب القانون الجنائي الخاص كذلك، وضعت الحكومة مجموعة من الأحكام التي تجرِّم على وجه التخصيص الأعمال غير القانونية التي تستهدف شبكات المعلومات والاتصالات والمعلومات الشخصية.

٨٩- وفي الممارسة العملية، وبصرف النظر عن النهج المتَّبع، تدل التجربة على أنَّ معظم الدول تعتمد نهجاً متعدد الجوانب في تناول التحقيق في الأعمال الإرهابية والملاحقة القضائية بشأنها، بما في ذلك الأعمال التي تُستخدم فيها الإنترنت بطريقة ما. فالجهات القائمة على إنفاذ القانون والملاحقة القضائية تعمد إلى استخدام ما يناسب الملابسات الخاصة بكل قضية من أحكام تشريعية أياً كانت.

٩٠- وتتشابه الصلاحيات التي تحتاجها جهات إنفاذ القانون للتحقيق في قضايا الإرهاب بفعالية تشابهاً كبيراً بصرف النظر عن الولاية القضائية المعنية، مع وجود اختلافات في السياسات العامة والتشريعات الوطنية، نتيجةً للتنوع في النظم القانونية، والترتيبات الدستورية وغيرها من العوامل (كالثقافات على سبيل المثال).

٩١- ويترك مجال التنظيم الرقابي للإنترنت ومراقبة محتواها مجالا واسعا للتباين فيما بين النُّهُج الوطنية. فلئن نصّ كل من الإعلان العالمي لحقوق الإنسان والعهد الدولي الخاص بالحقوق المدنية والسياسية على معايير دولية متعلقة بالتنظيم الرقابي للتعبير عن الأفكار ونقلها، فلا يوجد صك شامل ملزم دولياً يضع معايير نهائية وملزمة بشأن ما يُمكن اعتباره محتوى مقبولا على شبكة الإنترنت أو الطريقة التي ينبغي لكل دولة اتباعها في التنظيم الرقابي للأنشطة المتعلقة بالإنترنت داخل أراضيها. واستغلال الأطفال في المواد الإباحية هو، حاليا، المجال الوحيد الذي تحظر فيه الدول كافة هذه الأنشطة، وإن لم يوجد بشأنها صك أو تعريف ملزم عالمياً.[٨٣] لكنّ عدم وجود تعريف متفق عليه عالمياً للإرهاب يمثل، في سياق الإرهاب، عقبة حتى الآن أمام التوصّل إلى نهج متفق عليه دولياً من أجل التنظيم الرقابي المناسب لما يتعلق بالإرهاب من أنشطة ومحتويات على شبكة الإنترنت.

٩٢- ومن حيث الإجراءات القضائية أو الاستدلالية المتخصصة في مجال الإرهاب، فقد اعتمدت بعض الدول إجراءات قضائية وإدارية مخصصة لقضايا الإرهاب يمكن أن تنطبق على القضايا التي يستخدم فيها الإرهابيون شبكة الإنترنت. ومن المهم، عند اعتماد هذا النهج، أن تمتثل الآليات المتخصصة تمام الامتثال للالتزامات الدولية ذات الصلة في مجال حقوق الإنسان، بما في ذلك الالتزامات المتعلقة بالحق في الحرية وفي محاكمة عادلة.

(٨٣) Maura Conway, "Terrorism and Internet governance: core issues", *Disarmament Forum*, vol. 3 (2007), p. 27.

جيم- التشريعات

١- التجريم

٩٣- ليس من بين الصكوك العالمية لمكافحة الإرهاب، كما ذُكر آنفا، صكٌّ يلزم الدول بسنِّ تشريعات تستهدف خصيصاً استخدام الإنترنت من قبل الإرهابيين. ومن ثم فإذا كان من المرجَّح للغاية استخدامُ الجناة للإنترنت بطريقة ما في معظم قضايا الإرهاب، فمن المرجَّح كذلك أن تقوم السلطات في العديد من الدول، إلى جانب استخدامها أحكام تجريم تتعلق بالسلوكيات غير القانونية المنصوص عليها في الصكوك العالمية، بالاعتماد أيضا على أحكام تجريم أخرى وفق قوانينها الجنائية، بما في ذلك الجرائم غير المكتملة مثل التآمر والتحريض والتواطؤ الإجرامي، حتى يُمكن ملاحقة الجناة قضائياً.

٩٤- ويتناول هذا الباب أمثلة على أحكام تشريعية مختلفة من بعض الدول، بغية الوقوف على النُّهُج التي قد تتيح الأساس اللازم لاتخاذ تدابير فعَّالة في مجال العدالة الجنائية لمواجهة مختلف أنواع السلوك.

(أ) الأفعال أو الأقوال المناصرة للإرهاب على شبكة الإنترنت

٩٥- إضافةً إلى الأفعال المرتبطة بارتكاب أعمال إرهابية موضوعية (كالتفجيرات الإرهابية على سبيل المثال)، ثمة أدلة واضحة على استخدام الإرهابيين للإنترنت استخداما متزايدا للقيام بأعمال دعم مثل تجنيد الأعضاء وتدريبهم، وتبادل المعلومات المفيدة، ونشر الدعاية، والتحريض على ارتكاب أعمال إرهابية. ونظراً لطبيعة نسق الإنترنت ونطاق انتشارها العالمي، فثمة احتمال متزايد أن تشارك مختلف الجهات الفاعلة الموجودة فعليا في ولايات قضائية مختلفة في هذه الأنواع من الأنشطة.

٩٦- وفي المملكة المتحدة، يحتوي الجزء السادس من قانون الإرهاب لسنة ٢٠٠٠ على جرائم عديدة يُمكن أن تُتخذ سنداً لاتهام الأفراد الذين يستخدمون الإنترنت لدعم الأنشطة الإرهابية.

٩٧- وتجرِّم المادة ٥٤ من القانون جلبَ آخرين أو استقبالهم أو دعوتهم لتلقي تعليمات أو تدريبات عن صُنع الأسلحة النارية، أو المواد المشعة، أو ما يتصل بها من أسلحة أو متفجرات أو أسلحة كيميائية أو بيولوجية أو نووية، أو عن استخدام أي مما سبق.

٩٨- وتجرِّم المادة ٥٧ من القانون نفسه حيازة مواد في الحالات التي تبرر الاشتباه في وجود هذه المواد في حوزة الشخص المعني لغرض يتصل بالتحضير لعمل إرهابي أو التحريض عليه أو ارتكابه. وقد استُخدم هذا التجريم في السنوات الأخيرة استخداماً ناجحاً في الملاحقة القضائية للعديد من الأفراد الذين وُجدت لديهم مواد متنوعة منها أقراص صلبة، وأقراص فيديو رقمية، ومستندات حول كيفية صنع أو استعمال أدوات مثل مدافع الهاون والأحزمة الناسفة والنابالم.[٨٤] وللبرهنة على ارتكاب هذه الجريمة، يجب أن تُثبت النيابة العامة وجود صلة ما

(٨٤) Susan Hemming, "The practical application of counter-terrorism legislation in England and Wales: a prosecutor's perspective", *International Affairs*, vol. 86, No. 4 (July 2010), p. 963.

بين المواد المعنية وبين عمل إرهابي محدَّد. وبالرغم من النجاح في الملاحقة القضائية بشأن عدة جرائم وفقا لما هو منصوص عليه في المادة ٥٧، فقد اعتمدت المحاكم تفسيرا أضيق لنطاق تطبيق هذه المادة، كما يتضح من قضية *التاج البريطاني ضد ظفر وبوت وإقبال ورجاء ومالك* [٢٠٠٨] القضية (EWCA Crim 184).

التاج البريطاني ضد ظفر وبوت وإقبال ورجاء ومالك

في هذه القضية، التي تعود لعام ٢٠٠٧ في المملكة المتحدة، قُبلت طعون المدّعى عليهم، ظفر وبوت وإقبال ورجاء ومالك، في أحكام بالإدانة لحيازة مواد لغرض ذي صلة بارتكاب عمل إرهابي أو التحضير له أو التحريض عليه، بما يتنافى والمادة ٥٧ من قانون الإرهاب لسنة ٢٠٠٠.

وكان أربعة من الخمسة المدَّعى عليهم في القضية طلاباً في جامعة برادفورد. أما الخامس، رجاء، فكان تلميذاً بمدرسة إيلفورد. وقد اتصل هذا الأخير بإقبال عبر خدمة MSN لتبادل الرسائل عبر الإنترنت.

وقام رجاء بزيارة برادفورد لبضعة أيام، مقيماً في المنزل الذي كان إقبال وظفر يعيشان فيه، ومُحضراً معه ثلاثة أقراص مدمجة من صنعه تحتوي على مواد مختارة من الحاسوب تحت عنوان "أقراص الفلسفة". وألقت الشرطة القبض على رجاء عند عودته إلى دياره بعد انتهاء الزيارة.

وقد قادت التحقيقات اللاحقة الشرطةَ إلى إلقاء القبض على المتهمين الآخرين وتفتيش أماكن إقامتهم، الأمر الذي كشف أنَّه كان بحوزتهم أيضاً مواد جهادية متطرفة ومواد أخرى من قبيل دليل عسكري صادر في الولايات المتحدة ومُنزَّل من على الإنترنت. كما عُثر على أدلة على وقوع اتصالات عن طريق خدمة تبادل الرسائل عبر الإنترنت، بما في ذلك مناقشة بين المستأنفين الأربعة المقيمين في برادفورد جميعاً وقريبٍ لمالك يُدعى عمران ويعيش في باكستان.

وقد واجه المدَّعى عليهم في بادئ الأمر تهما بموجب المادة ٥٨ من قانون سنة ٢٠٠٠، إلا أن النيابة العامة أضافت، في مرحلة الإحالة، تهما بموجب المادة ٥٧ منبثقة من ذات الوقائع التي وُجهت وفقاً لها التهم بموجب المادة ٥٨. وبعد صدور عدد من الأحكام السابقة للمحاكمة بشأن ما إذا كان من الممكن اعتبار المعلومات المخزَّنة من بين المواد المقصودة في المادة ٥٧، اختارت النيابة العامة الشروع في المحاكمة مستندة إلى التهم الموجَّهة بموجب المادة ٥٧ وحدها.

وأثناء المحاكمة، بُـرِّئ كل من ظفر وإقبال من إحدى التهم الموجهة إليهما، ألا وهي تهمة حيازة ثلاثة من "أقراص الفلسفة" التي تحتوي على مواد مصدرها رجاء، إلا أنهما أدينا، وسائر المدَّعى عليهم، فيما يتعلق بجميع التهم الأخرى. وحُكم على مالك بالسجن ثلاث سنوات، وعلى كل من ظفر وإقبال بثلاث سنوات من الاحتجاز في إحدى مؤسسات الأحداث، وعلى بوت بـ٢٧ شهراً من الاحتجاز وعلى رجاء بسنتين من الاحتجاز.

وقد طعن المدَّعى عليهم في هذه الأحكام. واعتبرت محكمة الاستئناف أنَّ المسألة الحاسمة هي ما إذا كانت هنالك، استناداً إلى وقائع القضية، صلة تستوفي مقتضيات المادة ٥٧ فيما بين المواد المعنية وأعمال إرهابية.

فمعظم المواد التي ادَّعت النيابة العامة أنَّها كانت بحوزة المستأنفين بما يتنافى والمادة ٥٧ كانت عبارة عن أقراص مدمجة وأقراص صلبة تحتوي على مواد مخزَّنة إلكترونياً. وتشمل هذه المواد دعاية إيديولوجية واتصالات فيما بين المدَّعى عليهم، ادَّعت النيابة العامة أنَّها تبيِّن وجود خطة مبيَّتة لسفر المدَّعى عليهم إلى باكستان لتلقي التدريب والاشتراك في القتال الدائر في أفغانستان، وهو ما ادَّعت النيابة العامة أنَّه يعتبر في حكم الأعمال الإرهابية. ورأت محكمة الاستئناف أنَّه كان لزاماً على النيابة العامة أن تثبت أولا الغرض الذي احتفظ كل مستأنف بالمواد المخزنَّة لأجله، ثم أن تثبت أنَّ هذا الغرض كان "على صلة بارتكاب" الأعمال الإرهابية المتوخاة التي استندت إليها النيابة "أو التحضير لها، أو التحريض عليها"، أي القتال ضد الحكومة في أفغانستان.

وبنـاء علـى وقائع القضية، ارتأت المحكمـة، في معرض إشارتهـا إلى أن هذه القضية تطـرح أسئلة صعبة حول تفسـير نطاق تطبيق المادة ٥٧، أنَّ الصلة اللازمة ليست قائمة، وأن أحكام الإدانة المبنية عليها غير سليمة تبعا لذلك، ومن ثم قبلت الطعون.

٩٩- وقـد تبيَّن أنَّ المادة ٥٨ أفيد في العديد من القضايـا التي احتاجت فيها السلطات للتدخل بسبب عدم وجود أدلـة علـى أنَّ الفرد المعني ضالـع في نشاط مرتبط بالإرهاب. فالمادة تجرِّم جمـع أي سجلات لمعلومات أو صُنعها أو حيازتهـا، دونما عذر معقـول، إذا كانت نوع هذه السجلات مفيداً على الأرجح لشخص يرتكب عملا إرهابياً أو يحضِّر لعمل من هذا القبيل، أو حيازة أي مستند أو سجل يحتوي على معلومات من هذا القبيل.

١٠٠- وفي قضيـة *التاج البريطاني ضـد كاف* (3 All E.R. 526 [٢٠٠٨]) ، رأت المحكمة أنَّ المستندات لا تندرج ضمـن نطـاق المادة ٥٨ إلا إن كانت من نوع يُرجَّح أن يوفِّر مساعدة عملية لشخص يرتكب عملا إرهابياً أو يحضِّر لعمـل مـن هذا القبيل. وقد تأكَّد هذا النهج في قضية *التاج البريطاني ضد راء وجيم* (UKHL 13) [٢٠٠٩]، التي أكَّـدت فيهـا المحكمة على "معيار الاستخدام العملي"، الذي لا تعتـبر بموجبه حيازة مستند أو سجل جريمةً إلا إن كان لهذا المستند أو السجل استخدام عملي وكان بحوزة الشخص المعني دون عذر معقول.[٨٥] وليس ثمة تقييد لما قد يُمثِّل عذراً معقولا لهذا الغرض، شريطة إمكانية اعتبار هذا العذر حجة للدفاع أمام المحكمة.

١٠١- ولا تُلـزم المادة ٥٨ النيابة العامة بإثبات كون المتهـم إرهابيا أو حيازته لأية أشياء لغرض إرهابي، بيد أنَّه لا يجـوز للنيابة العامة الاستعانة بأدلة خارجية لإثبـات الاستخدام العملي لأي من الأشياء إلا في ظروف محدودة للغايـة. فعلـى سبيل المثال، يمكن الاستعانة بدليل لفك شفرة مستنَد، لكن لا يمكن الاستعانة بدليل لتفسير أهمية مواقع مشار إليها على خريطة. فالمعلومات يجب أن "تكون واضحة في حد ذاتها" وألا تكون معروضةً للتداول العام.

١٠٢- وفي قضية *التاج البريطاني ضد سلطان محمد* (EWCA Crim 227 [٢٠١٠]) ، رأت المحكمة أنَّه "إذا كان المستنـد المحتوي على المعلومـات لا يُستعمل استعمالا يوميا من قبل أفراد الجمهـور العاديين (كالجداول الزمنية والخرائـط علـى سبيل المثال) ، وكان بإمـكان هيئة محلفين حصيفة أن تتوصل إلى استنتـاج سليم منطقيا مفاده أنَّ المستنـد يحتـوي على معلومات من نوع مفيد على الأرجح لشخص يرتكب عملا إرهابياً أو يحضِّر لعمل من هذا القبيل، يصبح بإمكان المحلفين أن يقرروا ما إذا كانوا واثقين من أن المستند يحتوي على معلومات من هذا القبيل. فـإن قـرروا ذلك، وكان لدى المتهم القصد الجنائي اللازم، لا يتبقى سوى البـت في مسألة واحدة هي ما إذا كان للمدَّعى عليه عذر معقول".[٨٦] وبناءً على ذلك يجب على هيئة المحلفين أن تقرر ما إذا كان تفسير حيازة المستند تفسيراً معقولا في واقع الأمر إذا وضعت الوقائع والظروف المتعلقة بكل قضية في الاعتبار.[٨٧]

[٨٥] المرجع نفسه، الصفحة ٩٦٢.

[٨٦] اقتباس من المرجع التالي: "R. v. Muhammed [2010] EWCA Crim 227: terrorism — preparing an act of terrorism", *Criminal Law and Justice Weekly* (20 March 2010).

[٨٧] Hemming, "The practical application of counter-terrorism legislation in England and Wales", p. 963.

١٠٣- وقد أنشأ قانون الإرهاب لسنة ٢٠٠٦ (في المادة ٥ منه) جريمة "ارتكاب أعمال للتحضير للإرهاب". والغرض من هذه المادة هو تناول القضايا التي أوقف فيها أفراد يخططون بالفعل لأعمال إرهابية قبل إتمامهم لعمل إرهابي موضوعي أو شروعهم في القيام بعمل من هذا القبيل.[٨٨]

١٠٤- والمادة ٥ أكثر فائدة فيما يتعلق بالمجرمين الذين يعملون منفردين، أو عندما لا توجد أدلة كافية تُتخذ سندا لتوجيه تهمة التآمر لأنه لا يمكن إثبات ضلوع أكثر من شخص واحد، أو حين لا تعرف السلطات بالتفصيل ماهيّة الجريمة التي كان يجري التخطيط لها. فهذه الجريمة لا تقتضي إثبات عمل إرهابي نهائي محدَّد أو عدداً من هذه الأعمال، وإنما يجب على النيابة العامة إثبات وجود نية محددة لارتكاب عمل إرهابي أو لمساعدة شخص آخر على القيام بذلك. وقد أُدين العديد من الأفراد بهذه التهمة في المملكة المتحدة وحكم عليهم بالسجن لمدد متفاوتة، بما في ذلك السجن مدى الحياة.[٨٩]

١٠٥- وتُعدُّ قضية *التاج البريطاني ضد تيرينس روي براون* (EWCA Crim 2751 [٢٠١١]) مثالا على فائدة الأحكام من قبيل المادة ٥٨.

التاج البريطاني ضد تيرينس روي براون

كان تيرينس روي براون، وهو من مواطني المملكة المتحدة، يدير شركة على شبكة الإنترنت، حيث كان يُعلن عن إصدارات سنوية من قرص مدمج أسماه "Anarchist's Cookbook" (وصفات للفوضويين) (وهو عنوان يكاد يطابق عنوان كتاب معروف هو *The Anarchist Cookbook*)، كما كان يبيع هذه الأقراص. ولم تكن هذه الأقراص تحتوي على منشور وحيد، وإنمَّا على ٣٢٢ ١٠ ملفاً، بعضها عبارة عن منشورات كاملة في حد ذاتها. وكانت هذه المنشورات تتضمّن أدلة إرهابية كدليل تنظيم القاعدة وتعليمات حول صُنع مختلف أشكال المتفجرات وتركيب القنابل. وكانت الملفات الأخرى تتألف من تعليمات لصُنع السموم، وكيفية تجنّب لفت انتباه السلطات عند السفر، وتقنيات مناولة الأسلحة. وفي محاولة واضحة للالتفاف على القانون، قام السيد براون بنشر بيانات بإخلاء مسؤوليته على الموقع الشبكي الذي يُعلن فيه عن المنشور، مصرِّحاً أنَّ التعليمات الواردة فيه قد تكون غير قانونية أو من الخطر اتباعها، وأنَّ المقصود به هو "متعة القراءة والقيمة التاريخية فحسب". وقد تبينَّ جلياً من التحقيقات أن دوافع السيد براون كانت تجارية خالصة. كما تبدَّى أنَّه تعمَّد توسيع مجموعته في أعقاب تفجيرات لندن التي وقعت في تموز/يوليه ٢٠٠٥، وزاد من أرباحه زيادةً ذات شأن نتيجة لذلك.

وفي آذار/مارس ٢٠١١، أُدين السيد براون في سبعة تهم بموجب قانون الإرهاب لسنة ٢٠٠٠ (المادة ٥٨) فيما يتعلق بجمع معلومات يُمكن أن تستخدم في التحضير لعمل إرهابي أو لارتكاب عمل من هذا القبيل، وفي تهمتين بموجب قانون الإرهاب لسنة ٢٠٠٦ (المادة ٢) فيما يتعلق بنشر منشورات إرهابية، وفي تهمة واحدة بموجب قانون عائدات الجريمة لسنة ٢٠٠٢ فيما يتعلق بنقل ممتلكات إجرامية (أي استخدامه للأرباح التي جناها من عمله التجاري).[أ]

[٨٨] المرجع نفسه، الفقرة ٩٦٤.

[٨٩] المرجع نفسه.

وكان العـذر الـذي تقدَّم به السيد براون أثناء المحاكمة أنَّ أنشطتـه لم تعدُ كونها ممارسة قانونية لحقه في حرية التعبـير فيمـا يخص مـواد متاحة للجميع علـى الإنترنت ومشابهة من حيـث النوع، ولو لم تكـن كذلك من حيث الحجـم، لمـا يبيعه غيره مـن بائعي الكتب على الإنترنـت. وأثيرت النقاط نفسها في طلـب لم يلقَ قبولا للطعن في حكـم بالإدانة، حيـث قضت المحكمة أن تقييد حقوق براون المنصوص عليها في المادة ١٠ (من الاتفاقية الأوروبية لحقـوق الإنسـان) فيما يتعلق بالمواد التي كان من المرجَّح أن يستعين بها إرهابيون كان مبرراً ومتناسباً مع الجرم المرتَكـب. وأكَّـدت المحكمة أيضاً على حسن تقدير سلطات الادعـاء في عدم توجيه الاتهام لكل فرد يُحتمل أنَّه قد ارتكب جريمة، وإنَّما النظر في كل حالة وفقا لحيثياتها.

(أ) "Businessman who published bomb-makers' handbook 'facing lengthy spell in jail'", *Daily Mail*, 9 March 2011. متاح على الموقع www.dailymail.co.uk/news/article-1364621/Businessman-publishedbomb-makers-handbook-facing-lengthy-spell-jail.html#ixzz1j4gXbMLu.

١٠٦- وتُعـدُّ هـذه القضيـة واحـدة مـن بـين عـدة قضايـا، منهـا قضيـة *التـاج البريطـاني ضـد كاف* (QB 827 [٢٠٠٨]) وقضية *التاج البريطاني ضد غين* (1 AC 43 [٢٠١٠]) ، أوضحت فيها محاكم المملكة المتحدة السوابق القضائية المتعلقة بنطاق وتطبيق المادة ٥٨ من القانون، في ضوء ضمانات حقوق الإنسان ذات الصلة.

١٠٧- وبالإضافـة إلى الجرائـم المنصوص عليها في تشريعـات مكافحة الإرهاب، فإنَّ سلطـات المملكة المتحدة قـد استخدمت، حيثما استدعت الظروف ذلك، جريمة التحريض في ملاحقات قضائية ناجحة لأشخاص قاموا بأنشطـة مرتبطة بالإرهاب. ومن بـين الأمثلة على هذا النهج قضية *التاج البريطـاني ضد بلال ظهير أحمد*،(٩٠) التي أُدين فيها المدَّعى عليه بتهمة التحريض على القتل.

التاج البريطاني ضد بلال ظهير أحمد

هـذه القضيـة من المملكة المتحدة متعلقة بقضية سابقة عليها من العـام ٢٠١٠، ألا وهي القضية التي حُكم فيها على روشانارا شودري بالسجن مدى الحياة في ٢ تشرين الثاني/نوفمبر ٢٠١٠، لشروعها في قتل عضو البرلمان ستيفن تيمز.

فقـد قالـت شـودري، في إفادة لهـا، أنَّها كانت قد قـرّرت ارتكاب الجريمة قبـل أربعة أسابيـع تقريباً من وقوع الاعتـداء في أيار/مايـو ٢٠١٠، واشترت سكينين اثنين استعداداً لذلـك، ليكون السكين الثاني احتياطياً في حال انكسـر السكـين الأول إثر طعنهـا للضحية. وأخبرت شـودري الشرطة أنهـا كانت تشاهد أشرطـة فيديو لأنور العولقـي وعبد الله عزام، وأنَّها قد زارت الموقع الشبكي www.revolutionmuslim.com أثناء فترة تحولها إلى التطـرف. وكان هذا الموقع المعروف، والذي كان مُستضافاً علـى خواديم في الولايات المتحدة الأمريكية، يحتوي علـى مواد تروِّج للجهـاد بارتكاب أعمال عنف، بما في ذلك أشرطة فيديو وخُطـب تشجِّع على الإرهاب وروابط شبكية بمنشورات إرهابية.

وفي ١ تشريـن الثاني/نوفمـبر ٢٠١٠، نشر المدَّعى عليه رابطاً على صفحـة فيسبوك الخاصة به بمقال إخباري حول قضية تيمز/شودري، أضاف إليه التعليق التالي:

(٩٠) Nottingham Crown Court, 13 May 2011.

هذه الأخت قد أخجلتنا نحن الرجال. ينبغي أن نكون نحن من يقوم بهذا.

وفي ٤ تشرين الثاني/نوفمبر ٢٠١٠، نشر المدَّعى عليه مقالا بعنوان "أعضاء البرلمان الذين صوتوا تأييداً للحرب على العراق" على موقع www.revolutionmuslim.com باسم "بلال". وكان المقال مصدَّراً بشعار دولة العراق الإسلامية (إحدى توابع تنظيم القاعدة). وكان النص الافتتاحي اقتباساً من القرآن يرد فيه ما معناه أنَّ من مات دون أن يشارك في الجهاد فهو منافق.

وقد أخبر المقال القراءَ بأنه يمكنهم "تتبع" أعضاء البرلمان البريطانيين عبر رابط مشار إليه بموقع شبكي برلماني رسمي، بما يمكنهم من معرفة تفاصيل حول أماكن الجراحات التي سيخضع لها أعضاء البرلمان، حيث يمكن "الالتقاء بهم شخصياً".

وتلى ذلك ٢٩ اقتباساً دينياً، جميعها مترجم إلى الإنكليزية وجميعها يتعلق بالواجب المفروض على المسلمين بالاشتراك في الجهاد أو بـ"الشهادة". وبعد الاقتباسات مباشرة كان هناك رابط بصفحة شبكية تعرض سكيناً للبيع. وقام ضباط مكافحة الإرهاب البريطانيون بالاحتفاظ بنسخة من المقال باعتبارها دليل إثبات، كما تم الحصول على نسخة أخرى من الصفحة الشبكية من شركة غوغل بناء على طلب وارد في رسالة وُجهت إليها.

وفي ١٠ تشرين الثاني/نوفمبر ٢٠١٠، ألقت وحدة مكافحة الإرهاب التابعة لشرطة ويست ميدلاندز القبض على المدَّعى عليه بالقرب من منزله في ولفرهامبتون. وقد وُجد بحوزته جهاز حاسوب محمول قال للضباط الذين ألقوا عليه القبض أنَّه قد استخدمه في نشر مقاله حول أعضاء البرلمان في موقع www.revolutionmuslim.com. وقد كشف التحليل الجنائي للحاسوب المحمول عن أنَّ المدَّعى عليه قد حاول محو آثار أنشطته على شبكة الإنترنت قبل القبض عليه.

وفي ١٦ تشرين الثاني/نوفمبر، وُجِّهت للمدَّعى عليه تهمة التحريض على القتل فيما يتعلق بالمقال، وثلاث تهم بحيازة مواد يُرجَّح كونها ذات فائدة للإرهابيين بموجب المادة ٥٨ من قانون الإرهاب لسنة ٢٠٠٠. وقد أقرّ المدَّعى عليه لاحقاً بذنبه في هذه التهم، وكذلك في تهمة التحريض على الكراهية الدينية، بسبب تعليقات منشورة في منتدى على الإنترنت، وحُكم عليه بالسجن ١٢ عاماً، إلى جانب خمس سنوات إضافية من الإفراج المشروط تحت المراقبة.

١٠٨- وفي الولايات المتحدة، يقضي البند ٨٤٢ *(ع)* من الفصل ١٨ من المدونة القانونية للولايات المتحدة، المعنون "توزيع معلومات تتعلق بالمتفجرات، والأجهزة التدميرية، وأسلحة الدمار الشامل"، بتجريم قيام شخص بتوزيع معلومات، بأي وسيلة كانت، فيما يتعلق بصنع المتفجرات، أو الأجهزة التدميرية، أو أسلحة الدمار الشامل، أو استخدام أي مما سبق، بقصد أن تُستخدم هذه المعلومات في لتيسير ارتكاب جريمة من جرائم العنف، أو مع العلم بأنَّ الشخص الذي ستصله هذه المعلومات نتيجة لهذا التوزيع ينتوي استخدامها في تيسير ارتكاب جريمة من جرائم العنف. وقد استعين بهذا الحكم القانوني في الولايات المتحدة في الملاحقة القضائية لأشخاص قاموا بتوزيع معلومات من هذا القبيل على شبكة الإنترنت.

(ب) التحريض على الإرهاب

١٠٩- جريمة التحريض على أعمال إرهابية هي موضوع قرار مجلس الأمن ١٦٢٤ (٢٠٠٥). ففي هذا القرار، دعا المجلس جميع الدول إلى أن تعتمد من التدابير ما قد يكون لازماً ومناسباً ومتمشياً مع التزاماتها بموجب القانون الدولي، وأن تحظر بنص القانون التحريض على ارتكاب عمل أو أعمال إرهابية وأن تمنع مثل هذا التصرف.

١١٠- ويمثِّل استحداث قوانين تجرِّم التحريض على أعمال إرهابية وإنفاذ هذه القوانين، مع توفير الحماية الكاملة في الوقت نفسه لحقوق الإنسان من قبيل الحق في حرية التعبير والحق في حرية تكوين الجمعيات، تحدياً مستمراً يواجه مقرِّري السياسات العامة، والمشرعين، وجهات إنفاذ القانون، وأعضاء النيابة العامة. فالقضايا التي يصرح فيها أشخاص بأقوال على شبكة الإنترنت، خاصة حين يكون الجناة المزعومون وخدمات الإنترنت التي يستخدمونها والجمهور الذي يستهدفونه في ولايات قضائية مختلفة تنظِّمها قوانين وطنية وضمانات دستورية مختلفة، تطرح مزيدا من التحديات في مجال التعاون الدولي على المحققين وأعضاء النيابة العامة.

١١١- وتبرز الخبرة الدولية فيما يخص الملاحقة القضائية بشأن التحريض على ارتكاب أعمال إرهابية مسألتين: أولا، مدى أهمية التمييز في الممارسة العملية بين الدعاية الإرهابية (الأقوال التي تناصر وجهات نظر إيديولوجية أو دينية أو سياسية معيَّنة) والمواد أو الأقوال التي تعتبر في حكم التحريض على ارتكاب أعمال عنف إرهابية (وصعوبة هذا التمييز أحيانا)؛ ثانياً، ما يتطلبه إنفاذ القوانين التي تتناول أعمال التحريض المزعومة من تقييم دقيق للظروف والسياق في كل قضية على حدة، للوقوف على ما إذا كان الشروع في ملاحقة جريمة التحريض قضائياً مناسباً في قضية بعينها.

١١٢- وقد اتفق أعضاء فريق الخبراء الذين سبق لهم المشاركة في التحقيق أو الملاحقة القضائية بشأن جرائم تحريض على أعمال إرهابية، على الأهمية العملية لإجراء تقييم تام للسياق الذي صُرِّح فيه بالأقوال التحريضية المزعومة، وهو ما يتعدى الكلمات المستخدمة ليشمل المنبر المستخدم للتصريح بها، وأبرزوا تلك الأهمية العملية. كما سلط أولئك الخبراء الضوء على أنَّ سمات الجمهور الذي يُرجَّح تلقيه لهذه الأقوال قد تكون عاملا ذا أهمية بالغة في الوقوف على ما إذا كان من المناسب الشروع في الدعوى الجنائية ضد جريمة التحريض أو من المرجَّح نجاحها في قضية بعينها.

١١٣- وفي المملكة المتحدة، تجرِّم المادة ٥٩ من قانون الإرهاب لسنة ٢٠٠٠ تحريضَ الغير على ارتكاب عمل إرهابي كلياً أو جزئياً خارج المملكة المتحدة، إذا كان من شأن هذا العمل، إذا ارتُكب في إنكلترا وويلز، أن يشكِّل جريمة منصوصاً عليها في المادة (على سبيل المثال: القتل، أو الإصابة المتعمدة، أو التفجير، أو تعريض حياة الآخرين للخطر بإتلاف الممتلكات).

١١٤- وفي قضية شهيرة، هي قضية *التاج البريطاني ضد التسولي وآخرين*،[٩١] أقرَّ كل من يونس التسولي ووسيم مغال وطارق الداعور بكونهم مذنبين في التهم الموجَّهة إليهم بموجب قانون الإرهاب لسنة ٢٠٠٠ بالتحريض على القتل لأغراض إرهابية عن طريق إنشاء أعداد كبيرة من المواقع الشبكية ومنتديات الدردشة المستخدَمة لنشر مواد تحرِّض على أعمال قتل إرهابية، وعلى الأخص في العراق، وإدارة هذه المواقع والمنتديات.

[٩١] *R v. Tsouli* [2007] EWCA (Crim) 3300.

التاج البريطاني ضد التسولي وآخرين

المدَّعى عليهم في هذه القضية الشهيرة من المملكة المتحدة هم يونس التسولي ووسيم مغال وطارق الداعور. وقد وجهت إليهم في بادئ الأمر ١٥ تهمة. وقبل المحاكمة، اعترف التسولي ومغال بأنَّهما مذنبان في تهمة التآمر بغرض الاحتيال. وأثناء المحاكمة، أقرَّ الثلاثة جميعاً، بعد سماعهم لأدلة النيابة العامة، بأنَّهم مذنبون في تهمة التحريض على الإرهاب خارج البلاد، وأقرَّ الداعور بكونه مذنباً في تهمة التآمر بغرض الاحتيال.

فقد قام المدَّعى عليهم، في الفترة ما بين حزيران/يونيه ٢٠٠٥ واعتقالهم في تشرين الأول/أكتوبر ٢٠٠٥، بشراء عدد كبير من المواقع الشبكية ومنتديات الدردشة على الإنترنت وإنشائها وإدارتها، وقد نُشر على هذه المواقع والمنتديات مواد تُحرض على أعمال قتل إرهابية، وعلى الأخص في العراق. وتمت تغطية تكاليف شراء المواقع الشبكية وإدارتها من عائدات متأتية من الاحتيال في استخدام بطاقات ائتمانية. وقد شملت المواد المنشورة على المواقع تصريحات مفادها أن من واجب المسلمين شن الجهاد المسلح ضد اليهود والصليبيين والمرتدين وأنصارهم في جميع البلدان الإسلامية، وأنَّه من واجب كل مسلم أن يقاتلهم ويقتلهم أينما كانوا، مدنيين كانوا أم عسكريين.

وفي منتديات الدردشة على الإنترنت، زُوِّد الأفراد الذين أبدوا استعدادهم للانضمام لصفوف المتمردين بوصف لدروب يمكنهم سلكها للسفر إلى العراق وتعليمات حول صنع الأسلحة والمتفجرات. وقد تم العثور في منزل كل من المدَّعى عليهم على مواد إيديولوجية متطرفة تبيِّن التزامهم بالأفكار التي يبررون بها أعمال القتل التي كانت المواقع الشبكية ومنتديات الدردشة تحرِّض عليها.

وقد قام الداعور بتنظيم عملية الحصول على بطاقات ائتمانية مسروقة، لأغراضه الشخصية وكذلك لإمداد مغال بالأموال اللازمة لتأسيس المواقع الشبكية وإدارتها. كما كان الداعور ضالعاً في حالات أخرى للاحتيال باستخدام بطاقات ائتمانية لم تُستخدم العائدات المتأتية منها في دعم المواقع الشبكية. وقد بلغت خسائر شركات البطاقات الائتمانية جرَّاء هذا الجانب من أنشطة المدَّعى عليهم الاحتيالية ١,٨ مليون جنيه إسترليني.

ومن بين الأدلة التي كانت متاحة قائمة خطَّها التسولي بيده وعُثر عليها في مكتبه، وكان قد كتب فيها تفاصيل عدد من المواقع الشبكية ومن بطاقات الائتمان المسروقة، الأمر الذي كشف عن وجود ٣٢ من المواقع الشبكية المتاحة من عدد من شركات الاستضافة الشبكية المختلفة، والتي كان تسولي قد أسسها أو شرع في تأسيسها، ومعظمها في الأسبوع الأخير من حزيران/يونيه ٢٠٠٥ وإن كان بعضها قد استمر حتى تموز/يوليه وآب/أغسطس. وكان مصدر التمويل لإنشاء هذه المواقع الشبكية وإدارتها هو الاستخدام الاحتيالي لبيانات بطاقات الائتمان التي سرقت من حسابات حامليها، إما بالسرقة المباشرة لسجلات حاسوبية، أو بالاختراق الحاسوبي، أو عن طريق تسريب احتيالي داخل مؤسسات مالية. وكان المدَّعى عليهما الآخران قد حوّلا بيانات البطاقات الائتمانية المشار إليها إلى التسولي.

واستُخدمت المواقع الشبكية التي أنشأها التسولي وسيلةً لتحميل مواد جهادية تحرِّض على أعمال عنف خارج المملكة المتحدة في العراق. وكان دخول هذه المواقع مقصوراً على من أصدرت لهم أسماء مستخدمين وكلمات سر. وقد خلص قاضي المحاكمة إلى أنَّ المقصود من ذلك كان جعل المعرفة بما كان يُنشر على المواقع أصعب على الشركات المستضيفة للمواقع الشبكية وجهات إنفاذ القانون.

وفي ٥ تموز/يوليه ٢٠٠٧، حُكم على التسولي بالسجن ١٠ أعوام و٣ سنوات ونصف (في نفس الوقت) في تهمتين، وعلى مغال بالسجن ٧ سنوات ونصف و٣ سنوات ونصف (في نفس الوقت) في تهمتين، وعلى الداعور بالسجن ٦ سنوات ونصف و٣ سنوات ونصف (في نفس الوقت).

١١٥- وينص الجزء الأول من قانون الإرهاب لسنة ٢٠٠٦ على عدد من الجرائم الجديدة بهدف تعزيز قدرة السلطات على اتخاذ إجراءات في القضايا التي يصرح فيها أشخاص بأقوال تحرِّض على أعمال إرهابية أو تمجِّدها أو يُقصد بها تيسير ارتكاب هذه الأعمال على نحو آخر.

١١٦- ويجـرِّم الجزء الأول مـن القانون قيام شخص بنشر أقـوال يُقصد بها التشجيع المباشـر أو غير المباشر لأفـراد الجمهـور على أن يقومـوا بالتحضير لأعمال إرهابيـة أو التحريض على هذه الأعمـال أو ارتكابها، بما في ذلـك (على سبيـل المثال لا الحصر) التشجيع الـذي "يمجِّد" الأعمال الإرهابية، كما يجـرِّم ارتكاب الفعل نفسه عـن استهتار بما قد يترتب عليـه من نتائج. وفي الممارسة العملية، يتحدد المعنـى المفهوم من الأقوال على الأرجح بالرجوع إلى المحتوى ككل وإلى السياق الذي نُشرت فيه هذه الأقوال.

١١٧- وتجرِّم المادة الثانية من القانون نشر منشورات إرهابية (عمداً أو استهتاراً). وتُعرَّف المنشورات الإرهابية بأنَّهـا منشـورات يُرجَّح أن تشجِّـع الأعمال الإرهابية أو يُرجَّـح أن تكون مفيدة لشخص يخطـط لهذه الأعمال أو يرتكبهـا. وتشمـل الفئـة الثانية النـوع ذاته من المستنـدات أو المنشورات الـذي تنطبق عليه المـادة ٥٨ من قانون الإرهـاب لسنة ٢٠٠٠. وكما هو الحال بالنسبة للمادة ١ مـن قانون الإرهاب لسنة ٢٠٠٦، فإن الإجابة عن السؤال حـول ما إذا كانت المـواد المعنية تندرج ضمن تعريف "المنشورات الإرهابية" تتـم بالرجوع إلى محتواها ككل وإلى السياق الذي أُتيحت فيه.[٩٢]

١١٨- وفي المملكـة المتحدة، يمارس أعضاء النيابة العامة، عنـد اتخاذ قرارات بشأن بدء الملاحقة القضائية في قضية تحريض من عدمه، سلطة تقديرية واسعة، آخذين في اعتبارهم الحق في حرية التعبير والسياق العام الذي صـدرت فيه الأقـوال أو المنشورات أو نشرت، بما في ذلك المعنى المفهوم منها على الأرجح، سواء من قبل الجمهور العام أو الجمهور المستهدف.

١١٩- وفي الولايـات المتحـدة، يُتبع نهـجٌ قانوني مختلف إزاء تجـريم أعمال التحريض علـى الإرهاب والملاحقة القضائيـة بشأنهـا بسبب الضمانات الدستورية التي تحمي الحق في حرية التعبير بموجب التعديل الأول للدستور. فوفـق المبادئ المبيَّنـة في قضية براندنبورج ضد أوهايـو (395 US. 444) (١٩٦٩) التاريخية، يتعين على النيابة العامة، حتى يتسنى لها النجاح في ملاحقة شخص قضائياً لتحريضه على أعمال إجرامية (بما في ذلك الإرهاب)، أن تثبت قصد التحريض على عمل غير قانوني أو ارتكابه وكذلك احتمال أن يؤدي القول فعليا إلى التحريض على عمل غير قانوني وشيك.[٩٣]

١٢٠- وتعتمـد السلطـات في الولايـات المتحـدة، في الملاحقة القضائية بشـأن الأقوال التي تحرِّض على أعمال إرهابيـة، علـى الجرائم غير المكتملة مثـل التحريض والتآمـر، إلى جانب أحكام "الدعم الجوهـري" في القانون الجنائـي الأمريكي، التي تسمح في بعض الأحيان بالملاحقة القضائيـة بشأن السلوكيات التي تدعم أعمال العنف الإرهابية.[٩٤]

١٢١- ويُحظـر علـى الأشخاص بموجـب أحكام الدعـم الجوهـري في البنديـن ٢٣٣٩-ألـف و٢٣٣٩-باء من الفصـل الثامـن عشر من القانون الجنائي الأمريكي أن يوفروا دعماً جوهريـا أو موارد جوهرية لتنظيم إرهابي، أو أن يشرعـوا في توفيرهمـا، أو يتآمـروا لذلك، عـن علم أو عن عمد. وقـد وسَّع "قانون توحيـد أمريكا وتقويتها

(٩٢) Hemming, "The practical application of counter-terrorism legislation in England and Wales", p. 963.

(٩٣) Elizabeth M. Renieris, "Combating incitement to terrorism on the Internet: comparative approaches in the United States and the United Kingdom and the need for an international solution", *Vanderbilt Journal of Entertainment and Technology Law,* vol. 11, No. 3 (2009), pp. 681-682.

(٩٤) القانون الجنائي للولايات المتحدة، الفصل الثامن عشر، البندان ٢٣٣٩-ألف و٢٣٣٩-باء.

بإتاحة الأدوات المناسبة اللازمة لاعتراض أعمال الإرهاب وعرقلتها"، الصادر سنة ٢٠٠١، تعريفَ الدعم الجوهري ليشمل "أي ممتلكات، مادية أو غير مادية، أو خدمات، بما يشمل ... التدريب، أو المشورة أو المساعدة المتخصصة ... أو معدَّات الاتصال".[٩٥]

١٢٢- ويمكن، بناء على جريمتي التحريض أو التآمر المنصوص عليهما في البند ٣٧٣ *(أ)* من الفصل الثامن عشر في القانون الجنائي الأمريكي، توجيه تهمة التحريض إلى أي شخص إذا "حرَّض شخصاً آخر، أو أمره، أو حثه، أو سعى لإقناعه بغير ذلك من الوسائل، لكي يرتكب سلوكا إجراميا بقصد أن يرتكب الشخص الآخر هذا السلوك الإجرامي".

١٢٣- وقد استُخدم هذا النهج بنجاح في العديد من القضايا في الولايات المتحدة، للملاحقة القضائية للإرهابيين بشأن أقوال أو أفعال صدرت عنهم عبر الإنترنت. ومن بين هذه القضايا قضية *الولايات المتحدة الأمريكية ضد إيمرسون وينفيلد بيغولي*.

قضية الولايات المتحدة الأمريكية ضد إيمرسون وينفيلد بيغولي

اتُّهم طالبٌ في الثانية والعشرين من عمره (من مواطني الولايات المتحدة)، يدعى إيمرسون وينفيلد بيغولي، بالضلوع في نشر معلومات على شبكة الإنترنت تتعلق بصُنع قنابل والتحريض على ارتكاب أعمال عنف على التراب الأمريكي. ومن التهم الأخرى الموجّهة إليه الاعتداءُ على موظفين في مكتب التحقيقات الاتحادي وتهديدهم بسلاح ناري محشو.

وقد كان لبيغولي، المعروف رسمياً بالاسم المستعار "أسد الله الشيشاني"، دورٌ نشط في المنتدى الجهادي المعروف دولياً والمسمى "شبكة أنصار المجاهدين، منتدى الإنكليزية"، الذي شارك فيما بعد في إدارته بنشاط. وقد هيَّأ المنتدى الفرصة لبيغولي للتعبير عن انجذابه لوجهات نظر متطرفة مع القيام في الوقت نفسه بتشجيع غيره من المنتمين إلى عقيدته على ارتكاب أعمال إرهابية داخل الولايات المتحدة. وقد اشتملت مواده الدعائية أيضاً على نشر أشرطة فيديو تحتوي على تعليمات حول صُنع متفجرات للقيام بأعمال إرهابية. وتضمّنت الأماكن المستهدفة معابد يهودية، ومرافق عسكرية، وخطوط قطارات، ومراكز شرطة، وجسورا، وأبراجا للهاتف المحمول، ومحطات لمعالجة المياه.

وخلال فترة تسعة أشهر، نشر بيغولي عدة رسائل مطوَّلة ناقش فيها باستفاضة الحاجة إلى العنف. ومن بين الأدلة الهامة التي اشتمل عليها قرار توجيه الاتهام إلى بيغولي، الصادر في ١٤ تموز/يوليه ٢٠١١ من المحكمة المحلية الأمريكية للدائرة الشرقية بولاية فرجينيا، جزءٌ من المواد الدعائية التي نشرها بيغولي في أحد المنتديات على شبكة الإنترنت، كان نصه كالتالي:

> لا طائل من وراء الاحتجاجات السلمية. الكفار[أ] يرون أنَّ الحرب هي الحل لمشاكلهم، لذا فلا بد من أن نعتبر الحرب حلا لمشاكلنا أيضا. لا سلام، وإنما هو الرصاص، والقنابل، والعمليات الاستشهادية.

كما نشر بيغولي روابط بمستند على الإنترنت بعنوان "The explosives course" (تعليمات حول صنع المتفجرات)، وأتاحه للتنزيل من على الشبكة. ويحتوي المستند الذي يقع في ١٠١ صفحة، وهو من تأليف "الشهيد الشيخ الأستاذ أبو خباب المصري" (كما أشار إليه بيغولي)، على تعليمات تفصيلية حول إنشاء مختبر بمكونات كيميائية بسيطة لصُنع متفجرات. وأضيفت ملاحظة بأنَّه ينبغي لمن يودون تنزيل المحتوى أن يستخدموا برمجيات لإخفاء هويتهم حرصاً على سلامتهم.

[٩٥] Renieris, "Combating incitement to terrorism on the Internet", pp. 682-683.

وخلال هذا الوقت، كان بيغولي تحت مراقبة مستمرة من السلطات الاتحادية. وقام أحد موظفي مكتب التحقيقات الاتحادي بتنزيل المستند من أحد الروابط المحمَّلة، وهو ما أدى في نهاية المطاف إلى إلقاء القبض على بيغولي. وفي ١٤ نيسان/أبريل ٢٠١١، وُجِّهت إليه تُهَم القيام، عن عمد وبما يخالف القانون، بنشر معلومات على شبكة الإنترنت تتعلق بصُنع مواد متفجرة وتوزيعها، واستخدام أسلحة الدمار الشامل، والتحريض على القيام بتفجيرات في أماكن عامة، ومبانٍ حكومية، ووسائل مواصلات عامة. وفي ٩ آب/أغسطس ٢٠١١، أقرَّ بيغولي بذنبه بخصوص ي تهمة التحريضً على ارتكاب أعمال إرهابية، وهو الآن في انتظار صدور حكم عليه.

[أ] استفاض بيغولي في استخدام تعبير "الكفار" في مناقشاته على المنتديات الشبكية.

(ج) *استعراض للنهج القانوني المتبع تجاه التحريض*

١٢٤- في أوروبا، تُلزم كل من المادة ٣ من قرار مجلس الاتحاد الأوروبي الإطاري (2008/919/JHA) الصادر في ٢٨ تشرين الثاني/نوفمبر ٢٠٠٨ بتعديل القرار الإطاري (2002/475/JHA) بشأن مكافحة الإرهاب والمادة ٥ من اتفاقية مجلس أوروبا المتعلقة بمنع الإرهاب، الدولَ الأعضاء في الصك المعني بتجريم الأفعال أو الأقوال التي تشكِّل تحريضاً على ارتكاب أعمال إرهابية. وتُلزم اتفاقية مجلس أوروبا المتعلقة بمنع الإرهاب الدول الأعضاء بتجريم "التحريض العلني على ارتكاب عمل إرهابي"، إلى جانب كل من التجنيد والتدريب لأغراض إرهابية.

١٢٥- ويُلزم تنفيذ الاتفاقية، التي تستند جزئياً إلى المادة ٣ من البروتوكول الإضافي لاتفاقية الجريمة الإلكترونية بشأن تجريم الأفعال ذات الطبيعة العنصرية وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر، الدولَ بتحقيق توازن معقول بين متطلبات إنفاذ القانون وحماية حقوق الإنسان وحرياته. ومن ثم فقد أثارت مخاوف ومناقشات جدية. ومع ذلك، فإنَّ تطبيق المادة ٥ (مثله مثل تطبيق المادتين ٦ و٧ بشأن التجنيد والتدريب لأغراض إرهابية) لا بد وأن يسير جنباً إلى جنبٍ مع الحكم الرئيسي في المادة ١٢، الذي ينص على أن تنفيذ هذا التجريم لا بد وأن يكون بطريقة تحترم حقوق الإنسان، ولا سيما الحقوق في حرية التعبير وحرية تكوين الجمعيات وحرية المعتقد، كما هي مبينة في الصكوك المعنية بحقوق الإنسان، بما في ذلك الفقرة الأولى من المادة ١٠ من الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية.

١٢٦- وقد تناولت المحكمة الأوروبية لحقوق الإنسان بالفعل المادة ٥ من اتفاقية مجلس أوروبا المتعلقة بمنع الإرهاب، في تقييمها للضمانات التي تكفلها الفقرة الأولى من المادة ١٠ من الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية. ففي قضية شهيرة، هي قضية *لوروا ضد فرنسا*،[٩٦] لم تر محكمةٌ فرنسية أن هناك انتهاكاً للمادة ١٠ في قضية صحفي كان قد أُدين وغُرِّم لنشره رسماً كاريكاتورياً في صحيفة أسبوعية تصدر باللغة الباسكيَّة. ففي ١١ أيلول/سبتمبر ٢٠٠١، قدَّم الرسَّام إلى طاقم تحرير المجلة رسماً للهجوم على برجي مركز

[٩٦] حكم صادر في ٢ تشرين الأول/أكتوبر ٢٠٠٨ عن المحكمة الأوروبية لحقوق الإنسان (القسم الخامس)، قضية *لوروا ضد فرنسا*، الدعوى رقم ٠٣/٣٦١٠٩.

التجـارة العالمي، مذيـلا إياه بتعليق يحاكي بسخرية شعاراً إعلانياً لعلامة تجاريـة شهيرة: "كلُّنا راوده الحلم ... وفعلتها حماس" (إحالة إلى "فعلتها سوني"). ونُشر الرسم بعد ذلك في المجلة في ١٣ أيلول/سبتمبر ٢٠٠١.

١٢٧- وأشـارت المحكمة الأوروبية لحقوق الإنسان فيما أشـارت إليه في حيثيات حكمها، إلى المادة ٥ من اتفاقية مجلس أوروبـا المتعلقـة بمنع الإرهاب، وهي المـرة الأولى التي تأخـذ فيها المحكمة تلك الاتفاقيـة في اعتبارها في حكـم مـن أحكامهـا. ورأت المحكمة أن الرسم ذهـب إلى أبعد من مجرد انتقاد الولايات المتحـدة، بدعمه للدمار العنيـف الذي خلفته الهجمات وتمجيـده له. وأشارت المحكمة إلى التعليق الذي صاحـب الرسم، والذي يدل على دعـم المدعـي المعنوي للجناة المشتبـه في ارتكابهم لهجمـات ١١ أيلول/سبتمبر ٢٠٠١. ومن بـين العوامل الأخرى التـي أخذتها المحكمة بعين الاعتبار اختيارُ المدعي للصيغة اللغوية المستعملة، وتاريخ نشر الرسوم (الذي اعتبرت المحكمة أنه يزيد من مسؤولية الرسام)، والمنطقة الحساسة سياسياً التي نُشرت فيها الرسوم (منطقة الباسك). ورأت المحكمـة أن الرسـوم استثارت في الجمهور رد فعل معيَّن يُمكـن أن يثير العنف ويؤدي إلى تأثير غير مستبعد علـى النظام العام في المنطقة. ويمكن تطبيق المبادئ التي أرستها هذه القضية التاريخية بالمثل على القضايا التي يزعم فيها وقوع تحريض على الإرهاب عن طريق الإنترنت.

١٢٨- وقـد أُجريـت في أوروبا ملاحقات قضائية ناجحة بشأن أعمال التحريض. ففي ألمانيا مثلا، صدر حكم في عام ٢٠٠٨ بالإدانة بسبب التحريض في حق إبراهيم رشيد، وهو مهاجر كردي عراقي، بعدما وُجهت له تهمة شن "جهـاد افتراضي" على شبكة الإنترنـت. وادَّعى أعضاء النيابة العامة أنَّ رشيد كان يحاول، بنشره دعاية لتنظيم القاعدة في منتديات للدردشة على الإنترنت، تجنيد أفراد للانضمام إلى القاعدة والمشاركة في الجهاد.

١٢٩- وتحتـوي خلاصة قضايا الإرهاب[٩٧] الصادرة عـن مكتب الأمم المتحدة *المعني بالمخدِّرات والجريمة* على تلخيص مفيد للنُّهُج المتَّبعة في تجريم أعمال التحريض في إسبانيا الجزائر ومصر واليابان. ففي الجزائر، تنص المادة ٨٧ مكرر ١ من قانون العقوبات على معاقبة أعمال العنف الإرهابية بالإعدام، أو السجن المؤبد، أو غيره من عقوبات السجن لفترات طويلة. وتنص المادة ٨٧ مكرر ٤ على معاقبة كل من يشيد بالأعمال الإرهابية المذكورة أو يشجعها أو يمولها بالسجن من ٥ إلى ١٠ سنوات، وكذلك بالغرامة.[٩٨]

١٣٠- وفي مصـر، تجـرِّم المادة ٨٦ مكررا من قانـون العقوبات الأعمال التي تعتبر في حكـم المسؤولية التنفيذية أو مسؤوليـة الدعـم، والتخطيـط والإعداد لأعمـال إرهابية، والعضويـة في تنظيم غير قانـوني أو دعمه، وإمداد التنظيمـات الإرهابية بمعونات مادية أو مالية، كما تجرم التحريض. وعلاوة على ذلك، تنص المادة على عقوبات مشـددة علـى الترويـج (بأية طريقة كانت) لأغراض التنظيمات الإرهابيـة، وعلى حيازة أو إحـراز محررات أو مطبوعات أو تسجيلات (بالذات أو بالواسطة)، أيا كان نوعها، تتضمن ترويجاً أو تحبيذاً للأغراض المذكورة مع العلم بها.[٩٩]

[٩٧] مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة، *خلاصة قضايا الإرهاب* (٢٠١٠).

[٩٨] المرجع نفسه، الفقرة ١٠٠.

[٩٩] المرجع نفسه، الفقرة ١١١.

١٣١- وفي اليابان يُعاقب أي شخص حرَّض على جريمة، مباشرةً أو من خلال وسيط، كما لو كان المحرِّضُ أحد منفِّذي الجريمة الفعليين (المادة ٦١ من قانون العقوبات).[١٠٠] وثمة أحكام قانونية أخرى في اليابان، كالمواد من ٣٨ إلى ٤٠ من قانون منع الأنشطة التخريبية، تجرِّم التحريض على العصيان المسلح أو على إشعال الحرائق، بقصد الترويج لأي مذهب سياسي أو سياسة، أو تأييد هذا المذهب أو السياسة أو معارضتهما.

١٣٢- وفي إسبانيا، تعتبر المادتان ١٨ و٥٧٩ من قانون العقوبات الإسباني التحريضَ العلني على ارتكاب جريمة إرهابية بمثابة عمل تحضيري لجريمة التحريض. وتعاقب المادة ٥٧٨ على جريمة الإشادة بالإرهاب، وهي جريمة أُدرجت في قانون العقوبات بالقانون الأساسي ٧/٢٠٠٠ الصادر في ٢٢ كانون الأول/ديسمبر ٢٠٠٠. وتنص هذه المادة، حسب ترجمة غير رسمية، على أنَّ "الإشادة أو اختلاق الأعذار، بأية وسيلة من وسائل التعبير العلني أو النشر، فيما يخص الجرائم الواردة في المواد من ٥٧١ إلى ٥٧٧ من هذا القانون (جرائم الإرهاب)، أو الإشادة أو اختلاق الأعذار بخصوص أي شخص شارك في تنفيذها، أو ارتكاب أعمال فيها تشويه لسمعة ضحايا جريمة إرهابية أو احتقارهم أو إهانتهم، هم أو عائلاتهم، يُعاقَب عليها بالسجن لمدة تتراوح بين سنة واحدة وسنتين." كذلك نصَّ القانون الأساسي على عقوبة فقدان الأهلية المدنية لمدة معينة في حالة الإدانة.[١٠١]

١٣٣- وفي إندونيسيا، لا يوجد قانون يتناول خصيصاً الأنشطة التي يقوم بها الإرهابيون عن طريق الإنترنت، بما في ذلك التحريض على ارتكاب أعمال إرهابية. فالمادة ١٤ من القانون رقم ١٥/٢٠٠٣ بشأن القضاء على أعمال الإرهاب تتناول التحريض على القيام بأعمال إرهابية دون إشارة إلى أسلوب الاتصال الذي يستخدمه الجاني، وكذلك قانون العقوبات الإندونيسي، الذي يتناول موضوع التحريض على ارتكاب سائر الأعمال الإجرامية. وقد قامت السلطات الإندونيسية بملاحقات قضائية ناجحة لأشخاص قاموا بأنشطة تتعلق بالإرهاب على شبكة الإنترنت. ففي عام ٢٠٠٧، حُكم على أغونغ برابوو، الذي كان يبلغ من العمر ٢٤ عاماً والمعروف أيضاً باسم ماكس فيدرمان، بالسجن ثلاث سنوات (تبعاً للمادة ١٣ *(ج)* من اللائحة الحكومية التي حلت محل القانون رقم ١/٢٠٠٢ والقانون رقم ١٥/٢٠٠٣ بشأن القضاء على أعمال الإرهاب) لتسجيل الموقع الشبكي www.anshar.net واستضافته، بناءً على طلب من نور الدين م. توب، زعيم تنظيم الجماعة الإسلامية الإرهابي، من خلال وسيط اسمه عبد العزيز. وتفيد التقارير أنَّ عبد العزيز قد صمَّم موقع www.anshar.net في منتصف عام ٢٠٠٥ بناءً على طلب توب، وبهدف نشر الدعاية الجهادية. ولئن كان الموقع الشبكي يحتوي على معلومات عامة عن الإسلام والجهاد، فقد كان يحتوي أيضاً على "نصائح وتعليمات" محدَّدة عن كيفية القيام بهجمات إرهابية والأماكن التي يُمكن فيها ذلك، مع اقتراح طرق مؤدية إلى مراكز للتسوق ومكاتب وأماكن حصول الاختناقات المرورية ومواقع محدَّدة بالاسم يتوافد إليها أفراد الجمهور.[١٠٢] وفي قضية أخرى، حُكم على محمد جبريل عبد الرحمن، المعروف أيضاً باسم محمد ريكي أردان ("أمير الجهاد")، بالسجن لخمس سنوات لتواطئه في عمل إرهابي.

١٣٤- وفي سنغافورة، في سياق شبكة الإنترنت، تحظر المادة ٤-٢ *(ز)* من قواعد استخدام الإنترنت المواد التي "تمجِّد الكراهية أو الفتنة أو التعصب بدوافع عرقية أو إثنية أو دينية، أو تحرِّض على أي من ذلك أو تحبذه".

[١٠٠] المرجع نفسه، الفقرة ١٠٠.

[١٠١] المرجع نفسه، الفقرة ١١٥.

[١٠٢] انظر: www.indonesiamatters.com/624/wwansharnet-chatroom-jihad.

٢- *الاعتبارات المتعلقة بسيادة القانون في شأن تجريم التحريض*

١٣٥- نصّ قرار مجلس الأمن رقم ١٦٢٤ (٢٠٠٥) صراحة، عند دعوته الدول إلى أن تجرِّم التحريض على الأعمال الإرهابية، على وجوب أن تحرص الدول لدى اتخاذ أي تدبير من التدابير لتنفيذ التزاماتها على كفالة الامتثال لجميع التزاماتها بموجب القانون الدولي، ولا سيما القانون الدولي لحقوق الإنسان، وقانون اللاجئين، والقانون الإنساني.

١٣٦- وقد جرى التأكيد على هذا المبدأ، الذي يتجسد أيضا في الصكوك العالمية لمكافحة الإرهاب، لمرات عديدة على المستوى الدولي (في أطر من ضمنها الأمم المتحدة)، وهو عنصر أساسي من عناصر نهج "سيادة القانون" الذي يتَّبعه مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة إزاء تعزيز التدابير المتخذة للتصدِّي للإرهاب في مجال العدالة الجنائية بموجب النظام القانوني العالمي لمكافحة الإرهاب، كما أنَّه مدعوم بالعديد من صكوك مكافحة الإرهاب وصكوك حقوق الإنسان الإقليمية، ومن أبرزها الصكوك التي وضعها مجلس أوروبا، والتي أشير لها فيما سبق (انظر الباب ثانياً-دال أعلاه).[١٠٣]

١٣٧- ولا يسمح نطاق هذا المنشور بتحليل تام، في سياق احترام حقوق الإنسان المكفولة في حرية التعبير، لكل التعقيبات والمراجع القضائية المتاحة في شأن النطاق والتطبيق الصحيحين للأحكام المشترعة من قبل البلدان لتجريم التحريض على الأعمال الإرهابية.

١٣٨- ومع ذلك، فالواضح، رغم أنَّ ما هو متاح من فقه قانوني بشأن النطاق الدقيق للصكوك الدولية لحقوق الإنسان، مثل الفقرة ١ من المادة ١٠ من الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية والمادة ١٩ من العهد الدولي الخاص بالحقوق المدنية والسياسية يفسح المجال أمام استمرار النقاش، أنَّ تحقيق التوازن الصحيح، في الممارسة العملية، بين الحفاظ على الحق في حرية التعبير وإنفاذ التشريعات الجنائية التي تستهدف التحريض على أعمال إرهابية لم يزل تحدياً يواجه الحكومات.

٣- *صلاحيات إنفاذ القانون*

١٣٩- كثيراً ما تستوجب التحقيقات في قضايا الإرهاب التي يستخدم فيها إرهابيون مشتبه بهم الإنترنت أو غيرها من الخدمات ذات الصلة القيام بعمليات تفتيش أو مراقبة أو رصد تدخلية أو قسرية من قبل أجهزة الاستخبارات أو جهات إنفاذ القانون. ومن ثم فمن المهم، حتى تكون الملاحقة القضائية ناجحة، أن يؤذَن بتقنيات التحقيق المذكورة حسب الأصول بموجب القوانين الوطنية، وأن تحترم التشريعات ذات الصلة حقوق الإنسان الأساسية المحمية بموجب القانون الدولي لحقوق الإنسان.

[١٠٣] انظر تقارير المقرّر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، المقدَّمة إلى مجلس حقوق الإنسان والجمعية العامة، والتي عبر فيها المقرر الخاص عن قلقه تجاه ما قد يترتب على التشريعات التي تستهدف التحريض من تأثير على حرية التعبير بالتشجيع على تجريم أقوال لا تبلغ حد التحريض على الإرهاب. وقد سُلِّط الضوء على هذه المخاوف ووجهات النظر في مذكرة مكتوبة قُدِّمت إلى اجتماع فريق الخبراء الذي عقدته مفوضية الأمم المتحدة لحقوق الإنسان. وانظر أيضاً الإعلان المشترك بشأن حرية التعبير وشبكة الإنترنت، الصادر في ١ حزيران/يونيه ٢٠١١ عن المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، وممثل منظمة الأمن والتعاون في أوروبا المعني بحرية الإعلام، والمقرّرة الخاصة لمنظمة الدول الأمريكية المعنية بحرية التعبير، والمقرّرة الخاصة حول حرية التعبير والوصول إلى المعلومات التابعة للجنة الأفريقية لحقوق الإنسان وحقوق الشعوب، والذي أكدوا فيه مجددا على الأهمية الجوهرية للحق في حرية التعبير.

(أ) صلاحيات التفتيش والمراقبة والاعتراض

١٤٠- في إسرائيل، تندرج صلاحيات التحقيق فيما يخص جمع الأدلة الرقمية على الإنترنت، في كل من القضايا الجنائية العامة والقضايا المتعلقة بالإرهاب، في إطار قانون أجهزة الحاسوب لسنة ١٩٩٥، الذي يحدد بعض الصلاحيات لجمع الأدلة الرقمية. وقد عدل قانون أجهزة الحاسوب قانون التنصت على المحادثات، معتبراً الحصول على رسائل بين أجهزة حاسوب بمثابة تنصت، ومن ثم يتيح لسلطات التحقيق الحصول على إذن قضائي، أو إذن إداري في الحالات العاجلة والاستثنائية، بالحصول على البيانات المنقولة في رسائل بين أجهزة حاسوب.

١٤١- وفي عام ٢٠٠٧، سُنَّ قانون بيانات الاتصالات. وكان الغرض من هذا القانون هو التنظيم التدريجي للممارسات المعمول بها في الحصول على البيانات غير المتعلقة بالمحتوى من شركات الهاتف الثابت وشركات الهاتف المحمول، وكذلك من مقدِّمي خدمات الإنترنت. ولا ينطبق القانون على مقدِّمي خدمات الإنترنت الذين يقدِّمون خدمات أخرى، مثل تخزين المعلومات، ومشاطرة المعلومات، والبريد الإلكتروني، والخدمات الاجتماعية وما إلى ذلك. وفي الحالات التي تود فيها السلطات الحصول على معلومات من مقدِّمي خدمات الإنترنت، يطبَّق حاليا جزء سابق من القانون يمكِّنها على العموم من إصدار أمر بالحضور والحصول على معلومات من أي شخص لديه معلومات قد تفيد التحقيق.

١٤٢- وفي عام ٢٠١٠، روجت حكومة إسرائيل لمشروع قانون يهدف إلى تدوين صلاحيات التحقيق المتعلقة بكل من البيانات المادية والبيانات الرقمية. والغرض من المشروع تنظيم جمع البيانات الرقمية على مستوى عال، وهو يحتوي على ترتيب منظَّم للصلاحيات غير المنصوص عليها حاليا في التشريعات الإسرائيلية، مثل التفتيش السري لأجهزة الحاسوب (في حالة الجرائم البالغة الخطورة)، والحصول على معلومات معدة للتخزين (مستقبلا) على جهاز حاسوب بعينه، وطريقة الحصول على رسائل البريد الإلكتروني التي توجد في حوزة مقدِّم الخدمة، وتفتيش مواد حاسوبية بإذن إداري في ظروف معيَّنة. وسوف تنطبق هذه التدابير على قضايا الإرهاب التي تُستخدم فيها الإنترنت في حال إقرار هذا المشروع.

١٤٣- وفي عام ٢٠٠٦، أقرَّت حكومة فرنسا تشريعاً جديداً لمكافحة الإرهاب يسهل، في التحقيقات المتعلقة بالإرهاب، مراقبةَ الاتصالات وحصول الشرطة على بيانات الاتصالات من شركات خدمات الهاتف، ومقدِّمي خدمات الإنترنت، ومقاهي الإنترنت.

١٤٤- وينص القانون المتعلق بمكافحة الإرهاب وبأحكام متنوعة تخص الأمن ومراقبة الحدود (٢٠٠٦-٦٤ الصادر في ٢٣ كانون الثاني/يناير ٢٠٠٦) على أنه يجب على مقدِّمي خدمات الإنترنت، ومقاهي الإنترنت، ومقدِّمي خدمات الاستضافة، والمشغلين، أن يقدِّموا بيانات حركة المعلومات والأرقام المتصَل بها وعناوين بروتوكول الإنترنت، للجهات الحكومية المختصة في قضايا التحقيق في أنشطة من يشتبه في كونهم إرهابيين.

١٤٥- وينبغي لشركات الهاتف المحمول ومقاهي الإنترنت، أن تحتفظ بسجلات لاتصالات العملاء لمدة ١٢ شهراً وأن تتيح هذه السجلات للشرطة. كما أن القانون يصرِّح باستخدام كاميرات للمراقبة في الأماكن العامة

مثل محطات القطارات، والكنائس، والمساجد، والمتاجر، والمصانع، والمحطات النووية. وتسمح المادة ٨ للشرطة بمراقبة المركبات والركاب آلياً في الطرقات والطرق السريعة في فرنسا (بما في ذلك التقاط صور للوحات المعدنية للسيارات وللركاب) وبمراقبة الأشخاص في التجمعات العامة الكبيرة.[١٠٤]

١٤٦- وفي ١٤ آذار/مارس ٢٠١١، عُدِّل قانون الإجراءات الجنائية الفرنسي ليخول للسلطات صلاحيات إضافية في التحقيقات المتعلقة بالإرهاب. وتشمل هذه التعديلات الصلاحيات اللازمة لمصادرة مستندات ذات صلة بالتحقيق (بما في ذلك تحويل البيانات الحاسوبية ونقلها)، وفك شفرة البيانات الحاسوبية المحمية، والاختراق الرقمي، والاستيلاء على البيانات الحاسوبية (بما في ذلك الصور)، والتنصت، واعتراض أنواع أخرى من الاتصالات. وعلاوة على ذلك، فالقانون يضع الأساس القانوني لأنشطة مسؤولي إنفاذ القانون الذين يقومون، فيما يقومون به، بالمشاركة في مناقشات منتديات الدردشة على الإنترنت، في إطار التحقيق في جرائم تتعلق بالتحريض على الإرهاب. وهذا موضوع قانوني هام لعل الحكومات تود النظر فيه. وتخوِّل هذه المواد لسلطات إنفاذ القانون الفرنسية أموراً في جملتها صلاحيةُ الحصول على أدلة تتعلق ببيانات الاتصال الخاصة برسائل البريد الإلكتروني، والأنشطة الهاتفية، وعناوين بروتوكول الإنترنت.

١٤٧- وقد أشار الخبير الصيني إلى لوائح تنظيمية في بلاده يمكن للشرطة بموجبها، حين تضطلع بتحقيق جنائي بخصوص استخدام الإنترنت، أن تصدر أمراً لمقدِّم خدمات الإنترنت ولمقدِّم اتصال الإنترنت بتقديم السجلات والبيانات ذات الصلة، التي يلزمهم القانون بالاحتفاظ بها لمدة ٦٠ يوماً.

١٤٨- وفي المملكة المتحدة، يضع قانون تنظيم صلاحيات التحقيق لسنة ٢٠٠٠ إطاراً قانونياً ينظِّم خمسة أنواع من أنشطة المراقبة التي تضطلع بها الجهات الحكومية، وهي:

- اعتراض الاتصالات (مثل اعتراض المكالمات الهاتفية أو الاطلاع على محتويات رسائل البريد الإلكتروني)
- المراقبة التدخلية (مثل المراقبة السرّية في الأماكن أو المركبات الخاصة)
- المراقبة الموجَّهة (مثل المراقبة السرّية لهدف محدَّد في مكان عام)
- الاستعانة بأشخاص باعتبارهم مصادر سرّية للمعلومات الاستخبارية (مثل العملاء السريين)
- بيانات الاتصالات (مثل السجلات المتعلقة بالاتصالات لا بمحتواها).[١٠٥]

١٤٩- وبالإضافة إلى النص على أغراض هذه الأنشطة والإجراءات التي لا بد منها للحصول على تصريح باستخدامها، فإنَّ القانون يُلزم السلطات القائمة على المراقبة بالنظر فيما إذا كانت ممارسة هذه الصلاحيات والتدخل في حقوق الأفراد الخاضعين للمراقبة متناسبين، وأن تتخذ خطوات لتلافي ما يُعرف بـ"التدخل الجانبي"،

[١٠٤] www.edri.org/edrigram/number4.2/frenchlaw.

[١٠٥] "Summary of surveillance powers under the Regulation of Investigatory Powers Act", National Council for Civil Liberties.

حيث تتأثر حقوق أطراف غير الأطراف المستهدفة. كما أنَّ القانون يجرِّم امتناع الأطراف التي لديها مفاتيح تشفير الاتصالات المستهدفة عن تقديم هذه المفاتيح إلى السلطات المصرَّح لها بالحصول عليها.[١٠٦]

١٥٠- وفي عام ٢٠٠٠، أقرَّت حكومة الهند قانون تكنولوجيا المعلومات لسنة ٢٠٠٠، ثم عدَّلته في عام ٢٠٠٨، لينص على تجريم "الإرهاب السيبراني" (المادة ٦٦ واو) وغير ذلك من المسائل المتعلقة بالإنترنت. وتتناول المادة ٦٧-جيم (١) من القانون مسألة الاحتفاظ بالبيانات، فتنص على أن "يحتفظ" مقدمو الخدمات الخاضعون للتنظيم الرقابي "بالمعلومات التي تُحدِّدها تعليمات الحكومة المركزية، على أن تكون مدة الاحتفاظ وطريقته وشكله وفقاً للتعليمات ذاتها"، كما تجرِّم مخالفة هذا الالتزام مع العلم بوجوده (وتعاقب المخالفين بالسجن لمدة تصل إلى ثلاث سنوات والغرامة).

١٥١- وتمنح المادة ٦٩ (١) من القانون للسلطات الحكومية صلاحية إصدار أوامر بـ"اعتراض أي معلومات أحدثت على أي جهاز حاسوبي، أو نقلت عبره، أو استقبلت عليه، أو خزِّنت فيه، ومراقبة هذه المعلومات، وفك شفرتها"، كما تنص على الالتزامات القانونية والضمانات التي ينبغي كفالتها لهذه الإجراءات الحكومية، فيما تمنح المادة ٦٩-ألف (١) أجهزة الدولة صلاحية إصدار أوامر بحجب اطلاع عامة الجمهور على أية معلومات عبر أجهزة حاسوبية إذا رأت أن هذا الأمر ضروري أو مستصوب، أو يصب في مصلحة سيادة الدولة الهندية، أو سلامة أراضيها، أو أمنها وعلاقاتها الخارجية، أو لمنع التحريض على جرائم أخرى ذات صلة و"قابلة للملاحقة"، بما في ذلك الإرهاب. وأخيراً، تمنح المادة ٦٩-باء أجهزة معينة تابعة للدولة صلاحية المراقبة والجمع والتخزين فيما يخص بيانات حركة المعلومات أو المعلومات المحدثة أو المنقولة أو المستقبلة عن طريق جهاز حاسوبي.

١٥٢- وفي نيوزيلندا، يحدِّث قانون التفتيش والمراقبة لسنة ٢٠١٢ صلاحيات جهات إنفاذ القانون ويدعمها وينسقها، فيما يتعلق بتفتيش الاتصالات ومراقبتها واعتراضها، لمواكبة مستجدات التكنولوجيا. ويضع القانون تعريفاً جديداً لتعبير "تفتيش النظم الحاسوبية"، ويوسّع نطاقه ليشمل تفتيش أجهزة الحاسوب غير المتصلة داخلياً بشبكة ما، ولكن لها القدرة على الاتصال بهذه الشبكة عن بُعد.

١٥٣- ومن أجل تعزيز الضمانات القانونية، فإنَّ القانون ينص بوضوح على عدم السماح بتفتيش أجهزة الحاسوب عن بُعد إلا في حالتين اثنتين: حين يكون لجهاز الحاسوب المستخدم في التفتيش القدرة على الاتصال على نحو قانوني بالنظام الحاسوبي المراد تفتيشه ومن ثم يُعتبر جزءاً من هذا النظام؛ وحين لا يكون هناك مكان مادي يُمكن تفتيشه (مثلا في حالة حساب بريد إلكتروني على الإنترنت يدخل إليه مستخدمه من أماكن مختلفة، كمقاهي الإنترنت). وينص القانون أيضاً على أنَّه يجب على الشرطة، حين تضطلع بعملية تفتيش مصرَّح بها لمرافق بيانات على شبكة الإنترنت عن بُعد، أن ترسل إخطاراً إلكترونياً بالتفتيش إلى عنوان البريد الإلكتروني للمرفق الذي يجري تفتيشه.

(ب) المسائل المرتبطة بإتاحة إمكانية الاعتراض

١٥٤- حين الاضطلاع بالأنشطة الإلكترونية للرصد أو المراقبة أو الاعتراض، تطلب السلطات تعاون مقدمي خدمات الاتصالات العامة أو ما يتصل بها من خدمات. ولئن كان مقدمو الخدمات المنتمون إلى القطاع الخاص يبدون استعدادهم في كثير من الأحيان لمساعدة جهات إنفاذ القانون على أداء وظائفها القانونية،

[١٠٦] Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, 2007), p. 216.

فمن الواضح أنَّه ثمة حدود لما يمكنهم تخصيصه من وقت وموارد لهذا الغرض دون أي مقابل. ومن ثم فمن المستصوب أن تهيئ الحكومات أساساً قانونياً واضحاً للالتزامات المفروضة على الأطراف المنتمية إلى القطاع الخاص، بما في ذلك المواصفات التقنية المطلوبة لشبكاتها وكيفية تغطية التكاليف اللازمة لتوفير هذه الإمكانيات.

١٥٥- ففي إسرائيل، تنص المادة ١٣ من قانون الاتصالات لسنة ١٩٨٢ على أنَّه يجوز لرئيس الوزراء أن يصدر أمراً لمقدمي خدمات الإنترنت، داخل إسرائيل، بإدخال تعديلات تكنولوجية تبعاً لمتطلبات قوات الأمن (المعرّفة بأنها تشمل الشرطة، والأمن، وغير ذلك من الأجهزة الخاصة) لمكافحة الإرهاب. ولا ينطبق القانون إلا على مقدمي خدمات الإنترنت، الذين يحصلون على تصاريح عملهم من وزارة الاتصالات بموجب القانون الإسرائيلي. ولا ينطبق القانون على مقدمي خدمات تخزين البيانات أو مقدمي خدمات إدارة المحتويات العاملين داخل إسرائيل، حيث إنَّ هؤلاء المشغلين لا يحتاجون إلى تصريح من الوزارة.

١٥٦- وفي نيوزيلندا، يوضِّح قانون (إمكانية اعتراض) الاتصالات لسنة ٢٠٠٤ الالتزامات الواقعة على كاهل مشغلي الشبكات في مساعدة الجهات الحكومية المصرَّح لها على القيام بعمليات اعتراض أو في تقديم ما يصرَّح به من بيانات متعلقة بالمكالمات. ويُلزم القانون مشغلي الشبكات بضمان توافر إمكانية الاعتراض في كل شبكة اتصالات عامة أو خدمة اتصالات عامة يملكونها أو يتحكمون فيها أو يشغلونها. وتُعتبر هذه الإمكانية متوفرة في شبكة أو خدمة ما إذا كان بوسع الجهات الحكومية المصرَّح لها أن تعترض الاتصالات أو الخدمات بطريقة لا تكشف أو تعترض إلا الاتصالات المستهدَفة، وتوفر البيانات والمحتويات المرتبطة بالمكالمات (في شكل قابل للاستخدام)، وتتيح الاعتراض بفعالية وفي الوقت المناسب وبطريقة تكفل الحماية لخصوصية مستخدمي الاتصالات وتحول دون التطفل عليهم دون داع. كذلك فإنَّ القانون يُلزم مشغلي الشبكات بتوفير الوسائل لفك شفرة أي اتصال يجري على شبكاتهم إذا كان المحتوى مشفراً وكان مشغِّل الخدمة هو من وفَّر وسيلة التشفير.

١٥٧- وقد منح القانون مشغلي الشبكات المتضررين، إقرارا منه بما ينفقه بعضهم من وقت وموارد مالية امتثالاً لهذه المتطلبات، مهلةً تتراوح بين ١٨ شهراً وخمس سنوات (حسب حالة الشبكة المعنية) يتعين عليهم خلالها إتاحة هذه الإمكانية في شبكاتهم. وعلاوة على ذلك، فقد وافقت الحكومة على تغطية نفقات إتاحة إمكانية الاعتراض في الشبكات العاملة بالفعل في تاريخ بدء سريان القانون والتي لا تتيح إمكانية الاعتراض اللازمة.

١٥٨- وفي البرازيل ينظِّم القانون الاتحادي رقم ٩-٢٩٦ لسنة ١٩٩٦، إلى جانب المادة ٥ (ثاني عشر) من الدستور الاتحادي الصادر عام ١٩٨٨، التنصت الرسمي الذي تقوم به الجهات الرسمية المصرَّح لها. وفيما يسلِّم القانون بالحرمة المكفولة للاتصالات، فإنه ينص على استثناءات محدَّدة، رهناً بإذن قضائي، بغرض التحقيقات الجنائية أو الإجراءات العقابية. وينص القانون على الإجراءات الواجب اتباعها في قضايا التنصت التي تجري تحت إشراف قاض. فبعد تنفيذ التنصت، تُدوَّن نتائج التنصت وتُقدَّم إلى القاضي، مع ملخص لما اتُّخذ من إجراءات وفقاً للإذن الممنوح (المادة ٦).

١٥٩- وقد كان على شركات الاتصالات، حتى تتمكّن من الوفاء بالتزاماتها القانونية، أن تنشئ وحدات متخصصة وتدرب العاملين بهذه الوحدات وأن تستثمر في التكنولوجيا اللازمة. وفيما يخص تكاليف توفير إمكانية الاعتراض، يقع عبء إتاحة الموارد التقنية والبشرية اللازمة لدعم أنشطة الاعتراض المصرَّح بها على

كاهل شركات الاتصالات. والسبب في اتباع هذا النهج أن الدستور البرازيلي ينص على أن تمارس شركات الاتصالات عملها وفق امتياز تمنحه الحكومة، ويُعتبر تقديم خدمات الاتصالات خدمة عامة.

١٦٠- وفي إندونيسيا، أقرت الحكومة في أعقاب تفجيرات بالي في عام ٢٠٠٢، تشريعات لمكافحة الإرهاب تسمح لجهات إنفاذ القانون والأجهزة الأمنية باعتراض المعلومات المعرب عنها أو المرسَلة أو المستَقبلة أو المخزنة إلكترونياً أو بالاستعانة بجهاز مسح ضوئي، وفحص هذه المعلومات، في التحقيقات المتعلقة بالإرهاب. وفيما يخص مدة الاحتفاظ بملفات الإنترنت أو ملفات السجلات، فإنَّ هذا الأمر ينظِّمه القانون رقم ١١ لسنة ٢٠٠٨ بشأن المعلومات والمعاملات الإلكترونية، وبالأخص الفقرة الفرعية (أ) من الفقرة ١ من المادة ٦ من هذا القانون، التي تُلزم كل مشغِّل لنظام إلكتروني بأن يكون نظامه قادراً على أن يستنسخ بالكامل أي معلومات إلكترونية أو مستند إلكتروني طيلة مدة الاحتفاظ بالملفات المنصوص عليها في القانون.

١٦١- وفي الجزائر، اعتمدت الحكومة في عام ٢٠٠٦ قانوناً يسمح بالمراقبة بالأجهزة الصوتية والمرئية وباعتراض المراسلات، إذا جرى ذلك بتصريح من وكيل الجمهورية (المدعي العام) وتحت إشرافه المباشر. ويسمح القانون نفسه باستخدام تقنية التسرب (الاختراق) بغرض التحقيق في الجرائم المتعلقة بالإرهاب أو الجريمة المنظمة، كما يخوِّل للعميل القائم بعملية التسرب ارتكاب مخالفات بسيطة محدَّدة أثناء تلك العملية. ويحرص القانون على حماية هوية العميل، بيد أنَّ التسرب لا بد وأن ينفَّذ تحت إشراف وكيل الجمهورية أو قاضي التحقيق.[١٠٧]

١٦٢- وفي ماليزيا، يحتوي قانون الاتصالات والوسائط المتعددة لسنة ١٩٩٨ على العديد من الأحكام فيما يخص التنظيم الرقابي لشبكة الإنترنت وما يتعلق بها من تحقيقات جنائية. فعلى سبيل المثال، تنص المادة ٢٤٩ من القانون، التي تتناول مسألة إمكانية الاطلاع على بيانات حاسوبية أثناء التفتيش، على أن الاطلاع يشمل الحصول على "كلمات السر، ورموز التشفير أو فك الشفرة، والبرمجيات أو المعدات، وأي وسائل أخرى يتطلبها فهم بيانات محوسبة".

١٦٣- وبالإضافة إلى ذلك، فإنَّ الفصل الرابع من القانون، الخاص بالمسائل المتعلقة بالمصلحة الوطنية، يفرض التزاماً عاماً على مشغلي خدمات الإنترنت بأن يبذلوا "قصارى جهدهم" لضمان ألا تُستخدم المرافق الشبكية التي يقدِّمونها لارتكاب أي جريمة ينص عليها القانون الماليزي (المادة ٢٦٣)، وينص على أنَّه يجوز للوزير المسؤول أن يقرر، مع تحديد المتطلبات التقنية ذات الصلة، ما إذا كان ينبغي لمشغل مرخص له أو مجموعة من المشغلين المرخص لهم أن يوفِّروا إمكانية اعتراض الاتصالات حين يكون ذلك مصرَّحاً به (المادة ٢٦٥).

١٦٤- ويتناول الفصل الثاني من القانون مسألة المحتويات التي فيها تجريح، ويحظر على مقدمي خدمات تطبيقات المحتوى وعلى أي شخص يستخدم هذه الخدمات تقديم محتوى "فاحش، أو بذيء، أو كاذب، أو فيه تهديد أو تجريح، بقصد مضايقة أي شخص أو إيذائه أو تهديده أو التحرش به" (المادة ٢١١). ويُعتبر أنَّ من يخالف هذه الالتزامات قد ارتكب جريمة، وهو ما يعرِّضه لغرامة لا تزيد عن ٥٠ ٠٠٠ رينجيت (١٦ ٢٠٠ دولار أمريكي تقريباً) أو السجن لمدة لا تزيد عن سنة واحدة، أو للعقوبتين معاً، كما يعرِّضه لغرامة متكررة مقدارها ١ ٠٠٠ رينجيت (٣٢٥ دولاراً أمريكياً تقريباً) عن كل يوم أو جزء من يوم تستمر فيه المخالفة بعد حكم

[١٠٧] مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة، *خلاصة قضايا الإرهاب*، الفقرة ٢١٥.

الإدانــة. وتنص المادة ٢١٢ من القانــون على تعيين جهاز من القطاع المعني ليكون منتدى لوضع مدونة مهنية فيما يخص المحتوى.

١٦٥- وفي الولايــات المتحدة، يتعين على مشغلي خدمات الاتصــالات في الوقت الراهن، بموجب قانون المساعدة على إنفاذ القانون في مجال الاتصالات لسنة ١٩٩٤، أن يوفِّروا إمكانية الاعتراض لشبكات الهاتف والشبكات ذات النطاق الترددي العريض.

(ج) التنظيم الرقابي لمقاهي الإنترنت

١٦٦- ثمــة أدلــة على أنَّ الإرهابيــين قد استخدموا مقاهــي الإنترنت في بعض الحالات للقيــام بأعمال مرتبطة بالإرهاب؛ إلا أنَّه لا تتوفر بيانات حول النسبة التي يمثِّلها هذا النوع من الأنشطة مقارنة بحجم الأنشطة المشروعة التي تُمارس على الإنترنت عبر هذه المقاهي.

١٦٧- وتُعــدُّ مسألة المــدى الذي ينبغي على الحكومات أن تذهب إليه في التنظيــم الرقابي لمقاهي الإنترنت، من أجــل مكافحــة الإرهاب، من بين المسائــل المعقدة المرتبطة ارتباطا وثيقــا بقضايا حقوق الإنســان. فعلى المستوى الــدولي هنالــك تبايــن في النُّهُج المتبعة في هــذا الشأن. ففي بعض الــدول، بما في ذلــك الأردن وباكستان ومصر والهنــد، تطبِّــق الحكومات تدابير تشريعيــة أو تنظيمية مخصصة تُلزم مشغلي مقاهــي الإنترنت بالحصول على وثيقــة هويــة تحمل صورة فوتوغرافية من زبائنهــم، إضافة إلى عناوين إقامتهم، وبيانــات الاستخدام والاتصال الخاصة بهم، والاحتفاظ بكل ما سبق وتقديمه إلى جهات إنفاذ القانون عند الطلب.

١٦٨- ولئــن استطاعــت الحكومات أن تفرض التزامات علــى مشغلي مقاهي الإنترنت بغرض الحد من إساءة استخــدام هــذه المقاهــي من قبل الإرهابيين، فــإن الفائدة من وراء هــذه التدابير تبقى محــل نقاش، لا سيما في وجــود مرافق مثل خدمات الإنترنت الأخرى المتاحة لعامة الجمهــور (مثل أجهزة الحاسوب في المكتبات العامة أو الشبكات العامــة للاتصال اللاسلكي بالإنترنت (واي فاي)) تتيح فرصة مماثلة لاستخدام الإرهابيين للإنترنت دون الكشــف عــن هوياتهــم. ويلاحَظ أن حكومــة إيطاليا قــد فرضت، في عــام ٢٠٠٥، التزامــات تنظيمية على مشغلــي مقاهــي الإنترنت فيما يخص الوقوف على هوية الزبائن، إلا أن هذه القرارات التنظيمية أُلغيت في أواخر عــام ٢٠١٠، وهــو مــا يرجع جزئياً إلى مخــاوف بشأن ما قد يكون لهــذا الشكل من التنظيم مــن تأثير على تطور خدمات الإنترنت والإقبال عليها من قبل من يستخدمونها استخداماً مشروعاً.

(د) مراقبة المحتوى

١٦٩- وتُعــدُّ مسألــة المدى الذي ينبغي للحكومات أن تذهب إليه في تنظيــم محتويات الإنترنت المتعلقة بالإرهاب مثــار جــدل كبير. فالنُّهُــج المتَّبعة في هذا الصدد تتنوع تنوعــاً كبيراً، حيث تفرض بعض الــدول ضوابط تنظيمية صارمة على مقدمي خدمات الإنترنت وغيرها من الخدمات ذات الصلة، بما في ذلك استخدام التكنولوجيا لفرز بعض المحتويات أو حجب الوصول إليها في بعض الحالات، فيما تعتمد دول أخرى نهجاً تنظيمياً أقل صرامة، يعتمد فيه اعتمادا أكبر على التنظيم الرقابي الذاتي الذي يفرضه قطاع المعلومات على المنتمين إليه.

١٧٠- ولاحظت باربرا مانتل، في مقالها المعنون "الإرهاب والإنترنت: هل ينبغي إغلاق المواقع الشبكية التي تروِّج للإرهاب؟"،[١٠٨] أن "معظم الجهات المقدمة لخدمات الإنترنت، وشركات استضافة المواقع الشبكية، ومواقع تبادل

[١٠٨] Barbara Mantel, "Terrorism and the Internet: should web sites that promote terrorism be shut down?", *CQ Global Researcher*, vol. 3, No. 11 (November 2009).

الملفـات، ومواقـع التواصل الاجتماعي، لديها اتفاقات لشروط الخدمة تحظـر محتويات بعينها". فهي تذكر، على سبيـل المثال، أنَّ خدمة ياهوو لاستضافة المواقع الشبكية للشركات الصغيرة الحجم تحظر على وجه التخصيص قيـام المستخدمـين باستخدام الخدمة لتوفـير دعم جوهري أو مـوارد لأي منظمة أو مجموعـة منظمات أطلقت عليها حكومة الولايات المتحدة تسمية تنظيمات إرهابية أجنبية، وهو ما يعني وجود نوع من التنظيم الذاتي داخل قطاع المعلومات.

١٧١- وينبغي للحكومات، حين تقيِّم النهج الذي ستتبعه في هذا الميدان ومستوى تدخلها فيه، أن تأخذ في الاعتبار عدداً من العوامل، بما في ذلك المكان الذي يُستضاف فيه المحتوى، والضمانات الدستورية وغير الدستورية المتعلقة بالحـق في حرية التعبير، والمحتـوى نفسه، والآثار الاستراتيجيـة لرصد مواقع بعينهـا أو اختراقها أو حجبها من منظور الاستخبارات أو إنفاذ القانون.[١٠٩]

١٧٢- وفي المملكـة المتحدة، ثمـة أداة مبتكرة، متاحة للسلطات عند تناولها لقضايـا يحتمل فيها ارتكاب أعمال تحريضـ علـى شبكـة الإنترنت، واردة في المـادة ٣ من قانون الإرهاب لسنـة ٢٠٠٦، إذ تكفل هـذه المادة للشرطة صلاحية إصدار إشعار بـ "السحب" للأشخاص القائمين على تشغيل المواقع الشبكية أو غيرها من المحتويات على شبكة الإنترنت.

١٧٣- وتنطبـق المـادة ٣ من القانون علـى القضايا المتعلقة بجرائـم منصوص عليها في المـادة ١ أو المادة ٢ من القانـون، والتـي يجري فيها: "*(أ)* نَشرُ قـول في سياق تقديم خدمة مقدَّمة إلكترونيـاً أو استخدامها، أو على نحو مرتبط بهذا التقديم أو الاستخدام، أو التسبب في نشر هذا القول في سياق مماثل أو على نحو مماثل؛ أو *(ب)* القيام بسلـوك يقع تحـت طائلة الفقرة ٢ من المادة ٢ [توزيـع منشور إرهابي] في سياق تقديم خدمـة من هذا القبيل أو استخدامها، أو على نحو مرتبط بهذا التقديم أو الاستخدام".

١٧٤- وتنص الفقرة ٢ من المادة ٣ على أنَّه يجوز، في حالة تقصير الشخص الذي وُجِّه له إشعار بـ "السحب" عن إزالـة المحتـوى ذي الصلة بالإرهاب، وإذا وُجِّهت له جراء ذلك تهم بموجب المادة ١ أو المادة ٢ من قانون الإرهاب لسنة ٢٠٠٦، أن تقدَّم في المحاكمة قرينة غير قاطعة مفادها أنَّ المحتوى المعني كان يحظى بتأييده.

١٧٥- وبالرغـم مـن كون هذه الإشعارات بـ "السحـب" متاحة باعتبارها إجراء وقائيا، فـإنَّ هذه الصلاحية لم تُستخـدم بعد في الممارسة العملية. ففي معظم الحـالات، ولا سيما حين يكون المحتوى الذي فيه تجريح مُستضافاً علـى مواقـع شبكية يملكها طـرف ثالث، عادة ما يكون في هـذا المحتوى خرق للشروط والأحـكام الخاصة بمقدِّم الخدمـة، ومـن ثم تستطيع السلطـات أن تتفاوض بنجاح علـى إزالة المحتوى المعني. وفي واقـع الأمر، تقوم وحدة تلقـي الشـكاوى المعنية بمكافحـة الإرهاب على الإنترنت في المملكـة المتحدة بتنسيق التدابـير الوطنية لمعالجة ما يحيلـه إليهـا الجمهور، إلى جانب الحكومة ومختلف القطاعات، من شكاوى حول المحتويات والأعمال ذات الصلة بالإرهاب على شبكة الإنترنت، بوصفها هيئة مركزية لتقديم المشورة للشرطة.

[١٠٩] Catherine A. Theohary and John Rollins, "Terrorist use of the Internet: information operations in cyberspace", Congressional Research Service report (8 March 2011), p. 8.

٤- *التعاون الدولي*

١٧٦- تلتـزم الدول، بموجب العديد من الصكوك المعنيـة بالإرهاب والجريمة المنظمة العابرة للحدود الوطنية، منهـا الدولي والإقليمـي والمتعدد الأطراف والثنائي، بإرساء سياسات عامة وأطر تشريعية لتيسير التعاون الدولي الفعال في التحقيق في هذا النوع من القضايا وملاحقتها قضائياً.

١٧٧- وبالإضافـة إلى إقـرار سياسـات عامة وتشريعـات تُنشئ الجرائـم اللازمة للوفاء بمتطلبـات ازدواجية التجـريم، ينبغـي للـدول أن تسنَّ تشريعات شاملـة تكفل لسلطاتهـا الأساس القانوني اللازم للتعـاون الدولي مع نظيراتهـا الأجنبيـة في التحقيقـات المتعلقة بالإرهـاب العابر للحدود الوطنيـة. وفي القضايا التـي تُستخدم فيها الإنترنـت، يحتمـل أكثر ما يحتمـل أن يكون التعاون الدولي الفعال، بما في ذلك القـدرة على تبادل المعلومات، بما فيها البيانات المرتبطة بالإنترنت، بمثابة عامل رئيسي في نجاح أي ملاحقة قضائية جنائية.

١٧٨- ويعرض الفصل الخامس أدناه بمزيد من التفصيل للقضايا المتعلقة بالتعاون الدولي في قضايا الإرهاب.

رابعاً- التحقيقات وجمع المعلومات الاستخبارية

ألف- أدوات ارتكاب جرائم الإرهاب باستخدام الإنترنت

١٧٩- لقد أتاحت التطورات التكنولوجية العديد من الوسائل المتطورة التي قد يسيء بها الإرهابيون استغلال شبكة الإنترنت في أغراض غير مشروعة. وحتى تكون التحقيقات في أنشطة الإنترنت فعالة، ينبغي الاستناد فيها إلى مزيج من أساليب التحقيق التقليدية، ومعرفة الأدوات المتاحة أمام من يريد القيام بنشاط غير مشروع عن طريق الإنترنت، واستحداث ممارسات تستهدف الوقوف على هوية مرتكبي مثل هذه الأعمال، وإلقاء القبض عليهم، وملاحقتهم قضائياً.

١٨٠- وتُبيِّن إحدى القضايا من فرنسا كيف تستخدم، في آن واحد، مختلف أنواع تقنيات التحقيق، سواء التقليدي منها أو المتعلق خصيصاً بالأدلة الرقمية، لجمع الأدلة اللازمة للملاحقة القضائية الناجحة بشأن استخدام الإنترنت في أغراض إرهابية.

النائب العام ضد أرنو، وباداش، وغيهال، وآخرين

هناك عدد من المدَّعى عليهم في هذه القضية التي عرضت على المحاكم في فرنسا، وهم: راني أرنو، ونادر زاهر باداش، وأدريان لوسيانو غيهال، ويوسف العبار، الذين أدانتهم محكمة الجنح بباريس في ٢٦ كانون الثاني/يناير ٢٠١٢ وحكمت عليهم بالسجن لمدد تتراوح بين ١٨ شهراً و٦ سنوات لقيامهم بنشر مواد ذات صلة بالإرهاب، ضمن أمور أخرى.

وقد ألقي القبض على أرنو وباداش وغيهال في فرنسا في كانون الأول/ديسمبر ٢٠٠٨، بعد أن قام أرنو، مستخدماً اسم "عبد الله"، بنشر رسائل تدعو للجهاد ضد فرنسا على موقع دعائي (minbar-sos.com):

"لا تنسوا أنَّ فرنسا لا تزال تحارب إخواننا في أفغانستان وأنكم في دار حرب. سارعوا إلى الشهادة في أسرع وقت، قاطعوا اقتصادهم، بددوا ثرواتهم، ولا تدعموا اقتصادهم ولا تشاركوا في تمويل جيوشهم."

ونتيجة لهذا النشر، اعترضت السلطات حساب أرنو على شبكة الإنترنت، ووضعته تحت المراقبة الشخصية، وزرعت أجهزة للتنصت على خطه الهاتفي. وعقب إلقاء القبض على السيد أرنو، أجرى المحققون تحليلاً جنائياً لمحتويات أجهزة الحاسوب التي استخدمها، وخلصوا إلى أنَّه قد قام ببحوث حول مسائل تتعلق بارتكاب أعمال إرهابية، كالمواد التي يمكن استخدامها لصنع المتفجرات والمواد الحارقة، وتحديد الأهداف الممكنة، وتتبع أنشطة شركة تستخدم نترات الأمونيوم، على سبيل المثال. وقد كشفت التحريات عن أنَّ أرنو كان قد جنَّد غيهال وباداش، واشترك في اجتماعات ومناقشات للإعداد لهجوم، واتصل بأناس ضالعين في حركات جهادية طلباً للمساعدة في تنفيذ هذا الهجوم، وتلقَّى حوالات مالية لهذا الغرض. وتُعدُّ هذه الأعمال جرائم تبعاً للمواد ٤٢١-٢-١، و٤٢١-١، و٤٢١-٥، و٤٢٢-٣، و٤٢٢-٦، و٤٢٢-٧ من القانون الجنائي الفرنسي، والمواد ٢٠٣ و٧٠٦-١٦ وما بعدها من قانون الإجراءات الجنائية.

وقد خلصت المحكمة إلى أنَّ الخطة التي يُزعم اشتراك السيد أرنو فيها، بمعية المجرمين الآخرين، أي وضع متفجرات على شاحنة بحيث تنفجر عند وصولها للهدف، شكلت خطراً بالغاً على النظام العام. ومن ثم فقد حُكم عليه بالسجن ست سنوات في التهم المتعلقة بالانتماء إلى جماعة ترتكب أعمالا إجرامية بغرض التحضير لهجوم إرهابي، وحيازة عدة مستندات مزورة، والعبث بمستندات إدارية لإثبات حق أو هوية أو صفة أو الحصول على تصريح. وفي التهمة ذاتها، حُكم على السيد باداش بالسجن سنتين، مع إيقاف تنفيذ ستة أشهر منها، فيما حُكم على السيد غيهال بالسجن أربع سنوات، مع إيقاف تنفيذ سنة منها. أما السيد العبار، الذي كان يُحاكم لأعمال أخرى ذات صلة، فقد حُكم عليه بالحبس ١٨ شهراً.

١٨١- وتتطلب القضايا التي يستعان فيها بأدلة رقمية مهارات متخصصة في التحقيقات الجنائية حتى يتأتى التحقيق فيها والملاحقة القضائية بشأنها، فضلا عن الخبرات والمعارف اللازمة لتطبيق هذه المهارات في نظام افتراضي. ولئن كانت مقبولية الأدلة مسألة تتعلق بالقانون في نهاية المطاف، ومن ثم فهي من اختصاص النيابة العامة، فإنه ينبغي أن يكون المحققون على دراية بالمتطلبات القانونية والإجرائية اللازمة لكفالة المقبولية للأدلة في التحقيقات المحلية والدولية على حد سواء. وتعزز المعرفة العملية الصحيحة بالمتطلبات التي تفرضها قواعد الإثبات المنطبقة، ولا سيما الأدلة الرقمية، من فرص جمع المحققين لما يكفي من الأدلة المقبولة للنجاح في ملاحقة قضية من القضايا. وعلى سبيل المثال، يجب أن تضمن الإجراءات المستخدمة في جمع الأدلة الرقمية وحفظها وتحليلها وضوحَ "تسلسل العهدة" منذ الحصول عليها في المرة الأولى، حتى لا يكون قد تأتى العبث بها منذ لحظة ضبطها وحتى آخر مرة تُقدم فيها إلى المحكمة.[١١٠]

١- *الاتصالات عبر الإنترنت*

(أ) بروتوكول الاتصال الصوتي عبر الإنترنت

١٨٢- ازداد، على مدار العقد الماضي، الإقبال على التطبيقات التي تتيح للمستخدمين الاتصال آنياً باستخدام بروتوكول الاتصال الصوتي عبر الإنترنت، أو الدردشة بالفيديو، أو الدردشة بالرسائل النصية، كما ازداد تطورها. إذ تتيح بعض هذه التطبيقات خصائص متقدمة لتبادل المعلومات، فتتيح للمستخدمين على سبيل المثال تبادل الملفات أو القدرة على المشاهدة الآنية عن بعد لما يجري على شاشة مستخدم آخر. وقد بات بروتوكول الاتصال الصوتي عبر الإنترنت، على وجه الخصوص، يُستخدم استخداما متزايدا باعتباره وسيلة اتصال فعالة عبر الإنترنت. ومن بين مقدمي خدمة بروتوكول الاتصال الصوتي عبر الإنترنت المشهورين هنالك سكايب وفونيدج، اللذان يعملان عن طريق تحويل الصوت التناظري إلى شكل رقمي مضغوط، بما يتيح نقل حُزم معلومات رقمية عبر الإنترنت، باستخدام وصلات ذات نطاق ترددي ضيِّق نسبياً.

١٨٣- وحيث إنّ الاتصالات الهاتفية عن طريق بروتوكول الاتصال الصوتي عبر الإنترنت تنطوي على إرسال حُزم بيانات رقمية لا إشارات تناظرية، وأنَّ مقدمي الخدمات عادة ما يعدّون فواتير المشتركين الخاصة باستخدام الإنترنت على أساس الحجم الكلي للبيانات، فإنَّ إعداد فواتير مكالمات بروتوكول الاتصال الصوتي عبر الإنترنت لا يقوم على أساس كل مكالمة على حدة، كما هو الحال في المكالمات التقليدية التي تجرى عبر الهواتف المحمولة

[١١٠] انظر، على سبيل المثال: Association of Chief Police Officers (United Kingdom), *Good Practice Guide for Computer-Based Electronic Evidence*. على الرابط التالي: www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

أو الهواتف الثابتة. وقد يكون لهذا الاختلاف في أسلوب إعداد الفواتير تأثير كبير على التحقيقات في الاتصالات التي يُستخدم فيها بروتوكول الاتصال الصوتي عبر الإنترنت، إذ يصبح من الأصعب على سلطات إنفاذ القانون أن تؤكِّد إجراء هذه الاتصالات بعلامات استدلالية من قبيل وقت إجراء المكالمة وأماكن وجود المشاركين فيها. ومع ذلك فمن الممكن أن تتيح مؤشراتٌ أخرى، مثل توقيت وحجم حركة البيانات عبر الإنترنت، وسيلة لكشف مرتكبي الأنشطة غير القانونية على شبكة الإنترنت (انظر الفقرة ٢٠٥ أدناه). ولئن كان من الممكن، علاوة على ذلك، نقل الاتصال بين مصدر مكالمات الهاتف التقليدية ووجهتها عبر محوِّلات الخطوط الثابتة أو أبراج الاتصالات الخلوية، وهو ما يخلف وراءه آثاراً مادية يُمكن اقتفاؤها، فإنَّ الاتصالات التي يُستخدم فيها بروتوكول الاتصال الصوتي عبر الإنترنت والإنترنت لوحدها، والتي تجرى عبر شبكات لاسلكية على سبيل المثال، قد تطرح صعوبات على القائمين بالتحقيق. ومن بين العوامل الأخرى التي تزيد من تعقيد الأمور، والتي تنجم عن استخدام تكنولوجيا بروتوكول الاتصال الصوتي عبر الإنترنت، نقلُ المكالمات عبر شبكات الاتصال المباشر بين النظراء (P2P) وتشفير بيانات المكالمات (وهو ما سيناقَش بمزيد من التفصيل في القسم رابعاً-ألف-٢ أدناه).[١١١]

١٨٤- ومع ذلك، فإن تقديم طلبات للحصول على معلومات حسب الأصول إلى مقدمي خدمات بروتوكول الاتصال الصوتي عبر الإنترنت قد تتيح معلومات تعريفية قيِّمة مثل عنوان بروتوكول الإنترنت الخاص بمستخدم ما، أو بريده الإلكتروني، أو تفاصيل السداد الخاصة به.

(ب) البريد الإلكتروني

١٨٥- وتتيح خدمات البريد الإلكتروني الشبكي للإرهابيين وسيلةً سريةً للاتصال، يُمكن استغلالها في أغراض غير مشروعة. وعادة ما تحتوي رسائل البريد الإلكتروني المتبادلة بين الأطراف على عدد من العناصر التي قد يكون لها قيمة في التحقيق. فرسالة البريد الإلكتروني التقليدية تتكون من ترويسة المظروف، وترويسة الرسالة، ومتن الرسالة، وأي مرفقات ذات صلة. وقد لا يُعرض للمستخدم إلا نسخة مختصرة من ترويسة المظروف، وفقاً لخصائص البرمجية المستخدمة، إلا أنّ ترويسة المظروف الكاملة عادة ما تحتوي على سجل بكل خادوم بريد نُقلت الرسالة عبره في طريقها إلى آخر المتلقين لها، فضلا عن معلومات عن عنوان بروتوكول الإنترنت الخاص بالمرسِل.[١١٢] والمعلومات الواردة في ترويسة المظروف أقل عرضة للعبث بها (وإن لم تكن منيعة تماما) من المعلومات الواردة في ترويسة الرسالة، والتي عادة ما تتكون من معلومات يقدمها المستخدم في خانات من قبيل "إلى"، و"من"، و"مسار إعادة الرسالة"، و"التاريخ"، و"الوقت"، كما هو معروض على الجهاز الذي تُرسل منه الرسالة.[١١٣]

١٨٦- ومن بين التقنيات الشائعة الاستخدام للحد من الآثار الإلكترونية بين الأطراف، ومن ثم الحد من احتمال التعرض للكشف، الاتصالُ باستخدام رسائل مُخزَّنة وغير مرسلة في ملف المسودات في حساب البريد الإلكتروني. وهكذا تتاح هذه المعلومات لأطراف متعددة تستخدم كلمة سر مشتركة لفتح الحساب. ويمكن أيضاً اتخاذ خطوات إضافية لتلافي التعرض للكشف، كفتح الحساب عن بعد باستخدام محطة طرفية مفتوحة لعامة الجمهور، مثل المحطات المتاحة في مقاهي الإنترنت، للاطلاع على مسودة الرسالة. وقد استُخدِم هذا الأسلوب في سياق تفجيرات مدريد الإرهابية في عام ٢٠٠٤.

---

[١١١] مذكرة مكتوبة قدَّمها الخبير الممثل لمجموعة العمليات الخاصة التابعة لقوات الدرك الإيطالية (كارابينييري).

[١١٢] United States, Department of Justice, Office of Justice Programs, National Institute of Justice, *Investigations Involving the Internet and Computer Networks* (2007), p. 18 ff.

[١١٣] المرجع نفسه، الصفحة ٢٠.

١٨٧- ومن الممكن كذلك الاستعانة بتقنيات إخفاء الهوية (التي تناقَش بمزيد من التفصيل في القسم رابعاً-ألف-٢ أدناه) فيما يتعلق بمراسلات البريد الإلكتروني، بإخفاء عنوان بروتوكول الإنترنت المرتبط بالمرسِل على سبيل المثال. كما يمكن استخدام خوادم بريدية تمكّن من إخفاء الهوية، عن طريق إزالة المعلومات التعريفية من ترويسة المظروف قبل إرساله إلى خادوم البريد التالي.

أهمية التعاون الدولي في التحقيق في الأنشطة المتعلقة بالإرهاب على شبكة الإنترنت

بيَّن الخبير الممثل لمجموعة العمليات الخاصة التابعة لقوات الدرك الإيطالية (كارابينييري) الدور الرئيسي الذي يؤديه كل من التعاون الدولي وتقنيات التحقيق المتخصصة في التحقيق في استخدام الإنترنت في أغراض إرهابية من قبل التنظيم التركي المتطرف المسمى الجبهة الثورية لتحرير الشعب. فقد مكَّن التعاون الوثيق بين مسؤولي إنفاذ القانون في كل من تركيا وإيطاليا المحققين الإيطاليين من تحديد تقنيات التشفير وغيرها من تدابير تأمين البيانات التي يستخدمها أعضاء الجبهة الثورية لتبادل المعلومات دعماً لأغراض إرهابية، بطرائق منها خدمات البريد على الإنترنت. ويشار، على وجه التحديد، إلى أنّ أعضاء الجبهة الثورية استخدموا برمجية تقنية إخفاء المعلومات المسماة "كاموفلاج" لإخفاء البيانات في ملفات الصور من نوعي JPEG وGIF، والبرمجية المسماة "وين زيب" لتشفير الملفات التي كانت تُدرج باعتبارها مرفقات برسائل البريد الإلكتروني (انظر القسم رابعاً-ألف-٢ أدناه). وقام المحققون الإيطاليون باعتراض كلمات السر المستعملة في التشفير، أو حصلوا عليها بطرائق أخرى، وحددوا البرامج ذات الصلة للمساعدة على فك شفرة الرسائل. وتم الحصول على معلومات إضافية عبر التحليل الجنائي بالحاسوب، باستخدام البرمجية المسماة "إن كيس" (انظر القسم رابعاً-جيم أدناه) وتقنيات التحقيق التقليدية، لتمكين المحققين من الحصول على أدلة رقمية من أجهزة الحاسوب الخاصة بمشتبه به قيد التحقيق. وقد أسفرت نتائج هذا التحقيق، إلى جانب التعاون المكثف عبر الحدود، عن إلقاء القبض، في نيسان/أبريل ٢٠٠٤، على ٨٢ من المشتبه بهم في تركيا فضلا عن ٥٩ آخرين في ألمانيا، وإيطاليا، وبلجيكا، وهولندا، واليونان.

(ج) خدمات تبادل الرسائل عبر الإنترنت ومنتديات الدردشة

١٨٨- توفِّر خدمات تبادل الرسائل عبر الإنترنت ومنتديات الدردشة وسائل إضافية للتواصل الآني، بدرجات مختلفة من إمكانية إخفاء الهوية. وعادة ما تكون خدمات تبادل الرسائل عبر الإنترنت عبارة عن اتصالات ثنائية، فيما تتيح منتديات الدردشة التواصل المفتوح بين مجموعة من الأفراد. وعادة ما يستند التسجيل في خدمات تبادل الرسائل عبر الإنترنت إلى معلومات يقدِّمها المستخدم دون التحقق من صحتها، بيد أنَّ بعض خدمات الإنترنت تسجِّل كذلك عنوان بروتوكول الإنترنت المستخدَم في وقت التسجيل، وهو ما يُمكن أن تطلبه سلطات إنفاذ القانون، رهناً بالضمانات القانونية المنطبقة. وعادةً ما تُعرَّف الرسائل باسم يخصَّص للمستخدم ويظهر على الشاشة، إما عند التسجيل ليعرِّفه بصفة دائمة أو في كل حصة اتصال بالإنترنت. ويُذكر بصفة عامة أنّ مُقدِّم الخدمة لا يحتفظ بالمعلومات التي يجري تبادلها أثناء حصة تبادل الرسائل عبر الإنترنت، ومن ثم فقد لا يكون من الممكن استعادتها بعد إنهاء حصة الاتصال، وإن أمكن استرجاعُ البيانات عن طريق التحليل الجنائي للقرص الصلب لأحد المشاركين فيها.

١٨٩- وقد تستخدم التنظيمات الإرهابية والمتعاطفون معها منتديات الدردشة لا يمكن الدخول إليها إلا بكلمة سر لخلق شعور بالانتماء إلى جماعة واحدة في سياق عالمي. وقد تكون الرسائل المتبادلة في منتديات الدردشة موضع مراقبةٍ وحفظٍ للسجلات من قبل مقدمي الخدمات أكثر من المراسلات الثنائية، بما يزيد من احتمال

الحصـول على أدلة موثقة فيما يخص التحقيقات.[١١٤] وفي بعض الولايات القضائية، يُمكن للعاملين في الأجهزة المعنيـة بإنفـاذ القانون، رهناً بشروط معيَّنـة، أن يسجلوا أنفسهم في منتديات الدردشـة ويشتركوا في مناقشاتها باسم مستعار في إطار التحقيق.

١٩٠- فعلـى سبيـل المثال، تنص المادة ٧٠٦ من قانون الإجراءات الجنائيـة الفرنسي على أن يأذن عضو النيابة العامـة أو قاضـي التحقيـق بعمليـات اختراق من هـذا القبيل فيمـا يتصل بالجرائـم المرتكبة عـبر الاتصالات الإلكترونيـة (انظـر المناقشة في القسـم ثالثاً-جيم-٣(*أ*)). وقد يكـون الهدف من وراء هـذه العمليات هو جمع معلومات استخبارية أو اتخاذ إجراءات استباقية إزاء خطر إرهابي متوقَّع، في جملة أهداف أخرى. إلا أنَّه ينبغي توخـي العنايـة الواجبـة في بداية العملية لضمان ألا يكـون أي اختراق لمنتدى دردشة علـى الإنترنت، أو غير ذلك مـن المناقشـات التي تجرى على الإنترنت، بطريقة من شأنها أن تتيـح لمشتبه به الدفعَ بالاستدراج أثناء ملاحقته قضائياً، بناء على الادعاء بأنَّ سلطة حكومية قد استدرجته لارتكاب جريمة لم يكن ليرتكبها لولا ذلك.

(د) شبكات تبادل الملفات والحوسبة البعدية

١٩١- تتيح مواقع تبادل الملفات، مثل رابيدشير، ودروب بوكس، وفايل شير، للمستخدمين إمكانية تحميل ملفات الوسائـط المتعـددة، وتبادلها، والعثور عليهـا، والوصول إليها بسهولة عبر الإنترنت. كمـا تنطبق تقنيات التشفير وإخفـاء الهوية المستعملة في الأشكال الأخرى للاتصال عـبر الإنترنت على الملفات المتبادلة عبر الاتصال المباشر بـين النظـراء (P2P) وبروتوكول نقل الملفات (FTP)، ضمن تكنولوجيات أخرى. فعلـى سبيل المثال، قُدِّمت أدلة في قضيـة هيشر (انظر الفقرة ٢٠ أعلاه) علـى أنَّ الملفات الرقمية المستخدَمة لدعم الأنشطة الإرهابية قد جرى تبادلها عبر رابيدشير، بعد تشفيرها وضغطها لتأمينها. وربما تحتفظ بعض شبكات تبادل الملفات بسجلات لنقل الملفات أو بمعلومات السداد، وهو ما قد يكون مفيداً في التحقيق.

١٩٢- والحوسبـة البعديـة خدمة تتيح لمستخدميها الوصـول عن بعد إلى برامج وبيانات مخزَّنـة أو مشغَّلة على خواديم بيانات تابعة لطرف ثالث. وكما هو الحال في تبادل الملفات، توفر الحوسبة البعدية وسيلة ملائمة لتخزين المـواد وتبادلهـا ونشرها بصورة آمنـة على الإنترنت. ويقلِّل استخـدام تكنولوجيا الحوسبـة البعدية للوصول إلى معلومـات مخزَّنـة عن بعد من كمية البيانات المخزَّنـة داخلياً على الأجهزة الفردية، بمـا يقلل كذلك من إمكانية استرجاع أدلة قد تدعو الحاجة إليها في تحقيق يتعلق باستخدام الإنترنت في أغراض إرهابية.

١٩٣- كما أنَّ خواديم البيانات المستخدَمة لإتاحة هذه الخدمات قد تكون موجودة وجودا ماديا في ولاية قضائية غـير الولايـة التي يوجد فيها المستخدم المسجَّل، حيث تتفاوت مستويـات التنظيم الرقابي وقدرات إنفاذ القانون. ومـن ثمَّ فالتنسيق الوثيق مع سلطات إنفاذ القانون المحلية قد يكون لازماً للحصول على أدلة ذات أهمية جوهرية في الإجراءات القانونية.

٢- *تقنيات تشفير البيانات وإخفاء الهوية*

١٩٤- تشفـير البيانات يعني الحماية مـن إفشاء معلومات رقمية عن طريق تحويلها إلى نص مشفر، باستخدام خوارزميـة رياضيـة ومفتاح تشفير، بحيـث لا يفهمها إلا متلقيهـا المقصود. وقد تكـون أدوات التشفير عبارة عن

[١١٤] المرجع نفسه، الصفحات ٣٤ وما بعدها.

معـدات أو برمجيـات حاسوبية، أو مزيج من الاثنين. وقد يتطلب الاطلاع على المعلومات بعد تشفيرها كلمة سر أو عبـارة سـر أو "مفتاحا برمجيا" أو جهازا، أو مزيجا من هـذه الوسائل. وقد يُستخدم التشفير فيما يتعلق بكل من البيانـات "الساكنة"، أي الموجودة في أجهزة تخزين مثـل أقراص الحاسوب الصلبة، أو محركات أقراص فلاش، أو الهواتف الذكية، والبيانات "المتحركة"، أي البيانات المرسَلة عبر الإنترنت، عن طريق الاتصالات التي يستخدم فيهـا بروتوكول الاتصال الصوتي عبر الإنترنت أو البريد الإلكتروني علـى سبيل المثال. ومن الأمثلة على الأدوات الشائعة للتشفير باستخدام برمجيات حاسوبية الأدوات المدمجة في نظم أو تطبيقات التشغيل الحاسوبية، فضلا عن البرمجيات القائمة بذاتها مثل "بريتي غود برايفسي" (PGP) و"وين زيب".[١١٥] وفي البرازيل، فُتح التحقيق في قضيـة على أساس التعاون الدولي وتبادل المعلومات ضـد مشتبه به يُزعم اشتراكه في موقع شبكي جهادي ذي صلـة بتنظيمـات إرهابية معروفة، أبرزها تنظيـم القاعدة، وإدارته لهذا الموقع وتحكمـه في عملياته. وكان الموقع يستضيـف شرائط فيديـو، ونصوصاً، ورسائل من قيادات المقاتلين المتطرفين، بعد ترجمتها إلى الإنكليزية لتصل إلى جمهـور أوسع، كما كان يُستخدم للقيام بأنشطـة لجمع الأموال وحملات دعائية ذات دوافع عنصرية. وكانت العمليـة التـي نفذتها الشرطة وأسفرت عن احتجاز المشتبه به تستهـدف أخذ المتهم على حين غرة، في وقت يكون فيـه متصلا بالإنترنـت وبصدد القيام بالفعل بأنشطـة متعلقة بالموقع. وبإلقاء القبض علـى المشتبه به حين كان جهـاز الحاسـوب العائد له مُشغَّلا وكانت الملفـات ذات الصلة مفتوحة، استطاع المحققـون الاستغناء عن مفاتيح التشفـير المتناظر وغيرها من أساليـب التشفير وخصائص حماية المعلومات التي كان المشتبه به والمتواطئون معه يستخدمونهـا. ومن ثم فقد استطـاع المحققون الوصول إلى المحتوى الرقمي الذي لولا ضبط جهاز الحاسوب وهو مفتوح لكان الحصول عليه أصعب أو غير ممكن.

١٩٥- كمـا يُمكـن إخفاء الأنشطة الشبكية، أو هوية المستخدمين القائمين بها، عبر تقنيات متقدِّمة، بما في ذلك طمسـ عنوان بروتوكول الإنترنت للمرسِل، بانتحال عنوان بروتوكول الإنترنت الخاص بنظام آخر أو إعادة توجيه حركـة المعلومات على الإنترنت إلى عنوان مطموس.[١١٦] وتتيح الخواديم الوسيطة للمستخدمين الاتصالَ الشبكي غـير المباشر بخدمات شبكية أخـرى. وتتيح بعض الخواديم الوسيطة تصميم المتصفح الخاص بالمستخدم بحيث يوجِّه حركة التصفح تلقائياً عبر خادوم وسيط. ويطلب الخادوم الوسيط الخدمات الشبكية بالنيابة عن المستخدم ثـم يوجِّه النتائج عبر وسيط كذلك. ويُمكّن استخدام الخواديم الوسيطة من تحقيق مستويات متفاوتة من إخفاء الهوية. فقد يُخفي الخادوم الوسيط هوية المستخدم بتنفيذ طلبات الحصول على خدمات شبكية دون الكشف عن عنـوان بروتوكول الإنترنت الذي صدرت عنه الطلبـات، أو بتقديم عنوانٍ محرَّف عمداً لعنوان بروتوكول الإنترنت الخاص بالمصدر. فعلى سبيـل المثال قد تُستخدم تطبيقات مثل "أونيون راوتـر" لحماية سرية هوية المستخدمين بإعـادة توجيـه أنشطـة الإنترنت تلقائياً عـبر شبكة من الخـواديم الوسيطة بغرض عدم الكشـف عن مصدرها الأصلـي. وتـزداد درجة صعوبة تحديد هويـة المرسِل تحديدا دقيقا بسبب إعادة توجيـه حركة المعلومات الشبكية عبر خواديم وسيطة متعددة قد تكون واقعة في ولايات قضائية مختلفة.

١٩٦- وبدلا من ذلك، قد يقوم مشتبه به باختراق عنوان بروتوكول الإنترنت الخاص بمنظمة مشروعة، ويتصفح الإنترنت مستخدماً العنوان المخترَق، وهكذا ترتبط آثار هذا النشاط بعنوان بروتوكول الإنترنت الخاص بالمنظمة

(١١٥) United States, Department of Justice, Office of Justice Programs, National Institute of Justice, *Investigative Uses of Technology: Devices, Tools and Techniques* (2007), p. 50.

(١١٦) National Institute of Justice, Investigations Involving the Internet and Computer Networks, p. 9.

التي تعرضت للاختراق. كما يمكن لمشتبه به أن يدخل موقعا شبكيا عبر جهاز حاسوب مُخترَق أو أن يخزِّن برمجية ضارة (لاستخدامها، على سبيل المثال، للحصول على معلومات تخص بطاقات الائتمان أو غيرها من المعلومات المالية الشخصية) على مواقع مُخترَقة سعياً لتلافي الكشف عن هويته.

١٩٧- وثمة مجموعة متنوعة من البرامج الحاسوبية المتاحة لإخفاء أو تشفير البيانات المرسلة عبر الإنترنت لأغراض غير مشروعة. وقد تشمل هذه البرامج استخدام برمجيات مثل "كاموفلاج" لإخفاء المعلومات عن طريق تقنية إخفاء المعلومات أو تشفير الملفات وحمايتها بكلمة سر باستخدام برمجيات مثل "وين زيب". كما يُمكن استخدام طبقات متعددة من الحماية في ذات الوقت. فعلى سبيل المثال، يتيح "كاموفلاج" إخفاء الملفات بتشفير محتوياتها ثم إرفاقها في آخر ملف تمويهي من اختياره. وفيما يحتفظ الملف التمويهي بخواصه الأصلية فإنَّه يُستخدم في الوقت ذاته باعتباره وسيلة لتخزين أو إرسال الملف المخفي. ويُمكن استخدام هذه البرمجية في مجموعة واسعة من أنواع الملفات. بيد أنَّه يمكن كشف الملف المخفي بفحص البيانات الخام الواردة في الملف، وهو ما من شأنه أن يُظهر وجود الملف المخفي المرفق.[١١٧]

١٩٨- وفي المملكة المتحدة، يجرّم قانون التنظيم الرقابي لصلاحيات التحقيق لسنة ٢٠٠٠ رفضَ تسليم مفتاح تشفير عند طلب ذلك. بيد أنَّه ينبغي توخي الحذر لضمان ألا يسعى المشتبه بهم إلى الالتفاف على هذا الحكم باستخدام العديد من طبقات التشفير ومفاتيح متعددة لحماية مختلف مجموعات البيانات. فعلى سبيل المثال، يستطيع المشتبه به أن يقوم، عن طريق استخدام أحد خصائص برنامج "ترو كريبت"، وهو أداة تشفير مجانية شائعة، بتشفير قرص صلب ووضع كلمتي سر: إحداهما للقرص "النظيف" والأخرى تحتوي على المواد التي تدينه. ويمكن التغلب على ذلك بالتأكد من أنَّ التحليل الجنائي للقرص الصلب قد أخذ في الاعتبار ما إذا كان هنالك أي "قدر مفقود" من البيانات. وعلاوة على ذلك فإنَّ الجرائم من هذا النوع عادة ما تكون جُنحاً لا تزيد العقوبة فيها على السجن لستة أشهر. إلا أنَّ العقوبة القصوى على الجرائم التي تعرِّض الأمن القومي للخطر في المملكة المتحدة، تُشدَّد العقوبة القصوى لتبلغ السجن لمدة سنتين.

٣- *التكنولوجيا اللاسلكية*

١٩٩- تتيح تكنولوجيا الشبكات اللاسلكية لأجهزة الحاسوب وغيرها من الأجهزة الدخول إلى الإنترنت عبر إشارة لاسلكية بدلا من الوصلات السلكية، مثل وصلات الكابل. ولكي يتأتى استخدام شبكة حاسوب لاسلكية (واي فاي)، لا بد من أن يكون الاتصال من مكان قريب شيئا ما من مرافق الشبكة، وهو أمر يتوقف على قوة الإشارة اللاسلكية. وقد تصمَّم الشبكات اللاسلكية بحيث تتيح الدخول بحرية إلى الإنترنت دون أن يكون التسجيل ضروريا، أو بالتسجيل باستخدام عبارة سر أو مستويات متفاوتة من التشفير. وكثيراً ما يمكن الوصول إلى الشبكات اللاسلكية، المسجلة باسم أفراد أو شركات أو جهات عامة، من أماكن عامة. وقد يتيح الدخول إلى شبكات الواي فاي التي تكون مؤمنة أو غير مؤمنة دون الكشف عن الهوية للجناة أن يُخفوا الصلات ما بين نشاطهم على الإنترنت والمعلومات التي تحدِّد هويتهم.

٢٠٠- وعلاوة على ذلك، ظهر في السنوات الأخيرة مقدمو خدمات مثل فون، الذين يمكِّنون المستخدمين المسجلين لديهم من تقاسم جزء من النطاق الترددي لشبكات الواي فاي المنزلية الخاصة بهم مع مشتركين

[١١٧] مذكرة مكتوبة قدَّمها الخبير الممثل لمجموعة العمليات الخاصة التابعة لقوات الدرك الإيطالية (كارابينييري).

آخريـن، مقابل المعاملة بالمثل عند الوصول إلى شبكات الواي فاي الخاصة بالمشتركين في كل أنحاء العالم. وتُعقِّد الأنشطـة التـي تجري على شبكة واي فاي مشتركة تعقيدا كبيرا عملية إسناد عمل ما إلى جانٍ واحد يُمكن تحديد هويته في سياق التحقيق.[١١٨]

٢٠١- ومن بين التقنيات الجديدة ما يتعلق باستخدام أجهزة الاستقبال اللاسلكية العالية التردد والأداء والمعرَّفة برمجياً، والتي يتم توجيهها عبر جهاز حاسوب. وبذلك، لا يجري تبادل أي بيانات عبر خواديم ولا توضع سجلاتٌ للبيانـات. ومن الأصعـب على أجهزة إنفاذ القانـون والاستخبارات اعتراض الاتصـالات المرسلة بهذه الطريقة، سواء فيما يتعلق بتحديد موقع أجهزة الإرسال أو ما يخص التوقُّع الآني للتردد الذي تُبث عليه الرسائل.

باء- التحقيقات في جرائم الإرهاب المرتكبة باستخدام الإنترنت

١- *اتباع نهج منتظم في التحقيق في الجرائم المرتكبة باستخدام الإنترنت*

٢٠٢- ثمـة مجموعـة ضخمة من البيانات والخدمات المتاحة في الإنترنت والتـي يُمكن استخدامها في التحقيق لمكافحـة استخدام الإنترنت في أغراض إرهابية. ويمكّن اتباع نهج استباقي إزاء استراتيجيات التحقيق والأدوات المتخصصـة الداعمة لـه، بالاستفادة من الموارد المتطـورة التي تُتيحها الإنترنت، من تحقيـق الفعالية في تحديد البيانـات والخدمـات التي يُرجَّـح الاستفادة منهـا إلى أقصى حد في التحقيـق. وإقراراً من مجموعـة العمليات الخاصـة التابعـة لقـوات الـدرك الإيطالية (كارابينيـيري) بالحاجـة إلى اتباع نهـج منتظـم في الاستفادة من التطورات التكنولوجية ذات الصلة بالإنترنت في التحقيق، فقد وضعت المبادئ التوجيهية التالية، التي نُشرت عبر برنامج الماجستير في حوسبة التحليل الجنائي والجرائم السيبرانية التابع لجامعة دبلن (انظر القسم رابعاً-زاي أدناه)، وطبَّقتها سلطات إنفاذ القانون المحلية في العديد من الدول الأعضاء في المنظمة الدولية للشرطة الجنائية (الإنتربول) ومكتب الشرطة الأوروبي (اليوروبول).

بروتوكول خاص باتباع نهج منتظم

- جمـع *البيانات*: تشمل هذه المرحلة جمع البيانات عبر أساليب التحقيق التقليدية، من قبيل المعلومات المتعلقـة بالمشتبـه به، وبمن يشاركونـه المسكن إن وجدوا، أو بمن يعنيه الأمـر من زملائه في العمل أو غيرهـم ممن لهـم علاقة به، والمعلومـات المحصل عليها مـن أنشطة المراقبـة التقليدية عبر قنوات الاتصال، بما في ذلك استخدام الهواتف الثابتة والهواتف المحمولة.
- *البحـث عن معلومـات إضافية متاحة عـبر خدمات الإنترنـت*: تشمل هذه المرحلـة طلبات الحصول علـى معلومات مجمّعة ومُخزَّنة في قواعد بيانات التجـارة الإلكترونية والاتصالات وخدمات التواصل علـى الإنترنـت، مثل إي باي، وبـاي بال، وغوغل، وفيسبـوك، فضلا عن استخـدام محركات البحث المتخصصـة مثـل www.123people.com. كذلك فـإن البيانات التي تُجمـع بواسطة هذه الخدمات عبر سجلات التصفح (cookies) توفِّر معلومات هامة فيما يخص استخدام جهاز الحاسوب ذاته أو الجهاز المحمول ذاته من قبل مستخدمين متعددين.

[١١٨] المرجع نفسه.

- توفر أنشطة المرحلتين *(أ)* و*(ب)* أعلاه معلومات يمكن الجمع بينها أو ربط بعضها ببعض لإعداد ملف للفرد أو المجموعة الجاري التحري عنها، كما يمكن إتاحتها للتحليل أثناء المراحل اللاحقة للتحقيق.
- *طلبات خادوم بروتوكول الاتصال الصوتي عبر الإنترنت:* في هذه المرحلة، تطلب سلطات إنفاذ القانون من مقدمي خدمات بروتوكول الاتصال الصوتي عبر الإنترنت معلومات عن الأشخاص قيد التحقيق وأي شركاء معروفين لهم أو مستخدمين لنفس أجهزة الربط الشبكي التي يستخدمونها. ويمكن أيضاً استخدام المعلومات المجموعة في هذه المرحلة باعتبارها "نظام فرز" للتوثق من المعلومات التي تم الحصول عليها في المرحلتين السابقتين.
- *التحليل:* يجري تحليل الكمية الكبيرة من البيانات التي تم الحصول عليها من خواديم بروتوكول الاتصال الصوتي عبر الإنترنت ومن مقدمي شتى خدمات الإنترنت بهدف الوقوف على المعلومات والاتجاهات المفيدة للتحقيق. ويمكن تسهيل هذا التحليل باستخدام البرامج الحاسوبية التي يمكنها أن تصفِّي المعلومات أو تحوِّل ما تم جمعه من بيانات رقمية إلى رسوم بيانية لتسليط الضوء على أمور في جملتها الاتجاهات، أو التسلسل الزمني، أو وجود جماعة منظَّمة أو تسلسل هرمي للقيادة من عدمه، أو المواقع الجغرافية لأعضاء هذه الجماعة إن وجدت، أو العوامل المشتركة فيما بين مستخدمين متعددين، مثل وجود مصدر تمويل واحد لهم جميعاً.
- *تحديد الأشخاص مثار الاهتمام:* في هذه المرحلة، وعقب التحليل الانتقائي للبيانات، من الشائع تحديد الأشخاص مثار الاهتمام على أساس معلومات المشتركين المرتبطة بحساب مالي، أو حساب اتصال صوتي عبر الإنترنت، أو حساب بريد إلكتروني، على سبيل المثال.
- *أنشطة الاعتراض:* في هذه المرحلة، تستخدم سلطات إنفاذ القانون تقنيات اعتراض مشابهة للتقنيات المستخدَمة في قنوات الاتصال التقليدية، مع نقلها إلى وسيلة مختلفة هي قنوات الاتصال الرقمي. ويمكن الاضطلاع بأنشطة الاعتراض فيما يخص خدمات الاتصالات، من قبيل وصلات الإنترنت ذات النطاق الترددي العريض الثابت، ومثيلاتها المنقولة عبر النطاق الترددي العريض المحمول، والاتصالات اللاسلكية، فضلا عن الخدمات التي يوفِّرها مقدمو خدمات الإنترنت، مثل خدمات الاتصال عبر البريد الإلكتروني، والدردشة، والمنتديات. ويشار بالأخص إلى أن تجربة السنوات الأخيرة قد كشفت عن مواطن ضعف في تكنولوجيات الاتصالات الجديدة التي يمكن الاستفادة منها في التحقيقات أو جمع المعلومات الاستخبارية. وينبغي الحرص على ضمان سلامة بيانات التحليل الجنائي التي يجري جمعها، والتحقق قدر الإمكان من صحة أية معلومات استخبارية يتم جمعها بمحدِّدات موضوعية من قبيل إحداثيات النظام العالمي لتحديد المواقع، أو أختام توقيت البيانات، أو المراقبة بالفيديو.

كما يمكن لسلطات إنفاذ القانون، حيثما كان القانون المحلي يسمح بذلك، أن تستخدم تقنيات المراقبة الرقمية التي تتوفر عبر تركيب معدَّات أو تطبيقات حاسوبية من قبيل الفيروسات، أو برمجيات حصان طروادة الضارة، أو برمجيات رصد لوحات المفاتيح، على جهاز الحاسوب الخاص بالشخص المتَحرَّى عنه. ويمكن القيام بذلك عن طريق الدخول إلى جهاز الحاسوب المعني مباشرة أو عن بعد، بمراعاة المواصفات التقنية للمعدات التي ستُخترق (مثل وجود برامج للوقاية من الفيروسات أو جدران نارية) المواصفات الشخصية لكل من مستخدمي الجهاز، حتى يُستهدف الحساب ذو المواصفات الشخصية الأقل تعقيداً.

٢٠٣- وقد استجاب جهاز الشرطة الوطنية الكوري للحاجة لتوحيد ممارسات إنفاذ القانون المحلية فيما يخص التحاليل الجنائية الرقمية بإعداد دليلين إرشاديين وتطبيقهما وهما: *المبادئ التوجيهية الموحدة لمناولة الأدلة الرقمية* و*الدليل التقني للتحاليل الجنائية الرقمية*. وتتناول *المبادئ التوجيهية الموحدة* بتفصيل سبع خطوات لمناولة الأدلة الرقمية مناولة سليمة، وهي: الخطوات التحضيرية؛ وجمع الأدلة؛ وفحصها؛ وطلب الحصول عليها، واستلامها، ونقلها؛ وتحليلها؛ وتقديم تقارير عنها؛ وحفظها؛ وإدارتها. أمَّا *الدليل التقني للتحاليل الجنائية الرقمية* فيبيِّن الإجراءات اللازمة والنهج السليم لجمع البيانات الرقمية، بشأن أمور منها تهيئة الظروف الملائمة، وأدوات

التحليل الجنائي ومعداته؛ والخطوات التحضيرية من قبيل تركيب المعدات والبرمجيات، والوصلات الشبكية ودقة التوقيت؛ وتدابير ضبط أكبر قدر ممكن من الأدلة الرقمية؛ والتحليل المستقل للبيانات المضبوطة؛ وإعداد التقرير النهائي.[١١٩]

٢- *تعقب عناوين بروتوكول الإنترنت*

٢٠٤- يُعدُّ عنوان بروتوكول الإنترنت المرتبط باتصال على الإنترنت أداة تعريف هامة، ومن ثم فهو عنصر رئيسي في التحقيق في قضايا استخدام الإنترنت في أغراض إرهابية. ويعرِّف عنوان بروتوكول الإنترنت على وجه التحديد الشبكة والجهاز المستخدَمين للدخول إلى الإنترنت. ويمكن أن يكون عنوان بروتوكول الإنترنت متغيرا، أي مخصصاً بصورة مؤقتة لحصة اتصال واحدة بالإنترنت من بين مجموعة من العناوين المتاحة لأحد مقدمي خدمات الإنترنت، أو ثابتا (كما هو حال عناوين المواقع الشبكية). وعادة ما تُخصص عناوين بروتوكول الإنترنت المتغيرة لمقدمي خدمات الإنترنت حسب مجموعات مُعرَّفة استناداً إلى المنطقة الجغرافية التي يُتصل منها بالإنترنت. ومن ثم، يمكن في كثير من الأحيان، في حالة عدم استخدام تقنيات إخفاء الهوية أو غيرها من تقنيات التدخُّل، استخدام عنوان بروتوكول الإنترنت المتغير لتحديد المنطقة أو الدولة التي يتصل منها جهاز حاسوب ما بالإنترنت.

٢٠٥- وعلاوة على ذلك، فكثيراً ما يكون بوسع مقدمي خدمات الإنترنت أن يحدِّدوا، بناء على طلب مقدَّم إليهم حسب الأصول، حساب المشترك المرتبط بأحد عناوين بروتوكول الإنترنت في وقت معيَّن. ويمكن بعد ذلك استخدام أساليب التحقيق التقليدية للوقوف على هوية الشخص الذي يتحكم مادياً في الحساب المعني في ذلك الوقت. ففي قضية هيشر (انظر الفقرة ٢٠ أعلاه)، حُدِّدت هوية المدَّعى عليه بتعقب عنوان بروتوكول الإنترنت الثابت المستخدَم في الدخول إلى حساب البريد الإلكتروني المراقَب. ونتيجة لطلب قُدِّم لمقدم خدمات الإنترنت المعني، تمكنت السلطات من ربط عنوان بروتوكول الإنترنت بحساب اشتراك يستخدمه عدد من المقيمين في أحد المنازل، بينهم المدَّعى عليه. وباعتراض حركة البيانات الخاصة بهذا الحساب، استطاع المحققون الربط ما بين عنوان بروتوكول الإنترنت ونشاط على موقع شبكي مناصر للجهاديين، كان ينشر مواد تستهدف التدريب البدني والذهني لمقاتلين متشددين، ضمنَ أمور أخرى. ويُذكر على وجه التحديد أنه كان بوسع المحققين أن يربطوا ما بين الأوقات التي كانت تتم فيها اتصالات متعددة بمنتدى النقاش على الموقع الشبكي، وبين زيادات متزامنة مع تلك الاتصالات في كمية بيانات الإنترنت المرتبطة بحساب البريد الإلكتروني الشخصي الخاص بالمدَّعى عليه.[١٢٠]

٢٠٦- ونظراً لأهمية عامل الوقت في التحقيقات التي تُستخدم فيها الإنترنت واحتمال تعديل البيانات الرقمية أو حذفها بسبب القدرات المحدودة لخادوم مقدِّم خدمات الإنترنت المعني، أو وجود لوائح سارية لحماية البيانات، أو غير ذلك من الأسباب، فينبغي أيضاً أن يؤخذ في الاعتبار استصواب توجيه طلب إلى مقدِّم خدمات الإنترنت بحفظ البيانات المتصلة بتحقيق جنائي، ريثما تُستوفى الخطوات اللازمة لاستكمال ضبط البيانات المطلوبة باعتبارها أدلة إثبات.

٢٠٧- وفي حالة التحقيقات المتعلقة بأحد المواقع الشبكية، فلا بد أولا من تحديد عنوان بروتوكول الإنترنت المرتبط باسم النطاق المعني. وحتى يتأتى الوقوف على هذا العنوان، المسجل بدوره لدى شركة الإنترنت للأسماء والأرقام المخصصة، فإنَّ هناك عددا من المرافق المخصصة التي يمكن استخدامها لهذا الغرض. وتشمل المرافق

[١١٩] مذكرة مكتوبة قدَّمها الخبير الممثل لجمهورية كوريا.

[١٢٠] حكم صادر بتاريخ ٥ أيار/مايو ٢٠١٢ عن محكمة باريس الابتدائية بشأن القضية رقم ٠٩٢٦٦٣٩٠٣٦ (الغرفة الرابعة عشرة/٢)، باريس، الصفحة ٧ وما بعدها.

الشائعة المتاحة على الإنترنت "whois" و"nslookup".[١٢١] وفيما يلي، على سبيل المثال، نتيجةُ الاستعلام على "whois" عن اسم النطاق الخاص بمكتب الأمم المتحدة المعني بالمخدِّرات والجريمة (www.unodc.org):

Domain ID: D91116542-LROR

Domain Name: UNODC.ORG

Created On: 11-Oct-2002 09:23:23 UTC

Last Updated On: 19-Oct-2004 00:49:30 UTC

Expiration Date: 11-Oct-2012 09:23:23 UTC

Sponsoring Registrar: Network Solutions LLC (R63-LROR)

Status: CLIENT TRANSFER PROHIBITED

Registrant ID: 15108436-NSI

Registrant Name: Wiessner Alexander

Registrant Organization: United Nations Vienna

Registrant Street1: Vienna International Centre, P.O. Box 500

Registrant City: A-1400 Wien Vienna AT 1400

Registrant Postal Code: 99999

Registrant Country: AT

Registrant Phone: +43.1260604409

Registrant FAX: +43.1213464409

Registrant E-mail: noc@unvienna.org

إلا أنَّ مصدر هذه التفاصيل هو المسجِّل نفسه. ونتيجةً لذلك، فقد يقتضي الأمر مزيداً من الخطوات للتوثق المستقل من صحة بيانات المسجِّل. وكذلك فمن الممكن أن يكون النطاق مؤجراً أو تحت سيطرة طرف غير المسجِّل.

٢٠٨- كذلك ينبغي على الأشخاص القائمين على التحقيق في استخدام الإنترنت في أغراض إرهابية أن يكونوا مدركين لكون الأنشطة الشبكية المتعلقة بالتحقيق يمكن أن تخضع للمراقبة أو التسجيل أو التعقب من قبل طرف ثالث. ومن ثم ينبغي توخي الحذر الواجب لتلافي القيام باستعلامات على الإنترنت من أجهزة يُمكن تعقبها وصولا إلى الجهة القائمة على التحقيق.[١٢٢]

٣- *التطبيقات والمعدات المتخصصة في مجال التحقيقات*

٢٠٩- ثمة مجموعة من التطبيقات والمعدات المتخصصة المتاحة أمام المحققين الذين لديهم المهارات التقنية اللازمة، من بينها ما يُمكن إدماجه في نظام تشغيل جهاز خاضع للتحقيق، مثل "بينج" و"تريس روت". فقد

[١٢١] National Institute of Justice, *Investigations Involving the Internet and Computer Networks*, p. 10.

[١٢٢] المرجع نفسه.

يُستخدم "بينج"، على سبيل المثال، لإرسال إشارة إلى جهاز حاسوب متصل بالإنترنت ليبيِّن ما إذا كان متصلا أو غير متصل في وقت محدد، ما لم يكن محميا بجدران نارية أو غير ذلك من الخصائص الشبكية. وبالمثل فإنَّ "تريس روت" يمكن أن يُظهر المسار فيما بين جهازي حاسوب متصلين بشبكة، وهو ما قد يساعد على تحديد موقعيهما الماديين.

٢١٠- ومن بين البرامج الأخرى التي يمكن استخدامها، رهناً بالقوانين واللوائح المحلية المتعلقة بأمور في جملتها الدخول إلى الأجهزة واعتراض الاتصالات، برمجيات "حصان طروادة" أو برمجيات الإدارة عن بعد باستخدام "حصان طروادة" (RATs)، والتي يمكن دسُّها سراً في نظام حاسوبي لجمع المعلومات أو لإتاحة التحكم عن بُعد في الجهاز المخترَق. كما يُمكن تركيب أدوات لرصد لوحات المفاتيح على الأجهزة واستخدامها لرصد وتسجيل النشاط على لوحة المفاتيح. وتساعد أدوات رصد لوحات المفاتيح، سواء كانت معدات أو برمجيات، على جمع المعلومات عن أمور في جملتها كلمات السر، والاتصالات، وأنشطة المواقع الشبكية أو الشبكات المحلية التي تُنفَّذ باستخدام الجهاز المراقَب. وبالإضافة إلى ذلك، من الممكن استخدام "أدوات تشمُّم" حُزم البيانات لجمع البيانات المتعلقة بالتحقيق. وتجمع أدوات التشمُّم، التي قد تتخذ شكل معدات أو برمجيات، المعلومات مباشرة من شبكة ما، ويُمكن أن توفِّر معلومات فيما يتصل بمصدر الاتصالات ومحتواها، فضلا عن المحتوى المنقول عبر هذه الاتصالات.

جيم- حفظ بيانات التحليل الجنائي واسترجاعها

٢١١- من بين العناصر الهامة في الحصول على الأدلة في سياق القضايا التي تُستخدم فيها الإنترنت في أغراض إرهابية استرجاع البيانات الرقمية المخزَّنة. والهدفان الرئيسيان من استرجاع البيانات هما استعادة الأدلة ذات الصلة من أجل الفعالية في التحقيق والملاحقة القضائية، والحفاظ على سلامة مصدر البيانات وتسلسل العهدة لضمان مقبوليتها أثناء المحاكمة. وحتى يمكن الوقوف على الوسائل المثلى لحفظ البيانات، من المهم التفرقة بين البيانات المعرضة للتلف، التي تُخزَّن على أجهزة من قبيل ذاكرة الوصول العشوائي وقد تضيع للأبد إذا ما وقع انقطاع في الإمداد بالطاقة الكهربائية، والبيانات غير المعرضة للتلف، التي تبقى مخزَّنة بصرف النظر عن إمداد الجهاز بالطاقة الكهربائية. فعلى سبيل المثال، قد يغيِّر إطفاء جهاز حاسوب البيانات الواردة في أقراص التخزين في ذاكرة الوصول العشوائي، والتي قد تحتوي على أدلة هامة حول البرامج الحاسوبية التي استخدمها المشتبه به أو المواقع الشبكية التي زارها. وقد توفِّر البيانات المعرضة للتلف معلومات يُمكن أن تكون مفيدة في التحقيق بشأن العمليات الجارية على جهاز حاسوب مشتغل، مثل المعلومات المتعلقة بالمستخدمين، أو كلمات السر، أو البيانات غير المشفرة، أو الرسائل الفورية. وتتضمن الأمثلة على أجهزة تخزين البيانات غير المعرضة للتلف الأقراص الصلبة الداخلية والخارجية، ومحركات الأقراص المحمولة، وأجهزة التخزين على أقراص فلاش، وأقراص زيب.

٢١٢- وقد وضعت وزارة الأمن الوطني في الولايات المتحدة موجزاً قيِّماً لهذه العملية في دليل بعنوان "الممارسات المثلى لضبط الأدلة الإلكترونية: دليل الجيب لأوائل المتدخِّلين".[١٢٣] ويستعرض هذا الدليل الخطوات الآتية لحفظ الأدلة فيما يخص التحقيقات الجنائية في جرائم استخدمت فيها أجهزة حاسوب:

(١٢٣) United States, Department of Homeland Security, "Best practices for seizing electronic evidence: a pocket guide for first responders", 3rd ed. (٢٠٠٧). انظر الرابط التالي: www.forwardedge2.com/pdf/bestPractices.pdf.

الممارسات المثلى لحفظ البيانات

- لا تستخدم جهاز الحاسوب أو تحاول البحث عن أدلة
- إذا كان جهاز الحاسوب متصلا بشبكة، افصل قابس الكهرباء عن موجِّه الحركة (الراوتر) أو المودم
- قبل نقل أية أدلة، صوِّر جهاز الحاسوب فوتوغرافياً كما وُجد من مختلف الزوايا، بما فيها الأمام والخلف، وكذلك أي أسلاك أو أجهزة متصلة به والأماكن المحيطة به
- إذا كان جهاز الحاسوب مُطفأ، فلا تشغِّله
- إذا كان جهاز الحاسوب مُشغَّلا وهناك صورة تظهر على الشاشة، صوِّر الشاشة فوتوغرافياً
- إذا كان جهاز الحاسوب مُشغَّلا ولا شيء يظهر على الشاشة، حرِّك الفأرة أو اضغط على مفتاح المسافة (وهذا سوف يؤدي إلى ظهور الصورة المعروضة على الشاشة)، وبعد ظهور الصورة، صوِّر الشاشة فوتوغرافياً
- فيما يخص أجهزة الحاسوب المكتبية، افصل سلك الطاقة الموجود خلف صندوق الحاسوب
- فيما يخص أجهزة الحاسوب المحمولة، افصل سلك الطاقة؛ فإن لم ينطفئ الجهاز، اعثر على علبة البطارية وانزعها (عادة ما تكون البطارية موجودة أسفل الجهاز، وعادة ما يكون هناك زر أو مفتاح يتيح نزعها)؛ وفور نزع البطارية، لا تُعدْها إلى مكانها أو تخزِّنها في الجهاز (وهو ما يحول دون تشغيل الجهاز عن غير قصد)
- ارسم مخططاً للأسلاك وسمِّها حتى يمكن التعرف على الأجهزة المتصلة لاحقاً
- افصل جميع الأسلاك والأجهزة من صندوق الحاسوب أو الجهاز المحمول
- عبئ المكونات وانقلها (بما في ذلك موجِّه الحركة (الراوتر) والمودم، إن وجدا) باعتبارها بضائع قابلة للكسر
- قم، حيثما كان ذلك مسموحاً به بموجب بنود أي مذكرة تفتيش منطبقة، بضبط أية وسائل تخزين أخرى
- حافظ على كون جميع الوسائل، بما في ذلك صندوق الحاسوب، بعيدة عن المغنطيس وأجهزة الإرسال اللاسلكية وغيرها من العناصر التي قد تتسبب في إتلافها
- اجمع الأدلة الإرشادية، والوثائق، والملاحظات، مع الانتباه على وجه التحديد لأي شيء يمكن أن يبيِّن كلمة سر أو عبارة سر حاسوبية
- وثِّق جميع الخطوات المتَّبعة في ضبط جهاز الحاسوب ومكوِّناته.

٢١٣- وفيما يتعلق بالأجهزة النقالة، من قبيل الهواتف الذكية وأجهزة المساعدة الشخصية الرقمية، تُطبَّق مبادئ مماثلة، غير أنه يوصى بعدم إطفاء الجهاز، حيث إن هذا قد يؤدي إلى تفعيل الحماية بكلمة السر إن وجدت، بما يحول دون الوصول إلى الأدلة. ومن ثم ينبغي الإبقاء على الجهاز مشحوناً، على قدر الإمكان، أو إخضاعه للتحليل المتخصص في أقرب وقت ممكن قبل نفاد البطارية تجنباً لفقدان البيانات.

٢١٤- وتوضِّح القضية التالية من الهند أهمية التحليل الجنائي في الكشف عن البيانات الرقمية واسترجاعها، هي وغيرها من الأدلة على استخدام الإنترنت في أغراض إرهابية.

قضية ضياء الحق

المدَّعى عليه، ضياء الحق، الذي أُلقي القبض عليه في ٣ أيار/مايو ٢٠١٠ وينتظر المحاكمة في الوقت الراهن، هو عضو مزعوم في جماعة لشكر طيبه المسلحة التي تتخذ من باكستان مقراً لها، والتي تقاتل ضد السيطرة الهندية على كشمير. وقد تضمنت ادعاءات النيابة العامة، من بين جملة أمور، أنَّ ضياء الحق قد أغوي بالانضمام للجهاديين أثناء عمله في المملكة العربية السعودية بين عامي ١٩٩٩ و٢٠٠١، وتلقى تدريباً خارج الهند على استخدام السلاح والذخيرة والمتفجرات والاتصال عن طريق البريد الإلكتروني؛ واستقبل شحنة من الأسلحة والذخيرة والمتفجرات في دلهي في عام ٢٠٠٥، بعد أن طُلب منه ذلك عبر البريد الإلكتروني؛ واستخدم الإنترنت بعد ذلك للتنسيق مع أعضاء آخرين في لشكر طيبه، وتآمر لارتكاب أعمال إرهابية باستخدام الأسلحة والذخيرة والمتفجرات.

كما ادَّعت النيابة العامة أنَّ ضياء الحق قد استخدم، في ٧ أيار/مايو ٢٠٠٦، قنابل يدوية وردت إليه في شحنة الأسلحة التي أرسلتها له لشكر طيبه في هجوم على دار سينما أوديون في حيدر أباد.

وقد تم الحصول على مراسلات بالبريد الإلكتروني بين المدَّعى عليه ومرشده في التنظيم من مقدمي خدمات الإنترنت وجرى فحص محتوياتها. كما أخضعت أجهزة الحاسوب التي استخدمها الجاني في مقاهي الإنترنت للتحليل الجنائي، وتم الكشف عن الفندق الذي أقام فيه حين كان في دلهي لتسلم القنابل اليدوية، وتمت مطابقة توقيعه مع التوقيع في سجل النزلاء. وبينما كان المدَّعى عليه في السجن في انتظار المحاكمة، أُرسل التماسٌ بالتفويض القضائي من الهند إلى السلطة المركزية في بلد آخر لرفع دعوى ضد المرشد المزعوم.

وقد اتُّهم ضياء الحق بعدة جرائم في الهند، بما فيها جرائم بموجب المواد ١٥ و١٦ و١٧ و١٨ من قانون (منع) الأنشطة غير القانونية لسنة ١٩٦٧، بصيغته المعدَّلة في عامي ٢٠٠٤ و٢٠٠٨، والذي ينص على المعاقبة على الأنشطة الإرهابية، والتدريب والتجنيد لأغراض إرهابية، وجمع الأموال لأنشطة إرهابية، والتآمر لارتكاب أنشطة إرهابية.

٢١٥- ونظراً لقابلية الأدلة الرقمية للتلف، فالأفضل أن يتولى تقييمها والحصول عليها وفحصها خبراءُ تحليل جنائي مدربون خصيصا على ذلك. وفي إسرائيل، تُسلِّم التشريعات الوطنية بأهمية التدريب المتخصص، فتنص على ضرورة إسناد مهمة ضبط الأدلة الرقمية لمحققين لهم مؤهلات في مجال الحوسبة، ممن اجتازوا برنامجاً دراسياً مهنياً أساسياً، وتلقوا تدريبا مهنيا متقدما أثناء الخدمة حتى يتمكنوا من الإلمام بنظم الحاسوب، وبرمجيات متنوعة للتحليل الجنائي، والطرائق المثلى لاستخدامها. ومتى دعت الحاجة إلى تحقيق معقد للغاية، من قبيل استرجاع ملفات محذوفة، أو معيبة، أو معقدة البرمجة، أو مشفرة، يمكن الاستعانة بخبير خارجي، مع إمكانية استدعائه لاحقاً بوصفه شاهدا خبيرا من جانب النيابة العامة.[١٢٤]

٢١٦- ويُنصح بأن تُجرى أية فحوص على نسخة من الأدلة الأصلية، حتى يُمكن الحفاظ على سلامة بيانات المصدر الأصلي.[١٢٥] ويمكن إنشاء نسخة طبق الأصل من البيانات الرقمية باستخدام أدوات خاصة بالتحليل الجنائي، مثل برنامج "إن كيس" الصادر عن شركة "غايدانس" للبرمجيات وبرنامج "فورنسيك تول كيت"، أو

[١٢٤] مذكرة مكتوبة قدَّمها الخبير الإسرائيلي.

[١٢٥] United States, Department of Justice, Office of Justice Programs, National Institute of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (2004), p. 1. انظر الرابط التالي: www.ncjrs.gov/pdffiles1/nij/199408.pdf.

غيرهمـا من البدائـل المجانية. وينبغي، على قـدر الإمكان، استخـدام أداتي تحليل جنائـي مختلفتين على الأقل لإنشاء نسخ طبق الأصل، تحسباً لعدم التقاط إحدى الأداتين لكل البيانات كما يجب.[١٢٦]

٢١٧- ويُنشـئ "إن كيس" صورة طبق الأصل من البيانات على الجهـاز قيد الفحص، محللا كل شرائح القرص الصلب، بما في ذلك الشرائح غير المخصصة، لضمان الكشف عن أي ملفات مخفية أو محذوفة. ويمكن استخدام هذه البرمجية كذلك لتحليل بنية نظم الملفات على الوسائط الرقمية، وتنظيم الملفات قيد التحليل، وإعداد رسم بياني أو غير ذلك من التقارير المتعلقة بخصائص معينة للملفات، ضمن أمور أخرى. كذلك فإنَّ "إن كيس" يُنشئ ويسند للأدلة الرقمية أداة تعريف خاصة تسمى "قيمة الاختزال".[١٢٧]

٢١٨- وتأكيـداً لصحة الأدلة الرقمية في سياق الإجـراءات القانونية (انظر القسم رابعاً-دال أدناه)، فإن قيمة الاختـزال المسندة لملفات رقميـة، أو لأجزاء من ملفات رقمية، هي نتيجة خوارزمية رياضية تُطبَّق على خصائص مجموعة البيانات، بحيث يؤدي أي تغيير في مجموعة البيانات إلى توليد قيمة اختزال مختلفة. وتُولَّد قيم اختزال بخصوص مـا يلي: *(أ)* القرص الصلب الأصلـي قبل إنشـاء الصورة طبق الأصـل، و*(ب)* الصـورة أو الصور المستنسخة قبل الفحص التحليلي الجنائي، و*(ج)* الصورة أو الصور المستنسخة بعد الفحص. ويؤكد تطابقُ قيم الاختـزال عدم العبث بالأدلة الرقمية، وإمكانية اعتبـار النسخة التي خضعت للفحص التحليلي الجنائي مطابقة لبيانـات المصدر الأصلي في الإجراءات القانونيـة. وتشمل الخوارزميات الشائعة الاستخـدام خوارزمية خلاصة الرسائل (MD5) وخوارزمية الاختزال الآمن (SHA).[١٢٨]

دال- التأكد من صحة الأدلة الرقمية

٢١٩- ينبغي أن تقوم الملاحقة القضائية الفعالة لما يُشتبه فيه من حالات استخدام الإنترنت في أغراض إرهابية علـى أدلة تم جمعها بالطريقة الصحيحة وتوثيقها توثيقاً جيـداً (انظر القسم سادساً-زاي-٢). ويُعدُّ هذا الأمر ضروريـاً لإثبـات سلامة الأدلة الرقمية، حتى يتوفر لها كل من المقبوليـة في المحكمة والقدرة على الإقناع. ويمكن إثبـات سلامة الأدلة الرقمية بمزيج من تقنيات التحقيـق التقليدية والمتخصصة. ومن أهم الجوانب بهذا الشأن تسلسل العهدة لكل من الجهاز المادي المستخدَم في تخزين أو إرسال البيانات الإلكترونية والبيانات نفسها، وكذلك الإجراءات المتبعة لضبط هذه البيانات وأية انحرافات عن الإجراءات المعمول بها. وفيما يخص أساليب التحقيق التقليديـة، يجـوز لمسؤولي إنفاذ القانون القيـام بتحريات للوقوف قدر الإمكان على هويـة الجهات التي يمكن أن تكون قد قامت بمناولة الأدلة أو كانت لها القدرة على الوصول إليها قبل التحفظ عليها، وعلى الوقت الذي جُمعت فيه البيانات، وكيفية جمعها، والمكان الذي جُمعت منه.

٢٢٠- كذلـك فقـد يقتضـي الأمر من النيابـة العامة أن تبـيِّن، في جملة أمـور، أنَّ المعلومات التـي تم الحصول عليهـا نسخة صحيحة ودقيقة من البيانـات الأصلية الواردة في الوسائط وأنَّه يمكن نسبتها إلى المتَّهم. وتوفِّر قيم

(١٢٦) EC-Council Press, *Computer Forensics: Investigating Data and Image Files* (Clifton Park, New York, Course Technology Cengage Learning, 2010), p. 2-4.

(١٢٧) مذكرة مكتوبة قدَّمها الخبير الممثل لمجموعة العمليات الخاصة التابعة لقوات الدرك الإيطالية (كارابينييري).

(١٢٨) Barbara J. Rothstein, Ronald J. Hedges and Elizabeth C. Wiggins, "Managing discovery of electronic information: a pocket guide for judges" (Federal Judicial Center, 2007). انظر الرابط التالي: www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf.

الاختزال المولَّدة عن الأدلة الرقمية سنداً قوياً لعدم العبث بهذه الأدلة. ويمكن أيضاً أن تُقدَّم أدلة وشهادات أخرى إضافية إثباتاً لصحة المعلومات. ويُمكن الاطلاع على مثال إيضاحي لهذا النهج في قضية آدم باسبي، الذي أُدين في أيرلندا في عام ٢٠١٠ بإرسال تهديد بوجود قنبلة عبر البريد الإلكتروني إلى مطار هيثرو في لندن. فقد قدِّمت أثناء محاكمة باسبي، بالإضافة إلى أدلة تبيِّن أن رسالة البريد الإلكتروني قد أُرسلت من جهاز حاسوب معيَّن كان للمتهم القدرة على استخدامه، نسخ ورقية من سجلات جهاز الحاسوب ولقطات تلفزيونية مصحوبة بحاشية تعرض نص الحوار لإثبات الوقت الذي أُرسلت فيه رسالة البريد الإلكتروني وكون المتهم هو الشخص المتحكِّم في جهاز الحاسوب في ذلك الوقت.

هاء- وحدات عمليات الجرائم السيبرانية

١- *وحدات مكافحة الجرائم السيبرانية الوطنية أو الإقليمية*

٢٢١- لقد أدَّى الاعتماد المتزايد على تكنولوجيا الحاسوب إلى زيادة هائلة في الطلب على وحدات متخصصة في مكافحة الجرائم السيبرانية لتستجيب لطلبات استرجاع أدلة حاسوبية في إطار التحليل الجنائي، ولا يقتصر ذلك على القضايا الإرهابية التي يستخدم فيها الإنترنت. فالجريمة المنظمة من قبيل الاتِّجار بالمخدِّرات، والاتِّجار بالأشخاص، والعصابات الدولية لاستغلال الأطفال جنسياً، تُعدُّ أمثلة على حالات تفشَّى فيها استخدام الإنترنت استخداماً إجرامياً على نطاق واسع، إلا أنَّ السنوات الأخيرة قد شهدت زيادة في درجة احتواء القضايا على نوع من أنواع الأدلة الحاسوبية أو الإلكترونية. ويمكن أن يؤدي إنشاء وحدات وطنية لمكافحة الجرائم السيبرانية لديها مهارات متخصصة في التحقيق في هذه الجرائم إلى التعزيز كثيراً من قدرة الدولة التي تقوم بذلك على الاستجابة للطلبات بهذا الشأن عملياتياً. ومن الممكن، حسب العوامل الجغرافية والاحتياجات من الموارد، أن تتعزز الوحدات الوطنية بوحدات إقليمية أصغر لتلبية الاحتياجات المحلية. وبالإضافة لذلك، قد يكون وضع الوحدات الإقليمية تحت قيادة الإدارة الإقليمية المحلية أكثر كفاءة وتوفيراً للنفقات.

٢٢٢- ومن بين المسؤوليات التي يُمكن أن تضطلع بها وحدات مكافحة الجرائم السيبرانية الوطنية أو الإقليمية ما يلي:

(أ) جمع المعلومات الاستخبارية من مصادر علنية باستخدام تقنيات مراقبة الإنترنت المتخصصة من مواقع التواصل الاجتماعي، ومنتديات الدردشة، والمواقع الشبكية، ونظم لوحات الإعلان الإلكترونية، للكشف عن أنشطة الجماعات الإرهابية (ضمن العديد من العناصر الإجرامية الأخرى). وفيما يخص الجماعات الإرهابية، يمكن أن تُدرج هذه الوظيفة ضمن اختصاصات وحدات مكافحة الإرهاب التي يكون أفرادها مؤهلين ومحنكين بما يكفي للقيام بهذه المهمة، بيد أنَّ التدريب المتخصص في سياق الجرائم الحاسوبية يعتبر تدريبا أساسيا للاضطلاع بهذا الدور. كما أنَّ وظيفة جمع المعلومات الاستخبارية تستلزم التقييم والتحليل بما يساعد على وضع استراتيجية لمكافحة الخطر الذي يشكِّله استخدام الإرهابيين للإنترنت. إلا أنَّ تضارب المسؤوليات أو الأهداف فيما بين أجهزة الاستخبارات الوطنية قد يقف حائلا دون التنسيق بينها وترجمة المعلومات الاستخبارية إلى خطط عملياتية فعَّالة؛

(ب) الاضطلاع بالتحقيقات المتخصصة في الجرائم السيبرانية في القضايا الجنائية الوطنية والدولية المتعلقة بالتكنولوجيا، مثل قضايا الاحتيال عبر الإنترنت أو سرقة البيانات وغيرها من القضايا التي

تنشأ فيها مسائل معقدة فيما يخص التكنولوجيا والقانون والإجراءات، وترى إدارة وحدة مكافحة الجرائم السيبرانية ضرورة الاستعانة بخبراء التحقيق لديها؛

(ج) القيام بدور حلقة الوصل مع مختلف الدوائر المعنية ومع الجهات الدولية لإقامة شراكات مع أصحاب المصلحة الرئيسيين في مكافحة الجرائم السيبرانية، من قبيل قطاعات الخدمات المالية، وخدمات الاتصالات، والحوسبة، والجهات الحكومية المعنية، والمؤسسات الأكاديمية، والمنظمات الحكومية الدولية أو المنظمات الإقليمية؛

(د) إنشاء وحدة لتقييم قضايا الجرائم السيبرانية وطنياً ودولياً لتحديد أولوية التحقيق فيها من قبل وحدات مكافحة الجرائم السيبرانية الوطنية أو الإقليمية. كما يمكن أن تكون هذه الوحدة مسؤولة عن إعداد إحصاءات حول وقوع الجرائم السيبرانية؛

(هـ) توفير التدريب والبحث والتطوير، إذ إنَّ الطبيعة المعقَّدة والمتغيرة للجرائم السيبرانية تتطلب دعما علميا من المؤسسات الأكاديمية المتخصصة لضمان تزويد الوحدات الوطنية والإقليمية بكل ما يلزم من مهارات وأدوات تكنولوجية، وتدريب، وتثقيف، للقيام بفحوص التحليل الجنائي للوسائط الحاسوبية وللتحقيق في الجرائم السيبرانية.

٢- *وحدات فرز الأدلة الحاسوبية بغرض التحليل الجنائي*

٢٢٣- يُمكن إنشاء وحدات لفرز الأدلة الحاسوبية بغرض التحليل الجنائي لمساندة وحدات مكافحة الجرائم السيبرانية الوطنية أو الإقليمية. ويتلقى أفراد هذه الوحدات تدريباً على الفحص الحاسوبي بغرض التحليل الجنائي باستخدام أدوات برمجية مُعدَّة خصيصاً لهذا الغرض في المواقع الخاضعة للتفتيش. فيمكن أن يُجري أحد أعضاء فرق الفرز فحصاً أولياً في الموقع، إما لاستبعاد أجهزة حاسوب أو معدات حاسوبية طرفية من التحقيق لأنها بلا قيمة استدلالية، أو لمصادرة الأدلة الحاسوبية وفقاً لتقنيات التحليل الجنائي السليمة، فضلا عن مساعدة فرق التحقيق المحلية في استجواب المشتبه بهم فيما يخص ما تم اكتشافه من أدلة حاسوبية. ويُمكن، عند الضرورة، أن تُسلَّم الوسائط الحاسوبية التي ضبطتها وحدات الفرز إلى وحدة مكافحة الجرائم السيبرانية الإقليمية المعنية أو إلى الوحدة الوطنية لمكافحة هذه الجرائم، حسب الاقتضاء، حتى يتأتى إخضاعها لتحليل جنائي شامل.

٢٢٤- وثمة، في الوقت الراهن، باحثون من جامعة دبلن يعملون على إعداد مجموعة من البرمجيات باعتبارها أدوات للتحليل الجنائي لتسهيل التحليل الأولي. وهي أدوات ستتاح لمسؤولي إنفاذ القانون دون مقابل. ويندرج إعداد هذه الأدوات في إطار حل استراتيجي أعم يستكشفه حاليا كل من مركز الأمن السيبراني والتحقيق في الجرائم السيبرانية التابع لجامعة دبلن ووحدة التحقيق في الجرائم الحاسوبية للشرطة الوطنية الإيرلندية، بهدف مساعدة وحدات مكافحة الجرائم السيبرانية التي تعاني من نقص الموارد بسبب ميزانياتها وعدد أفرادها المحدودَيْن على تصريف أعمالها. وتهدف هذه المبادرة إلى إنشاء مختبر تحليل جنائي "مفتوح المصدر" بالكامل. وسوف يتلقى المحققون المشاركون تدريبا بشأن إحداث معدات تخزين الأدلة الحاسوبية ومعالجتها، كما سيُدرَّبون على استخدام أدوات التحليل الجنائي المجانية.

واو- جمع المعلومات الاستخبارية

٢٢٥- يعـدُّ جمع المعلومات الاستخبارية من بـين المكوِّنات الرئيسية لأنشطة مكافحة الإرهـاب، إذ إنَّ المعلومات التي يتم الحصول عليها عبر هذه القنوات كثيراً ما تكون حافزاً لإجراء تحقيقات تؤدي إلى ملاحقة المشتبه فيهم قضائيـاً، أو تُستخدم باعتبارها أدلة في المحاكمة، في حدود ما يسمح به القانون والقواعد الإجرائية على الصعيد الوطنـي. غـير أنَّ اختلاف الأغراض التـي تُجمع من أجلها المعلومـات الاستخبارية، واختـلاف الجهات التي قد تحصـل على هذه المعلومات أو تستخدمها، قد يقتضيان الموازنة الدقيقة فيما بين المصالح المتضاربة. فعلى سبيل المثـال، قد تـولي أجهزة إنفاذ القانون أو الاستخبـارات المعنية بالحصول على معلومـات استخبارية عناية كبيرة لحماية سرية مصادر المعلومات، في حين يتعين علىَ مسؤولي المحكمة، في جملة أمور، أن يضعوا بعين الاعتبار حق المدَّعـى عليـه في المحاكمة العادلة وحصوله على فرصة متكافئة للاطلاع على الأدلة المقدمة ضده. ومن ثم ينبغي إيـلاء العناية الواجبـة لضمان وجود ضوابط وموازيـن ملائمة فيما يخص حقوق الإنسـان الأساسية المنصوص عليها في الاتفاقيات الدولية المنطبقة.[١٢٩]

٢٢٦- ولا تُقبـل في بعض الدول الأعضـاء المصادر المجهولـة باعتبارها أدلـة في المحكمة؛ إلا أنَّـه يُمكن النظر في المعلومـات الاستخباريـة المعزَّزة بمصادر موثوقـة أو بأدلة إضافية. فعلى سبيل المثـال، ففي إيرلندا، قد تعتبر المعلومـات الاستخباريـة التي تُجمـع عن الإرهابيين في حكـم القرينة الظاهرة على عضوية فـرد بعينه في تنظيم غـير قانـوني إذا ما قدَّم هذا الدليل بعد تأديـة اليمين ضابطٌ شرطة لا تقل رتبته عن رئيـس. وقد أيَّدت المحكمة الإيرلندية العليا استخدام معلومات استخبارية من هذا القبيل باعتبارها أدلة، في وجود أدلة أخرى تعززها، حين يحول الخوف من الانتقام دون الإدلاء بشهادة مباشرة ويكون الشاهد الذي يقدِّم الدليل ضابطا رفيعا.[١٣٠]

٢٢٧- كمـا سلَّـط العديد من الخبراء الضـوء على التضارب فيما بـين الحاجة لتشجيع توافـر المعلومات بشأن الأنشطة الإرهابية التي قد تُرتكب عن طريق الإنترنت والحاجة لاعتقال مقترفي هذه الأنشطة وملاحقتهم قضائياً. فعلـى سبيل المثال، قد تدرس أجهزة الأمن القومي، بعد الوقوف على أنشطة يُحتمل اتصالها بالإرهاب على موقع شبكـي، الآثار الطويلة الأمد والقصيرة الأمد لعمليات التصدي للأنشطة المذكورة. وقد تشمل هذه التدابير رصد النشاط على الموقع الشبكي لأغراض استخبارية، أو الانخراط سراً في المناقشة مع المستخدمين الآخرين للحصول علـى مزيد مـن المعلومـات لأغراض مكافحة الإرهـاب، أو إغـلاق الموقع الشبكـي. فالأهـداف والاستراتيجيات المختلفـة باختلاف الجهات المحلية والأجنبية المعنيـة هي التي توجِّه اختيار إجراءات معينة لمكافحة الإرهاب دون غيرها.[١٣١]

٢٢٨- وقـد سلَّـط تقرير حديث صادر عن مركـز بحوث الكونغرس بالولايات المتحدة الضـوء على الاعتبارات العملية عند تقييم القيمة الاستخبارية مقابل مستوى الخطر الذي يشكِّله نشاط ما على الإنترنت:

---

[١٢٩] انظـر، علـى سبيـل المثـال، المادة ١٠ مـن الإعلان العالمي لحقـوق الإنسان، والمـادة ١٤ من العهـد الدولي الخاص بالحقـوق المدنية والسياسية، والمادة ٦ من الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية.

[١٣٠] *People (DPP) v. Kelly,* [2006] 3 I.R. 115.

[١٣١] Catherine Theohary and John Rollins, Congressional Research Service (United States), "Terrorist use of the Internet: information operations in cyberspace" (8 March 2011), p. 8.

على سبيل المثال، صمَّمت [وكالة الاستخبارات المركزية الأمريكية] وحكومة المملكة العربية السعودية، وفق ما ورد من أنباء، فخاً شبكياً ("هاني بوت") على هيئة موقع جهادي لجذب الأنشطة الإرهابية ورصدها. وقد استخدم محللو الاستخبارات المعلومات التي تم جمعها من الموقع لتتبع الخطط العملياتية للجهاديين، وهو ما أسفر عن إلقاء القبض على عدد منهم قبل تمكنهم من تنفيذ الهجمات المخطط لها. غير أنَّ الأنباء تفيد كذلك بأنَّ الموقع كان يُستخدم لإرسال خطط عملياتية لجهاديين يدخلون العراق للقيام بعمليات ضد القوات الأمريكية. وخلصت المناقشات فيما بين [وكالة الأمن القومي، ووكالة الاستخبارات المركزية، ووزارة الدفاع، ومكتب مدير الاستخبارات الوطنية، ومجلس الأمن القومي] إلى أنَّ الخطر على القوات في مسرح العمليات أكبر من القيمة الاستخبارية لرصد الموقع الشبكي، وفي نهاية المطاف قام فريق مختص بالشبكات الحاسوبية [تابع لفرقة العمل المشتركة- عمليات الشبكية العالمية] بتفكيك الموقع.[١٣٢]

وكما هو مبيَّن في الحالة المذكورة، فإنَّ التنسيق فيما بين مختلف الجهات عامل مهم في التصدي بنجاح للمخاطر التي يتم الوقوف عليها.

٢٢٩- وقد أشارت دول أعضاء أخرى، مثل المملكة المتحدة، إلى أنَّها قد أولت عناية كبيرة لإرساء علاقات عمل وإبرام مذكرات تفاهم بين النيابة العامة من ناحية وأجهزة إنفاذ القانون والاستخبارات من ناحية أخرى، وهو ما أسفر عن نتائج إيجابية. وبالمثل، يعد المركز المتكامل للاستخبارات والتحقيقات (CI3) الجهة المحلية التي تنسِّق التحقيقات في الأنشطة الإرهابية المشتبه بها في كولومبيا بالاستعانة باستراتيجية تقوم على دعائم ست. وبموجب هذا النهج، يتولى مسؤول رفيع المستوى من الشرطة الوطنية القيادة العامة لمختلف مراحل التحقيق، بما يشمل جمع الأدلة، والتحقق منها، وتحليلها، إلى جانب مرحلة قضائية تجمع فيها الشرطة المعلومات عن الأطراف والأماكن المرتبطة بارتكاب أي جريمة.[١٣٣]

٢٣٠- وقد بيَّن الخبير الفرنسي معالم النهج المحلي تجاه تنسيق مختلف الجهات لتدابير التصدي للأنشطة الإرهابية التي يتم الوقوف عليها:

- المرحلة الأولى: تقف جهات المراقبة والاستخبارات على تهديد عبر رصدها لأنشطة الإنترنت
- المرحلة الثانية: تُخطر جهات المراقبة النيابة العامة بالتهديد الذي تم الوقوف عليه. وبعد ذلك يُمكن للقاضي أو لعضو النيابة العامة أن يصرِّح لسلطات إنفاذ القانون بمراقبة النشاط الشبكي للشخص الذي كُشف عن كونه مشتبها به. واعتباراً من عام ٢٠١١، تُتيح التشريعات للقاضي الرئيسي التصريح لسلطات إنفاذ القانون بتسجيل البيانات الحاسوبية للشخص المرصود. وعلاوة على ذلك، يُمكن طلب البيانات الشخصية (مثل الاسم، ورقم الهاتف، ورقم بطاقة الائتمان) من مقدمي الخدمات المعنيين
- المرحلة الثالثة: يُجرى التحقيق على أساس الأدلة التي يتم جمعها من المصادر المبيَّنة في المرحلتين الأولى والثانية.

[١٣٢] المرجع نفسه، الصفحة ١٣.

[١٣٣] مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة، *خلاصة قضايا الإرهاب*، الفقرة ١٩١.

زاي- التدريب

٢٣١- يحتاج مسؤولو إنفاذ القانون القائمون على التحقيق في قضايا استخدام الإنترنت في أغراض إرهابية إلى تدريب متخصص في الجوانب التقنية المتعلقة بالطريقة التي يُمكن بها للإرهابيين وغيرهم من المجرمين أن يستخدموا شبكة الإنترنت لدعم أغراض غير مشروعة، وكذلك بالطريقة التي يمكن بها لسلطات إنفاذ القانون أن تستخدم الإنترنت بفعالية باعتبارها وسيلة لرصد أنشطة الجماعات الإرهابية. ويمكن إتاحة التدريب عبر مبادرات من القطاع العام أو القطاع الخاص، أو عبر مزيج من الاثنين معاً.

٢٣٢- ويمكن إتاحة برامج دراسية حول التحليل الجنائي لتكنولوجيا المعلومات والتحقيق في الجرائم السيبرانية على المستوى الإقليمي أو الدولي من قِبل منظمات مثل اليوروبول والإنتربول. وبالإضافة إلى ذلك، وضع عدد من البلدان برامج تدريب خاصة به لإنفاذ القانون في مجال مكافحة الجرائم السيبرانية، إما فرادى أو بالتعاون مع معاهد أكاديمية. ويمكن إتاحة التدريب أيضاً عبر دورات تدريبية حسب الحاجة وندوات ومؤتمرات وبرامج تدريب عملية، يقدِّمها القطاع العام أو أصحاب المصلحة في القطاعات ذات الصلة.

٢٣٣- كما يمكن إتاحة التدريب المتخصص عبر مؤسسات أكاديمية، مثل جامعة دبلن في إيرلندا، التي أنشأت في عام ٢٠٠٦ مركز الأمن السيبراني والتحقيق في الجرائم السيبرانية. وتشمل البرامج التي تقدِّمها الكلية دراسات مخصصة للعاملين في مجال إنفاذ القانون للحصول على درجة الماجستير في حوسبة التحليل الجنائي والتحقيق في الجرائم السيبرانية. كما توفِّر برامجُ دراسيةٌ أخرى التدريبَ لأوائل المتدخلين لدعم دورهم العملياتي فيما يتصل بقضايا الجرائم السيبرانية.

٢٣٤- وشبكة المراكز المتميزة للتدريب والبحوث والتثقيف في مجال مكافحة الجرائم السيبرانية هي مشروع ممول من قبل المفوضية الأوروبية أُطلق في عام ٢٠١٠، بهدف إنشاء شبكة من المراكز المتميزة للتدريب والبحوث والتثقيف في مجال مكافحة الجرائم السيبرانية في أوروبا. وهناك مراكز في إستونيا وإيرلندا وبلجيكا وفرنسا في طور التأسيس. ويقوم كل مركز وطني على أساس شراكة بين ممثلين عن سلطات إنفاذ القانون والقطاع المعني وأكاديميين للتعاون على تحديد البرامج التدريبية والمؤهلات اللازمة، إلى جانب أدوات تُستخدم في مكافحة الجرائم السيبرانية. ويتولى مركز الأمن السيبراني والتحقيق في الجرائم السيبرانية التابع لجامعة دبلن دورا قياديا وتنسيقيا في المشروع.[١٣٤]

٢٣٥- كما يمكن إتاحة التدريب على مكافحة الإرهاب على شبكة الإنترنت عبر منبر التعلّم في مجال مكافحة الإرهاب التابع لمكتب الأمم المتحدة المعني بالمخدِّرات والجريمة، الذي أُطلق في عام ٢٠١١.[١٣٥] والمنبر أداة تفاعلية مصمَّمة خصيصاً لتدريب الأخصائيين الممارسين في مجال العدالة الجنائية على مكافحة الإرهاب، مع إتاحة إمكانية التقائهم في مجتمع افتراضي واحد يمكنهم من تبادل خبراتهم ووجهات نظرهم في مجال مكافحة الإرهاب. وبالإضافة للسماح للممارسين الذين سبق لهم المشاركة في التدريب الذي يوفره مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة بالتواصل مع نظرائهم، فإنَّ المنبر يتيح لهم مواكبة التطورات القانونية في المجال، والاطلاع على فرص التدريب المقبلة، والانخراط في أنشطة التعلم المستمر.

[١٣٤] انظر: www.2centre.eu.

[١٣٥] انظر: www.unodc.org/unodc/en/terrorism/unodc-counter-terrorism-learning-platform.html.

خامساً- التعاون الدولي

ألف- مقدِّمة

٢٣٦- إنَّ السرعة التي يُمكن أن يستخدم بها الإرهابيون الإنترنت في الترويج لأفكارهم أو في تيسير ارتكاب أعمالهم الإرهابية وامتداد هذا الاستخدام على النطاق العالمي وإمكانية إخفاء هويتهم نسبيا، إلى جانب التعقيدات المتعلقة بمكان وجود البيانات ذات الصلة بالإنترنت والاحتفاظ بها وضبطها وتقديمها، كلها أمور تجعل فعالية التعاون الدولي وتوقيته المناسب من العوامل المتزايدة الأهمية في نجاح التحقيقات والملاحقة القضائية في العديد من قضايا الإرهاب.

باء- الصكوك والترتيبات المتعلقة بالتعاون الدولي

١- *الصكوك العالمية لمكافحة الإرهاب*

٢٣٧- تحتوي الصكوك العالمية لمكافحة الإرهاب، التي تتألف من اتفاقيات وبروتوكولات دولية فضلا عن قرارات مجلس الأمن ذات الصلة، على آليات شاملة للتعاون الدولي فيما يخص الإجراءات الجنائية المتعلقة بالإرهاب. وتنص هذه الصكوك على تسليم المطلوبين، وتقديم المساعدة القانونية المتبادلة، ونقل الإجراءات الجنائية والأشخاص المدانين، والتنفيذ المتبادل للأحكام، وتجميد الموجودات وضبطها، وتبادل المعلومات فيما بين أجهزة إنفاذ القانون.

٢٣٨- وتشمل العناصر الرئيسية المتعلقة بالتعاون الدولي في صكوك مكافحة الإرهاب:

- الالتزام بتقديم مرتكبي الأعمال الإرهابية للعدالة
- الالتزام بتسليم المطلوبين أو ملاحقتهم قضائياً (مبدأ: إما التسليم وإما المحاكمة)
- الالتزام بتحديد الاختصاص القضائي في ظروف محددة
- الالتزام بعدم اعتبار استثناء الجرائم السياسية أساساً لرفض طلب للتعاون
- احترام سيادة القانون وحقوق الإنسان
- احترام مبدأ ازدواجية التجريم
- احترام قاعدة التخصص
- احترام مبدأ "*عدم جواز المحاكمة على ذات الجريمة مرتين*".[١٣٦]

[١٣٦] مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة، *دليل التعاون الدولي في المسائل الجنائية لمكافحة الإرهاب* (٢٠٠٩)، الباب ١.

٢٣٩- وتندرج المبادئ العامة المنطبقة على تسليم المطلوبين والمساعدة القانونية المتبادلة في قضايا الإرهاب أو الجريمة المنظمة العابرة للحدود الوطنية في إطار الآليات الشاملة المنصوص عليها في الصكوك العالمية لمكافحة الإرهاب وغيرها من الصكوك التي تتناول الجريمة المنظمة العابرة للحدود الوطنية (كاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية على سبيل المثال).[١٣٧] وليس من بين مقاصد هذا المنشور أن يسرد أو يحلل بتفصيل الطريقة التي ينبغي للدول أن تنفِّذ بها هذه المبادئ على المستوى الوطني، وإنما ينصب التركيز هاهنا على تحديد المسائل التي تخص قضايا الإرهاب التي تُستخدم فيها الإنترنت، في إطار التعاون الدولي العام الذي تؤسس له هذه الصكوك، وبالإشارة إلى المبادئ والآليات المقررة، بغية توجيه مقرري السياسات العامة والممارسين بشأن النهوج أو الاستراتيجيات التي تتبع فيها الممارسات الجيدة الراهنة.

(أ) عدم وجود صك عالمي بشأن المسائل السيبرانية

٢٤٠- لئن كان من المرجح أن تهيئ آليات التعاون الدولي في الصكوك العالمية لمكافحة الإرهاب، في حال تنفيذها تنفيذا تاما، أساساً قانونياً للتعاون في العديد من القضايا التي ترتكب فيها أعمال عبر الإنترنت يقوم بها أشخاص ضالعون في ارتكاب تصرفات غير قانونية تجرّمها هذه الصكوك، فليس من بين هذه الصكوك ما يتناول خصيصاً الأعمال ذات الصلة بالإنترنت في حد ذاتها. وفي ظل عدم وجود صك لمكافحة الإرهاب يتناول خصيصاً قضايا الإنترنت المتصلة بالإرهاب، فستستمر السلطات، حين تُحقق في هذه القضايا وتلاحق الجناة قضائياً، في استنادها إلى ما هو قائم من المعاهدات أو الترتيبات الدولية أو الإقليمية التي وُضعت لتيسر التعاون الدولي على التحقيق في جرائم الإرهاب أو الجريمة المنظمة العابرة للحدود الوطنية بشكل عام والملاحقة القضائية بشأنها.

٢٤١- ومن الواضح أنَّ عدم وجود صك لمكافحة الإرهاب يتناول خصيصاً المسائل السيبرانية يعرقل، إلى حد ما، التعاون الدولي بشأن التحقيق في قضايا الإرهاب التي تُستخدم فيها الإنترنت في أغراض إرهابية والملاحقة القضائية بشأنها. بيد أنّ هذه الوثيقة لا تهدف إلى تقييم المزايا النسبية للحجج المؤيدة أو المعارضة لوضع صك عالمي شامل يتناول، ضمن أمور أخرى، التعاون الدولي في القضايا الجنائية (بما يشمل الإرهاب) التي تنطوي على مسائل سيبرانية، وإنما ينصب التركيز هاهنا على تحديد العقبات الموجودة في الإطار الدولي القائم أمام هذا التعاون، والطريقة التي يُمكن أن تستخدم بها السلطات الوطنية ما هو متاح من الصكوك والترتيبات القائمة لتيسير أو تعزيز التعاون الدولي في قضايا الإرهاب التي تنطوي على جانب من جوانب استخدام الإنترنت.

(ب) صكوك أخرى: اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية واتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي

٢٤٢- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية هي الصك الدولي الرئيسي الذي يتناول التعاون الدولي بشأن الأشكال الخطيرة من الجريمة المنظمة العابرة للحدود الوطنية. فالمواد ١٦ (تسليم المجرمين)، و١٨ (المساعدة القانونية المتبادلة)، و١٩ (التحقيقات المشتركة)، و٢٧ (التعاون في مجال إنفاذ

[١٣٧] الأمم المتحدة، *مجموعة المعاهدات*، المجلد ٢٢٢٥، الرقم ٣٩٥٧٤.

القانـون) من الاتفاقية تتناول التعاون الدولي. وبالرغم من أنَّ التصرفات غير القانونية المشار إليها في الاتفاقية تتناول الجريمة المنظمة العابرة للحدود الوطنية، لا الإرهاب، فإنَّ مبادئ الاتفاقية وآلياتها الأساسية فيما يخص التعـاون الدولي تشبـه كثيراً المبادئ والآليـات المنصوص عليهـا في الصكوك العالمية لمكافحـة الإرهاب. ومن ثم يفترض أن يكون لدى الـدول الأطراف التي نفَّذت التزاماتها فيما يخص التعـاون الدولي بموجب هذه الصكوك أطر وآليات متساوقة إلى حد كبير.

٢٤٣- وبالإضافـة إلى اتفاقيـة مجلس أوروبـا المتعلقة بجرائم الفضـاء الحاسوبي، فإنَّ اتفاقيـة مجلس أوروبا المتعلقـة بمنع الإرهـاب، والاتفاقية الأوروبيـة بشأن تسليم المطلوبـين،[١٣٨] وبروتوكولاتها الثلاثـة الإضافية،[١٣٩] والاتفاقيـة الأوروبيـة للمساعـدة المتبادلـة في المسائـل الجنائيـة،[١٤٠] وبروتوكوليهـا الإضافيـين،[١٤١] وقانـون مجلـس الاتحاد الأوروبـي 2000/C 197/01 [الصـادر في ٢٩ أيار/مايـو ٢٠٠٠] الذي أنشأ، وفقـاً للمادة ٣٤ من معاهـدة الاتحـاد الأوروبـي، الاتفاقيـة بشـأن المساعـدة المتبادلـة في المسائل الجنائيـة بين الـدول الأعضاء في الاتحـاد الأوروبي، قـد تهيئ أساساً قانونياً للتعـاون الدولي في قضايا الإرهاب المنطويـة على عنصر من عناصر استخدام الإنترنت.

٢٤٤- وتحتـوي اتفاقية مجلس أوروبـا المتعلقة بجرائم الفضاء الحاسوبي على أحكام تهدف إلى تشجيع التعاون الدولي من خلال آليات لتعاون الشُرطة والقضاء وتدابير مؤقتة في الحالات العاجلة، مثل توفير المعلومات تلقائياً بصفة غير رسمية عند الطلب (المادة ٢٦) وإنشاء نقاط اتصال تعمل على مدار الساعة طيلة أيام الأسبوع (المادة ٣٥). ويمكـن أن يصحـب هـذه الطلبات طلـب بعدم الإفشـاء، كما يمكنهـا أن تتيح آليـة قانونية تمكّن مـن استخدام الوسائـل غـير الرسميـة للاتصال وتبـادل المعلومات بين أطـراف الاتفاقية، ولو لم يكن ذلـك منصوصاً عليه في تشريعاتها الوطنية.

٢٤٥- وتجـدر الإشـارة إلى أنَّ اتفاقيـة مجلـس أوروبـا المتعلقـة بجرائـم الفضـاء الحاسوبي ليسـت مفتوحة أمـام أعضـاء مجلـس أوروبـا أو الـدول غير الأعضـاء التي شاركـت في وضعها فحسـب، وإنما يُمكـن أن ينضم إليهـا أيضـاً غيرها من الـدول غير الأعضاء، شريطـة موافقة الدول المتعاقـدة التي يحق لهـا المشاركة في لجنة الوزراء بالإجماع.

٢- *الترتيبات الأخرى الإقليمية أو المتعددة الأطراف*

٢٤٦- بالإضافة إلى الصكوك الدولية والإقليمية المذكورة آنفاً، قد تختار الدول الدخول في معاهدات أو ترتيبات ثنائيـة أو متعـددة الأطراف تنص خصيصـاً على التعاون فيما يخصـ الأنشطة السيبرانيـة المرتبطة بالإرهاب أو الجريمـة العابـرة للحـدود الوطنية. وعادة مـا يُنظَّم كل مـن تسليم المطلوبـين والمساعدة القانونيـة المتبادلة إمـا بالمعاهـدات أو "القانون غـير الملزم" الذي تتفق عليه تجمعـات من البلدان. ومع ذلـك، فالمنظمات الإقليمية

(١٣٨) Council of Europe, *European Treaty Series*, No. 24.

(١٣٩) المرجع نفسه، الأرقام ٨٦ و٩٨ و٢٠٩.

(١٤٠) المرجع نفسه، رقم ٣٠.

(١٤١) المرجع نفسه، رقما ٩٩ و١٨٢.

ودون الإقليمية تؤدي كذلك دوراً هاماً في تيسير تبادل المعلومات والتعاون بموجب هذه الترتيبات المتفق عليها اتفاقا متبادلا.

(أ) أمر التوقيف الأوروبي: إطار عمل شينغن

٢٤٧- يعد أمر التوقيف الأوروبي المندرج في إطار عمل شينغن أداةً للتعاون يُمكن استخدامها في جميع الدول الأعضاء في الاتحاد الأوروبي؛ وقد ثبت أنَّها مفيدة للغاية في تعزيز التعاون القانوني في التحقيق في القضايا الجنائية والملاحقة القضائية بشأنها، بما في ذلك القضايا المتعلقة بالإرهاب في أوروبا. ويقتضي أمر التوقيف، فور إصداره، أن تقوم سلطات دولة عضو أخرى، على أساس المعاملة بالمثل، بإلقاء القبض على الشخص المشتبه بكونه ارتكب جريمة أو الشخص المحكوم عليه ونقله إلى الدولة التي أصدرت الأمر حتى تتأتى محاكمة ذلك الشخص أو إيداعه السجن لاستكمال مدة حبسه. وفي هذا السياق، تجدر الإشارة إلى أنَّ أمر التوقيف الأوروبي ينص، في جملة أمور أخرى، على تسليم المطلوبين الذين يحملون جنسية الدولة العضو التي يصدر عنها الأمر،وهو مفهوم كان غير مألوف قبل ذلك في الأحكام القانونية (الدستورية في كثير من الأحيان) للعديد من الدول التي تعتمد ما يسمى بالنظام الأوروبي القاري.

(ب) الأمر الأوروبي بالبحث عن الأدلة

٢٤٨- أصبح هناك، منذ دخول الأمر الأوروبي بالبحث عن الأدلة حيز النفاذ في عام ٢٠٠٩، وعلى غرار أمر التوقيف الأوروبي فيما يخص التوقيف، إجراءٌ مبسط لتقديم ونقل الأدلة، بما في ذلك الأشياء والوثائق والبيانات، فيما بين الدول الأعضاء لاستخدامها في الإجراءات القانونية. ويمكن أن تشمل الأدلة المجموعة في إطار الأمر الأوروبي بالبحث عن الأدلة بيانات العملاء ذات الصلة بالإنترنت.[١٤٢]

٢٤٩- وباستخدام هذه القرارات الإطارية وغيرها من الصكوك الدولية، أرست الدول الأوروبية، مجتمعة، نهجاً جماعياً إلى حد كبير ومتطورا للغاية لجمع الأدلة وإرسالها عبر الحدود وتسليم المطلوبين من الجناة في إطار الإجراءات القانونية. ولعل الحكومات الأخرى تستصوب، على المستوى السياسي والعملياتي، اعتماد نهج جماعي في تنسيق جهودها للتعاون في التحقيقات والملاحقة القضائية عبر الحدود فيما يخص الجرائم المتعلقة بالإرهاب وتكييف هذا النهج وفقاً لاحتياجاتها على المستوى الإقليمي أو دون الإقليمي.

(ج) نظاما الكومنولث المتعلقان بتسليم المطلوبين والمساعدة القانونية المتبادلة

٢٥٠- يوفر نظام الكومنولث لنقل المجرمين المدانين (نظام لندن)، على غرار أمر التوقيف الأوروبي المندرج في إطار عمل شينغن، آلية مبسَّطة لتسليم المطلوبين بين بلدان الكومنولث، إذ يتيح توقيف المجرمين احتياطياً استناداً إلى أمر توقيف صادر من بلدان أعضاء أخرى، دونما حاجة لتقييم كفاية الأدلة ضد المشتبه به. ويعتبر النظام الفعلَ المجرم في كلا البلدين الذي يعاقَب عليه بالسجن لسنتين أو أكثر جريمةً تستدعي تسليم المطلوبين.

(١٤٢) Voislav Stojanovski, "The European evidence warrant", *Dny práva — 2009 — Days of Law: the Conference Proceedings*, 1st. ed., David Sehn?lek and others, eds. (Brno, Czech Republic, Masaryk University, 2009).

٢٥١- وبالمثل، فإنَّ نظام الكومنولث المتعلق بالمساعدة المتبادلة في المسائل الجنائية (نظام هراري) يهدف إلى زيادة مستوى التعاون وتوسيع نطاقه فيما بين بلدان الكومنولث في المسائل الجنائية عبر تيسير الكشف عن هوية الأشخاص وأماكن وجودهم، وتبليغ الوثائق القضائية، وسؤال الشهود، والتفتيش وضبط الأدلة، واستدعاء الشهود، والنقل المؤقت للأشخاص المحتجزين للإدلاء بشهادتهم، وتقديم السجلات القضائية أو الرسمية، واقتفاء أثر عائدات الجريمة أو الوسائل المستخدمة فيها وضبطها ومصادرتها، وحفظ البيانات الحاسوبية.

٢٥٢- ونظاما الكومنولث، وإن لم يكونا معاهدتين بكل معنى الكلمة، نموذجان من الترتيبات غير الملزمة، أو "القانون غير الملزم"، اتفقت بموجبهما دول بعينها على أن تدرج في قوانينها المحلية تشريعات متساوقة طبقا للمبادئ المتفق عليها، لتبسيط عمليات تسليم المطلوبين والمساعدة القانونية المتبادلة فيما بينها في القضايا الجنائية، بما في ذلك التحقيقات والملاحقات القضائية المتعلقة بالإرهاب.

(د) مجلس أوروبا

٢٥٣- بالإضافة إلى وضع صكوك تهدف إلى تعزيز التعاون الدولي في القضايا الجنائية السيبرانية، بما في ذلك قضايا الإرهاب، أنشأ مجلس أوروبا أيضاً (بموجب المادة ٣٥ من اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الحاسوبي) شبكة نقاط الاتصال الدائم التابعة لمجلس أوروبا التي تعمل على مدار الساعة طيلة أيام الأسبوع لتيسير التعاون الدولي في قضايا الجرائم السيبرانية. ويدعم مشروعا مجلس أوروبا والاتحاد الأوروبي الإقليميين CyberCrime@IPA وCybercrime@EAP، ضمن مشاريع أخرى، مشاركةَ نقاط الاتصال الدائمة في الأنشطة التدريبية، وهو ما يتيح الفرصة أمامها للتواصل فيما بينها وكذلك مع أعضاء شبكة مجموعة البلدان الثمانية.

٢٥٤- ومنذ عام ٢٠٠٦، يساعد مجلس أوروبا البلدان في جميع أنحاء العالم، عبر مشروعه العالمي بشأن الجرائم السيبرانية، على تعزيز التشريعات؛ وتدريب القضاة وأعضاء النيابة العامة والمحققين في مجال إنفاذ القانون على مسائل متعلقة بالجرائم السيبرانية والأدلة الإلكترونية؛ وفي ميادين التعاون بين جهات إنفاذ القانون ومقدمي الخدمات، والتعاون الدولي.[١٤٣] ومن المجالات التي انصب عليها التركيز منذ عام ٢٠١٠ تدفقات عائدات الجريمة والتحقيقات المالية على الإنترنت، بما في ذلك تمويل الإرهاب عبر الإنترنت.[١٤٤]

(هـ) خطة عمل الاتحاد الأوروبي: مركز الجرائم السيبرانية

٢٥٥- في ٢٦ نيسان/أبريل ٢٠١٠، قام مجلس الاتحاد الأوروبي، إقراراً منه بالدور الأساسي لتكنولوجيا المعلومات والاتصالات في المجتمع الحديث، وبتزايد عدد المخاطر ونطاقها وتعقيدها وأثرها المحتمل على الولايات القضائية المتعددة، بما يزيد من الحاجة إلى تعزيز التعاون بين الدول الأعضاء والقطاع الخاص، فقد اعتمد المجلس عدداً من الاستنتاجات فيما يخص وضع خطة عمل لمكافحة الجرائم السيبرانية، على أن تُدمج هذه الخطة في برنامج ستوكهولم للفترة ٢٠١٠-٢٠١٤ وفي استراتيجية الأمن الداخلي المستقبلية المرتبطة به.

---

[١٤٣] انظر الرابط التالي: www.coe.int/lportal/web/coe-portal/what-we-do/rule-of-law/terrorism.

[١٤٤] Council of Europe, Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, *Criminal Money Flows on the Internet: Methods, Trends and Multi-Stakeholder Counteraction* (2012).

٢٥٦- وبموجب الخطة، اتفق الأعضاء على أمور في جملتها تكليف المفوضية الأوروبية بالقيام، بالتعاون مع يوروبول، بتحليل الفائدة والجدوى من إنشاء مركز أوروبي للجرائم السيبرانية لتعزيز المعلومات والقدرات والتعاون بشأن المسائل المتعلقة بالجرائم السيبرانية، ثم التقدم بتقرير عن نتائج هذا التحليل. وقد انتهت المفوضية من هذه المهمة ووضعت مقترحاً سيقوم اليوروبول بموجبه باستضافة مرفق جديد لتلقي ملفات العمل التحليلي المتعلقة بالجريمة المنظمة الخطيرة والإرهاب ومعالجة هذه الملفات.

٣- *دور المنظمات واتفاقات التعاون الإقليمية الأخرى*

٢٥٧- تؤدي اتفاقات التعاون الرسمية القائمة على المستوى الإقليمي أو دون الإقليمي بين أجهزة إنفاذ القانون أو الاستخبارات دوراً رئيسياً كما ذُكر آنفا في الجهود التي يبذلها المجتمع الدولي لتعزيز تدابير مكافحة الإرهاب والجريمة المنظمة العابرة للحدود الوطنية والتنسيق بينها. وإذا كان التعاون بموجب هذه الترتيبات عادة ما لا يستند إلى معاهدات ملزمة أو غير ذلك من الصكوك، فإنَّها مع ذلك قادرة على تهيئة آليات في منتهى الفعالية للتعاون بين البلدان الأعضاء المشتركة فيها.

٢٥٨- وثمة أمثلة عديدة، على المستوى الدولي، على هذه الترتيبات، إلا أنَّ ثلاثة منها، مطبَّقة في أوروبا وأفريقيا ومنطقة المحيط الهادئ، توضح كيف يُمكن لمجموعات من البلدان ذات المصالح والأهداف المتوافقة في مجالي الأمن وإنفاذ القانون أن تعمل سوياً بنجاح لإرساء دعائم تعاون وثيق في مجال التحقيقات الجنائية.

٢٥٩- فقد أُنشئ في عام ١٩٩٨ المركز الفرنسي-الألماني للتعاون بين الشرطة والجمارك، المعروف أيضاً بمركز أوفنبورغ، لأهداف منها دعم تنسيق عمليات تقوم بها أجهزة متعددة (مثل عمليات التفتيش والمراقبة وتبادل المعلومات التي يتم جمعها) عبر الحدود المشتركة بين هذين البلدين. ويعمل في المركز أفراد من أجهزة الشرطة والجمارك ومراقبة الحدود على المستويين الاتحادي والمحلي، ويتلقى عدة آلاف من الطلبات كل عام، وهو وسيلة لإيجاد حلول عملية للمسائل التي تنشأ بين الأجهزة الشريكة وإرساء الثقة والتعاون فيما بين هذه الأجهزة.

٢٦٠- وفي أفريقيا، اتفق أعضاء منظمة التعاون الإقليمي بين رؤساء الشرطة في الجنوب الأفريقي ومنظمة تعاون رؤساء الشرطة في شرق أفريقيا على مجالات بعينها لتعاون أجهزة الشرطة، بما في ذلك التبادل الدائم للمعلومات المتعلقة بالجريمة، والتخطيط للعمليات المشتركة وتنسيقها وتنفيذها، بما يشمل العمليات السرية، ومراقبة الحدود ومنع الجريمة في المناطق الحدودية، إلى جانب عمليات المتابعة، والتسليم المراقَب للمواد غير المشروعة أو غيرها من الأشياء، والمساعدة التقنية والخبرات حسب الاقتضاء.[١٤٥]

٢٦١- وفي منطقة المحيط الهادئ، يعتبر مركز التنسيق المعني بالجريمة عبر الوطنية في منطقة المحيط الهادئ بمثابة مركز لجمع بيانات الاستخبارات الجنائية التي تجمعها شبكة من الوحدات الوطنية المعنية بالجريمة العابرة للحدود الوطنية الواقعة في البلدان الأعضاء عبر المنطقة، علاوة على تنسيق هذه البيانات

(١٤٥) Charles Goredema, "Inter-State cooperation", in *African Commitments to Combating Organised Crime and Terrorism: A review of eight NEPAD countries* (African Human Security Initiative, 2004).
انظر الرابط التالي: http://www.iss.co.za/pubs/Other/ahsi/Goredema_Botha/pt1chap5.pdf.

وتحليلها ومشاطرتها. كما أن المركز، الذي يديره مسؤولون منتدبون من شتى أجهزة إنفاذ القانون ومراقبة الحدود في بلدان جزر المحيط الهادئ، بمثابة حلقة وصل بين البلدان الأعضاء والإنتربول وأجهزة إنفاذ القانون الأخرى في جميع أنحاء العالم، عبر الشبكة الدولية لجهاز الشرطة الاتحادية الأسترالي، الذي يقوم بدعم المبادرة.

٢٦٢- كما أنّ البلدان التي لها مصالح مشتركة في المجالات المتعلقة بالأمن وإنفاذ القانون، وإن لم تكن بالضرورة قريبة من بعضها البعض جغرافياً، قد تعقد ترتيبات جماعية تتيح تبادل المعلومات والمعلومات الاستخبارية.

(أ) مجموعة إيغمونت لوحدات المخابرات المالية

٢٦٣- مجموعة إيغمونت لوحدات المخابرات المالية من بين الأمثلة على الترتيبات المذكورة، التي لها تأثير على التحقيقات المتعلقة بتمويل الإرهاب. ودائماً ما تنطوي التحقيقات في ما يُشتبه في كونه تمويلا إرهابياً على جمع سجلات مالية أو مصرفية موجودة في ولاية قضائية واحدة أو أكثر، فضلا عن مشاطرة هذه المعلومات وتحليلها. وتكون قدرة وحدات الاستخبارات المالية على التعاون وتبادل المعلومات الاستخبارية المالية عنصراً رئيسياً على الأرجح في نجاح التحقيق والملاحقة القضائية في هذه القضايا. وتعمل مجموعة إيغمونت، وهي هيئة دولية تأسست في عام ١٩٩٥، على تعزيز التعاون بين وحدات الاستخبارات المالية وتحسين نوعيته سعياً إلى مكافحة غسل الأموال وتمويل الإرهاب، وتشجيع التوسع في التعاون الدولي على تبادل المعلومات ومنهجة هذا التعاون، ضمن أمور أخرى. وتوصي مجموعة إيغمونت أعضاءها بإبرام مذكرات تفاهم تتفق فيها على تبادل المعلومات الاستخبارية المالية ذات الصلة بالتحقيق والملاحقة القضائية في قضايا تمويل الإرهاب، وغسل الأموال، وما يتصل بذلك من الأنشطة الإجرامية.

٢٦٤- وحتى تضمن السلطات كون وحداتها الوطنية المعنية بالاستخبارات المالية قادرة على التعاون بفعالية مع نظيراتها الأجنبية في قضايا من هذا القبيل، ينبغي لها أن تقرر ما إذا كان المستصوب عقد اتفاقات أو ترتيبات مناسبة لتبادل المعلومات مع النظراء الأجانب. وتتضمن مذكرة التفاهم النموذجية التي اقترحتها مجموعة إيغمونت إرشادات مفيدة بشأن أنواع المسائل التي قد يتعين التصدي لها.

(ب) المنظمة الدولية للشرطة الجنائية

٢٦٥- إنَّ العديد من الصكوك الدولية، بما في ذلك الاتفاقية الدولية لقمع تمويل الإرهاب[١٤٦] (الفقرة ٤ من المادة ١٨)، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية (الفقرة ١٣ من المادة ١٨)، والعديد من قرارات مجلس الأمن، بما في ذلك القرار ١٦١٧ (٢٠٠٥)، تحث البلدان صراحةً على العمل ضمن إطار عمل الإنتربول للتعاون في مجال تبادل المعلومات.

٢٦٦- ومن بين الوظائف الرئيسية للإنتربول تعزيز التعاون الدولي بين أجهزة إنفاذ القانون الدولية والتبادل السريع والمأمون للمعلومات المتعلقة بالأنشطة الإجرامية وتحليلها. وتقوم المنظمة بذلك عن

[١٤٦] الأمم المتحدة، مجموعة *المعاهدات*، المجلّد ٢١٧٨، الرقم ٣٨٣٤٩.

طريق منظومة الاتصالات الشرطية العالمية التي تديرها، والمتاحة لمسؤولي إنفاذ القانون في جميع الدول الأعضاء.

٢٦٧- ويُمكن للمكاتب المركزية الوطنية، باستخدام منظومة الاتصالات الشرطية العالمية، أن تبحث وتدقق في مجموعة كبيرة ومتنوعة من البيانات، بما يشمل معلومات عن الإرهابيين المشتبه بهم ومجموعة متنوعة من قواعد البيانات. وتهدف المنظومة إلى تيسير إجراء التحقيقات الجنائية بمزيد من الفعالية عبر توفير معلومات أوسع نطاقا للمحققين.

٢٦٨- ويتيح برنامج مكافحة الجرائم السيبرانية التابع للإنتربول شبكةَ منظومة الاتصالات الشرطية العالمية، كما يهدف إلى تشجيع تبادل المعلومات بين البلدان الأعضاء عبر فرق عمل ومؤتمرات إقليمية، وتنظيم دورات تدريبية لوضع المعايير المهنية وترسيخها، وتنسيق العمليات الدولية والمساعدة فيها، ووضع قائمة عالمية بمسؤولي الاتصال بغرض التحقيق في الجرائم السيبرانية، ومساعدة البلدان الأعضاء في حالة تعرضها لهجمات سيبرانية وفي تحقيقاتها بشأن الجرائم السيبرانية عبر إتاحة خدمات في مجالي التحقيق وقواعد البيانات، وإقامة شراكات استراتيجية مع منظمات دولية أخرى وهيئات القطاع الخاص، والوقوف على المخاطر المستجدة وتبادل هذه المعلومات الاستخبارية مع البلدان الأعضاء، وإتاحة بوابة شبكية آمنة للاطلاع على المعلومات والوثائق العملياتية.[١٤٧]

٢٦٩- وتتعاون الإنتربول تعاونا وثيقا مع جامعة دبلن منذ عام ٢٠٠٩ على التدريب المتخصص والتبادل الأكاديمي لتعزيز خبرات أجهزة إنفاذ القانون في التحقيقات المتعلقة بالجريمة الإلكترونية. ففي آب/أغسطس ٢٠١١، شارك محققون في الجرائم السيبرانية وأخصائيون في التحليل الجنائي الحاسوبي من ٢١ بلدا في الدورة التدريبية الصيفية الأولى المشتركة بين الإنتربول وجامعة دبلن بشأن مكافحة الجرائم السيبرانية. وقد اشتملت الدورة، التي أعدتها الكلية ودامت أسبوعين، على تمارين لمحاكاة القضايا، وقام بالتدريب محترفون من أجهزة إنفاذ القانون وجامعة دبلن، والقطاع الخاص. وقد استهدفت الدورة تكوين رصيد من المعارف النظرية والعملية والمهارات في عدد من المجالات لمساعدة المحققين على القيام بتحقيقات أكثر فعالية في الجرائم السيبرانية، كما زودت المشاركين بمهارات في مجالات مثل نسخ الأقراص بالتصوير، والتحليل الجنائي للبيانات الفعلية، والتحليل الجنائي للهواتف المحمولة، والتحقيقات في غسل الأموال، وتقنيات التفتيش والضبط، وتحقيقات بروتوكول الاتصال الصوتي عبر الإنترنت والشبكات اللاسلكية، والكشف عن البرمجيات الضارة وتحليلها.[١٤٨]

٢٧٠- وأخيراً، فإنَّ وحدة الإنتربول المعنية بمكافحة الجرائم المرتبطة بالتكنولوجيا المتطورة تيسِّر التعاون العملياتي بين البلدان الأعضاء عبر اجتماعات لفرق خبراء وحلقات عمل تدريبية بشأن الجرائم السيبرانية، على المستويين العالمي والإقليمي، فضلا عن التعاون فيما بين أجهزة إنفاذ القانون، والقطاعات المعنية، والأكاديميين. كما تساعد الوحدة البلدان الأعضاء في حالة تعرضها لهجمات سيبرانية وفي تحقيقاتها بشأن الجرائم السيبرانية عبر إتاحة خدمات في مجالي التحقيق وقواعد البيانات.

(ج) مكتب الشرطة الأوروبي (اليوروبول)

٢٧١- الهدف الأساسي من الولاية المسندة لليوروبول هو تحسين فعالية سلطات إنفاذ القانون في الدول الأعضاء في الاتحاد الأوروبي والتعاون فيما بينها بشأن منع الإرهاب وغيره من أشكال الجريمة المنظمة العابرة للحدود

[١٤٧] انظر الرابط التالي: www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

[١٤٨] المرجع نفسه.

الوطنيــة ومكافحتهــا. ويؤدي اليوروبــول دوراً رئيسياً في فرقة العمل الأوروبية المعنيــة بالجرائم الحاسوبية، وهي فرقــة خبراء مُشكَّلة من ممثلين عــن اليوروبول، ووحدة التعــاون القضائي التابعة للاتحــاد الأوروبي، والمفوضية الأوروبيــة، يعملــون إلى جانــب رؤساء وحدات مكافحــة الجرائم السيبرانيــة في بلدان الاتحــاد الأوروبي لتيسير مكافحــة هذه الجرائم عبر الحــدود. ويقدِّم اليوروبول أشكال الدعم التالية للــدول الأعضاء في الاتحاد الأوروبي فيما يخص المسائل المتعلقة بالجرائم السيبرانية:

- قاعــدة بيانات الجرائم السيبرانية: يدعم اليوروبول الدول الأعضاء في الاتحاد الأوروبي في ما تجريه من تحقيقات وتحليل بخصوص الجرائم السيبرانية وييسر التعاون وتبادل المعلومات عبر الحدود
- يقــوم نظام تقييم المخاطر بشأن الجريمــة المنظمة المرتكبة باستخــدام الإنترنت (iOCTA) بتقييم اتجاهــات الجرائــم السيبرانية الحالية والمستقبلية، بما في ذلك الأنشطــة الإرهابية، والهجمات على الشبكات الإلكترونية، وهو تقييم يُستند إليه في كل من الأنشطة العملياتية وسياسات الاتحاد الأوروبي
- يوجــد كل مــن النظام الشبكــي للإبلاغ عــن جرائم الإنترنــت (ICROS) ومنتدى خــبراء الإنترنت والتحليل الجنائي (IFOREX) قيد الإعداد. وسوف يتيح هذان النظامان التنسيق المركزي للبلاغات الصادرة عن سلطات الدول الأعضاء في الاتحاد الأوروبي بشأن الجرائم السيبرانية، كما سيستضيفان بيانات وبرامج تدريبية تقنية للعاملين في مجال إنفاذ القانون.[١٤٩]

٢٧٢- وبالإضافــة لهذا الدعــم، فإنَّ اليوروبول يسهم إسهامــاً كبيراً على مستوى العمليــات، بالتعاون مع وحدة التعــاون القضائــي التابعة للاتحاد الأوروبــي، في إنشاء فرق تحقيق مشتركة وفي دعم هــذه الفِرق، ويقدِّم الدعم للــدول الأعضاء فيمــا يخص التحقيقات عبر نظــام ملفات العمل التحليلــي والاجتماعات التنسيقيــة والتكتيكية بشأن القضايا. وبموجب نظام اليوروبول لملفات العمل التحليلي، تُخزَّن البيانات الاسمية (كالمعلومات التي تخص الشهــود، والضحايا، وأرقام الهاتف، والمواقع، والمركبات، والوقائع) وتخضع لعملية تحليل دينامي تقوم على ربط الأشيــاء والكيانــات والبيانات فيما بين التحريات والتحقيقات الوطنية. ويوضع علــى البيانات "رمز مناولة" يبيِّن بوضوح شروط الاستخدام المرفقة بعنصر معين من البيانات.

(د) وحدة التعاون القضائي التابعة للاتحاد الأوروبي

٢٧٣- يشمــل عمل وحــدة التعاون القضائي التابعة للاتحاد الأوروبــي (يوروجست) في مجال مكافحة الإرهاب، في إطــار الولاية المسنــدة إليها، تيسير تبادل المعلومــات بين السلطات القضائية في مختلف الــدول الأعضاء التي تقوم بتحقيقات وملاحقات قضائية تتعلق بالإرهاب،[١٥٠] ودعم السلطات القضائية في الدول الأعضاء في إصدار أوامــر التوقيــف الأوروبية وتنفيذهــا، وتيسير تدابير التحقيق وجمــع الأدلة اللازمة للــدول الأعضاء حتى تتمكن مــن الملاحقة القضائية بشأن جرائم الإرهاب المشتبه بارتكابهــا (مثل شهادة الشهود، والأدلة العلمية، والتفتيش والضبط، واعتراض الاتصالات). ويتخذ الأعضاء السبعة والعشرون الوطنيون في وحدة التعاون القضائي التابعة للاتحــاد الأوروبي (من قضــاة أو أعضاء في النيابات العامة أو مسؤولــين في الشرطة ممن لديهم الاختصاصات

[١٤٩] انظر: "Cybercrime presents a major challenge for law enforcement", European Police Office press release, 3 January 2011. على الرابط التالي: www.europol.europa.eu/content/press/cybercrime-presents-major-challenge-law-enforcement-523.

[١٥٠] يُلــزم قرار مجلس الاتحاد الأوروبي 2005/671/JHA الصادر في ٢٠ أيلول/سبتمبر ٢٠٠٥ بشأن تبادل المعلومات والتعاون فيما يخص جرائــم الإرهــاب جميعَ الدول الأعضــاء بتعيين مراسلين وطنيين معنيين بمسائــل الإرهاب عليهم إبلاغُ وحدة التعــاون القضائي التابعة للاتحاد الأوروبي بكل الأنشطة الإرهابية في بلدانهم، بدءاً بالمراحل الأولى لمقابلة المشتبه بهم حتى مرحلة توجيه الاتهام، وبدءاً بأوامر التوقيف الأوروبية الصادرة فيما يخص الإرهاب وحتى طلبات المساعدة القانونية المتبادلة وصدور الأحكام.

نفسها، كلٌّ في دولته العضو) من مدينة لاهاي بهولندا مقراً لهم، وهم على اتصال دائم بالسلطات الوطنية في دولهم الأعضاء، إذ قد تطلب إحداها دعم الوحدة في سياق تحقيقات أو ملاحقات قضائية بعينها تتعلق بمكافحة الإرهاب (في فض المنازعات حول الولايات القضائية أو تيسير جمع الأدلة على سبيل المثال).

٢٧٤- كما أنَّ الوحدة تشجِّع وتدعم إنشاء فرق تحقيق مشتركة وعملها عبر توفير المعلومات والمشورة للممارسين. وقد باتت فرق التحقيق المشتركة أداة يتزايد التسليم لها بالفعالية في الاستجابة القضائية للجريمة العابرة للحدود ومنتدى مناسباً لتبادل المعلومات العملياتية حول قضايا إرهاب بعينها. ويمكن لأعضاء الوحدة الوطنيين أن يشاركوا في فرق التحقيق المشتركة، سواء بالنيابة عن الوحدة أو بصفتهم ممثلين عن السلطات الوطنية المختصة بالإرهاب. فعلى سبيل المثال، هناك قضية دانمركية متعلقة بأنشطة إرهابية، جرى فيها إحالة طلب بإنشاء فريق تحقيق مشترك إلى السلطات البلجيكية، وقام المكتبان الدانماركي والبلجيكي في الوحدة بتأسيس الفريق المشترك بين السلطتين الوطنيتين المختصتين. كما أنَّ الوحدة تقدِّم المساعدة المالية واللوجستية للعمليات التي تقوم بها هذه الفرق وتستضيف الأمانة الدائمة لفرق التحقيق المشتركة.

٢٧٥- كما يستهدف مرصد *أحكام الإدانة الصادرة في قضايا الإرهاب* التابع للوحدة تقديم أمثلة للممارسين على الأحكام الصادرة في أحد البلدان والتي قد تكون مفيدة في بلد آخر، ولا سيما فيما يخص تفسير تشريعات الاتحاد الأوروبي بشأن الإرهاب. فقد تضمّن العدد الصادر في أيلول/سبتمبر ٢٠١٠ من *المرصد* تحليلا معمَّقاً لقضيتين لهما خصائص مشتركة، كالأعمال الإرهابية التي يقوم بها جهاديون، والدفع باتجاه التطرف، واستخدام الإنترنت.[١٥١] وكانت إحدى القضايا، التي قدَّمتها السلطات البلجيكية، قضية *مليكة العروض وآخرين*، المشار إليها أدناه (انظر الفقرة ٢٧٧). ويعقد فريق *مكافحة الإرهاب* التابع للوحدة اجتماعات تكتيكية واستراتيجية منتظمة بشأن اتجاهات الإرهاب، يتبادل فيها قضاة وخبراء بارزون في مجال قانون الإرهاب من بلدان الاتحاد الأوروبي وغيرها من البلدان خبراتهم حول مسائل ملموسة. وتشمل الأمثلة على هذه الاجتماعات اجتماع عام ٢٠١٠ الاستراتيجي المتعلق باستخدام تكنولوجيا بروتوكول الاتصال الصوتي عبر الإنترنت في أغراض إرهابية والحاجة إلى اعتراض هذه الاتصالات بطريقة قانونية، واجتماع تكتيكي عُقد في نيسان/أبريل ٢٠١١ حول العنف بدافع التطرف والإرهاب المرتبط بقضية واحدة. ويتم في هذه الاجتماعات تحديد المشاكل المشتركة وتعميم الممارسات المثلى والاستنتاجات على مقرري السياسات العامة بالاتحاد الأوروبي، مع استكشاف سبل تحقيق مزيد من الفعالية في تنسيق جهود مكافحة الإرهاب.

جيم- الأطر التشريعية الوطنية

٢٧٦- إنَّ وجود إطار تشريعي، على المستوى الوطني، ينص على التعاون الدولي هو عنصر رئيسي من عناصر قيام إطار فعال لتيسير التعاون الدولي على التحقيق والملاحقة القضائية في قضايا الإرهاب. وينبغي أن يدرَج في القانون المحلي للبلاد، بموجب هذه التشريعات، مبادئ التعاون الدولي المعتمدة في الصكوك العالمية لمكافحة الإرهاب.

[١٥١] يمكن الحصول على نسخة من تقرير *Terrorism Convictions Monitor* بتوجيه طلب إلى فريق مكافحة الإرهاب بوحدة التعاون القضائي التابعة للاتحاد الأوروبي.

٢٧٧- وبالإضافة إلى إصدار عدد من المنشورات التي تهدف إلى مساعدة البلدان على إدماج آليات التعاون الدولي في تشريعاتها، يقدم فرع منع الإرهاب التابع لمكتب الأمم المتحدة المعني بالمخدِّرات والجريمة خدمات تشمل الدعم الاستشاري والتدريب وبناء القدرات بشأن هذه المسائل، في إطار الخدمات التي يتيحها للبلدان بشأن تنفيذ التزاماتها الدولية في مجال مكافحة الإرهاب.

دال- التدابير غير التشريعية

٢٧٨- لئن كان الانضمام إلى الصكوك الثنائية والمتعددة الأطراف واعتماد تشريعات ذات صلة من المكونات الرئيسية لأي نظام فعال للتعاون الدولي، فإنّهما غير كافيين. فمن بين العناصر الأساسية في فعالية التعاون الدولي وجودُ سلطة مركزية لديها ما يكفي من الموارد والقدرة على أخذ زمام المبادرة، بما يمكِّنها من تيسير التعاون بفعالية والوقت المناسب، استناداً إلى أية آليات متاحة (رسمية أو غير رسمية).

٢٧٩- فالتعاون الدولي الناجح يقتضي تحقق شرط مسبق هام، وهو وجود تنسيق فعال فيما بين أجهزة إنفاذ القانون، وأجهزة الاستخبارات المتخصصة (كوحدات الاستخبارات المالية) والسلطات المركزية على المستوى الوطني، مدعوماً بالتشريعات اللازمة، وإجراءات واضحة ومبسطة للتعامل مع الطلبات.

٢٨٠- والقضية التالية، التي عُرضت على المحكمة في كولومبيا وكانت موضوع تعاون رسمي وغير رسمي مكثف بين السلطات، مثال جيد على التعاون على المستويين الوطني والدولي.

قضية القوات المسلحة الثورية لكولومبيا

في ١ آذار/مارس ٢٠٠٨، قامت القوات المسلحة الكولومبية بتنفيذ عدة عمليات ضد أعضاء مزعومين في القوات المسلحة الثورية لكولومبيا. وأثناء هذه العمليات، قُتل شخص يُشتبه في كونه أحد القيادات العليا للقوات الثورية وعدة أعضاء آخرين في التنظيم، وجُمعت أدلة منها أجهزة إلكترونية مثل أجهزة الحاسوب ودفاتر تدوين رقمية وناقلات تسلسلية عامة (USB). وأحيلت الأشياء المحتوية على أدلة رقمية إلى الشرطة القضائية الكولومبية لاستخدامها فيما قد يجرى من تحقيقات وملاحقات قضائية.

وكشفت البيانات المسترجعة من الأجهزة الرقمية عن معلومات تتعلق بالشبكة الدولية الداعمة للتنظيم، بما في ذلك صلات ببلدان عدة في أمريكا الوسطى والجنوبية. وكان الهدف الرئيسي للشبكة هو جمع الأموال لأنشطة القوات الثورية، وتجنيد أعضاء جدد، والترويج لسياسات التنظيم، بما في ذلك شطب اسمه من عدد من القوائم المتعلقة بالإرهاب التي وضعها الاتحاد الأوروبي وبعض البلدان. واستناداً إلى الأدلة المسترجعة، فتح النائب العام الكولومبي تحقيقات جنائية ضد الأشخاص المزعوم دعمهم وتمويلهم للقوات الثورية.

وقد أسفرت الأدلة، التي شاطرتها السلطات الكولومبية مع نظيراتها في إسبانيا، عن الوقوف على هوية قائد القوات الثورية في إسبانيا، المعروف بالاسم المستعار "ليوناردو". وكان "ليوناردو" قد دخل إلى إسبانيا عام ٢٠٠٠، ومُنح حق اللجوء السياسي.

وحصل النائب العام الكولومبي على ما يكفي من الأدلة ليأمر بإصدار أمر توقيف لتسليم "ليوناردو" واستخدم القنوات الدبلوماسية وغيرها من قنوات التعاون الدولي القانونية لطلب تسليمه إلى كولومبيا من أجل محاكمته.

وأُلقي القبض على "ليوناردو" في إسبانيا، وكشف تفتيش منزله ومقر عمله عن مستندات وأجهزة إلكترونية تحتوي على أدلة على صلاته بالجرائم قيد التحقيق. وأُفرج عنه بكفالة في وقت لاحق، حيث إنّ وضعه القانوني كلاجئ حال دون تسليمه فوراً.

وبدأت الدعوى الجنائية غيابياً ضد "ليوناردو" في كولومبيا لضلوعه المزعوم في تمويل الإرهاب. وفي قرار لمحكمة العدل العليا في كولومبيا، اعتُبرت المعلومات التي تم الحصول عليها في عملية ١ آذار/مارس ٢٠٠٨ من الأجهزة الإلكترونية المضبوطة غير مقبولة في المحاكمة. بعدها، استخدم النائب العام، بالتعاون مع نظرائه في عدد من البلدان الأخرى التي كان أعضاء من شبكة دعم القوات الثورية موجودين فيها، جميع قنوات التعاون الدولي المتاحة للوقوف على هوية أعضاء الشبكة في إسبانيا وغيرها من البلدان الأوروبية وجمع المزيد من الأدلة دعماً للقضية.

وعلاوة على ذلك، واستجابة لالتماسات التفويض القضائي الصادرة من النائب العام الكولومبي، أرسلت السلطات القضائية الإسبانية إلى نظيراتها الكولومبية كل المعلومات التي تم جمعها أثناء اقتحام منزل "ليوناردو" وتفتيشه. وقد أثبتت هذه المعلومات، حسب الشرطة القضائية الإسبانية، تورط "ليوناردو" وأشخاص آخرين في تكوين خلية إرهابية تابعة للقوات الثورية في إسبانيا. كما أثبتت تورط "ليوناردو" في تمويل الإرهاب وقوّت من افتراض وجود صلات بين "ليوناردو" وأشخاص تجري ملاحقتهم قضائياً لصلاتهم بالجماعة الإرهابية إيتا (وطن الباسك والحرية). وقد أسفرت عمليات التفتيش التي جرت في إسبانيا عن ضبط مزيد من الأدلة الوثائقية والرقمية الشبيهة من حيث محتواها بالأدلة التي أصدرت المحكمة قرارا بعدم مقبوليتها. وباستخدام هذه الأدلة الجديدة التي وفرتها السلطات الإسبانية، واصل النائب العام الكولومبي الدعوى المرفوعة ضد "ليوناردو". وعلاوة على ذلك، فقد بيَّنت الأدلة الجديدة أنَّ القوات الثورية قد بذلت جهوداً كي تتيح لأعضائها إمكانية الوصول إلى الجامعات والمنظمات غير الحكومية وغيرها من كيانات الدولة حيث يمكنهم البحث عن فرص للتمويل وتجنيد أعضاء جدد.

كما أكدَّت الأدلة وجود "لجنة دولية" داخل القوات الثورية تستخدم برنامجاً أمنياً للاتصالات، وخاصة الاتصالات المرسلة عبر الإنترنت أو الموجات الإذاعية (وهي وسيلة الاتصال الدائمة بين قيادات التنظيم وأعضاء شبكة الدعم الدولية)، بتشفير المعلومات المرسلة، باستخدام تقنية إخفاء المعلومات لإخفاء الرسائل، وإرسال رسائل متطفلة بالبريد الإلكتروني وحذف سجلات التصفح لضمان عدم استرجاع المعلومات من قبل سلطات التحقيق أو السلطات القضائية. وفي هذا الصدد، تعاونت السلطات في إسبانيا وكولومبيا على "كسر" المفاتيح وفك شفرة محتوى الرسائل المتبادلة بين القادة المزعومين للقوات الثورية في كولومبيا وإسبانيا.

وقبل الشروع في الدعوى ضد "ليوناردو"، تقدم النائب العام الكولومبي بطلب لقاضٍ باعتبار الأدلة الجديدة "أدلة تم تلقيها في وقت لاحق" ومن " مصدر مستقل". وكان الهدف من هذه الطلبات، التي حظيت بالقبول، هو السماح بإدراج الأدلة في الدعوى دون استثارة الأسباب التي كان من شأنها استبعاد أدلة مشابهة.

وتجري حاليا محاكمة المدَّعى عليه "ليوناردو" غيابياً في التهم المتعلقة بتمويل الإرهاب، في انتظار نتائج إجراءات التسليم.

٢٨١- في القضية أعلاه، استفادت السلطات من كل من الآليات الرسمية للمساعدة القانونية المتبادلة والعلاقات غير الرسمية. ورغم الاختلافات في مدى قدرة السلطات في مختلف البلدان على تقديم المساعدة المتبادلة في حال عدم وجود معاهدة أو طلب رسمي، فإنَّ لدى السلطات في العديد من البلدان القدرة إلى حد ما على تقديم المساعدة استناداً إلى طلبات غير رسمية من نظيراتها الأجنبية في التحقيقات المتعلقة بالإرهاب. وقد سلط اجتماع فريق الخبراء الضوء على عدة حالات وظروف أمكن، أو يُمكن، فيها الاستعانة بتعاون غير رسمي من هذا القبيل للتحقيق بنجاح في قضايا استخدام الإنترنت من قبل إرهابيين.

١- *أهمية العلاقات*

٢٨٢- على المستوى العملياتي، من المهم أيضاً أهمية قصوى أن تقوم أجهزة إنفاذ القانون والنيابات العامة الوطنية، بالتشجيع على إقامة علاقات مبنية على الثقة بالنظراء الأجانب الذين قد تحتاج إلى التعاون معهم في التحقيقات الجنائية عبر الحدود، وإرساء تلك العلاقات والحفاظ عليها.

٢٨٣- ونظراً لأن الكثير من الأنشطة الإرهابية وما يتعلق بها من أنشطة إجرامية يمارَس عبر الحدود، فإنَّ الطبيعة الشديدة التعقيد والحساسية للتحقيقات المستندة إلى معلومات استخبارية والحاجة للتحرك بسرعة في خضم أحداث وتحقيقات متلاحقة، فإنَّ الثقة فيما بين أجهزة إنفاذ القانون والنيابة العامة، سواء على المستوى الوطني أو الدولي، كثيراً ما تكون عاملا حاسماً في نجاح التحقيق والملاحقة القضائية في جرائم الإرهاب. وتزيد أهمية هذا الأمر في سياق الإنترنت، حيث كثيرا ما يكون حفظ بيانات الاستخدام والأدلة الرقمية المخزنة في أجهزة منها مثلا أجهزة الحاسوب وغيرها من الأجهزة المحمولة في ولاية قضائية واحدة أو أكثر في كثير من الأحيان، دليلا حاسما في الملاحقة القضائية، ولا بد من أن يتم في غضون مهلة زمنية قصيرة. فالعلاقات الشخصية بالنظراء في الولايات القضائية الأخرى، والإلمام بما يتبعونه من إجراءات، والثقة فيهم، جميعها عوامل تسهم في التعاون الدولي الفعال.

٢٨٤- ورغم اختلاف وسائل التعاون غير الرسمي باختلاف البلدان، فمن الممكن الوقوف على بعض الممارسات الجيدة في تقديم المساعدة غير الرسمية في التحقيقات المتعلقة بالإرهاب.

(أ) وضع آليات فعالة لتبادل المعلومات: الاستعانة بمسؤولي اتصال

٢٨٥- أشار خبراء عديدون في اجتماع فريق الخبراء إلى أنَّ أجهزة إنفاذ القانون الوطنية في بلدانهم تُدير شبكة من نقاط الاتصال الدولية التي تساعد كثيراً في تيسير طلبات التعاون الدولي. فعلى سبيل المثال، يوجد لدى مكتب الشرطة الجنائية الاتحادية الألمانية مسؤول اتصال ونقاط اتصال مباشرة في ما يقرب من ١٥٠ بلدا. وعلاوة على ذلك، فإنَّ شبكة الخبراء الأوروبيين في مسائل الإرهاب، التي تأسست في عام ٢٠٠٧، تجمع بين خبراء من المؤسسات الأكاديمية وأجهزة الشرطة والاستخبارات، وقد تبيَّن أنَّها قناة اتصال بالغة الفعالية لتبادل المعلومات والخبرات بين الأعضاء على أساس تعدد التخصصات.

٢٨٦- وتُعدُّ قضية *التاج البريطاني* (النيابة العامة الكندية) *ضد سعيد ناموح* مثالا على النجاح البالغ للتعاون الدولي غير الرسمي بالكامل، بين سلطات إنفاذ القانون والنيابة العامة في كندا والنمسا في التحقيق والملاحقة القضائية لأشخاص موجودين في هاتين الولايتين القضائيتين يستخدمون الإنترنت للقيام بنشاط مرتبط بالإرهاب.

التاج البريطاني (النيابة العامة الكندية) ضد سعيد ناموح

كان السيد سعيد ناموح مواطناً مغربياً يعيش في بلدة صغيرة في كندا.

وفي ١٠ آذار/مارس ٢٠٠٧، نُشر مقطع فيديو على هيئة رسالة "مفتوحة" يقرأها الشيخ أيمن الظواهري على أحد المواقع الشبكية. في هذا المقطع، أنذر الظواهري حكومتي ألمانيا والنمسا بمواجهة العواقب في حال عدم سحب قواتهما من بعثات دعم السلام في أفغانستان. ومن ضمن ما جاء في رسالة الظواهري:

> طريق السلام ذو اتجاهين. إن كنا آمنين، فسوف تكونون آمنين. وإن كنا في سلام، فسوف تكونون في سلام. وإن كنا سنُقتل، فسوف نحاربكم ونقتلكم إن شاء الله. هذه هي المعادلة الصحيحة. حاولوا إذن أن تفهموها، إن كنتم تفهمون.

وكانت خلفية مقطع الفيديو، وتصريحات الظواهري المرفقة به، عبارة عن مجموعة متنوعة من الصور المركبة لسيارات مدرَّعة عليها أعلام وطنية وسياسيين ألمان ونمساويين بارزين. وفي بعض أجزاء المقطع، كانت هناك صور للظواهري وأشخاص ملثمين آخرين.

وفي أعقاب بث المقطع، فتحت السلطات النمساوية تحقيقاً اشتمل على عمليات تنصت على عدة اتصالات صادرة من محمد محمود، وهو مواطن نمساوي يعيش في فيينا. وكانت هذه الاتصالات تتكون من حصص استُخدم فيها بروتوكول الاتصال الصوتي عبر الإنترنت وحصص دردشة على الإنترنت باللغة العربية كشفت عن كون السيد محمود ضالعاً في اتصالات متعلقة بالنشاط الجهادي مع شخص في كندا، بما في ذلك مخططات لتنفيذ هجمة إرهابية، في أوروبا على الأرجح. وقد ناقش المشاركون في الاتصالات استخدام المتفجرات وغير ذلك من الترتيبات المتعلقة بتنفيذ الهجمة.

ونتيجة لأنشطة الاعتراض، كُشف عن هوية سعيد ناموح، المقيم في كندا، بصفته أحد المشاركين في الاتصالات المذكورة. وفي تموز/يوليه ٢٠٠٧، انضمت شرطة الخيالة الملكية الكندية إلى التحقيق، الذي كان يجري بالتنسيق فيما بين السلطات الكندية والنمساوية عبر مسؤول الاتصال لدى أجهزة إنفاذ القانون الكندية في فيينا. ورغم وجود معاهدة رسمية للمساعدة القانونية المتبادلة بين النمسا وكندا، فلم يقدَّم أيّ طلب رسمي للحصول على هذه المساعدة بموجب المعاهدة، وتم التعاون بالكامل عبر قنوات غير رسمية.

وقد كشفت التحقيقات عن أنّ شخصا ما قضى ما بين تشرين الثاني/نوفمبر ٢٠٠٦ وأيلول/سبتمبر ٢٠٠٧ وقتا طويلا على الإنترنت مستخدماً وصلة الإنترنت الخاصة بالسيد ناموح، وكان الشخص نفسه على اتصال دائم بالجهاديين في مختلف أنحاء العالم، بوسائل منها الجبهة الإعلامية الإسلامية العالمية، وهي واحدة من أقدم الجماعات الجهادية الافتراضية وأبرزها. وتؤدي الجبهة دور الذراع الإعلامي لجيش الإسلام، بدعم من مركز الفجر. وتقوم الجبهة بأنشطة منها نشر الدعاية وتزويد الجهاديين بالأدوات التي يحتاجونها (مثل أدلة صنع القنابل، وبرمجيات التشفير) لتنفيذ العمليات الجهادية. وكان الكثير من أنشطة السيد ناموح على الإنترنت عبارة عن مشاركات في عدد من منتديات النقاش التي يرتادها الجهاديون.

وفي أيار/مايو ٢٠٠٧، اختُطف صحفي البي بي سي ألان جونستون في غزة من قبل جيش الإسلام. ونشرت الجبهة الإعلامية الإسلامية العالمية عدة مقاطع فيديو متعلقة بهذا الحدث، لكن ما استرعى الاهتمام بشكل خاص بينها كان مقطع فيديو عُرض في ٩ أيار/مايو ٢٠٠٧، وأعلن فيه جيش الإسلام مسؤوليته عن الاختطاف، فضلا عن مقطعين عُرضا يومي ٢٠ و٢٥ حزيران/يونيه، وتضمّنا تهديداً بإعدامه إذا لم تُلبَّ مطالب معيَّنة. ولحسن الحظ فقد أُطلق سراح السيد جونستون سالما معافى في ٣ تموز/يوليه ٢٠٠٧.

وفي يومي ٧ و٨ أيار/مايو، كشفت اتصالات قام بها السيد ناموح عبر منتدى للدردشة على الإنترنت واعترضتها السلطات، عن أنَّ السيد ناموح كان يشارك في مناقشات تتعلق باختطاف ألان جونستون، وتحديداً في مناقشات حول إعداد رسالة الجبهة الإعلامية الإسلامية العالمية بخصوص إعلان المسؤولية، التي بُثت بعد ذلك بوقت قصير في ٩ أيار/مايو. ووفقاً للنسخة المدوّنة من الدردشة التي جرت على الإنترنت في ٨ أيار/مايو، والتي قُدِّمت ضمن الأدلة في المحاكمة (مترجماً من العربية إلى الفرنسية)، فقد نشر السيد ناموح ما محتواه: "أخي الحبيب أبا عبيدة، ابق معنا على الخط، عسى الله أن يرزقك مالاً حتى يتبين لك ما يجب عمله، سيصدر البيان اليوم إن شاء الله".

وإجمالا، جرت ٣١ محادثة بين ناموح ومحمود ما بين ٣ حزيران/يونيه و٩ أيلول/سبتمبر ٢٠٠٧. وقد كشفت هذه المحادثات أنَّهما يخططان للقيام بتفجير في موقع لم يُكشف عنه في أوروبا، ويناقشان كيفية الحصول على أحزمة ناسفة أو صنعها، والمسائل المتعلقة بالتمويل، ومخططات للسفر لمقابلة أشخاص آخرين في المغرب العربي ومصر لإتمام التحضيرات النهائية. وقد تبدّى من هذه المحادثات أنَّ منفِّذ العملية الانتحارية حسب الخطة كان هو السيد ناموح.

وفي ١٢ أيلول/سبتمبر ٢٠٠٧، قامت السلطات في كندا والنمسا، خشية أن يكون المشتبه بهم على وشك تنفيذ مخططاتهم، بإلقاء القبض على ناموح ومحمود في الوقت نفسه.

وفي كندا، اتُّهم السيد ناموح بالتآمر لاستخدام المتفجرات (في موقع لم يكشف عنه بأوروبا)، والاشتراك في أنشطة جماعة إرهابية، وتيسير أنشطة إرهابية، وابتزاز حكومة أجنبية (مقطع الفيديو الذي يحتوي على تهديد لألمانيا والنمسا).

وفي المحاكمة، طعن دفاع السيد ناموح في عدد من جوانب الادعاء، بوسائل منها الدفع بحجج دستورية تستند إلى الحق في حرية التعبير (فيما يتعلق بمسألة ما إذا كانت الجبهة الإعلامية الإسلامية العالمية تنظيماً إرهابياً). كما دُفع بعدد من الاعتراضات على موضوعية الشاهد الخبير الرئيسي الذي استدعته النيابة العامة للإدلاء بشهادته حول تنظيم القاعدة، وفروعه، والأنشطة الجهادية العالمية (بما في ذلك الأنشطة الجهادية على الإنترنت) وطرائق دعاية الجبهة وأساليبها واستخدامها للإنترنت. كما طعن الدفاع في كون الأنشطة التي تضطلع بها الجبهة والجماعات المرتبطة بها تشكّل أعمالا إرهابية، وكذلك في موثوقية الأدلة المحصل عليها باعتراض الاتصالات عبر الإنترنت في كندا والنمسا ومدى الدقة في ترجمة سجلات هذه الاتصالات من العربية إلى الفرنسية. وطلب الدفاع من المحكمة أن تخلص إلى أنَّ مختلف الرسائل التي نشرها السيد ناموح بالنيابة عن الجبهة ينبغي أن تفسَّر تفسيرا مجازيا وألا تعتبر أعمالا الغرض منها الحث أو التشجيع على الإرهاب.

وخلصت المحكمة، في سياق نظرها في حجج الدفاع فيما يتعلق بطبيعة المواد المنشورة أو المنقولة بالنيابة عن الجبهة، إلى ما يلي:

> لا يساور المحكمة أدنى شك في هذا الموضوع. فسياق هذه الرسائل يشير بوضوح إلى أفعال حقيقية تحث عليها الجبهة، والإشارات إلى الموت والدمار تتخلل جميع أجزائها. إن الجهاد الذي تروج له الجبهة جهاد عنيف. وهذا الترويج يشكل بوضوح شكلا من أشكال الحث وتهديداً بتنفيذ أنشطة إرهابية في بعض الأحيان. ومن ثم، فإنَّ هذه الأنشطة تندرج بوضوح ضمن تعريف الأنشطة الإرهابية في سياق المعنى المقصود في القسم ٨٣-١ من القانوني الجنائي.

وأشارت المحكمة، عند إدانتها للسيد ناموح في تهمة الحث أو التشجيع على ارتكاب أعمال إرهابية، إلى الاتصالات المعترَضة التي تحتوي على تصريحات تبيِّن مشاركته بحماس ونشاط في أنشطة الجبهة. ومن بين الأمور الهامة كذلك في نظر المحكمة عدة مشاركات، بما في ذلك المشاركة التالية التي جرت في يوم ١٢ كانون الأول/ديسمبر ٢٠٠٦، عبَّر فيها المدعى عليه عن رغبته في إخفاء أنشطته، وأنشطة الجبهة، عبر إزالة البيانات الحاسوبية التي تدينهما:

[ترجمة]
عاجل عاجل عاجل
السلام عليكم ورحمة الله وبركاته
أريد أن أمحو كل الأفلام والكتب الجهادية الموجودة على جهاز الحاسوب الخاص بي دون ترك أي أثر،
بارك الله فيكم، لأنني أشك أن شخصاً ما قد فحص جهاز الحاسوب الخاص بي.
والسلام عليكم ورحمة الله وبركاته.

وفي محادثات أخرى، تساءل المدعى عليه عن استخدام برمجيات إخفاء الهوية والأدوات المشابهة التي يمكن استخدامها لإخفاء أنشطته. وفي أعقاب المحاكمة صدر في تشرين الأول/أكتوبر ٢٠٠٩ حكم بإدانة المتهم في التهم كافة، وحُكم عليه بعد ذلك بالسجن مدى الحياة.

(ب) التحقيقات المشتركة

٢٨٧- لئن كان مفهوم "التحقيقات المشتركة" مذكورا في بعض المعاهدات الدولية (كما في المادة ١٩ من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية)، فليس ثمة إشارة واضحة إلى هذه الاستراتيجية في الصكوك العالمية لمكافحة الإرهاب. ومع ذلك، فإنَّ هذا النهج إزاء التحقيقات يتفق تماماً مع المبادئ والروح الكامنتين وراء العناصر المتعلقة بالتعاون الدولي في هذه الصكوك. وقد اعتمدت بعض البلدان في أوروبا هذا النهج بنجاح في عدد من التحقيقات المتعلقة بالإرهاب، وتجدر الإشارة إلى الدور الهام الذي يؤديه اليوروبول في إنشاء فرق التحقيق المشتركة ودعمها. والغرض الرئيسي من هذه الفرق، التي يشترك في عضويتها مسؤولون وطنيون عن إنفاذ القانون ومسؤولون من اليوروبول على حد سواء، هو إجراء تحقيقات لغرض معيَّن ولمدة محددة في دولة أو أكثر من الدول الأعضاء.[١٥٢]

٢٨٨- ويعمل اليوروبول مع منظومة من الوحدات الوطنية، تتكون من مسؤولي اتصال معيَّنين ضمن قوات الشرطة الوطنية. وييسر المكتب تبادل المعلومات فيما بين الدول الأعضاء ويشجِّع عليه عبر شبكة رقمية آمنة، ويوفِّر منظومة من ١٧ من ملفات العمل التحليلي ضمن إطار العمل القانوني لليوروبول، وهو ما يهدف في المقام الأول إلى تمكين السلطات المشاركة من ضمان التنسيق والتعاون الكاملين.

٢٨٩- وعلى الرغم من صعوبة إجراء تقييم على المستوى الدولي لمدى تعاون البلدان على هذا النحو، فإنَّ النقاشات في اجتماع فريق الخبراء قد سلطَّت الضوء على تزايد الوعي لدى دوائر إنفاذ القانون والدوائر الأمنية بأنَّ طبيعة الإرهاب الحديث وطرائق عمل الإرهابيين تجعل من التعاون الوثيق في التحقيقات المتعلقة بالإرهاب عاملا متزايد الأهمية في نجاح الجهود الرامية لإحباط الأعمال الإرهابية ومنعها والملاحقة القضائية بشأنها.

(١٥٢) Eveline R. Hertzberger, *Counter-Terrorism Intelligence Cooperation in the European Union* (Turin, Italy, United Nations Interregional Crime and Justice Research Institute, July 2007).

هاء- التعاون الرسمي مقابل التعاون غير الرسمي

٢٩٠- من الممكن أن يتخذ التعاون الدولي في قضايا الإرهاب التي يكون أحد العناصر المكونة لها ذا طابع عابر للحدود أشكالا عديدة، حسب طبيعة الجريمة التي يجري التحقيق فيها، ونوع المساعدة المطلوبة، والتشريعات الوطنية المنطبقة، ووجود معاهدات أو ترتيبات داعمة وحالة هذه المعاهدات أو الترتيبات.

٢٩١- وبالرغم من التحسن في المستوى العام للكفاءة والفعالية في الإجراءات الرسمية للمساعدة القانونية المتبادلة في القضايا الجنائية، فلم يزل ممكناً أن تستغرق هذه الإجراءات وقتا طويلا وتتطلب قدرا كبيرا من البيروقراطية في كل من الدولة الطالبة والدولة متلقية الطلب. وفي العديد من قضايا الإرهاب، ولا سيما القضايا التي تنطوي على جرائم ذات صلة بالإنترنت، يتبيَّن أنَّ التعاون غير الرسمي له من الأهمية ما للقنوات الرسمية، بحيث يمكّن من تلافي الكثير من التأخير في الحالات التي يكون فيها اتخاذ تدابير عاجلة (مثل حفظ بيانات استخدام الإنترنت) ذا أهمية جوهرية في التوصل إلى نتيجة إيجابية في الملاحقة القضائية. وقد سلط المشاركون في اجتماع فريق الخبراء الضوء على أهمية مبادرة أجهزة الاستخبارات وسلطات إنفاذ القانون وأعضاء النيابات العامة الوطنية باستحداث واستخدام آليات تتيح تيسير قنوات للتعاون الدولي الرسمي وغير الرسمي على حد سواء حيثما كان ذلك ممكناً.

٢٩٢- وفي العديد من القضايا، قد يمكن للسلطات، حين تطلب في أحد البلدان حفظَ بيانات الإنترنت الموجودة لدى مقدم خدمات في بلد آخر، أن تلجأ إلى التعاون غير الرسمي لحفظ هذه البيانات بغرض التحقيق أو الملاحقة القضائية بشأن فعل إجرامي.

٢٩٣- وقد تكون المسائل القانونية المرتبطة بإجراء التحقيقات الجنائية ذات الصلة بالإنترنت، ولا سيما المسائل المتعلقة بالولاية القضائية، معقدة للغاية. ففي الحالات التي يحتاج فيها المحققون في بلد ما أن يسترجعوا معلومات في أجهزة حاسوب موجودة في بلد آخر، قد تطرح أسئلة معقدة حول السلطة القانونية والسند اللذان يخولان لهم القيام بذلك. ولئن أمكن للسلطات في أحد البلدان أن تتعامل مباشرة مع الأطراف الحائزة للمعلومات التي تسعى للحصول عليها من بلد آخر، فقد يتفاوت رد فعل هذه الأطراف إزاء هذا النهج. وكقاعدة عامة، يُستصوب أن تعمل السلطات مع نظيراتها الأجنبية، في إطار التعاون غير الرسمي إن أمكن، للحصول على هذه المعلومات.

٢٩٤- ويتوقف شكل التعاون وطريقته إلى حد كبير على طبيعة المساعدة المطلوبة والغرض المقصود منها. فعلى سبيل المثال، قد تستطيع السلطات في أحد البلدان أن تقدِّم مساعدة غير رسمية لنظيراتها الأجنبية بأن تطلب من مقدمي خدمات الإنترنت أن يحفظوا بيانات متعلقة بالإنترنت طوعياً، لكن تفتيش هذه البيانات وضبطها عادة ما يتطلب تصريحاً قضائياً لا يمكن الحصول عليه إلا عن طريق القنوات الرسمية.

٢٩٥- وفي بعض الأحيان، يكون تقديم طلبات رسمية هو الأسلوب الوحيد الذي يُمكن للسلطات تبادل التعاون المطلوب عبره. وفي هذه الحالات يكون من المهم أن يكون لدى البلدان تشريعات وإجراءات تنص على الاستجابة الفعالة في الوقت المناسب لهذه الطلبات، لتعظيم احتمال نجاح هذه المساعدة بقدر الإمكان.

التعاون غير الرسمي

٢٩٦- نظـراً لأنّ تحديد موقع بيانات الإنترنت في تحقيقات الإرهاب والحصول على هذه البيانات أمران مهمّان وملحّـان، واحتمـال وجود هذه البيانات في بلد آخر، فقد يقتضـي الأمر من المحققين أن يأخذوا بعين الاعتبار كلا مـن الوسائل الرسميـة وغير الرسمية للحصـول عليها. وإذا كانت درجـة اليقين التي تتيحهـا القنوات الرسمية للمساعـدة القانونيـة المتبادلة أكبر فيمـا يخص المسائل القانونيـة ذات الصلة، فإنَّها تحتـاج كذلك لوقت أطول وتتطلب قدرا أكبر من البيروقراطية مقارنةً بالقنوات غير الرسمية.

٢٩٧- وفي اجتمـاع فريـق الخـبراء، شدَّد الخبير الكندي على الـدور الحاسم للتعاون غـير الرسمي بين شرطة الخيالـة الملكية الكنديـة والوكالة الاتحادية لحماية الدولة ومكافحة الإرهـاب في النمسا، والذي قام على تيسيره مسـؤول الاتصـال الكنـدي في فيينا، في نجاح نتيجة الملاحقـة القضائية. وبالإضافة لهـذه القضية، أشار خبراء آخرون إلى أمثلة أخرى مشابهة كان للاستعانة فيها بمسؤول اتصال لتيسير التعاون غير الرسمي دورٌ جوهري في تحقيق نتيجة إيجابية.

٢٩٨- ومـن المرجـح أن تكون البيانات المتعلقـة بالإنترنت، مثل بيانات استخدام العمـلاء الموجودة لدى مقدمي خدمـات الإنترنـت، أدلة حاسمـة في قضايا الإرهاب التي تُستخـدم فيها أجهزة الحاسـوب والإنترنت. فإذا كان بوسع المحققين أن يضمنوا الحيازة المادية لأجهزة الحاسوب التي استخدمها مشتبه به، وكذلك بيانات استخدام الإنترنـت المتعلقـة بهذه الأجهـزة والموجودة لدى مقدمي خدمـات الإنترنت، فإنَّ فرصهم تزيـد في الربط ما بين المشتبه به وارتكاب الجريمة.

٢٩٩- ومن المهم، بأخذ ما سبق في الاعتبار، أن يكون المحققون وأعضاء النيابة العامة مدركين تماما لما قد يكون للبيانـات المتعلقـة بالإنترنت مـن أهمية وللحاجة لاتخاذ خطـوات في أسرع وقت ممكن لحفظهـا بطريقة تضمن مقبوليتهـا كأدلة محتملة في أي دعاوى ترفع لاحقاً. وينبغي لأجهـزة إنفاذ القانون الوطنية أن تضع قدر الإمكان، إما بالتعاون مباشرة مع مقدمي خدمات الإنترنت أو مع نظيراتها في البلدان الأخرى، إجراءات واضحة تتكون من عناصر رسمية وغير رسمية على حد سواء، بهدف ضمان الإسراع ما أمكن بالاحتفاظ ببيانات استخدام الإنترنت المطلوبة لتحقيق جنائي وبتقديمها.

٣٠٠- وفي الولايـات المتحدة الأمريكية، حيث توجد العديد من كبرى شـركات تقديم خدمات الإنترنت، تستعين السلطـات بنهـج "مزدوج" لمساعدة نظيراتهـا الأجنبية في الاحتفاظ بالبيانات المتعلقـة بالإنترنت والموجودة لدى مقدمـي خدمات الإنترنت الذين تقع مقراتهم في الولايات المتحدة وتقـديم هذه البيانات للأغراض الاستدلالية. وبموجـب هذا النهج، يمكـن التعامل مع الطلبات الأجنبيـة بالاحتفاظ بمعلومات حسـاب المستخدم لدى مقدمي خدمات الإنترنت وتقديم هذه المعلومات بطريقتين:

(أ) *الإجراءات غير الرسميـة*: ثَمَّ طريقان يمكن لسلطات التحقيق أن تسلكهما لضمان الاحتفاظ بما هـو موجود في الولايـات المتحدة من بيانات متعلقـة بالإنترنت بالسبل غـير الرسمية: أولا، يمكن للسلطـات الأجنبية أن تقيم علاقة مباشـرة بمقدمي خدمات الإنترنت، وتتقدم بطلب غير رسمي مباشـر للاحتفـاظ بالبيانات المطلوبة وتقديمهـا؛ ثانياً، يمكن للسلطـات الأجنبية، في حالة عدم وجـود علاقـة مباشرة، أن تتقدم بطلب غير رسمي عبر مكتـب التحقيقات الاتحادي، الذي يحيل الطلب إلى مقدم خدمات الإنترنت؛

(ب) *الإجـراءات الرسميـة*: يمكن للسلطـات الأجنبية بموجب هذه الإجـراءات أن تتقدم بطلب رسمي للمساعـدة القانونيـة المتبادلة عبر مكتـب العلاقات الخارجية بوزارة العـدل الأمريكية للحصول

على البيانات المتعلقة بحساب مستخدم معيَّن. ويعرض الطلب عند تلقيه على نظر قسم مكافحة الإرهاب بالوزارة للوقوف على ما إذا كان مرتبطاً بأي تحقيق تجريه سلطات الولايات المتحدة. فإن لم يكن كذلك، يُقدَّم الطلب إلى محكمة اتحادية للحصول على الأمر اللازم بالتصريح بجمع المعلومات المطلوبة وإرسالها لسلطات البلد الطالب.

٣٠١- وقد استُخدم النهج المبيَّن أعلاه في تقديم البيانات المتعلقة بمقدمي خدمات الإنترنت بنجاح في العديد من التحقيقات في قضايا الإرهاب التي اضطلعت بها سلطات المملكة المتحدة والولايات المتحدة. ففي إحدى القضايا، أسفرت الإجراءات عن قيام أحد مقدمي الخدمات في الولايات المتحدة بتقديم كمية كبيرة من بيانات الإنترنت التي اتضحت أهميتها الحاسمة كأدلة في ملاحقة قضائية في المملكة المتحدة.

واو- التحديات والقضايا المطروحة

٣٠٢- إنَّ الإنترنت، بحكم طبيعتها ونطاق تغطيتها الجغرافية الافتراضية وبنيتها المجزأة وسرعة تطور التكنولوجيا المستخدمة فيها، تطرَح باستمرار تحديات وقضايا أمام سلطات إنفاذ القانون والعدالة الجنائية المعنية بالتحقيق والملاحقة القضائية في قضايا الإرهاب. وقد سلط النقاش في اجتماع فريق الخبراء الضوء على بعض المجالات التي تطرح صعوبات في الوقت الراهن فيما يخص التعاون الدولي، بما فيها ما يخص استيفاء مقتضيات ازدواجية التجريم في طلبات تسليم المطلوبين والمساعدة القانونية المتبادلة. فقد شهد بعض الخبراء حالات تأخرت فيها تلبية طلبات تسليم المطلوبين أو المساعدة القانونية المتبادلة أو قوبلت بالرفض بسبب مشكلات في استيفاء مقتضيات ازدواجية التجريم. وحدث ذلك نتيجةً لعدم التوافق فيما بين أحكام التجريم في بعض الأحيان، وللتفسير الضيق أكثر من اللازم لأحكام التجريم المقابلة من قبل القضاء في أحيان أخرى. وقد اعتبر العديد من الخبراء أن هذا الموقف يسلط الضوء على الحاجة لتدريب أعضاء الهيئات القضائية بشأن مسائل التعاون الدولي.

١- *حماية المعلومات الحساسة*

٣٠٣- أشار خبراء من عدة بلدان في اجتماع فريق الخبراء إلى التحديات التي لا تزال مطروحة بخصوص مشاطرة أجهزة إنفاذ القانون وأجهزة الاستخبارات الوطنية لمعلومات استخبارية حساسة مع نظراء أجانب. ففي جميع الأحوال، تستند التحقيقات والملاحقات القضائية الجنائية في قضايا الإرهاب، في مراحلها الأولى على الأقل، إلى معلومات استخبارية تشمل معلومات حساسة سرية ومشمولة بالحماية. فالكشف عن معلومات من هذا القبيل ينطوي على مخاطر كبيرة، لا تقتصر في كثير من الأحيان على مصدر هذه المعلومات وإنما تمتد إلى الجهاز أو الأجهزة التي تحوزها، ولا سيما إذا كان من شأن الكشف عن هذه المعلومات أن ينال من تحقيقات أو عمليات جارية أو مستقبلية.

٣٠٤- وقد يكون أي قرار تتخذه السلطات الوطنية بشأن مشاطرة هذه المعلومات من عدمها، والظروف أو الشروط التي يُمكن أن يتم فيها ذلك، عمليةً معقدة تتطلب مراعاة عدد من العوامل. ومع ذلك، وبغض النظر عن المعايير المحددة التي تُستخدم لتقييم قرار المشاطرة المحتملة للمعلومات، في جميع القضايا وأيا كانت الظروف،

يتعين على الجهة التي تكشف المعلومات أن تتأكد من أنَّ الجهة المتلقية سوف تلتزم بتهيئة ما يُتفق عليه من ضمانات وحماية للمعلومات عندما تصبح في حوزتها.

٢- *السيادة*

٣٠٥- إنَّ مفهوم السيادة، بما يشمل حق الأمم في تقرير وضعها السياسي وممارسة السيادة الدائمة في حدود ولايتها الإقليمية، مبدأ معترف به على نطاق واسع في العلاقات الدولية والقانون الدولي. فقد تطرح القضايا التي تقتضي التحقيق أو الملاحقة القضائية في أنشطة يقوم بها إرهابيون أو غيرهم من المجرمين عبر الحدود مشاكل سيادية للبلدان التي يتعيَّن إجراء التحقيق على أراضيها.

٣٠٦- وفي بعض الحالات، يُمكن أن تقف مخاوف السلطات الوطنية مما تعتبره مساسا بسيادة الدولة التي تنتمي إليها، سواء أكان لتلك المخاوف أساس من الصحة أم لا، حائلا أمام التعاون الدولي الفعال في القضايا الجنائية. ومن ثم فمن المهم، عند النظر في اتخاذ إجراءات للتحقيق بجمع أدلة تتعلق بأجهزة حاسوب أو بالإنترنت، أن يأخذ المحققون وأعضاء النيابة العامة بعين الاعتبار الآثار المحتملة لإجراءات التحقيق هذه على سيادة الدول الأخرى (كما هو الحال حين تقوم السلطات في أحد البلدان بعملية تفتيش عن بعد لجهاز حاسوب يشغله مشتبه به موجود في بلد آخر).

٣٠٧- وبصفة عامة، ينبغي للسلطات الوطنية التي تدرس إمكانية اتخاذ خطوات للتحقيق بشأن أشخاص موجودين أو أشياء موجودة في ولاية قضائية أخرى أن تخطر نظيراتها الأجنبية في البلدان ذات الصلة بهذه الإجراءات وتنسقها معها متى كان ذلك ممكناً.

٣- *الاحتفاظ بالبيانات المتعلقة بالإنترنت وتقديمها*

٣٠٨- هناك، كما ذُكر آنفا، جزء هام من الأدلة ضد من يشتبه في كونهم جناة في العديد من قضايا الإرهاب يتعلق بجانب من جوانب الأنشطة التي يقوم بها المشتبه به على الإنترنت (مثل معلومات السداد بالبطاقات الائتمانية وبيانات الاستخدام المتعلقة بالعملاء بخصوص الاتصالات على الإنترنت من قبيل البريد الإلكتروني، وبروتوكول الاتصال الصوتي عبر الإنترنت، وسكايب، أو المتعلقة بشبكات التواصل الاجتماعي أو غيرها من المواقع الشبكية). ويتعين على سلطات التحقيق في العديد من القضايا ضمان الاحتفاظ ببيانات الإنترنت ذات الصلة وحفظها حتى تُستخدم لاحقاً ضمن الأدلة في الدعاوى المرفوعة. وفي هذا الصدد، من المهم أن نشير إلى الفرق ما بين "الاحتفاظ" بالبيانات و"حفظ" البيانات. ففي العديد من البلدان، يُلزِم القانون مقدمي خدمات الإنترنت بالاحتفاظ بأنواع معيَّنة من البيانات لمدة زمنية محددة. أما الحفظ فيعني واجبا مفروضاً على مقدم خدمات الإنترنت، تبعاً لأمر قضائي أو مذكرة قضائية أو توجيه قضائي، بحفظ البيانات وفقاً لأحكام وشروط محددة لتُقدَّم كأدلة في الدعاوى الجنائية.

٣٠٩- ومن بين المشكلات الكبرى التي تواجه أجهزة إنفاذ القانون كافة الافتقارُ إلى إطار عمل دولي متفق عليه للاحتفاظ بالبيانات الموجودة لدى مقدمي خدمات الإنترنت. وإذا كانت حكومات العديد من البلدان قد فرضت واجبات قانونية على مقدمي خدمات الإنترنت المحليين بالاحتفاظ بالبيانات المتعلقة بالإنترنت بغرض إنفاذ القانون، فليس هنالك على المستوى الدولي أية مدة زمنية موحّدة تحظى بالإجماع ويُلزَم كل مقدم من مقدمي خدمات الإنترنت بالاحتفاظ بهذه المعلومات طيلتها.

٣١٠- ونتيجة لذلك، يكون المحققون في البلدان التي تلزِم مقدمي خدمات الإنترنت بالاحتفاظ بالبيانات متيقنين إلى حد ما، حين يجرون تحقيقات محلية بالكامل، من نوعية بيانات الإنترنت التي يحتفظ بها مقدمو خدمات الإنترنت ومدة احتفاظهم بها، إلا أن هذا القول لا يصح في حالة التحقيقات التي تتطلب منهم جمع بيانات موجودة لدى أحد مقدمي خدمات الإنترنت في بلد آخر.

٣١١- وفي الولايات المتحدة، يتطلب النهج المتبع في الوقت الراهن من مقدمي خدمات الإنترنت أن يحتفظوا ببيانات الاستخدام عند تلقيهم طلباً محدداً بذلك من أجهزة إنفاذ القانون، على أن سياسات مدد الاحتفاظ بالبيانات تتفاوت تفاوتاً كبيرا بين مختلف مقدمي الخدمات، بحيث تتراوح بين بضعة أيام وعدة شهور.

٣١٢- ورغم بذل بعض الجهود، لعل أبرزها في الاتحاد الأوروبي، لتحقيق شيء من الاتساق في هذا المجال، فما زالت الصعوبات تكتنفه، حتى على مستوى الاتحاد الأوروبي. فبموجب التوجيه 2006/24/EC الصادر عن البرلمان الأوروبي ومجلس الاتحاد الأوروبي في ١٥ آذار/مارس ٢٠٠٦ بشأن الاحتفاظ بالبيانات التي يتم توليدها أو معالجتها في إطار توفير خدمات الاتصالات الإلكترونية المتاحة للجمهور أو شبكات الاتصالات العامة، الذي يعدَّل بموجبه التوجيه 2002/58/EC، فيما يتعلق بالاحتفاظ بالبيانات الموجودة لدى مقدمي خدمات الاتصالات الإلكترونية وشبكات الاتصالات العامة، تلتزم الدول الأعضاء في الاتحاد الأوروبي بضمان احتفاظ مقدمي الخدمات الخاضعين للتنظيم الرقابي ببيانات اتصالات محددة لمدة تتراوح بين ستة أشهر وعامين. ومع ذلك، ليست هناك حتى الآن، بالرغم من التوجيه، مدة واحدة يتفق جميع مقدمي خدمات الإنترنت الموجودين في الاتحاد الأوروبي على الاحتفاظ بالبيانات طيلتها، إذ تتراوح مدد الاحتفاظ بين ستة أشهر وعامين كما هو منصوص عليه في التوجيه. ونتيجة لذلك، ثمة اختلافات في المدد التي يحتفظ مقدمو خدمات الإنترنت العاملون في الاتحاد الأوروبي خلالها بالبيانات، رغم أن درجة اليقين بشأن هذه المسائل قد ارتفعت حتى داخل الاتحاد نفسه.

٣١٣- وقد رأى عدة مشاركين في اجتماع فريق الخبراء أنَّ من شأن وضع إطار عمل تنظيمي مقبول عالمياً يفرض واجبات موحدة على كل مقدمي خدمات الإنترنت فيما يخص نوعية ومدة الاحتفاظ ببيانات الاستخدام المتعلقة بالعملاء أن يعود بفائدة كبيرة على أجهزة إنفاذ القانون وأجهزة الاستخبارات التي تحقق في قضايا الإرهاب.

٣١٤- ونظراً لعدم وجود معايير أو واجبات متفق عليها عالمياً تُفرض على مقدمي خدمات الإنترنت وغيرهم من مقدمي خدمات الاتصال فيما يخص الاحتفاظ بالبيانات المتعلقة بالإنترنت، فمن المهم في التحقيقات الجنائية أن يتأكد المحققون وأعضاء النيابة العامة في أسرع وقت ممكن مما إذا كانت هذه البيانات موجودة، ومن المدة الزمنية للاحتفاظ بها، ومما إذا كان من المرجَّح أن تكون ذات فائدة للملاحقة القضائية، ومن مكان وجودها، وكذلك من المدة الزمنية التي على الجهة التي توجد البيانات في حوزتها أن تحتفظ بها طيلتها، في حال تحديد تلك المدة. وفي حال الشك في وجود البيانات، من الحصافة أن تتصل السلطات بنظيراتها في البلد الذي توجد فيه البيانات وتتخذ ما قد يلزم من خطوات (رسمية أو غير رسمية) لضمان حفظ البيانات ليتأتى تقديمها في المحاكمة إن اقتضى الأمر ذلك. ويمكن للسلطات أن تنظر، حسب الظروف، بما في ذلك سابق المعرفة بين السلطات ومقدم خدمات الإنترنت المعني أو العلاقة بينهما، في الاتصال بمقدم خدمة الإنترنت مباشرة طلباً لمساعدته بصفة غير رسمية. إلا أنَّ مستوى تجاوب مقدمي خدمات الإنترنت مع هذه الطلبات غير الرسمية المباشرة قد يتفاوت تفاوتاً كبيراً، نظراً للحساسيات الناتجة عن الامتثال للقوانين المتعلقة بسرية بيانات العملاء والقوانين الوطنية المتعلقة بالخصوصية. ومن الحصافة في جميع الأحوال أن يقوم المحققون وأعضاء النيابة العامة بالاتصال بنظرائهم الأجانب وتنسيق جهودهم معهم لضمان حفظ هذه المعلومات وتقديمها.

٤- *المتطلبات المتعلقة بالأدلة*

٣١٥- يتعين على المحققين وأعضاء النيابة العامة أن يتوخوا الحذر الشديد لضمان الامتثال في الوسائل المتبعة في جمع الشهادات والأحراز وغيرها من المعلومات أو حفظها أو تقديمها أو إرسالها تمامَ الامتثال للقوانين المنطبقة، والمبادئ القانونية، وقواعد الإثبات، حتى تكون مقبولة كأدلة في الدعاوى الجنائية. ومن شأن عدم مراعاة المتطلبات المتعلقة بمقبولية الأدلة إضعافُ حجة الادعاء، إلى الحد الذي قد يؤدي إلى اضطرار السلطات إلى وقف الملاحقة القضائية أو سحبها. ففي قضية *ناموح*، استطاع أعضاء النيابة الكندية، بالتعاون الوثيق مع نظرائهم النمساويين، أن يضمنوا جمع الأدلة الحيوية المتعلقة باستخدام المدَّعى عليه لمنتديات الدردشة على الإنترنت والمواقع الشبكية وإرسال هذه الأدلة إلى كندا بشكل يمكن قبوله بالرغم من وجود اختلافات بين البلدين في قواعد الإثبات المعمول بها.

٣١٦- وهناك، في إطار قضايا الإرهاب، عدد من المسائل التي قد تطرح تحديات ذات شأن أمام السلطات من حيث قدرتها على ضمان قبول أنواع معينة من المعلومات. ولم يزل التغلب على هذه التحديات بنجاح من الصعوبات التي يلاقيها جميع الممارسين القائمين بالتحقيق والملاحقة القضائية في القضايا المتعلقة بالإرهاب، التي كثيراً ما تنطوي على خصائص يمكن أن تقف حائلا دون قبول المعلومات. فالطبيعة العابرة للحدود الوطنية لقضايا الإرهاب، بما يشمل الاستخدام المكثف للمعلومات الاستخبارية (التي يقدمها في كثير من الأحيان شركاء أجانب بشروط صارمة) أو أساليب التفتيش والمراقبة والاعتراض العالية التخصص، والتي غالباً ما تكون سرية وتطفلية، باعتبارها أساساً لجمع الأدلة، يمكن أن تضع عقبات كأداء في طريق السلطات التي ترغب في تقديم أدلة تحظى بالمقبولية لدى محكمة أو هيئة قضائية.

٣١٧- وفي سياق الإرهاب، يظل النهج العام المتبع من قبل المحققين وأعضاء النيابة العامة كما هو فيما يتصل بوجه خاص بالمسائل المتعلقة بالأدلة التي قد تنشأ بشأن تكنولوجيا الإنترنت أو الحاسوب. ويرجَّح أن يكون من بين المسائل التي لها أهمية خاصة الحاجةُ لتأمين الحيازة المادية في أسرع وقت ممكن لأجهزة الحاسوب أو غيرها من الأجهزة المشابهة المزعوم استخدامها من قبل المشتبه بهم، والحاجةُ لإعمال تدابير مناسبة، بما يتفق والممارسات الجيدة المتعارف عليها، لحماية سلامة هذه الأحراز (أي تسلسل العهدة/الأدلة) والاضطلاع بما يلزم من تحاليل جنائية رقمية. ومن شأن عدم اتباع هذه الإجراءات احتمال التأثير على مقبولية هذا النوع من الأدلة. ومن بين الأشكال الأخرى للأدلة التي قد تتطلب عناية خاصة الموادُ التي يتم الحصول عليها نتيجة لأنشطة التفتيش أو المراقبة أو كليهما معاً، والتي يجب ألا تنفَّذ إلا في حدود ما يسمح به تصريح قضائي صادر لهذا الغرض حسب الأصول.

٣١٨- ومن المهم، عند تناول المسائل المتعلقة بالأدلة في مرحلة التحقيق، أن يكون لدى المحققين فكرة واضحة عن القواعد والمبادئ القانونية المنطبقة على إجراءات التحقيق التي يضطلعون بها في إطار التحقيق و/أو أن يتواصلوا تواصلا وثيقا مع أعضاء النيابة العامة، سواء بإطلاعهم على آخر التطورات أو بطلب المشورة القانونية منهم. وفي الحالات التي يجري فيها جمع الأدلة من قبل السلطات في أحد البلدان لتُستخدم في ملاحقة قضائية في بلد آخر، يكون التواصل والتنسيق الوثيقان مع النظراء الأجانب بشأن الإجراءات المتبعة لجمع وحفظ الأدلة مهمّين للغاية. ومن المهم، في إطار هذا التنسيق، أن يكون لدى السلطات التي تضطلع بإجراءات التحقيق فكرة واضحة عن متطلبات الأدلة والآثار المترتبة على ما يتخذونه من إجراءات في الولاية القضائية التي ستُستخدم

فيهـا الأدلـة في نهاية المطاف. ويتناول تقريـر مكتب الأمم المتحدة المعني بالمخـدِّرات والجريمة المعنون "خلاصة قضايا الإرهاب" المسائل المرتبطة بمقبولية الأدلة الأجنبية في *قضايا الإرهاب* بمزيد من التفصيل.[١٥٣]

٥- *ازدواجية التجريم*

٣١٩- من بين المتطلبات الشائعة في الصكوك العالمية لمكافحة الإرهاب وغيرها من الصكوك الدولية والإقليمية والثنائيـة المتعلقة بالإرهاب والجريمة المنظمة العابرة للحدود الوطنيـة، أن التصرفات غير القانونية التي تشكِّل جرائـم في كل مـن الدولة الطالبـة والدولة متلقية الطلب هي التي تُتخذ دون غيرهـا أساساً للتعاون الدولي. ومن الممكـن أن يطـرح هذا المتطلـب، المعروف باسـم "ازدواجية التجـريم"، صعوبات في كل التحقيقـات والملاحقات القضائيـة الجنائية، لا المتعلقة منهـا بالإرهاب فحسب، التي يكون التعاون الدولي جانبـا من جوانبها. وقد أشار العديـد مـن المشاركين في اجتماع فريق الخبراء إلى مسألة ازدواجية التجـريم بوصفها مشكلة أساسية مطروحة حتـى الآن، بحيـث كثيراً ما تقود إلى رفض طلبات المساعدة القانونيـة المتبادلة أو تسليم المطلوبين إذا ما اعتبرت السلطات في البلدان متلقية الطلب أنَّ متطلب ازدواجية التجريم لم يُستوف.

٣٢٠- ومـن المرجح، في سيـاق الإرهاب، وفي ظل عدم وجود أي التزام عام علـى جميع الدول بتجريم تصرفات غـير قانونية محـددة على الإنترنت، أن تعتمـد السلطات، عند تقديمهـا أو تلقيها لطلبات التعـاون الدولي، على الجرائـم المنصوص عليها في التشريعـات المتعلقة بالإرهاب أو قوانين العقوبات الوطنية لديها. فعلى سبيل المثال، قـد يقتضي الأمـر، في حالة الادعاء بوقوع أعمال تحريض على الإرهاب علـى الإنترنت، أن تستند طلبات التعاون الدولي، نظراً للاختلافات في النُّهج القانونية التي تتبعها الدول في التعامل مع أعمال من هذا القبيل، إلى جرائم غير مكتملة مثل جريمة التحريض.

٣٢١- وعنـد تنـاول الحكومات لهـذه المسألـة، يُستصـوب أن تصيغ أحكام تجـريم التصرفات غـير القانونية ذات الصلـة بالإرهـاب بعبـارات تقترب قـدر الإمكان من العبـارات الـواردة في الصكوك المعنيـة. وعلاوة على ذلـك، ينبغـي أن تُصـاغ التشريعـات، إلى الحد المسموح بـه في النظم القانونيـة الوطنيـة، دون تقييد لا مبرر له فيمـا يخص مسألـة ازدواجية التجريم، بحيث تتيح للسلطات المركزية والقضـاة مجالا كافياً للتركيز على جوهر التصـرف غـير القانوني موضوع الطلب وتقييمه. ومـن شأن اعتماد الدول هذا النهـج التشريعي على نحو موحَّد تحقيـق فوائـد التجانـس التشريعـي المقصـود في الصكوك كاملـةً، وتقليل احتمـال وقوع مشـكلات فيما يخص ازدواجية التجريم.

٣٢٢- وعلى الرغم من أن المسائل المتعلقة بازدواجية التجريم قد تعقّد القضايا الجنائية التي تتطلب تعاونا دوليا بصفة عامة، فإنَّ هذه المسائل قد تعقّد بالأخص القضايا التي تنطوي على جرائم إرهاب معينة تُرتكب باستخدام الإنترنـت (مثـل التحريض)، حيث يزيد احتمال عدم التوافق فيما بين أطر العمل التشريعية والدستورية الوطنية في مختلـف الـدول. ومن بين الأمثلة على ذلك ما نوقش في اجتماع فريق الخبراء بشـأن موقف الولايات المتحدة تجـاه تسليـم الأشخاص الموجودين على أراضيهـا والمتهمين بجريمـة التحريض. ففي هذا البلـد، ثمة ضمانات دستورية قوية فيما يتعلق بحرية التعبير، منصوص عليها في التعديل الأول لدستور الولايات المتحدة. وينص قانون

[١٥٣] انظر مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة، *خلاصة قضايا الإرهاب*، الفقرات ٢٩٢-٢٩٥.

الولايـات المتحـدة على أن الأقوال التي تعتبر في حكم المناصـرة المستقلة لأي موقف إيديولوجي أو ديني أو سياسي لا تُعتـبر أعمـالا إجرامية في حد ذاتها، بالرغم من أنها قد تُشـكِّل أعمالا تعتبر في حكم تقديم معلومات بناءً على توجيهـات تنظيم إرهابـي أو سعياً للسيطرة على تنظيم إرهابي، أو قد تنـدرج في إطار جريمة التحريض. ونظراً لهذا الموقف، فإنَّ طلبات المساعدة القانونية المتبادلة أو تسليم المطلوبين المتعلقة بأعمال تحريض وقع أحد أركانها داخل الولايات المتحدة قد تطرح صعوبات من منظور ازدواجية التجريم، بما يقتضي من السلطات في كلا البلدين أن تتخذ نهجاً مرناً وعملياً.

٣٢٣- وبالإضافـة إلى وجود تشريعات متوافقة والاستنـاد إلى نهج مرن في تطبيق هذه التشريعات، من المهم أن يكون للمحققين وأعضاء النيابة العامة والقضاة إلمام جيد بهذه المواضيع، وأن يفهموا موقع آليات التعاون الدولي في سياق تصدي المجتمع الدولي للإرهاب والجريمة المنظمة العابرة للحدود الوطنية.

٦- *الاختلاف في تطبيق الضمانات الدستورية وضمانات حقوق الإنسان*

٣٢٤- هنـاك صلـة بين الأمـور المتعلقة بضمانات حقـوق الإنسان والضمانـات الدستورية والعديـد من المسائل المرتبطـة بالتحقيق في الإرهاب والملاحقة القضائية بشأنه، بما فيهـا مسائل التعاون الدولي. وبالاستعانة مجددا بمثال الأعمال المتعلقة بالتحريض على الإرهاب، من الممكن أن يتبدى اختلاف النُّهُج القانونية في اختلاف النُّهُج الوطنيـة إزاء تطبيـق الحقوق الدستورية أو حقوق الإنسان أو كليهما معـاً. وقد يؤدي ذلك إلى صعوبات في قضايا التعـاون الدولي التي تسعى فيها الـدول إلى طلب المساعدة أو تقديمها. فعلى سبيل المثال، عندما تتقدم السلطات في أحـد البلدان بطلـب لنظيراتها في بلد آخر بتقديم بيانات متعلقة بالإنترنت تخص أقوالا صدرت على الإنترنت تعتـبر في حكـم التحريض علـى ارتكاب الإرهـاب في ولايتها القضائية، فمـن الأهمية بمكان تقرير مـا إذا كانت الأعمـال المزعومـة تشكِّل جريمة في البلد متلقي الطلب أيضـاً. وفي سياق أعم، هو مراقبة محتويات الإنترنت، قد يختلف ما هو مطبَّق من قوانين وضمانات دستورية لحقوق من قبيل الحق في حرية التعبير عندما تسعى السلطات في أحـد البلـدان إلى إزالة محتوى تعتبره يحرض على الإرهاب، ويكون هذا المحتوى مستضافاً على خادوم موجود في ولاية قضائية أخرى.

٣٢٥- وتجـدر الإشارة على وجه الخصوص إلى بعض أنـواع المحتويات المتعلقة بالإرهاب على البريد الإلكتروني أو الإنترنـت التـي تمر عبر مقدمين لخدمـات الإنترنت موجودين في الولايات المتحدة أو تُخـزَّن لديهم. فحسب طبيعـة وسيـاق هذا المحتوى، قد تطـرح هذه الحالات، التي تندرج في نطاق اختصاص الولايات المتحدة، مشاكل نظـراً للحمايـة القويـة التي تحظى بها حريـة التعبير بموجب التعديـل الأول لدستور الولايـات المتحدة. وفي هذه الحـالات، يتعين علـى السلطات في مختلف البلدان أن تتواصل عن كثب للوقـوف على ما يمكن اتخاذه من تدابير وقائية أو تدابير الملاحقة القضائية، إن وجدت، وفقا لقوانينها الوطنية، وقواعدها القانونية ومعاييرها الثقافية، والتزاماتها الدولية بمكافحة الإرهاب.

٧- *الاختصاص المشترك*

٣٢٦- يُمكـن أن تُطـرح مسائل معقدة بشـأن اختصاص النظر في قضايا الإرهاب التـي تنفَّذ فيها أعمال تشكل أركان جريمة على الإنترنت، ولا سيما حين يكون أحد من يشتبه في كونهم جناة موجوداً في أحد البلدان ويستخدم مواقـع أو خدمـات على الإنترنت يستضيفهـا مقدمو خدمات في بلد آخر ليقوم بأعمـال تشكِّل أركان جريمة. وقد

كانت هناك حالات أنشأ فيها أشخاص مقيمون في أحد البلدان مواقع شبكية وأداروها لاستخدامها في الترويج للأنشطة الجهادية وغير ذلك من الأغراض المتعلقة بالإرهاب.

٣٢٧- وتعدُّ القضية البلجيكية *مليكة العروض وآخرون* (انظر الفقرة ٣٧٧) أحد الأمثلة على هذه القضايا. فالمدَّعى عليها، التي كانت مقيمة في بلجيكا، كانت تدير موقعاً شبكياً مستضافاً في كندا، واستخدمته في الترويج للأنشطة الجهادية ولأغراض أخرى تهدف إلى دعم الأنشطة الإرهابية. وتعتمد الملاحقة القضائية بشأن الأنشطة المتعلقة بالإرهاب في هذه الحالات اعتماداً كبيراً على التعاون الدولي الفعال.

٣٢٨- وليس ثمة قواعد مُلزمة بموجب القانون الدولي تتناول مسألة الطريقة التي ينبغي أن تتعامل بها الدول مع الحالات التي تدعي فيها أكثر من دولة واحدة أنَّ لها اختصاص الملاحقة القضائية بشأن جريمة ارتكبها نفس المشتبه به. وبالرغم من أنَّ لدى الدول سلطة تقديرية واسعة فيما يخص المعايير المطبَّقة، فإنَّ هذه الحالة عادة ما تتطلب الموازنة فيما بين عدد من العوامل، بما قد يشمل "الصلة" النسبية بين الجريمة المزعومة ودولة بعينها، بما في ذلك جنسية المشتبه به، والمكان الذي وقعت فيه شتى الأعمال المكوِّنة لأركان الجريمة، والمكان الذي يوجد فيه الشهود المعنيون والأدلة ذات الصلة، والصعوبات النسبية التي قد تطرح في جمع الأدلة وإرسالها وتقديمها في ولاية قضائية بعينها. وفي بعض الدول، بما فيها إسبانيا وبلجيكا وكندا، تُعتبر أشكال معينة من الاختصاص فرعية بالمقارنة مع أشكال أخرى. فالدول التي لها صلات وثيقة بجريمة ما (كما في حالة ارتكاب الجريمة على أراضيها أو من قبل أحد رعاياها) تُعتبر صاحبة الاختصاص الأساسي، ولا تستطيع البلدان التي تدعي لنفسها الاختصاص استناداً إلى أسباب أخرى ممارسةَ هذا الاختصاص إلا عندما تكون الدولة صاحبة الاختصاص الأساسي غير راغبة في الملاحقة القضائية أو غير قادرة عليها.[١٥٤]

٣٢٩- ويطبق بعض البلدان، بما فيها كندا، اختبار "الصلة الفعلية والجوهرية" حين تُقرر وجود الولاية القضائية الجنائية من عدمه.[١٥٥] وفي إسرائيل، يُحقق على الصعيد المحلي في طلبات التعاون الدولي الواردة من بلدان أخرى لتقرير ما إذا كان من الممكن إثبات ارتكاب جريمة بموجب القانون الإسرائيلي ينبغي ملاحقتها قضائياً في إسرائيل. فإن لم يفض هذا التحقيق إلى ملاحقة قضائية، تقوم السلطات الإسرائيلية بإرسال كل الأدلة المتاحة [ونقل من يشتبه بكونه جانيا] عبر القنوات الرسمية إلى الدولة الطالبة بغرض ملاحقته قضائياً هناك. وفي المملكة المتحدة، يمكن للسلطات البريطانية، بموجب التشريعات والسوابق القضائية المتعلقة بجرائم إرهاب معينة تنفَّذ فيها أنشطة خارج المملكة المتحدة (بوسائل منها الإنترنت)، ممارسةُ اختصاصها إذا كان من الممكن إثبات أنَّ "قدراً جوهرياً" من الأنشطة المكوِّنة للجريمة قد وقع في المملكة المتحدة، وإذا كان من الممكن الدفع في حدود المعقول بأنَّه لا ينبغي لبلد آخر ممارسة اختصاص النظر في هذه الأنشطة.

٣٣٠- ويتعين على السلطات المركزية (أعضاء النيابة العامة غالباً)، في سياق سعيها لحل المسائل المتعلقة بالاختصاص المشترك أو ما يتصل بذلك من أنشطة التعاون الدولي، أن تدرك في مرحلة مبكرة الحاجة إلى الإسراع بالتواصل والتعاون مع نظيراتها في الولايات القضائية الأخرى، التي قد يكون لها مصلحة في رفع دعوى ضد نفس الشخص المشتبه في كونه جانيا. وينبغي أن يُبتّ في توقيت وكيفية بدء هذا التواصل حسب

(١٥٤) International Bar Association, Legal Practice Division, *Report of the Task Force on Extraterritorial Jurisdiction* (2008), pp. 172-173.

(١٥٥) *R. v. Hape* [2007] 2 SCR.292, 2007 SCC 26, para. 62.

كل حالة على حدة، بعد الدراسة الكاملة لشتى العوامل التي قد يكون لها دور في القضية محل النظر. ويمكن لأعضاء النيابة العامة أن يجدوا إرشادات مفيدة في هذا الصدد في التقرير الصادر عن النائبين العامين للملكة المتحدة والولايات المتحدة عام ٢٠٠٧ بعنوان "إرشادات حول كيفية التعامل مع القضايا الجنائية التي تشترك المملكة المتحدة والولايات المتحدة في اختصاص النظر فيها".[١٥٦] ويوصي التقرير، في سياق "القضايا الجنائية الأكثر خطورة أو حساسية أو تعقيداً" (التي يشير إليها التقرير)، بتحسين تبادل المعلومات والتواصل فيما بين أعضاء النيابة العامة في البلدين. وللمساعدة على البت فيما إذا كان ينبغي بدء هذا التواصل، يقترح التقرير طرح السؤال التالي: "هل يبدو أنَّ هناك إمكانية حقيقية لأن يهتم أحد أعضاء النيابة العامة [في البلد الآخر] بملاحقة هذه القضية قضائياً؟ عادة ما يكون لقضية كهذه صلات وثيقة [بالبلد الآخر]". وإذا كان توقيت بدء التواصل بشأن المسائل المتعلقة بالاختصاص والتعاون الدولي وطريقة هذا التواصل يتفاوتان تبعاً لظروف كل قضية على حدة، فيمكن لأعضاء النيابة العامة الاسترشاد بهذا الاختبار في أداء عملهم.

٨- *القوانين الوطنية بشأن الخصوصية وحماية البيانات*

٣٣١- قد تحد القوانين الوطنية بشأن الخصوصية وحماية البيانات في كثير من الأحيان من قدرة أجهزة إنفاذ القانون وأجهزة الاستخبارات على مشاطرة المعلومات مع نظيراتها الوطنية والأجنبية على حد سواء. وهناك في هذا السياق أيضا تحد ما زال مطروحا أمام الحكومات هو تحقيق التوازن الملائم فيما بين حق الإنسان في الخصوصية وبين المصلحة المشروعة للدولة في التحقيق في الجرائم والملاحقة القضائية الفعالة بشأنها، وهو مدعاة للقلق في بعض الحالات (ومنها تدابير التصدي للإرهاب).[١٥٧]

٣٣٢- وبالإضافة إلى التشريعات التي تتضمن إرشادات واضحة للمحققين وأعضاء النيابة العامة ومقدمي خدمات الإنترنت الحائزين للبيانات (في حالة بيانات الإنترنت) بشأن الالتزامات المتعلقة بجمع البيانات الشخصية واستخدامها، من المهم أيضا أن تنشئ البلدان آليات فعالة للإشراف على أجهزة الاستخبارات وأجهزة إنفاذ القانون وتشغلها. وينبغي للحكومات أن تضمن إدراج آليات مناسبة في قوانينها الوطنية لتمكين السلطات من مشاطرة المعلومات ذات الصلة بالتحقيق والملاحقة القضائية في قضايا الإرهاب، رهناً بوجود ضمانات مناسبة للخصوصية، مع نظيراتها الوطنية والأجنبية على حد سواء.

٩- *الطلبات المستندة لمعاهدات مقابل الطلبات غير المستندة لمعاهدات*

٣٣٣- تتفاوت النُّهُج الوطنية تجاه تيسير طلبات التعاون غير المستندة لمعاهدات، حيث توجد في بعض البلدان قيود لا تسمح لها بالتعاون الرسمي في حالة عدم وجود معاهدة. وإقراراً بذلك، تنص الصكوك العالمية لمكافحة الإرهاب والجريمة المنظمة العابرة للحدود الوطنية على أن تُعتبر الصكوك نفسها بمثابة أساس قانوني للتعاون

[١٥٦] انظر الرابط التالي: www.publications.parliament.uk/pa/ld200607/ldlwa/70125ws1.pdf.

[١٥٧] انظر تقرير المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب لعام ٢٠٠٩ (A/HRC/10/3)، والذي أعرب فيه المقرر الخاص عن مخاوف بشأن الاعتداء على حق الفرد في الخصوصية بسبب تزايد المراقبة وتبادل المعلومات الاستخباراتية فيما بين الأجهزة الحكومية.

وللتعامل مع تصرفات غير قانونية محددة بوصفها جرائم تكفي لأغراض المساعدة القانونية المتبادلة وتسليم المطلوبين ضمن القوانين الوطنية للدول الأطراف.

٣٣٤- ويعتمد العديد من البلدان، بما فيها الصين، على مبدأ المعاملة بالمثل أساساً للتعاون الدولي. وبموجب القانون الصيني، يُمكن لأجهزة إنفاذ القانون والسلطات القضائية أن تضطلع بأنشطة التعاون الدولي، بما في ذلك المساعدة المتبادلة والتعاون القضائي (بما يشمل تسليم المطلوبين)، على أساس تعاهدي. وفي حالة عدم وجود معاهدة، يُمكن كذلك للمعاملة بالمثل أن تكون أساساً للمساعدة المتبادلة والتعاون في تسليم المطلوبين. وسلط الخبير الصيني الضوء في اجتماع فريق الخبراء على أحد الأمثلة على التعاون الدولي الناجح بين السلطات في الصين والولايات المتحدة، بحيث أمكن إغلاق أكبر موقع شبكي إباحي باللغة الصينية في العالم، والذي كان مستضافاً في الولايات المتحدة ومستهدِفاً لمستخدمي الإنترنت في الصين وبلدان آسيوية أخرى.

٣٣٥- وأشار عدد من المشاركين في اجتماع فريق الخبراء إلى المسائل المتعلقة بالطبيعة الحساسة للكثير من المعلومات (المستندة في كثير من الأحيان إلى الاستخبارات) المرتبطة بتحقيقات الإرهاب والتحديات الكامنة، ليس في سياق التعاون الدولي فحسب وإنما كذلك على المستوى الوطني، التي تواجه الأجهزة التي تود مشاطرة معلومات من هذا القبيل مع نظيراتها. وسلط العديد من الخبراء الضوء على الطبيعة الشديدة الحساسية لكثير من المعلومات، بحيث تصعب مشاطرتها في ظل عدم وجود آلية رسمية لتبادل المعلومات تفرض شروطا مناسبة فيما يخص استخدام هذه المعلومات والإفصاح عنها.

٣٣٦- وسوف تناقَش هذه المسألة بمزيد من التفصيل في الفصل التالي، المعني بالملاحقات القضائية، في سياق المسائل المتعلقة بالأدلة والمرتبطة بتحويل المعلومات الاستخبارية إلى أدلة يمكن قبولها والكشف عن الأدلة في الدعاوى الجنائية.

سادساً- الملاحقة القضائية

ألف- مقدِّمة

٣٣٧- يعـدُّ الواجب المفروض على الدول بالامتناع عن توفير الملاذ الآمـن لمرتكبي الأعمال الإرهابية وتقديمهم للعدالـة، أينمـا كان مكان وقوع هذه الأعمـال، جزءاً لا يتجزأ من الإطار القانوني العالمـي لمكافحة الإرهاب، ومن استراتيجيـة الأمم المتحـدة العالمية لمكافحة الإرهـاب. وحتى يمكن تحقيق هذه الأهـداف كاملةً، لا تحتاج الدول إلى تشريعـات فعَّالـة لمكافحة الإرهاب وتجريم الأعمـال الإرهابية وتيسير التعاون الدولي الـلازم فحسب، وإنما كذلك إلى القدرة على إعمال تقنيات متخصصة للتحقيق واستراتيجيات متخصصة للملاحقة القضائية لضمان الحصـول علـى الأدلة (التـي كثيرا ما تكون مستنـدة إلى معلومـات استخبارية) وحفظها وتقديمهـا ومقبوليتها أثنـاء الملاحقـة القضائية لمن يشتبه بكونهـم إرهابيين، مع ضمان المعايير الدولية لمعاملـة الأشخاص المتهمين في الوقت نفسه.

٣٣٨- وقـد بـات دور أعضـاء النيابـة العامة في الملاحقـة القضائية بشأن قضايـا الإرهاب أكـثر فأكثر تعقيدا وصعوبة. فبالإضافة إلى مسؤوليتهم عن إقامة الدعوى الجنائية، صار لأعضاء النيابة العامة دور أكبر في مراحل التحقيـق وجمع المعلومـات الاستخبارية في قضايا الإرهـاب، إذ يقومون بالتوجيه أو الإشـراف فيما يتعلق بالآثار القانونية أو الاستراتيجية لاستخدام مختلف تقنيات التحقيق. ويعرض هذا الفصل بالدراسة لدور أعضاء النيابة العامـة في قضايا الإرهاب التي تُستخدم فيها الإنترنـت في أغراض إرهابية، بغية الوقوف، من وجهة نظر النيابة العامـة، على التحديات أو المعوقـات الشائعة والاستراتيجيات والنُّهُوج التي ثبتـت فعاليتها في الملاحقة القضائية الناجحة للجناة.

باء- اتباع نهج قائم على سيادة القانون في الملاحقات الجنائية

٣٣٩- إنَّ في إجـراء التحقيقات والملاحقات القضائية على نحو لا يتفق تمام الاتفاق والمبادئ التي ترتبط عموماً بسيـادة القانـون والمعايير الدولية لحقـوق الإنسان خطرا على بُنيـان المعايير الاجتماعيـة والمؤسسية التي يسعى الإرهابيـون أنفسهـم لتقويضها. ولذا فمن المهم للغاية إيلاء أهمية قصـوى للحاجة إلى ضمان العدل في محاكمة ومعاملة الأشخاص المتهمين أثناء أي ملاحقة قضائية لمرتكبي الأعمال الإرهابية.

٣٤٠- والمبدأ، المعترف به على نطاق واسع، الذي يقضي بأن يُكفل لمن يشتبه في كونهم إرهابيين نفس الضمانات الإجرائيـة التـي ينصـ القانـون الجنائي علـى كفالتهـا لغيرهم ممـن يشتبه في كونهـم مجرمين، مـن المبادئ الـواردة والراسخـة في الصكوك العالمية لمكافحـة الإرهاب وعلى المستـوى السياسي دولياً. وليـس قرار الجمعية

العامــة ٥٩/١٩٥، بشأن حقوق الإنسان والإرهاب، والذي سلطـت فيه الجمعية العامة الضوء على الحاجة لتعزيز تدابير التعاون الدولي في مجال مكافحة الإرهاب وفقا للقانون الدولي، بما يشمل القانون الدولي لحقوق الإنسان والقانــون الإنســاني الدولي، إلا مثالا واحداً من بين أمثلة عديدة على الاعــتراف بهذا المبدأ على أعلى المستويات. وبالإضافة إلى إدراج الأمم المتحدة لهذا المبدأ الأساسي على المستوى السياسي، فإنَّها تقدم، عبر مقررها الخاص المعنــي بتعزيز وحماية حقــوق الإنسان والحريات الأساسية في سياق مكافحــة الإرهاب، تقارير دورية إلى مجلس حقوق الإنسان والجمعية العامة بشأن المسائل المثيرة للقلق في الجوانب المتصلة بحقوق الإنسان في تدابير العدالة الجنائيــة التــي تستهدف الإرهاب، كمــا تقدِّم توصيــات بالإجــراءات التصحيحية المطلوب مــن الجهات المعنية اتخاذها. ومن المسائل التي أثارها المقرر الخاص احتجاز المشتبه بهم وتوجيه الاتهام لهم.[١٥٨]

٣٤١- وثمة عدة منشورات تتناول على وجه الخصوص الترويج لاحترام حقوق الإنسان وسيادة القانون، وتشجع عليهمــا، ضمن اختصاصات أعضاء النيابة العامة ومسؤولي العدالة الجنائية القائمين على الملاحقات القضائية لجرائم الإرهاب. وفي عام ٢٠٠٣، أصدرت مفوضية الأمم المتحدة لحقوق الإنسان *مجموعة قرارات الأمم المتحدة والمنظمات الإقليمية بشأن حماية حقوق الإنسان في سياق مكافحة الإرهاب*. وفي إطار مجلس أوروبا، الذي أقر وأدمج بالكامــل الالتزامَ بتفعيل حماية حقوق الإنسان بوصفه مبدأ أساسيــا في صكوكه التي تتناول المسائل المتعلقة بمنع الجريمة والعدالة الجنائية، بما في ذلك الإرهاب، أُعيد تأكيد هذا المبدأ في المبادئ التوجيهية الصادرة عن لجنة الوزراء بمجلس أوروبا بشأن حقوق الإنسان ومكافحة الإرهاب، التي اعتمدتها اللجنة في ١١ تموز/يوليه ٢٠٠٢.[١٥٩] وتتضمن هذه الوثائق إرشادات قيِّمة لأعضاء النيابة العامة العاملين في مجال مكافحة الإرهاب.

جيم- دور أعضاء النيابة العامة في قضايا الإرهاب

٣٤٢- يختلف دور أعضاء النيابة العامة في إقامة الدعوى الجنائية، بما يشمل قضايا الإرهاب، باختلاف الدول. ففي بعض البلدان، ولا سيما في الولايات القضائية التي تأخذ بنظام القانون المدني، يضطلع أعضاء النيابة العامة بالمسؤوليــة الرسمية عن مراقبة إقامــة الدعوى الجنائية، والإشراف على فرق المحققــين طيلة التحقيق، واتخاذ القرارات بشأن أنشطة التفتيش والمراقبة، والاتهام أو الإدانة، وتولي المسؤولية عن مسائل التعاون الدولي، وإقامة الدعاوى أمام المحاكم.

٣٤٣- وفي النظــم القضائيــة التحقيقية مثل النظام الفرنسي، تُسند إلى أعضــاء النيابة العامة عادة مهمة بدء الإجــراءات القانونيــة والتحقيقات الأولية، وتحديد نطاق الجرائم؛ إلا أن قاضي التحقيق هو الذي يضطلع بمهام التحقيــق القضائي الرسمي وجمع *الأدلة* وفحصها. وحين يمكن عدم إدانة المشتبه به في التهم الموجهة إليه، يغلق قاضــي التحقيــق ملف الدعوى، وفيما عدا ذلك يُقدَّم المشتبه بــه للمحاكمة أمام قاض آخر. وفي قضايا الإرهاب، لرئيس هيئة الادعاء أن يقوم، علاوة على تقديم دفوع الادعاء للقاضي، بالتقدم بالتماس أو اقتراح بإجراء المزيد من التحقيقات.

---

[١٥٨] المرجع نفسه.

[١٥٩] يجب أن يكون أي نص صادر في إطار مجلس أوروبا، بغض النظر عن كون هذا النص اتفاقية ملزمة أو صكاً من صكوك "القانون غير الملــزم"، مثلمــا هو حال التوصيات أو القرارات الصادرة عن الجمعية البرلمانية أو لجنة الوزراء، وبما يشمل أية مبادئ توجيهية بشأن موضوعات متنوعة، متفقاً على الدوام مع السوابق القضائية العديدة للمحكمة الأوروبية لحقوق الإنسان بشأن المسألة المعنية.

٣٤٤- وفي بلدان أخرى، ولا سيما في الولايات القضائية التي تأخذ بنظام القانون العام، كانت المشاركة المباشرة لأعضاء النيابة العامة في إجراء التحقيقات الجنائية أو المسؤولية عن تلك التحقيقات، التي عادة ما تقوم عليها جهات إنفاذ القانون، أقل مما هو عليه الحال الآن. وبصفة عامة، يضطلع أعضاء النيابة العامة في هذه الولايات القضائية بالمسؤولية الرسمية عن الدعاوى ابتداء من مرحلة توجيه التهم وحتى البت نهائياً في الدعوى. فعلى سبيل المثال، تضطلع الشرطة الوطنية في نيجيريا بالمسؤولية عن القيام بالتحقيقات الجنائية. وتحال القضايا بعد البت فيها إلى هيئة ادعاء تتولى مسؤولية توجيه التهم وإقامة الدعوى الجنائية.

٣٤٥- وتتبع إندونيسيا نهجاً مشابهاً، حيث يُفصل بين التحقيق والإدعاء في القضايا الجنائية. فبعد البدء في تحقيق جنائي، يجب على المحقق أن يقدم تقارير عن سير التحقيق للنائب العام (الفقرة ١ من المادة ١٠٩ من قانون الإجراءات الجنائية الإندونيسي)، وفور الانتهاء من التحقيق، يجب عليه أن يسلِّم ملفات القضية إلى النائب العام (الفقرة ١ من المادة ١١٠ من قانون الإجراءات الجنائية)، ليقرر الأخير ما إذا كان من الممكن عرض القضية أمام المحاكم (المادة ١٣٩ من قانون الإجراءات الجنائية).

٣٤٦- وبصرف النظر عن خصوصيات كل ولاية قضائية، فإنَّ الدور الذي يؤديه أعضاء النيابة العامة في قضايا الإرهاب لم يزل يتطور للوفاء بالمتطلبات المتزايدة بسبب التغيرات المستمرة في نوعية الجرائم ذات الصلة بالإرهاب وأساليبها وتعقيدها، وفي قوانين مكافحة الإرهاب، وتقنيات التحقيق الجديدة، وترتيبات التعاون الدولي.

٣٤٧- وتبيِّن التجربة أنَّ أعضاء النيابة العامة مطالَبون أكثر فأكثر بمزيد من المشاركة المباشرة لا في مرحلة الملاحقة القضائية فحسب وإنما في التحقيق في الجرائم أيضا. ويتولى أعضاء النيابة العامة دوراً تقنياً واستراتيجياً متزايدا لا يقتصر على المساعدة في توجيه ما يتصل بمكافحة الإرهاب من سياسات وتشريعات، وإنما يمتد ليشمل تقديم المشورة والإرشادات القانونية والاستراتيجية بشأن المسائل القانونية أثناء التحقيق بما يزيد من احتمال نجاح أية ملاحقات قضائية تتمخض عن التحقيق. وتفيد التجربة بأنَّ أعضاء النيابة العامة غالبا ما يضطلعون بدورهم هذا في إطار فريق متعدد التخصصات أو متعدد الولايات القضائية.[١٦٠]

٣٤٨- وعلاوة على ذلك، يؤدي أعضاء النيابة العامة، بالنظر إلى تسليط الضوء على الملاحقات القضائية المتعلقة بالإرهاب وتمحيصها، بما يشمل التغطية الإعلامية والرصد الذي تقوم به جماعات حقوق الإنسان والهيئات الدولية، دوراً محورياً في ضمان أن تكون التحقيقات والملاحقات القضائية، مظهراً وجوهراً، عادلة وفعالة ومُراعيةً للمعايير الدولية لحقوق الإنسان.

دال- مرحلة التحقيقات

٣٤٩- كثيراً ما يكون على أعضاء النيابة العامة، أثناء مرحلة جمع المعلومات الاستخبارية أو مرحلة التحقيق في عمليات مكافحة الإرهاب، أن يقدِّموا المشورة القانونية بشأن المسائل المتعلقة باستخدام تقنيات التحقيق المتخصصة.

(١٦٠) Yvon Dandurand, "The role of prosecutors in promoting and strengthening the rule of law", paper presented to the Second World Summit of Attorneys General, Prosecutors General and Chief Prosecutors, held in Doha from 14 to 16 November 2005.

١- *تقنيات التحقيق المتخصصة*

٣٥٠- لئن أتاحت التكنولوجيا وتقنيات التفتيش والمراقبة الجديدة أو المستجدة مزيداً من الفرص أمام أجهزة الاستخبارات وأجهزة إنفاذ القانون لاستهداف الأنشطة الإرهابية على الإنترنت، فإنها تحمل في طياتها كذلك مخاطر قانونية في سياق الملاحقات القضائية ينبغي لأعضاء النيابة العامة أخذها في الحسبان على الدوام. وعلاوة على ذلك، تشتد هذه المخاطر، نظراً للاختلافات في القوانين الوطنية فيما يخص جمع الأدلة وقبولها، حين تقع الأفعال وتُترك أدلة عليها في ولاية قضائية غير الولاية القضائية التي تُجرى فيها الملاحقة القضائية. وعلى المستوى الأوروبي، وضع مجلس أوروبا، من منطلق إدراكه لهذه المخاطر وما تنطوي عليه من مسائل تتعلق بحقوق الإنسان، توصيةً بشأن تقنيات التحقيق الخاصة فيما يتعلق بالجرائم الخطرة، بما في ذلك الأعمال الإرهابية،[١٦١] تتضمن، في جملة أمور، مبادئ عامة، ومبادئ توجيهية عملياتية، وفصلا عن التعاون الدولي.

٣٥١- وتزيد المخاطر القانونية المتعلقة بتقنيات التحقيق المستجدة من الحاجة لمشاركة أعضاء النيابة العامة مشاركة فاعلة، في أبكر مرحلة ممكنة، في القرارات التي تُتَّخذ أثناء مرحلة التحقيق في قضايا الإرهاب لضمان ألا تؤدي الإجراءات المتَّخذة أثناء جمع الأدلة المحتملة إلى تقويض نجاح أي ملاحقة قضائية تتمخض عن التحقيق. وسوف تكون المسائل المتعلقة بمقبولية الأدلة موضوع المناقشة بمزيد من التفصيل في موضع آخر مما تبقى من هذا الفصل.

٣٥٢- وتُبرز التغيرات المستمرة والسريعة في القدرات التكنولوجية لأجهزة الاستخبارات وأجهزة إنفاذ القانون فيما يخص المراقبة ورصد المعلومات الاستخبارية أو الأدلة المتعلقة بالأنشطة الإرهابية وجمع هذه المعلومات أو الأدلة الأهميةَ الحاسمة لدور أعضاء النيابة العامة في إسداء المشورة للمحققين بشأن الآثار القانونية لهذه الأنشطة على الملاحقات القضائية. وعلاوة على ذلك، ونظراً لتزايد الاحتمال، ولا سيما في القضايا التي تنطوي على القيام بأنشطة ذات صلة بالإنترنت عبر الحدود الوطنية، بأن يصبح من الضروري قيام السلطات بتنسيق جهودها مع نظيراتها الأجنبية والتعاون معها فيما يتعلق بالمسائل القانونية ذات الصلة (مثل حفظ البيانات المتعلقة بالإنترنت الموجودة لدى مقدمي خدمات الإنترنت)، فثمة أهمية متزايدة للإسراع ما أمكن باستشارة أعضاء النيابة العامة وإشراكهم في القرارات التي تُتَّخذ بشأن استراتيجيات التحقيق.

٢- *الاستعانة بالفرق المتعددة التخصصات*

٣٥٣- تستعين السلطات على نحو متزايد بالفرق المتعددة التخصصات أو الفرق المتعددة الأجهزة، التي تضم في عضويتها أجهزة إنفاذ القانون وأجهزة الاستخبارات، بالإضافة إلى أعضاء من النيابة العامة، في اعتراض الأنشطة الإرهابية، وإحباطها، وملاحقتها قضائياً. ومن الضروري تعزيز الثقة والتنسيق والتواصل فيما بين الأجهزة الوطنية المعنية بإنفاذ القانون والاستخبارات والملاحقة القضائية، بوصفها عناصر حيوية لتحقيق التعاون الفعَّال على المستوى الدولي حسبما ذُكر في اجتماع فريق الخبراء. وعلى الرغم من عدم وجود نهج واحد يُمكن من خلاله تعزيز هذه العناصر، فإنَّ الفهم الواضح لمهمة كل جهاز من الأجهزة المشاركة ودوره، ووضع الصلاحيات والآليات المناسبة لتبادل المعلومات ومشاطرتها (ربما على أساس مذكرات تفاهم أو ترتيبات أخرى مشابهة)، وعقد اجتماعات دورية للتنسيق أو أنشطة للتدريب، جميعها عوامل من شأنها المساعدة على تعزيز هذه الشراكات الوطنية الهامة.

(١٦١) Committee of Ministers of the Council of Europe, Recommendation Rec (2005)10 (20 April 2005).

٣٥٤- ولئن كانت هناك اختلافات في الطريقة التي تعتمدها السلطات في مختلف البلدان لتنسيق التحقيقات المتعددة الأجهزة وإجرائها، فثمة العديد من القواسم المشتركة بينها. ففي الولايات المتحدة، يتبع نهج يقوم على فرق العمل، بالاستعانة بفرق متعددة التخصصات من جميع الأجهزة المعنية، بما في ذلك أعضاء النيابة العامة، في إجراء التحقيقات المتعلقة بالإرهاب في البلاد.

٣٥٥- وبموجب هذا النهج، يلتحق أعضاء في النيابة العامة بفرق من أجهزة الاستخبارات وأجهزة إنفاذ القانون وغيرها من الأجهزة المتخصصة التي ترصد مختلف جوانب التحقيق في الأنشطة الإرهابية المشتبه بها وتُقيِّمها وتراجعها، ويشكِّلون جزءاً لا يتجزأ من هذه الفرق. وتقوم فرق العمل المعنية بمكافحة الإرهاب بتنسيق المجهودات بين أجهزة إنفاذ القانون على المستوى المحلي والاتحادي وعلى مستوى الولايات وبين مكاتب النيابة العامة. ويشترك العديد من مكاتب النيابة العامة على مستوى الولايات والمستوى الاتحادي في فرق العمل هذه، وتتراوح الأساليب المتبعة والمهام المضطلع بها بين حضور الاجتماعات ما بين الأجهزة، وتقاسم مكاتب مشتركة وتقديم المشورة القانونية بشأن الحصول على أوامر التفتيش القضائية، وحتى مراجعة القضايا وتقديم التوصيات بشأن التهم.[١٦٢]

٣٥٦- وفي كندا، تستخدم السلطات فرق إنفاذ الأمن الوطني المتكاملة. وفي قضية ناموح، تضمنت عضوية الفريق المتكامل شرطة الخيالة الملكية الكندية، وجهاز خدمات الحدود الكندي، وجهاز استخبارات الأمن الكندي، وشرطة كيبيك الإقليمية، وجهاز شرطة مونتريال، والنيابة العامة الكندية.

٣٥٧- ومن الممارسات الشائعة التي تقوم بها الشرطة اليابانية في التحقيقات المتعلقة بالإرهاب، بالرغم من استقلاليتها بموجب القانون، أن تُبلغ النيابة العامة بالقضية في المراحل المبكرة للتحقيق وتتشاور معها عند تقييم الأدلة وتفسير القوانين.[١٦٣] وتطبِّق مصر نهجاً مشابهاً في هذا الصدد.

٣٥٨- وحتى يتأتى تعزيز فعالية وكفاءة الملاحقات القضائية في مجال مكافحة الإرهاب، كثيرا ما تنشئ الحكومات، داخل أجهزة النيابة العامة الوطنية، أقساماً أو وحدات متخصصة للتعامل مع القضايا المتعلقة بالإرهاب. وهذا هو الحال في إندونيسيا، التي اعتمدت عدداً من التدابير الخاصة، بما في ذلك إنشاء فرقة عمل داخل مكتب المدعي العام تختص بالملاحقة القضائية في جرائم الإرهاب والجريمة المنظمة العابرة للحدود الوطنية. وتضطلع هذه الفرقة بتيسير إنفاذ القانون وتسريعه، أثناء كل من مرحلة التحقيق، عبر التنسيق مع الشرطة (كما في حالة إشراك أعضاء النيابة العامة أثناء استجواب المشتبه بهم)، وأثناء أي ملاحقة قضائية لاحقة، وحتى التنفيذ النهائي لحكم المحكمة.

٣٥٩- وفيما قد تتفاوت، على المستوى الدولي، أساليب اشتراك أعضاء النيابة العامة في التحقيقات الجنائية أو إدماجهم فيها، فإنَّ النهج العام المتَّبع في العديد من البلدان يسلِّط الضوء على استصواب هذا الإدماج واستصواب النهج الشامل المتعدد التخصصات إزاء القرارات الاستراتيجية والعملياتية التي تُتَّخذ أثناء مرحلة التحقيق في قضايا الإرهاب.

---

(١٦٢) M. Elaine Nugent and others, *Local Prosecutors' Response to Terrorism* (Alexandria, Virginia, American Prosecutors Research Institute, 2005).

(١٦٣) مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة، *خلاصة قضايا الإرهاب*، الفقرة ٢١٢.

هاء- التعاون الدولي

٣٦٠- سبق تناول المسائل المتعلقة بالتعاون الدولي في الفصل السادس أعلاه ولا داعي لتكرار ما قيل هاهنا. أما المسائل التي تهم أعضاء النيابة العامة تحديدا، والتي أثارها المشاركون في اجتماع فريق الخبراء، في القضايا التي يكون التعاون الدولي أحد عناصرها، فتتعلق بالوساطة في المشكلات المتعلقة بأسلوب التعاون، والمسائل المتعلقة بالاختصاص، ومتطلبات ازدواجية التجريم، ومقبولية الأدلة الأجنبية، وحل هذه المشكلات، وهي تحديات يتبين من التجربة أنها ما زالت مطروحة. ونظراً لما لجميع الدول من مصلحة مشتركة في الملاحقة القضائية الناجحة للجرائم المتعلقة بالإرهاب، فليس المهم هو وجود أطر تشريعية لتيسير هذا التعاون فحسب، وإنمَّا كذلك أن يبادر أعضاء النيابة العامة إلى حل هذه المشكلات في إطار التعاون.

واو- مرحلة الاتهام

١- *القرارات المتعلقة بالاتهام من عدمه*

٣٦١- يكون لأعضاء النيابة العامة في معظم البلدان سلطة تقديرية واسعة في اتخاذ القرار بإقامة الدعاوى الجنائية من عدمها والتهم التي سيتم توجيهها. وكثيراً ما تتخذ هذه القرارات وفقاً لمبادئ توجيهية أو مُدوَّنات يكون الغرض منها أن تُمارس هذه السلطة بكل عدل وشفافية واتساق. فعلى سبيل المثال، يتخذ أعضاء النيابة العامة في المملكة المتحدة هذه القرارات وفقاً لمدوَّنة أعضاء نيابة التاج البريطاني العامة، والتي تنص على حد أدنى يبدأ عنده توجيه التهم بناءً على كفاية الأدلة والمصلحة العامة. فلا بد أن يقتنع أعضاء النيابة العامة بأنَّ الأدلة المتوافرة لديهم تتيح "إمكانية واقعية للإدانة" قبل توجيه اتهام معين إلى مشتبه به.[١٦٤] وتطبِّق مصر نهجاً مشابهاً في هذا الصدد.

٣٦٢- وفي سياق الإرهاب، من الأرجح أن يكون لعامل المصلحة العامة أهمية قصوى عند النظر في توجيه الاتهام من عدمه، نظراً للحاجة إلى الملاحقة القضائية بشأن الأعمال الإرهابية أو الجرائم المرتبطة بها، متى كان ذلك ممكناً، لحماية عامة الجمهور وردع الجرائم المشابهة. وفي كثير من الحالات، قد تكون المسائل المتعلقة بكفاية الأدلة المتاحة عوامل حاسمة وقد تتأثر بالقدرة على استخدام أدلة استخبارية دون المساس بمصادر هذه المعلومات أو وسائل الحصول عليها أو بتحقيقات أخرى. ولهذا السبب قد يضطر أعضاء النيابة العامة إلى اتخاذ قرار بتوجيه تهم غير متعلقة بالإرهاب إلى المشتبه بهم حمايةً لسلامة المعلومات الاستخبارية.

٢- *الاستعانة بجرائم عامة أو غير متعلقة بالإرهاب تحديداً*

٣٦٣- في الحالات التي تحتاج السلطات فيها إلى التدخل لمنع ارتكاب أعمال إرهابية قبل أن تتوفر أدلة كافية لإقامة الدعوى بخصوص الأعمال الإرهابية التي يجري التخطيط لها، قد تحتاج إلى الاعتماد على أفعال أخرى مجرمة تتخذها أساسا قانونيا لما تقوم به من إجراءات. وفي كثير من الحالات التي استخدم فيها المشتبه في

(١٦٤) Crown Prosecution Service, "The Code for Crown Prosecutors" (London, 2010). انظر الرابط التالي: www.cps.gov.uk/publications/docs/code2010english.pdf.

كونهم إرهابيين الإنترنت في إطار أنشطتهم الإجرامية، استعانت السلطات بنجاح بجرائم أخرى مثل التحريض أو التآمر أو الاشتراك في جماعات إرهابية أو تقديم الدعم المادي لجماعات إرهابية، بدلا مما كان يعتزم ارتكابه من جرائم إرهاب في حد ذاتها. وفي هذا السياق، من المفيد أيما إفادة وجود جرائم منصوص عليها من قبيل التحريض أو التآمر أو التواطؤ الإجرامي. وفي بعض الحالات، كان بوسع السلطات الاستعانة بجرائم أخرى عامة مثل الاحتيال أو الجرائم المتعلقة بحيازة مواد غير قانونية أو استخدامها (مثل وثائق الهوية أو السفر المزورة، والأسلحة)، وهو ما يتيح للمحققين وأعضاء النيابة العامة فرصة لإحباط أنشطة الجماعات الإرهابية قبل أن يتأتى لها تنفيذ الهجمات أو الأنشطة المخطَّط لها.

زاي- مرحلة المحاكمة: المسائل المتعلقة بالأدلة

١- *المسائل المتعلقة باستخدام الأدلة الاستخبارية*

٣٦٤- لم يزل إدماج الأنشطة الاستخبارية في نظم العدالة الجنائية مشكلة رئيسية تواجه السلطات في تصديها للإرهاب. فكما ذُكر آنفاً، كانت الأدلة التي استخدمتها النيابة العامة في العديد من قضايا الإرهاب مستمدة من مصادر استخبارية. وكثيرا ما تواجه السلطات في جميع البلدان صعوبة في الملاحقة القضائية بشأن قضايا الإرهاب تتمثل في كيفيةُ حماية المعلومات السرية الواردة في الأدلة الاستخبارية مع الوفاء في الوقت نفسه بالتزاماتها بضمان محاكمة عادلة ودفاع فعَّال للأشخاص المتهمين، بما في ذلك الالتزام بالكشف للدفاع عن كل الأدلة الجوهرية التي تشكل جزءاً من دفوع النيابة العامة.

٢- *المسائل المتعلقة بجمع الأدلة الرقمية واستخدامها*

٣٦٥- الأدلة الرقمية جزء هام من دفوع النيابة العامة في قضايا الإرهاب التي تستخدم فيها أجهزة الحاسوب أو الأجهزة المشابهة أو الإنترنت. وفي الحالات التي لا يكون فيها للمشتبه بهم وجود فعلي في المكان الذي وقع فيه العمل الإرهابي، مع كونهم قد دعموا ارتكاب هذا العمل عبر تصرف ما على شبكة الإنترنت، فإنَّ إظهار "بصماتهم الرقمية" قد يكون دليلا دامغاً على تورطهم وإثبات التهمة عليهم في هذه الأعمال.

٣٦٦- وتبيِّن التجربة أنَّ استخدام الأدلة الرقمية يؤدي على الدوام إلى إثارة مشاكل متعلقة بالمقبولية. ومن ثم فمن المهم للغاية أن يُتوخى الحذر الشديد طيلة التحقيق والملاحقة القضائية لضمان كون الأساليب المستخدمة لجمع الأدلة الرقمية وحفظها وتحليلها وتقديمها تتفق تمام الاتفاق وقواعد الإثبات أو القواعد الإجرائية المعنية، وكذلك الممارسات الجيدة المعمول بها.

٣٦٧- وقد تكون الأدلة الرقمية معقَّدة تقنياً ومشتملة على مصطلحات ومفاهيم غير مألوفة للقاضي أو للمحلفين أو الهيئة القضائية التي تنظر القضية. ولذا فإنَّ الأمر يقتضي من أعضاء النيابة العامة أن يتدارسوا، بالتنسيق عن كثب مع المحققين والخبراء، الطريقة المثلى لعرض هذه الأدلة بحيث يسهل فهمها والاقتناع بها. وفي هذا الصدد، قد يكون من المفيد استخدامُ الأشكال الإيضاحية وما شابهها من وسائل الإيضاح المرئية التي تبيِّن حركة البيانات أو الصلات فيما بين أجهزة الحاسوب والمستخدمين.

٣٦٨- ويقتضي الأمر من النيابة العامة، في إطار دفوعها في الملاحقات القضائية المستندة لشكل ما من أشكال استخدام الحاسوب، أن تبيِّن أنَّ المدَّعى عليه هو من استخدم، في الوقت المعني، جهاز الحاسوب أو الجهاز الإلكتروني أو خدمة الإنترنت، التي استعين بها على ارتكاب الجريمة التي هو متهم بارتكابها، وإقامة صلات لإثبات ذلك. وثمة طرائق عديدة للقيام بذلك، منها ما يلي: *(أ)* من الممكن أن يعترف المدَّعى عليه أو يقر بذلك؛ أو *(ب)* من الممكن إثبات وجود المدَّعى عليه في مكان وجود جهاز الحاسوب عبر قرائن ظرفية (مثل كونه الشخص الوحيد الموجود في مكان وجود جهاز الحاسوب أو كونه الشخص المسجَّل مستخدما للجهاز المعني أو البرمجية المعنية في الوقت المعني، أو وجود معلومات أخرى على جهاز الحاسوب لا تتأتى معرفتها إلا للمدَّعى عليه)؛ أو *(ج)* من الممكن إقامة الصلة عبر تحليل محتويات الجهاز/الخدمة التي يُزعم استخدام المدَّعى عليه لها، وهو ما قد يتطلب تقديم النيابة العامة لأدلة حول مواصفات محددة للمواد الموجودة على الجهاز (مثل مستند ما) أو تعليق قيل في اتصال مُعترض مما يتفرد به المدَّعى عليه. وأخيراً، فإنَّ أختام الوقت والتاريخ على الملفات الرقمية قد تكون وسيلة مقنعة، رغم عدم خلوها تماما من العيوب، للربط بين المدَّعى عليه والجهاز المعني في الأوقات ذات الصلة بارتكاب جريمة ما.[١٦٥]

٣٦٩- وتتبع المحاكم في العديد من البلدان نهجا عاما، وإن اختلفت التفاصيل أحيانا، عند تقرير مقبولية الأدلة في المحاكمات الجنائية يستند إلى الصلة والموثوقية ويجاب فيه عن السؤال التالي: هل الأدلة التي يسعى أحد الأطراف إلى تقديمها ذات صلة بالموضوع، وهل هي موثوقة؟ وفي حالة الأدلة الرقمية ذات الصلة، يكون التحدي أمام أعضاء النيابة العامة في كثير من الأحيان هو إقناع المحكمة بموثوقيتها، من حيث محتوى هذه الأدلة والأساليب التي استخدمت للحصول عليها وتقديمها للمحكمة. وغالباً ما يتطلب إقناع المحكمة بمقبولية الأدلة الرقمية إثبات شرعية الوسائل التي استخدمت للحصول عليها وحفظ سلامتها منذ الحصول عليها وحتى تقديمها في المحكمة. وهذا هو ما يُعرف بـ"تسلسل العهدة" أو "تسلسل الأدلة"، أي الإجراءات التنفيذية والقانونية المتبعة لحفظ سلامة الأدلة. وثمة قواعد قانونية صارمة في معظم البلدان بشأن تسلسل العهدة، تقتضي أن تُسجَّل الأدلة وتُجمع في مكان مركزي واحد وتُختم على الفور وتُحمى من العبث بها ريثما تبدأ المحاكمة، وذلك تحت إشراف مسؤول قضائي في بعض الأحيان.

٣٧٠- وفي قضايا الإرهاب التي يتم فيها جمع واستخدام أدلة مستقاة من الاتصالات المعترَضة أو أدلة التحليل الجنائي الرقمية، ينبغي لأعضاء النيابة العامة التأكد، بالتعاون الوثيق مع أجهزة الاستخبارات أو أجهزة إنفاذ القانون أو معهما معاً، من أنَّ الحصول على هذه الأدلة وحفظها قد تمّا وفقا للقانون ومن أنها ستقدَّم بطريقة تستوفي متطلبات الإثبات لدى الولاية القضائية التي سوف تُستخدم فيها في نهاية المطاف. ويُعدُّ الحصول على البيانات الرقمية وتقديمها باعتبارها أدلة تحظى بالمقبولية، ولا سيما حين تكون حيازة هذه الأدلة عن بُعد لدى مشتبه به أو طرف ثالث ذي صلة به في ولايات قضائية أخرى، مهمةً صعبةً أمام المحققين وأعضاء النيابة العامة على حد سواء. فبالإضافة إلى التعقيدات التقنية المتعلقة بالحصول على البيانات المطلوبة وحفظ سلامتها، من الضروري في بعض الحالات الاعتماد على تعاون أجهزة أجنبية للاستخبارات أو إنفاذ القانون أو النيابة العامة، تعمل وفق قوانين وإجراءات مختلفة لتنظيم الحصول على هذه البيانات واستخدامها، مما قد يؤدي إلى استغراق هذه العمليات وقتا طويلا والحاجة فيها إلى موارد كثيرة.

[١٦٥] United States Department of Justice, Office of Justice Programs, National Institute of Justice, *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors* (2007), chap. 4, sect. IV. انظر الرابط التالي: www.ncjrs.gov/pdffiles1/nij/211314.pdf.

٣٧١- وفي التحقيقات التي يتم فيها الحصول على بيانات رقمية موجودة بالكامل في ولاية قضائية واحدة، من المرجَّح أن تتمحور المسائل المتعلقة بمقبولية هذه البيانات باعتبارها أدلة حول السند القانوني الذي تم الحصول عليها على أساسه وحول مناولتها وحفظها بعد ذلك (أي تسلسل العهدة أو تسلسل الأدلة). وكما هو الحال دوماً، ينبغي توخي الحذر لضمان اتفاق السند القانوني للحصول على الأدلة، وفحصها بالتحليل الجنائي، وحفظها، وتقديمها، تمام الاتفاق مع ما هو مطبَّق من معايير وإجراءات فيما يخص مقبولية الأدلة.

٣٧٢- وفي حالة الأدلة الرقمية التي تم الحصول عليها في ولاية قضائية واحدة أو عدة ولايات قضائية لاستخدامها في دعوى جنائية في ولاية قضائية أخرى، فإنَّ الموقف يغدو أكثر تعقيداً بكثير ويقتضي من المحققين وأعضاء النيابة العامة توخي الحذر الشديد.

٣٧٣- وينبغي للمحققين وأعضاء النيابة العامة أن يستكشفوا، في أقرب وقت بعد الوقوف على هوية الطرف الحائز للبيانات ومكان وجود هذه البيانات في ولاية قضائية أجنبية، الوسائل الرسمية وغير الرسمية للحصول عليها وحفظها بغرض استخدامها كأدلة. ويفضَّل استخدام قنوات غير رسمية للحصول على البيانات لاستخدامها لاحقاً كأدلة متى كان ذلك ممكناً ومجدياً، بشرط اتفاق الأساليب المتبعة في الحصول على هذه البيانات وحفظها وإرسالها إلى البلد المتلقي مع قواعد وإجراءات الإثبات المنطبقة. وقد يحتاج المحققون، بغية الحصول على هذه البيانات، إلى النظر في أن يطلبوا من نظرائهم الأجانب أن يحصلوا على أوامر تفتيش للتفتيش عن البيانات وضبطها، أو قد يحتاجون إلى النظر في استخدام وسائل أخرى (مثل الصفحات الشبكية المتاحة لعموم الجمهور) أو الاستعانة بشهود أجانب متطوعين.

٣٧٤- وتبيِّن قضية من ألمانيا، انتهى النظر فيها عام ٢٠٠٩ وتتعلق بملاحقة قضائية ناجحة لأربعة أعضاء في اتحاد الجهاد الإسلامي، حجم وتعقيد العديد من التحقيقات والملاحقات القضائية في قضايا الإرهاب. وقد شارك في القضية، التي استغرق التحقيق فيها ما يربو على التسعة أشهر، أكثر من ٥٠٠ شرطي، وأنفقت فيها ساعات عديدة على اعتراض ومراقبة الاتصالات الإلكترونية وجمع العديد من الأحراز، فضلا عن تعاون دولي مكثف فيما بين السلطات الألمانية ونظيراتها في تركيا والولايات المتحدة. ويسلِّط حجم القضية وتعقيدها الضوء على الموارد ذات الشأن التي يُمكن أن يتطلبها الاضطلاع بالتحقيقات والملاحقات القضائية وضرورة اللجوء إلى نهج يقوم على العمل الجماعي ومزايا ذلك النهج.

فريتز غيلوفيتش، وآدم يلمظ، ودانييل شنايدر، وأتيلا سيليك

في أيلول/سبتمبر ٢٠٠٧، وبعد تحقيقات مستفيضة، ألقت السلطات الألمانية القبض، بناءً على معلومات استخبارية تلقتها من نظيراتها في الولايات المتحدة، على أربعة أعضاء في اتحاد الجهاد الإسلامي (يطلق عليهم في كثير من الأحيان "خلية زاورلاند")، كانوا في المراحل الأخيرة من التحضير لسلسلة من التفجيرات في عدة أماكن عامة في ألمانيا. وقد تضمنت الأهداف المقصودة حانات ونوادٍ ليلية في عدة أماكن في ميونيخ، وكولونيا، وفرانكفورت، ودوسلدورف، ودورتموند، فضلا عن قاعدة القوات الجوية الأمريكية في رامشتاين. وقد بلغ مجموع المواد المتفجرة التي ظنَّ المدَّعى عليهم أنهم قد حصلوا عليها (إذ إنَّ السلطات كانت قد قامت سرّا باستبدالها بمادة أضعف مفعولا وغير ضارة) حجماً هائلا، بما قد يكفي لتجاوز قوة التفجيرات الإرهابية في مدريد (٢٠٠٤) ولندن (٢٠٠٥).

وقد كان ثلاثة من المدَّعى عليهم — غيلوفيتش وشنايدر وسيليك — مواطنين ألمان، فيما كان الرابع، يلمظ، مواطناً تركياً. وعلى مدار عدة أشهر، حصل المدَّعى عليهم على ٧٨٠ كغ من بيروكسيد الهيدروجين من مصادر مشروعة. وفي ٤ أيلول/سبتمبر ٢٠٠٧، ألقت السلطات القبض على المدَّعى عليهم أثناء التقائهم في منزل لقضاء العطلات يقع في منطقة زاورلاند الألمانية وشروعهم في "طبخ" بيروكسيد الهيدروجين بإضافة مكوِّنات أخرى إليه لزيادة قوته الانفجارية (ولم يكن المدَّعى عليهم يعلمون أنَّ السلطات كانت قد استبدلت محلول بيروكسيد الهيدروجين بمحلول أضعف مفعولا وغير ضار).

وفي آب/أغسطس ٢٠٠٨، وجهت النيابة العامة الاتحادية تهما إلى غيلوفيتش وشنايدر ويلمظ. وسلَّمت تركيا سيليك في تشرين الثاني/نوفمبر استجابة لطلب تسليم مقدَّم بموجب الاتفاقية الأوروبية بشأن تسليم المطلوبين ووجهت إليه في كانون الأول/ديسمبر ٢٠٠٨ تهما منها التآمر على ارتكاب القتل العمد، والتحضير للقيام بتفجير، والانتماء إلى تنظيم إرهابي.

وبدأت محاكمة المدَّعى عليهم الأربعة جميعاً في نيسان/أبريل ٢٠٠٩، واستمرت لثلاثة أشهر قبل أن يقرر المدَّعى عليهم الإقرار بالذنب في التهم الموجهة إليهم. وكان حجم الأدلة التي كانت النيابة العامة تنتوي تقديمها هائلا، بما يشمل ٥٢١ من حافظات الملفات (ما يكفي لملء رف بطول ٤٢ متراً) وما يُقدَّر بـ ٢١٩ شاهداً. وكان جزء كبير من دفوع النيابة يتعلق بما اضطلعت به السلطات الألمانية من رصد ومراقبة إلكترونيين مكثفين أثناء التحقيق. وقد شملت تقنيات التحقيق الإلكترونية استخدامَ أجهزة تنصت على المكالمات بين المدعى عليهم وأجهزة تنصت مزروعة في المركبات والمنزل الذي التقى فيه المتهمون لتحضير بيروكسيد الهيدروجين المراد استخدامه في جهاز التفجير، فضلا عن اعتراض حركة بريدهم الإلكتروني. وقد اقترحت النيابة العامة تقديم أدلة رقمية مستفيضة، إلا أنَّه كانت هنالك مؤشرات واضحة أثناء التخطيط للعمل الإرهابي على أنَّ المدَّعى عليهم كانوا يتوخون الحيطة إزاء المراقبة أو الرصد. وعلى مدار التحقيق الذي استغرق تسعة أشهر، واجهت السلطات عدداً من التحديات التقنية. فعلى سبيل المثال، كان المدَّعى عليهم يتواصلون عبر مسودات البريد الإلكتروني (أي عبر فتح وقراءة مسودات رسائل في حسابات للبريد الإلكتروني) للحيلولة دون تنصت أجهزة إنفاذ القانون عليهم، كما كانوا يستخدمون وصلات شبكات لاسلكية غير محمية على الإنترنت لمواطنين أبرياء، وكذلك اتصالات مشفَّرة عبر مقدمي خدمات بروتوكول الاتصال الصوتي عبر الإنترنت (مثل سكايب).

وكان غيلوفيتش، قائد الجماعة المزعوم، قد استعان بالدخول العشوائي إلى الإنترنت عبر شبكات سكنية محلية خاصة وغير محمية، واستخدم ما لا يقل عن ١٤ حساباً للبريد الإلكتروني، وغيَّر لوحات معدنية لمركبات، واستخدم جهازا ماسحاً خاصاً بالشرطة لرصد اتصالات الشرطة عبر الراديو. وقام بتشفير البيانات الموجودة على جهاز الحاسوب الخاص به لحمايتها، وهي بيانات حاول خبراء التحليل الجنائي فك شفرتها والاطلاع عليها دون جدوى. وفي نهاية المطاف سلَّم غيلوفيتش مفتاح التشفير، إلا أنَّ المحققين لم يعثروا إلاّ على آثار لبيانات تم التخلص منها.

وأثناء المحاكمة، طعن الدفاع في صحة الملاحقة القضائية، مشككاً في السند الذي قام عليه التحقيق، وأكَّد أنّ هذا السند معيب في جوهره لكونه مستنداً إلى معلومات استخبارية من الولايات المتحدة قال إنها شملت الرصد الإلكتروني لاتصالات المدَّعى عليهم، وهو أمر يخالف القانون وتم القيام به بما يخل بالحقوق المكفولة لهم في الدستور الألماني.

وفي ٤ آذار/مارس ٢٠١٠، أدانت المحكمة المتهمين الأربعة في التهم كافة وأصدرت في حقهم أحكاما بالسجن كما يلي: ١٢ سنة لغيلوفيتش وشنايدر، و١١ سنة ليلمظ، و٥ سنوات لسيليك.

٣- *المسائل المتعلقة باستخدام الأدلة الأجنبية*

٣٧٥- كثيراً ما تختلف المبادئ والإجراءات القانونية المتعلقة بالحصول على الأدلة ومقبوليتها في الدعاوى الجنائية باختلاف الولايات القضائية. ومن بين التحديات الكبرى التي يواجهها المحققون وأعضاء النيابة العامة

في أي تحقيق جنائي أو ملاحقة قضائية جنائية لهما طابع عابر للحدود (في كل من الدولة الطالبة والدولة متلقية الطلب) التأكدُ من الحصول على الأدلة اللازمة وحفظها وإرسالها وتقديمها بما يتفق وإجراءات وقواعد الإثبات القانونية المطبقة في الولايات القضائية المعنية في صورة تحظى بالمقبولية في مكان إجراء المحاكمة.

٣٧٦- وقد تكون عملية "الوساطة" فيما بين البلدان بشأن مختلف جوانب الأدلة عملية معقدة تستغرق وقتاً طويلا، إلا أنها تُعدُّ عاملا حاسماً في نجاح الملاحقات القضائية. ومن شبه المؤكد أنَّ أي قصور قانوني في الوسائل التي تُجمع بها الأدلة لاستخدامها في المحكمة في نهاية المطاف أو تقدَّم بها هذه الأدلة سيتعرض للطعن من قبل محامي الدفاع.

٣٧٧- ومن الأمثلة المفيدة التي تسلِّط الضوء على أنواع المسائل التي يمكن أن تنشأ في هذا السياق قضيةُ *مليكة العروض وآخرين* البلجيكية. وتتعلق هذه القضية بأنشطة مجموعة من المدَّعى عليهم الضالعين في تأسيس عدة مواقع شبكية وإدارتها، لاستخدامها في نشر الدعاية الإرهابية والمعلومات ذات الفائدة للإرهابيين وكذلك لتكون بمثابة منتدى للتواصل. وكان العديد من المدَّعى عليهم مقيمين في بلجيكا، إلا أنَّ الموقع الشبكي الرئيسي الذي كانوا يمارسون فيه أنشطتهم (minbar-sos.com) كان مستضافاً في كندا.

مليكة العروض وآخرون

مقدِّمة

في كانون الأول/ديسمبر ٢٠٠٨، وبعد تحقيقات طويلة ومستفيضة ومعقدة جرى تنسيقها فيما بين سلطات الاستخبارات وإنفاذ القانون والنيابة العامة في فرنسا وبلجيكا وسويسرا وإيطاليا وتركيا والولايات المتحدة وكندا، أُلقي القبض على عدد من الأشخاص المشتبه في صلتهم بتنظيم القاعدة الإرهابي ووجهت إليهم مجموعة من التهم الجنائية في فرنسا وبلجيكا، بما في ذلك الاشتراك بصفة عضو في تنظيم إرهابي، وتمويل الإرهاب، وإمداد تنظيم إرهابي بمعلومات ودعم مادي.

واستخدم المشتبه بهم شبكة الإنترنت استخداما مكثفا في قيامهم بالأعمال المنسوبة إليهم المتخذة سندا لهذه التهم. وقد شمل التحقيق في أنشطتهم مراقبة إلكترونية معقدة والتنصت وغير ذلك من أشكال الرصد من قبل أجهزة الاستخبارات وأجهزة إنفاذ القانون. وكان من الضروري، لإنجاح القضية، التعاون بين السلطات في ولايات قضائية متعددة عبر قنوات رسمية وغير رسمية على حد سواء.

وتعدُّ القضية مثالا على التعاون الناجح للغاية في الملاحقات القضائية الجنائية المتعلقة بالإرهاب، التي يكون استخدام الإنترنت أحد جوانبها، فيما بين السلطات الوطنية للدول المشاركة، وتسلِّط الضوء على العديد من جوانب الممارسات الجيدة المشار إليها في هذا المنشور. وتتخلل الفصلين الخامس والسادس، بشأن التعاون الدولي والملاحقات القضائية، إشارات إلى هذه الجوانب.

والمحور الأساسي لهذه القضية، التي لها صلات بقضايا أخرى في بلدان عدة، هو أنشطة مليكة العروض، وهي مواطنة بلجيكية من أصل مغربي، وزوجها معز غرسلاوي، وهو تونسي الجنسية. وقد كان كلاهما ضالعاً في نشر دعاية جهادية متطرفة وفي تجنيد مجموعة من الشباب من بلجيكا وفرنسا وتنظيمهم وتوجيههم وتمويلهم للمشاركة في أعمال جهادية في أفغانستان وغيرها.

وإذا كان بعض هذه الأنشطة قد نُفِّذ بالاستعانة بأساليب أخرى غير الإنترنت، فإنَّ الزوجين قد استخدماه استخداما مكثفا للاضطلاع بهذه الأعمال، لأغراض منها التواصل. وبالإضافة إلى مليكة العروض ومعز غرسلاوي (الذي حوكم غيابياً، ومعه شريك آخر يُدعى هشام بيايو)، كان المدَّعى عليهم الآخرون في المحاكمة هم علي الغنوتي، وسعيد حريزي، وجان-كريستوف تريفوا، وعبد العزيز باستين، ومحمد الأمين باستين، وهشام بوهالي زريول.

وللقضية البلجيكية صلة وثيقة بقضية فرنسية المدَّعى عليهم فيها هم وليد عثماني، وحمادي عزيري، وسميرة غامري ملوك، وهشام بن راشد، ويوسف المرابط، والذين حوكموا وأدينوا أمام محكمة باريس الابتدائية،[أ] وتحقيقٍ وملاحقة قضائية في إيطاليا بشأن بسام عياشي ورفائيل جندرون.

خلفية

في آب/أغسطس ٢٠٠٧، تلقَّت السلطات البلجيكية معلومات من نظيراتها الفرنسية فيما يخص الأنشطة على موقع Minbar SOS الشبكي (المستضاف في كندا)، والذي اشتبهوا في كونه يُستخدم في نشر دعاية سلفية تدعو للجهاد ضد فرنسا. وكانت العروض وغرسلاوي يديران الموقع حسب ما ادّعي. وباتساع نطاق التحقيق، كُشف عن مواقع شبكية أخرى مشابهة.

واشتبهت السلطات في قيام العروض وغرسلاوي، بالعمل معاً عبر الموقع، بالبحث عن أفراد من بلجيكا وتجنيدهم للقتال في أفغانستان. ونشرت العروض مواد تحريضية تدعو الشباب إلى الانضمام للجهاد.

مليكة العروض ومعز غرسلاوي

كانت أجهزة مكافحة الإرهاب الأوروبية تعرف مليكة العروض ومعز غرسلاوي معرفة جيدة قبل هذه القضية. ففي عام ٢٠٠٣، حوكمت العروض وبرئت من قبل محكمة بلجيكية في تهمة الاشتراك في شبكة للدعم اللوجستي للجهاديين استُخدمت في قتل أحد قادة المقاومة المناهضة لطالبان في أيلول/سبتمبر ٢٠٠١. وكان زوج العروض الأول أحد الشخصين اللذين نفَّذا عملية القتل.

وفي عام ٢٠٠٧، حوكمت العروض في سويسرا، إلى جانب غرسلاوي، زوجها الثاني، بتهمتي توفير "الدعم لتنظيم إجرامي" و"التحريض العلني على العنف والجريمة" عبر مواقع شبكية مختلفة كانا قد أنشآها في سويسرا. وأدينت العروض وحُكم عليها بالحبس ستة أشهر مع وقف التنفيذ من قبل المحكمة الجنائية الاتحادية في بيلينزونا.

وفي ٢١ كانون الأول/ديسمبر ٢٠٠٧، أُلقي القبض على العروض في بلجيكا اشتباهاً في محاولتها مساعدة السجين نزارت. على الهرب، إلا أنَّه تمَّ الإفراج عنها بعد ٢٤ ساعة، نظراً لعدم كفاية الأدلة. وكان نزارت. قد أُدين في عام ٢٠٠٤ من قبل محكمة في بلجيكا وحُكم عليه بالسجن ١٠ سنوات بتهمة التحضير لهجوم إرهابي على القاعدة العسكرية الأمريكية في كلينه-بروغل في عام ٢٠٠٧. وقد ألقي عليها القبض في هذا الشأن في نفس الوقت الذي كانت التحقيقات في أنشطتها المشتبه بها على Minbar SOS جارية.

المواقع الشبكية

كانت المواقع التي أنشأتها العروض، بما فيها Minbar SOS، تُستخدم بوصفها منابر لنشر الدعاية (كأشرطة الفيديو والصور) وتوزيع الكتب والمنشورات والتواصل. وكان يُعطى لكل عضو اسم مستخدم/اسم مستعار وعنوان إلكتروني حتى يُمكن للأعضاء تبادل رسائل خاصة، مشفَّرة في بعض الأحيان، داخل منتديات دردشة مغلقة تستضيفها المواقع. وكانت هذه الرسائل تتضمن تعليمات، ومعلومات استخبارية، ودعاية، ودعوات مستمرة للجهاد الشامل. وكانت بعض المواد تحتوي على إشارات واضحة إلى قيادة تنظيم القاعدة وإعلانات عن هجمات على القوات الأمريكية في العراق.

وكانت تُنشر رسائل تتضمن تهديدات صريحة (مثل رسالة بعنوان "حل واحد فقط للإرهاب الفرنسي في أفغانستان")، علاوة على خريطة لشبكة القطارات السريعة في باريس، وُضعت عليها علامات عند بعض المحطات الرئيسية برموز النشاط الإشعاعي أو التلوث البيولوجي. وكانت بعض الرسائل تتضمن تعليمات صريحة بشأن طريقة تحويل الأموال للجهاديين. وبحلول نهاية العام ٢٠٠٨، كان هناك ما يربو على ٤٠٠١ مشترك في الموقع الرئيسي Minbar SOS.

وقامت السلطات البلجيكية والفرنسية، في إطار تحقيق مشترك، باعتراض اتصالات عبر مواقع شبكية وحسابات بريد إلكتروني ومكالمات هاتفية، ورصدت تدفقات مالية وتتبعتها. ومع ذلك، ورغم ما قامت به أجهزة الأمن البلجيكية من رصد عن كثب للأنشطة التي كانت تستهدف تجنيد أشخاص للقتال في أفغانستان على موقع Minbar SOS الشبكي، فلم يكن بوسعها إلا القليل للحيلولة دون قيام العروض بإدارة الموقع نظراً لما تتمتع به حرية التعبير من حماية كبيرة في القانون البلجيكي.

أما الهيئة القضائية الفرنسية، التي تولت في نهاية المطاف المحاكمة فيما يخص هذا البلد، فقد لاحظت في إشارتها للمواقع الشبكية أنَّه:

> لا يمكن تحليل النشاط على هذه المواقع الشبكية بوصفه مجرد بحث عن المعلومات أو المعلومات الاستخبارية، بل إنه يشكّل، على العكس من ذلك، مشاركة عن بيّنة في عمل أو مهمة الغرض منهما الإرهاب.

وعلاوة على ذلك، قال المدَّعى عليهما سعيد حريزي وهشام بيايو، على الترتيب، ما يلي في معرض إفادات أدليا بها في محاكمات لاحقة: "أعتبر نفسي ضحية للدعاية على الإنترنت" و"إنَّ المواقع من نوعية Ribaat وMinbar SOS تؤثر على أمثالي ممن ذهبوا للقتال"، وهو ما يبيِّن ما للأنشطة التي كانت تجري عبر الموقع من تأثير قوي على بعض الأفراد.

وسمَّت العروض نفسها، في مقابلة نادرة أجريت معها في إطار مقال نُشر في صحيفة نيويورك تايمز في ٢٨ أيار/مايو ٢٠٠٨، "مجاهدة من أجل القاعدة. وتصر (...) على أنَّها لا تنتوي حمل السلاح بنفسها. بدلا من ذلك، هي تستفز الرجال المسلمين ليذهبوا للقتال وتحشد النساء للانضمام للقضية. "ليس دوري أن أفجِّر القنابل—هذا كلام سخيف. عندي سلاح، وهو أن أكتب. أن أتكلم بصوت عال. هذا هو جهادي. يمكن للمرء أن يفعل الكثير بالكلمات. الكلمات هي أيضاً قنابل."[ب]

سفر المجندين إلى المناطق القبلية الخاضعة للإدارة الاتحادية في باكستان

بالإضافة إلى ما كان يقوم به غرسلاوي من أنشطة على المواقع الشبكية، فقد كان يتجول أيضاً في أحياء المهاجرين في بروكسل للتجنيد المباشر. وقد اعترف هشام بيايو، وهو مواطن بلجيكي من أصل مغربي عمره ٢٣ سنة ألقي عليه القبض في القضية وكان مديراً لموقع Minbar SOS قبل سفره إلى باكستان، بأنَّه قد جُنِّد بهذه الطريقة.

ولم تكن مجهودات التجنيد التي بذلها غرسلاوي مقتصرة على بلجيكا، فقد قام كذلك بتجنيد اثنين من المشتركين الفرنسيين في Minbar SOS. وأشار أحد هذين المجندين، الذي سافر إلى المناطق القبلية الخاضعة للإدارة الاتحادية في باكستان وأُلقي عليه القبض لاحقاً، إلى دعوات "الجهاد" على Minbar SOS بوصفها "لا تنقطع" وقال إنَّ شريط الفيديو الدعائي الذي شاهده على الموقع جعله يرغب في التطوع.

وفي كانون الأول/ديسمبر ٢٠٠٧، قام غرسلاوي وستة مجندين، بمن فيهم هشام بيايو وعلي الغنوتي وي. حريزي، بالسفر إلى المناطق القبلية الخاضعة للإدارة الاتحادية عبر تركيا وجمهورية إيران الإسلامية. وظلت المجموعة هناك حتى النصف الثاني من عام ٢٠٠٨. وكان غرسلاوي، أثناء وجوده هناك، على اتصال منتظم مع العروض عبر البريد الإلكتروني وسكايب أحيانا. وكان غرسلاوي ينشر تصريحات كما كان يدخل بين الفينة والأخرى إلى منتديات Minbar SOS، بالإضافة إلى إرسال صور وغيرها من المواد الدعائية.

وفي ٢٦ أيلول/سبتمبر ٢٠٠٨، نشر غرسلاوي تصريحاً على Minbar SOS يدعو لهجمات في أوروبا: "إنَّ الحل، يا أخوتي وأخواتي، ليس الفتاوى وإنما الانفجارات".

إلقاء القبض على المدَّعى عليهم

بدأ عدد من المشتبه بهم العودة إلى بلجيكا على مدى عدة أشهر في النصف الثاني من عام ٢٠٠٨. ووُضعت الأجهزة الأمنية البلجيكية في حالة استنفار عقب عودة الغنوتي وحريزي من المناطق القبلية الخاضعة للإدارة الاتحادية. وفي ٤ كانون الأول/ديسمبر ٢٠٠٨ عاد بيايو نفسه إلى بلجيكا.

وقُدِّمت تفسيرات متباينة لأسباب عودة المجندين إلى بلجيكا في هذا الوقت بالذات. فقد ألمح بعض المشتبه بهم إلى استيائهم من المعاملة والظروف السائدة في المناطق القبلية الخاضعة للإدارة الاتحادية، بما في ذلك القيود على قدرتهم على المشاركة في الجهاد، وأنكروا وجود أية "خلية نائمة" تستهدف تنفيذ هجمات في بلجيكا. بيد أنَّ السلطات البلجيكية اعتبرت أنَّ هناك أسبابا قوية، بناء على المؤشرات المستقاة من الاتصالات المعترضة، للاشتباه في أن المجموعة ربما كانت في المراحل الأخيرة من التخطيط لعملية إرهابية انتحارية (مع إمكانية تنفيذها على يد هشام بيايو) داخل بلجيكا، وهو ما استدعى التدخل على الفور.

وفي ١١ كانون الأول/ديسمبر، وبعد أسبوع من عودة بيايو، أغارت السلطات البلجيكية على ١٦ موقعاً داخل بلجيكا وألقت القبض على ٩ من المشتبه بهم، بمن فيهم العروض وغرسلاوي وبيايو. كما نُفِّذت عمليات مشابهة في فرنسا وإيطاليا.

الدعاوى الجنائية

بلجيكا

في المحاكمة، طعن محامو الدفاع في عدد من جوانب دفوع النيابة العامة، بما في ذلك الأسس الإجرائية ومقبولية بعض الأدلة، بما في ذلك البيانات المتعلقة بالإنترنت التي تمَّ الحصول عليها بطريقة غير رسمية من مكتب التحقيقات الاتحادي الأمريكي فيما يخص مقدمي خدمات الإنترنت الموجودين في الولايات المتحدة. وسيعرض المنشور لاحقا للمسائل المتعلقة بهذه الأدلة بالتفصيل.

وكانت السلطات في المغرب قد استجوبت بيايو في ٢٠ أيار/مايو ٢٠٠٨. ودفع محاموه بوقوع انتهاك للحق في المحاكمة العادلة، استناداً إلى الاشتباه في قيام السلطات المغربية بتعذيب المحتجزين المشتبه في ضلوعهم في الإرهاب. وقد رفضت المحكمة هذه الدفوع.

أنشطة برايان نيل فيناس (الولايات المتحدة)

في كانون الثاني/يناير ٢٠٠٩، سافر المواطن الأمريكي برايان نيل فيناس إلى أفغانستان، حيث حاول قتل جنود أمريكيين أثناء هجوم بالصواريخ شنَّه تنظيم القاعدة على قاعدة عسكرية. وقد أُلقي عليه القبض بعد ذلك وأعيد إلى الولايات المتحدة الأمريكية، حيث وُجِّهت إليه تهم بالتآمر لقتل مواطنين أمريكيين، وتوفير الدعم المادي لتنظيم القاعدة، وتلقي تدريبات عسكرية على يد التنظيم. وقد أقر فيناس بذنبه في التهم الموجهة إليه وحكم عليه بالسجن.

وقدمت السلطات البلجيكية القائمة على الملاحقة القضائية لبيايو، أحد شركاء العروض، أدلةً من محاكمة فيناس لإثبات نطاق أنشطة العروض وشركائها ومدى ضلوعهم في شبكة تنظيم القاعدة. ففي تصريحات لفيناس، أقرَّ بأنه قد التقى بعض المجندين البلجيكيين. وطعن الدفاع في مقبولية هذا الدليل لعدد من الأسباب، إلا أنَّ المحكمة رفضت هذه الدفوع.

نتيجة المحاكمة

عقب المحاكمة، بتّت محكمة بروكسل الابتدائية في ١٠ أيار/مايو ٢٠١٠ أحكامها في قضايا تسعة من المدَّعى عليهم الذين تمت ملاحقتهم قضائياً في تهم مختلفة مقسَّمة إلى ثلاث مجموعات هي ألف وباء وجيم.

وشملت التهم الموجهة في إطار المجموعتين ألف وجيم، على الترتيب، المشاركة كعضو قيادي في تنظيم إرهابي والمشاركة في أنشطة تنظيم إرهابي، بوسائل منها توفير المعلومات أو الدعم المادي أو أي شكل من أشكال التمويل لأنشطة تنظيم إرهابي، مع العلم بأنَّ من شأن هذه المشاركة أن تسهم في ارتكاب ذلك التنظيم لجريمة من الجرائم.

وشملت التهم الموجهة في إطار المجموعة باء ارتكاب جرائم أو المساعدة على تنفيذ جرائم من خلال التبرع، أو تقديم الوعود، أو التهديدات، أو إساءة استغلال السلطة أو النفوذ، أو التآمر بقصد ارتكاب جريمة ضد أشخاص أو ممتلكات بغرض التسبب في ضرر بالغ، وكذلك الجرائم التي يمكن، بحكم طبيعتها أو سياقها، أن تضر بلداً ما أو منظمة دولية ما ضررا بالغا والتي ترتكب عمدا بغرض الترويع الشديد لجماعة من الناس أو إجبار السلطات العامة أو منظمة دولية بطريقة غير مشروعة على اتخاذ إجراء معين، أو بغرض زعزعة استقرار الهياكل السياسية أو الدستورية أو الاقتصادية أو الاجتماعية الأساسية لبلد ما أو منظمة دولية ما أو تدمير هذه الهياكل.

وصدرت الأحكام التالية بخصوص التهم الموجهة في إطار المجموعة ألف:

- مليكة العروض: السجن ثماني سنوات وغرامة قدرها ٥ ٠٠٠ يورو
- معز غرسلاوي: السجن ثماني سنوات وغرامة قدرها ٥ ٠٠٠ يورو (غيابياً)
- هشام بيايو: السجن خمس سنوات وغرامة قدرها ١ ٠٠٠ يورو (غيابياً).

وصدرت الأحكام التالية بخصوص التهم الموجهة في إطار المجموعة باء:

- علي الغنوتي: البراءة
- سعيد حريزي: البراءة.

وصدرت الأحكام التالية بخصوص التهم الموجهة في إطار المجموعة جيم:

- علي الغنوتي: السجن ثلاث سنوات وغرامة قدرها ٥٠٠ يورو
- سعيد حريزي: السجن أربعين شهراً وغرامة قدرها ٥٠٠ يورو
- هشام بوهالي زريول: السجن خمس سنوات وغرامة قدرها ٢ ٠٠٠ يورو (غيابياً)
- عبد العزيز باستين: السجن أربعين شهراً وغرامة قدرها ٥٠٠ يورو
- محمد الأمين باستين: السجن أربعين شهراً وغرامة قدرها ٥٠٠ يورو
- جان-كريستوف تريفوا: البراءة.

فرنسا

في فرنسا، حوكم خمس من المشتبه بهم (جميعم يحملون الجنسية الفرنسية ومن أصول شمال-أفريقية) أمام محكمة باريس الابتدائية. ووُجهت إلى وليد عثماني، وحمادي عزيري، وسميرة غامري ملوك، وهشام بن راشد، ويوسف المرابط، عدة تهم هي: تمويل الإرهاب، والتآمر لارتكاب عمل إرهابي، والاشتراك في تنظيم مشكَّل بغرض التحضير لعمل إرهابي منصوص عليه في المادة ٤٢١-١ من قانون العقوبات الفرنسي.

إيطاليا

وجهت السلطات الإيطالية لكل من بسام عياشي ورفائيل جندرون (وكلاهما فرنسي الجنسية) تهمة التآمر الإجرامي بهدف الإرهاب بموجب الفقرة ١ من المادة ٢٠٧ مكررا من القانون الجنائي الإيطالي، التي تنص على عقوبة بالسجن من ٧ سنوات إلى ١٥ سنة في حق أي شخص يدان في تهمة تشكيل جماعات تعتزم القيام بأعمال عنف دعماً لأهداف الإرهاب أو قلب النظام الديمقراطي للدولة، أو الترويج لهذه الجماعات، أو تنظيمها، أو إدارتها، أو تمويلها، كما تنص على عقوبة بالسجن من ٥ إلى ١٠ سنوات للأشخاص الذين ينتسبون لهذه التنظيمات.

وقد أثبتت القضية وجود صلة بين المدَّعى عليهما وبعض المدَّعى عليهم في الدعوى البلجيكية، فضلا عن قواسم مشتركة فيما بين الأدلة، بما في ذلك دليل على قرص فيديو رقمي يحتوي على رسالة انتحار كتبها أحد المشتبه بهم البلجيكيين.

وفي ٣ حزيران/يونيه ٢٠١١، حُكم على عياشي وجندرون بالسجن ثماني سنوات.

المصدر: Eurojust, *Terrorism Convictions Monitor,* Issue 8, September 2010.

(أ) حكم صادر في ١٨ شباط/فبراير ٢٠١١ (رقم القضية ١٠١٥٢٣٩٠١٤).

(ب) انظر: "Al Qaeda warrior uses Internet to Rally Women", The New York Times (28 May 2008). على الرابط التالي: www.nytimes.com/2008/05/28/world/europe/28terror.html?_r=1&pagewanted=all.

٣٧٨- وكانت الأدلة التي قدمتها النيابة العامة في قضية العروض عبارة عن بيانات مستقاة من الإنترنت منها تعليقات منشورة ومناقشات في منتديات الدردشة. وفيما يتعلق برسائل البريد الإلكتروني (التي أُرسلت من حسابات لدى شركتي ياهو ومايكروسوفت)، كانت البيانات موجودة على خواديم في الولايات المتحدة. وقَدَّم مكتب التحقيقات الاتحادي للسلطات البلجيكية (في غضون أسبوعين)، بناء على طلب غير رسمي للمساعدة، قرصاً مدمجاً يحتوي على بيانات متعلقة بحسابي البريد الإلكتروني المعنيين وغيرهما من الحسابات ذات الصلة. وقد أفاد مكتب التحقيقات الاتحادي بأنّ كلا من ياهو ومايكروسوفت قدّمتا هذه البيانات طوعاً، كما هو مسموح به بموجب أحكام قانون توحيد أمريكا وتقويتها بإتاحة الأدوات اللازمة لاعتراض أعمال الإرهاب وعرقلتها.

٣٧٩- وقد طعن الدفاع في مقبولية هذه الأدلة، مؤكِّدا على أنَّ الإجراءات المستخدمة في الحصول على الأدلة وإرسالها وتقديمها لم تكن قانونية، إذ إنَّ الحصول عليها تم دون أمر تفتيش قضائي، ولعدم اتباع الأساليب المعهودة في التبادل الدولي للمعلومات القضائية في تلك الإجراءات غير الرسمية، مما يخالف الفقرة ١ من المادة ٧ من قانون بلجيكي صادر في ٩ كانون الأول/ديسمبر ٢٠٠٤ بشأن المساعدة الدولية المتبادلة في المسائل الجنائية.

٣٨٠- وقد رفضت المحكمة هذه الدفوع، ورأت: *(أ)* أنَّ تبادل المعلومات لم يقع ضمن إطار المساعدة الدولية المتبادلة؛ *(ب)* لم يعين قاض للتحقيق في القضية في الوقت المعني، حيث كانت القضية قائمة على أساس التعاون غير الرسمي بين الشرطة في البلدين؛ *(ج)* المبرر وراء الإجراءات التي استُخدمت هو صبغة الاستعجال التي كانت ظروف القضية تكتسيها (أي اكتشاف رسالة انتحار منشورة على موقع Minbar SOS الشبكي من قبل أحد المشتبه بهم، وهو ما قاد إلى الاعتقاد بأنَّ هجوماً على التراب الفرنسي من تدبير مليكة العروض وشركائها قد بات وشيكاً). ورأت المحكمة أنَّ القاضي الاتحادي كان لديه، استناداً إلى هذه الأسباب، ما يبرر التوصل إلى

استنتاج مفاده أنَّ هذا التعاون العاجل بين الشرطة كان مبنياً على أحكام الفقرة (ب) من المادة ١٥ من الاتفاقية الدولية لقمع الهجمات الإرهابية بالقنابل (١٩٩٧)،[١٦٦] التي تنص على "تبادل المعلومات الدقيقة المتحقق منها وفقا لقانونها الداخلي وتنسيق التدابير الإدارية وغير الإدارية المتخذة حسب الاقتضاء لمنع ارتكاب الجرائم المنصوص عليها في المادة ٢".[١٦٧]

٣٨١- وأخيراً، فقد رأت المحكمة أنَّه، وحيث إنَّ الأساس القانوني للمعلومات التي أرسلتها سلطات الولايات المتحدة إلى الشرطة البلجيكية كان سليماً، من الممكن استخدامها بحكم الواقع من قبل السلطات القضائية البلجيكية. وأضافت المحكمة أنَّ التحليل المتعلق بعناوين البريد الإلكتروني الموجودة في الولايات المتحدة (أو أغلب هذه العناوين) قد أدرج في الملف القضائي إثر التماس تفويض قضائي بالإنابة القضائية صادر في فرنسا.[١٦٨]

٣٨٢- وتسلط هذه القضية الضوء على ضرورة إمعان للنظر، أثناء مرحلة التحقيق في القضايا التي يستعان فيها بأدلة أجنبية، في الأساليب المستخدمة في الحصول على هذه الأدلة وفي إرسالها، الأمر الذي يزيد من أهمية إشراك أعضاء النيابة العامة في التحقيق بأسرع ما يمكن، وهو ما أكَّد عليه العديد من المشاركين في اجتماع فريق الخبراء، للوقوف على ما قد ينشأ من مسائل تتعلق بالأدلة واللجوء إلى الوساطة في حلها قبل المحاكمة.

٣٨٣- وقد كان على النيابة العامة، في قضية ناموح (كندا)، أن تقدِّم في المحاكمة أدلة حصل عليها أحد أفراد الشرطة النمساوية، مما طرح مشاكل في وقت لاحق. فبموجب القانون النمساوي، يُمكن قبول شهادة أفراد الشرطة باعتبارها أدلة في حال تقديمها على شكل إفادة مكتوبة. أما القانون الكندي فيستبعد بصفة عامة الأدلة المستندة إلى ترديد الأقاويل ويقتضي مثول الشاهد أمام المحكمة ليدلي بشهادة شفهية. وحتى يتأتى تقديم شهادة الشرطي المعني، كان على النيابة العامة الكندية أن تتواصل عن كثب مع الشرطة والنيابة العامة النمساويتين لشرح قواعد الإثبات المطبَّقة بموجب القانون الكندي، فضلا عن التواصل مع محامي الدفاع لتيسير الاتفاق على إمكانية إدلاء الشرطي بشهادة مكتوبة.

٤- *الاستعانة بشهادة الخبراء*

٣٨٤- كثيراً ما يكون من اللازم على أعضاء النيابة العامة في قضايا الإرهاب أن يقدِّموا شهادة الخبراء لإثبات جانب متخصص من جوانب القضية. إلا أنَّ نطاق المسائل التي يُمكن أن تفرض استخدام هذا النوع من الأدلة واسع للغاية. ويمكن، باستقراء الملاحقات القضائية التي وقعت بالفعل لقضايا نُفِّذت فيها أنشطة إرهابية على الإنترنت، الوقوف بصفة عامة على بعض المجالات التي قد يحتاج فيها المحققون أو أعضاء النيابة العامة إلى النظر في هذه المسألة.

٣٨٥- وفي هذا السياق، ما فتئت مجالات التكنولوجيا والاتصالات تتطور بوتيرة سريعة، مع تزايد في تعقيدها وتخصصها. ومن ثمَّ فثمة احتمال كبير لأن يحتاج أعضاء النيابة العامة للعديد من الشهود الخبراء ليقوموا بشرح جوانب تقنية مختلفة، وإنما مرتبطة ببعضها البعض، لنظم الحاسوب أو الاتصالات أو ما يتصل بها من

[١٦٦] الأمم المتحدة، مجموعة *المعاهدات*، المجلد ٢١٧٨، الرقم ٣٨٣٤٩.

[١٦٧] Eurojust, *Terrorism Conviction Monitor,* Issue 8, September 2010.

[١٦٨] المرجع نفسه.

أنشطة في سياق الدعوى نفسها، ولا سيما حين يكون هنالك ما يثبت أنَّ مشتبهاً به قد استخدم جهاز حاسوب بعينه أو غير ذلك من الأجهزة أو الخدمات المتعلقة بالإنترنت.[١٦٩]

٣٨٦- وبالإضافة إلى الأدلة المتعلقة بالتحليل الجنائي الحاسوبي في القضايا التي يشتبه فيها بالاشتراك في جماعات إرهابية أو توفير الدعم المادي لها، أو بالتحريض أو التجنيد أو التدريب، قد يقتضي الأمر شهادة خبراء بشأن المعتقدات الإيديولوجية والأهداف والأنشطة والهياكل التنظيمية المتعلقة بجماعات إرهابية معينة أو أفراد معينين.

٣٨٧- وعادة ما تتطلب القضايا التي تحتاج إلى الاستعانة بشهادة الخبراء ثلاث خطوات أو مراحل هي: *(أ)* تحديد المسائل التي تحتاج إلى رأي خبير (ونطاق هذه المسائل) بوضوح؛ *(ب)* اختيار خبراء مؤهلين؛ *(ج)* ضمان استخدام الخبراء المؤهلين لوسائل يمكن قبولها في المحكمة.[١٧٠]

(أ) تحديد المسائل بوضوح

٣٨٨- ينبغي لأعضاء النيابة العامة، الذين يعملون بالتنسيق الوثيق مع المحققين، أن يحددوا بأسرع ما يمكن المسائل التي يعتبرون أنهم سيحتاجون فيها إلى شهادة الخبراء، وأن يستعينوا بالخبراء لإجراء التحليل اللازم، ويقدموا إليهم إرشادات واضحة بشأن العناصر الرئيسية للأدلة.

(ب) اختيار خبراء مؤهلين

٣٨٩- يتعين على أعضاء النيابة العامة، عند اختيار شهود خبراء ليدلوا بشهادتهم بشأن الجوانب المتخصصة للأدلة في الملاحقات القضائية لقضايا الإرهاب، النظر فيما إذا كان ينبغي الاستعانة بخبراء حكوميين أو غير حكوميين. فلئن كانت الاستعانة بالخبراء الحكوميين جائزة ولها بعض المزايا، فإنَّ ذلك قد لا يكون مستصوباً إذا كان من المحتمل أن تؤدي إجراءات إفشاء المعلومات المنفذة قبل المحاكمة أو استجواب أولئك الشهود من طرف محامي الدفاع أثناء المحاكمة إلى الكشف عن مصادر حساسة للمعلومات الاستخبارية أو عن الأساليب المتبعة في الحصول على المعلومات التي يستندون إليها في آرائهم. وحتى يتأتى تلافي هذا المأزق المحتمل، فلعل أعضاء النيابة العامة يفضلون الاعتماد على خبراء أكاديميين أو غير حكوميين، ممن يمكنهم إرساء أدلتهم على أساس معلومات متاحة علناً يمكن الكشف عنها دون تردد ودون الوقوع في خطر الإضرار بالمصادر أو الأساليب الاستخبارية.[١٧١]

٣٩٠- وتعدُّ قضية *نامـوح* من بين الأمثلة الجيدة على القضايا التي استعانت فيها النيابة العامة بخبراء غير حكوميين. ففي هذه القضية استدعي شاهدان ليقوما بشرح أهداف الجبهة الإعلامية الإسلامية العالمية وطرائق عملها. ويرد وصف لخلفية هذه الشهادة في الفقرة ٣٩٤ أدناه.

٣٩١- وقد يكون اختيار الخبير المناسب، ولا سيما في التخصصات الدقيقة، تحدياً كبيراً في الولايات القضائية الأقل تطورا. وينبغي لأعضاء النيابة العامة، بالتعاون مع المحققين، أن يتبعوا نهجاً سباقاً وحذراً، باستكشاف كل السبل حتى يجدوا (متى كان ذلك ممكناً) الشهود ذوي الخبرات اللازمة على المستوى الوطني، على أن يتخذوا خطوات، عند الضرورة، لإيجاد الشهود ذوي الخبرات اللازمة على المستوى الدولي.

---

[١٦٩] Walden, *Computer Crimes and Digital Investigations,* p. 383.

[١٧٠] National Institute of Justice, *Digital Evidence in the Courtroom,* chap. 3, sect. III.E.

[١٧١] مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة، *خلاصة قضايا الإرهاب*، الفقرة ١٩٤.

(ج) ضمان استخدام الخبراء المؤهلين لوسائل يمكن قبولها في المحكمة

٣٩٢- من الواضح أنَّ من الأهمية بمكان أن يتَّبع شهود النيابة العامة الممارسات الجيدة المتعارف عليها ويطبِّقوها في أي فحص أو تحليل يجرونه في المجال المحدد الذي يُستدعون للشهادة بشأنه. ويصح هذا القول أكثر ما يصح في أي تحليل جنائي متخصص يعتمدون عليه في الآراء التي سوف يطرحونها في إطار ما تقدمه النيابة العامة من أدلة. ومن ثم ينبغي للمحققين وأعضاء النيابة العامة أن ينظروا، بأسرع ما يمكن، فيما إذا كان الأمر سوف يقتضي الاستعانة بشهادة الخبراء في أي جانب متخصص من دفوع النيابة. فإن كان الأمر كذلك، وجب عليهم أن يستشيروا خبراء مؤهلين ويستعينوا بهم بأسرع ما يمكن لضمان الحفاظ على الأساس الذي تقوم عليه أي شهادة لاحقة يُدلي بها هؤلاء الخبراء بحيث يحظى بالقبول أمام المحكمة.

٣٩٣- وقد تكون الأدلة معقدة تقنياً في بعض القضايا، ولا سيما القضايا التي تستخدم فيها تكنولوجيا الحاسوب، فيحتاج أعضاء النيابة العامة والخبراء الشهود إلى النظر في الاستعانة بأساليب مبتكرة لعرض هذه الأدلة على القضاة أو هيئات المحلفين أو غيرهم من متقصِّي الحقائق أثناء المحاكمة بطريقة واضحة ومقنعة وسهلة الفهم. فعلى سبيل المثال، قد يساعد العرض البياني لتصميمات النظم أو حركة البيانات، عوضاً عن الشهادة الشفهية وحدها، متقصِّي الحقائق على فهم الجوانب التقنية ذات الصلة بنظم الحاسوب أو نظم الاتصالات فهما أفضل. ولا شك أنَّ من المهم أيضاً أن يكون لدى عضو النيابة العامة القائم على الملاحقة القضائية معرفة عملية جيدة بالموضوع المعني، بحيث يستطيع شرح المصطلحات والمفاهيم للقاضي أو هيئة المحلفين أو الهيئة القضائية والإقناع بدفوع النيابة.

٣٩٤- وقد استُعين كثيرا في قضية *ناموح* الكندية بشهادة الخبراء (من خبير في التحاليل الجنائية الرقمية في شرطة الخيالة الملكية الكندية) بشأن المسائل المتعلقة بالأدلة الرقمية. وقد تمحورت هذه المسائل حول زعم استخدام المدَّعى عليه لجهاز حاسوب (ضُبط في منزله)، وما اتصل بذلك من استخدام للإنترنت، أثناء مشاركته في منتديات النقاش على الإنترنت، وقيامه بتحميل مواد على مواقع شبكية، والتواصل مع شريك آخر موجود في النمسا. وكانت شهادة الخبير المفصلة بشأن مسائل التحاليل الجنائية الرقمية ضرورية لإقناع المحكمة بأنَّ المتهم كان هو الشخص المشغِّل لأجهزة الحاسوب التي أُرسلت منها الرسائل دليل الإدانة، فضلا عن وصف المعتقدات الإيديولوجية للجبهة الإعلامية الإسلامية العالمية، وهي التنظيم العالمي الذي كان المتهم مشاركاً فاعلا فيه، والأساليب التي تتبعها.

٣٩٥- وركَّز جزء من دفاع ناموح على التشكيك في هذا الجانب من دفوع النيابة. فقد أكَّد الدفاع على عدم إمكانية استخدام الإنترنت، نظراً لقابلية الخطأ التي هي من سماته الأساسية، بوصفه مصدراً موثوقاً للمعلومات بما يسمح للخبير الشاهد بأن يكوِّن رأياً بشأن الجبهة وغيرها من التنظيمات الإرهابية. وأكَّد الدفاع بصفة خاصة على أنَّ الشهود الخبراء لا يمكنهم أن يتأكدوا مما إذا كانت المواد المنشورة على منتديات الدردشة في الإنترنت، وغيرها من أنواع الاتصالات الإلكترونية، هي في واقع الأمر من تأليف إرهابيين مزعومين أو أشخاص يعملون لحساب الدولة بغرض الاستدراج. وفي هذه القضية، أدلى خبير عن النيابة العامة بشهادة كانت كافية لإقناع المحكمة بموثوقية الأساليب والمواد المتعلقة بالإنترنت التي اعتُمد عليها، ولمنح نفس الدرجة من الثقة لشهادة الخبير.

٣٩٦- ومن الجدير بالذكر أنَّ هذه الاتصالات الإلكترونية كانت قد جرت باللغة العربية وتُرجمت إلى الفرنسية، وقُدِّمت الترجمة الفرنسية إلى المحكمة من قبل النيابة العامة إلى جانب النص العربي الأصلي. ويسلِّط هذا

الجانب من جوانب القضية الضوء أيضاً على ضرورة أن تبذل السلطات العناية الواجبة حين تسعى لتقديم ترجمات لمحادثات أو مستندات ضمن الأدلة، بما في ذلك النصوص المدوَّنة للاتصالات المعترضة.

٣٩٧- وبالإضافة إلى شهادة الخبراء بشأن الأدلة الرقمية البالغة الأهمية، فقد استعانت النيابة العامة بشهادة الخبراء بشأن أنشطة الجبهة الإعلامية الإسلامية العالمية وأهدافها، وأساليبها في التنسيق مع الأعضاء الجدد وتجنيدهم، وفي الترويج للأفكار المتطرفة، وفي التدريب العسكري، والأساليب التي تتواصل بها عبر الإنترنت. وقدَّمت النيابة في واقع الأمر تقريرين مكتوبين أعدَّهما اثنان من الخبراء في هذه الموضوعات، وأدلى أحد الخبيرين بشهادته في المحكمة تأييداً لما خلص إليه في تقريره. وقد أكَّد الخبير الكندي في اجتماع فريق الخبراء على أهمية أن يكون لدى النيابة العامة أكثر من شاهد خبير واحد في المسائل الرئيسية المتعلقة بالأدلة، زيادةً في التأكيد وتحسباً لأي طارئ.

٣٩٨- وتتبين قيمة هذا النوع من شهادات الخبراء في الملاحقات القضائية التي تُوجه فيها تهم بدعم تنظيم إرهابي، في التصريح التالي لقاضي المحاكمة، الذي أشار فيه إلى "الأفعال الحقيقية التي كانت الجبهة الإعلامية الإسلامية العالمية تدعو إليها"، وهو الموضوع الذي أدلى فيه الخبير المستدعى من قِبل النيابة بشهادته:

> إنَّ ممثل الدفاع يدعو المحكمة إلى اعتبار مختلف الرسائل التي نشرتها الجبهة الإعلامية الإسلامية العالمية ذات معنى مجازي. ولا يساور المحكمة أدنى شك في هذا الصدد. فسياق هذه الرسائل يشير بوضوح إلى أفعال حقيقية كانت الجبهة تدعو إليها. والإشارات إلى الموت والدمار مبثوثة في جميع أجزائها. والجهاد الذي تروِّج له الجبهة جهاد عنيف [التوكيد مضاف]. ومن الواضح أنَّ هذا الترويج يعدُّ بمثابة دعوة إلى القيام بأنشطة إرهابية وتهديداً بذلك في بعض الأحيان. ونتيجة لذلك، فإنَّ هذا النشاط يندرج بوضوح ضمن تعريف النشاط الإرهابي وفقاً للبند ٨٣-٠١ [من] القانون الجنائي.[١٧٢]

حاء- مسائل أخرى

١- *الحاجة للتخطيط للطوارئ والاستمرارية*

٣٩٩- يحبَّذ كثيرا، بسبب تعقيد الملاحقات القضائية المتعلقة بالإرهاب ولا سيما الملاحقات التي تتطلب التعاون الدولي أو تشمل عناصر تقنية معقدة، أن يتولى فريق من أعضاء النيابة العامة المسؤولية عن القضايا، على أن يكون كل منهم مُلمّاً بالدعاوى، وقادراً، إذا اقتضى الأمر، على مواصلتها إن تعذر على أي من أعضاء الفريق الاستمرار في القضية على نحو مفاجئ. ومن شأن هذا التحوط أن يضمن تسيير الدعاوى تسييرا جيدا ويقلل من احتمال الفشل إلى أدنى حد. وتُعدُّ قضيتا ناموح (كندا) وغيلوفيتش-يلمظ-شنايدر-سيليك (ألمانيا) من بين الأمثلة المفيدة على ملاحقات قضائية معقدة وكبيرة الحجم استدعت اللجوء إلى نهج يقوم على العمل الجماعي، مع اشتراك عضو واحد على الأقل من أعضاء النيابة العامة في مراحل القضية كافة. ومما تجدر الإشارة إليه في القضية الألمانية أنَّ مدة المحاكمة كانت قد قُدِّرت في الأصل بسنتين، إلا أنَّ المدة الفعلية كانت أقصر كثيراً نظراً لإقرار المدَّعى عليهم بذنبهم في التهم الموجَّهة إليهم، ومع ذلك فقد استغرقت المحاكمة نفسها ثلاثة أشهر.

[١٧٢] Justice C. Leblond, 1 October 2009.

٢- *الحاجة لتعزيز التدريب والقدرات*

٤٠٠- حتى يتأتى ضمانُ نهج متكامل يقوم على سيادة القانون والحفاظُ على اكتمال تدابير التصدي للإرهاب في مجال العدالة الجنائية، ينبغي أن يكون لدى البلدان إجراءات قوية ودائمة لتعزيز قدرة أعضاء النيابة العامة على تنفيذ التشريعات الوطنية لمكافحة الإرهاب والتزامات التعاون الدولي ذات الصلة. فطبيعة تشريعات مكافحة الإرهاب والتحقيقات في هذا المجال، والسرعة التي تجري بها الأنشطة المتعلقة بالإنترنت وتعقيدات هذه الأنشطة وطبيعتها العابرة للحدود تعني أنَّه يتعين على أعضاء فرق التحقيق، بمن فيهم أعضاء النيابة العامة، أن يتخذوا العديد من القرارات فيما يخص شتى جوانب القضية رغم ضيق الوقت. ومن المهم أن يكونوا مؤهلين تأهيلا كافيا ولديهم من الكفاءة ما يتيح لهم الاضطلاع بوظائفهم الأساسية في قضايا الإرهاب.

٤٠١- وفي البلدان التي يرتفع فيها احتمال وقوع أنشطة إرهابية، مع تدنٍّ في القدرات المؤسسية لأجهزة النيابة العامة وغيرها من أجهزة العدالة الجنائية، ينبغي إيلاء أولوية قصوى لاستحداث قدرات متخصصة داخل هذه الأجهزة، سواء من حيث الملاحقة القضائية للقضايا وما يتعلق بذلك من آليات التعاون الدولي.

سابعاً- التعاون مع القطاع الخاص

ألف- دور جهات القطاع الخاص المعنية

٤٠٢- لئن كانت مسؤولية مكافحة استخدام الإنترنت في أغراض إرهابية تقع في نهاية المطاف على عاتق الدول الأعضاء، فإنَّ للتعاون مع أهم جهات القطاع الخاص المعنية أهميةً حاسمةً في فعالية التنفيذ. فالبنية التحتية الشبكية التي تقوم عليها خدمات الإنترنت غالباً ما تكون مملوكة، كلياً أو جزئياً، لكيانات خاصة. كذلك عادة ما تملك الشركات الخاصة منتديات التواصل الاجتماعي التي تيسِّر تعميم محتويات يعدها المستخدمون أنفسهم على جمهور واسع، فضلا عن محركات البحث على الإنترنت ذات الشعبية الكبيرة، والتي تقوم بفرز المحتويات على أساس معايير يُقدِّمها المستخدم.

٤٠٣- إنَّ فعالية الإنترنت باعتبارها وسيلة لنشر محتويات متعلقة بالأعمال الإرهابية تتوقف على كل من مُنشئ الاتصال وامتلاك جمهوره للقدرة على الوصول إلى تكنولوجيات الإنترنت. ولذا فإنَّ الوسيلتين الأساسيتين للحد من تأثير هذه الاتصالات هما إما التحكم في الوصول إلى البنية التحتية للشبكة، أو فرض الرقابة على محتويات الإنترنت، أو مزيج من الوسيلتين معا.[١٧٣] ولئن كان مستوى التنظيم الرقابي الحكومي للإنترنت يتفاوت تفاوتاً كبيراً فيما بين الدول الأعضاء، بسبب عدم وجود هيئة عالمية مركزية مسؤولة عن هذا التنظيم، فما زالت الجهات المعنية في القطاع الخاص مثل مقدمي الخدمات، والمواقع الشبكية التي تستضيف محتويات يعدها المستخدمون أنفسهم، ومحركات البحث على الإنترنت، تؤدي دوراً هاماً في التحكم في إتاحة المحتويات المتعلقة بالإرهاب التي يجري نشرها عبر الإنترنت. كما قد يساعد التنظيم الرقابي الذاتي من قبل هذه الجهات المعنية في القطاع الخاص على التصدي لأنشطة الاتصالات والتحريض والدفع باتجاه التطرف والتدريب ذات الصلة بالإرهاب والتي تُنفَّذ عبر الإنترنت. كذلك فإنَّ شركات الرصد الخاصة تؤدي دوراً في الوقوف في الوقت المناسب على الأنشطة التي قد تروِّج للأعمال الإرهابية على الإنترنت.

١- *مقدمو خدمات الإنترنت*

٤٠٤- تتحكم جهات غير حكومية، في العديد من الدول الأعضاء، في قدرة المستخدمين على الوصول إلى الإنترنت، مثل مقدمي خدمات الاتصالات المنتمين إلى القطاع الخاص، ممن يملكون أو يديرون البنية التحتية الشبكية. وقد يكون مقدمو الخدمات هؤلاء في موقع يؤهلهم للمساعدة في الحصول على بيانات الاتصالات أو للكشف عن هذه البيانات، حسب الاقتضاء،[١٧٤] دعماً لتحقيق بعينه تقوم به أجهزة إنفاذ القانون والعدالة الجنائية والاستخبارات بشأن نشاط إرهابي محتمل. وقد تشكِّل بيانات الاتصالات الموجودة لدى مقدمي خدمات الإنترنت أدلة رئيسية ضد مرتكبي جرائم متعلقة بالإنترنت، أو قد تقود إلى الوصول إلى أدلة إضافية أو لشركاء للجناة بما يفيد التحقيق.

---

(١٧٣) Conway, "Terrorism and Internet governance: core issues", p. 26.

(١٧٤) رهناً بالضمانات والأنظمة المنطبقة بشأن الخصوصية.

٤٠٥- فعلى سبيل المثال، قد يُلزم مقدمو خدمات الإنترنت المستخدمين بتزويدهم بمعلومات تثبت هويتهم قبل الوصول إلى محتويات وخدمات الإنترنت. ومن الممكن أن يساعد الحصول على معلومات إثبات الهوية وحفظها كثيراً في إجراءات التحقيق والملاحقة القضائية. ويشار على وجه الخصوص إلى أنَّ اشتراط التسجيل لاستخدام شبكات الإنترنت اللاسلكية (واي فاي) أو مقاهي الإنترنت يُمكن أن يتيح مصدراً مهماً للبيانات في التحقيقات الجنائية. ولئن طبَّق بعض البلدان، كمصر، تشريعات تشترط على مقدمي خدمات الإنترنت التوثق من هوية المستخدمين قبل السماح لهم بالوصول إلى الإنترنت، فيمكن لمقدمي خدمات الإنترنت تنفيذ تدابير من هذا القبيل طوعاً.

(أ) التعاون مع السلطات الحكومية

٤٠٦- نظراً للحساسيات المرتبطة بقضايا الإرهاب، فمما قد يشجِّع جهات القطاع الخاص المعنية على التعاون مع سلطات إنفاذ القانون التأثيرُ الإيجابي لهذا التعاون على سمعتها، إذا تحقق فيه التوازن عن طريق إيلاء العناية الواجبة لاحترام حقوق الإنسان الأساسية، مثل حرية التعبير، واحترام حرمة الحياة الخاصة والمنازل والمراسلات، والحق في حماية البيانات. كما أنَّ تلافي الآثار السلبية الناجمة عن عدم التعاون قد يكون عاملا محفِّزاً بدوره. فعلى سبيل المثال، قد يُقبِل مقدمو خدمات الإنترنت على التعاون خشية إثارة دلالات سلبية حول كونهم مرتبطين بدعم النشاط الإرهابي. كما أنَّ المخاوف بشأن المسؤولية القانونية المرتبطة باستضافة أنواع معينة من محتويات الإنترنت قد تؤثر على مستوى تعاون كيانات القطاع الخاص.

٤٠٧- وأشار الخبير المصري إلى أن التجربة الوطنية في مصر تشير إلى أن جهات القطاع الخاص المعنية تتجاوب من منطلق روح التعاون مع الطلبات المعقولة الواردة من السلطات الحكومية لمنع الوصول إلى محتويات الإنترنت ذات الصلة بالإرهاب. وبالإضافة إلى ذلك، كما أن إقبال مقدمي خدمات الإنترنت في مصر على التعاون يعزى جزئيا، حسب ما قيل، إلى إدراك أن لديهم مصالح مشتركة مع السلطات الحكومية، إذ إنَّهم قد يكونون هم أنفسهم هدفاً لهجوم إرهابي والحال أن السلطات الحكومية تسعى لمنع هذه الأعمال الإرهابية وملاحقتها.

٤٠٨- وقد تبدي جهات القطاع الخاص استعدادها لإزالة المحتويات غير القانونية طواعية، لكن من الممكن أيضاً أن تُلزم بفعل ذلك بموجب التشريعات المحلية. فعلى سبيل المثال، تنص المادة ٣ من قانون الإرهاب لسنة ٢٠٠٦ في المملكة المتحدة على إشعارات "بالسحب" يجوز لسلطات إنفاذ القانون أن تصدرها لمقدمي خدمات الإنترنت (انظر الفقرة ١٧٢ أعلاه وما بعدها). وتُستخدم الإشعارات بالسحب لإخطار القائمين على استضافة المحتويات بأن هذه المواد تُعتبر ذات صلة بالإرهاب ومن ثم مخالفة للقانون في رأي مسؤول إنفاذ القانون. ويكون مقدمو خدمات الإنترنت الذين أُصدر إليهم إشعار بالسحب ملزمين بإزالة المحتويات ذات الصلة بالإرهاب في غضون يومي عمل. وفيما تستخدم ولايات قضائية أخرى الإشعارات بالسحب في بعض الجرائم، فإنَّ الأشيع أن يُطبَّق ذلك فيما يخص قضايا انتهاك حقوق التأليف والنشر أو المحتويات الجنسية الصريحة.

٤٠٩- وسلطت دولة إسرائيل الضوء على نجاحاتها فيما يخص التعاون مع ممثلي القطاع الخاص الأجنبي في إسرائيل. فعلى سبيل المثال، قُدمت طلبات في إطار عدة تحقيقات في جرائم حاسوبية إلى ممثلي مايكروسوفت وغوغل في إسرائيل. وقُدِّمت المعلومات التي طلبتها سلطات التحقيق على الفور عند استلام أوامر من المحكمة

حسب الأصول القانونية المرعية. وفي بعض الحالات التي كانت تتطلب توجيه الطلبات إلى ممثلين للقطاع الخاص موجودين في الولايات المتحدة، عادة ما كانت تتبع الإجراءات الرسمية لطلب المساعدة القانونية عبر السلطات الحكومية، مع اللجوء أحياناً إلى التقدم بطلبات مباشرة إلى شركات أجنبية خاصة للحصول على بيانات إثبات الهوية.

(ب) الاحتفاظ بالبيانات

٤١٠- أُحدثت مؤخرا، أو اقتُرح إحداث، تشريعات في عدة دول أعضاء، تُلزم مقدمي خدمات الاتصالات بجمع بيانات الاتصالات المتعلقة بمستخدميهم وأرشفتها. ففي عام ٢٠٠٦، قام الاتحاد الأوروبي، لأسباب منها الهجومان الإرهابيان في مدريد عام ٢٠٠٤ وفي لندن عام ٢٠٠٥[١٧٥] باشتراع توجيه بشأن الاحتفاظ الإلزامي ببيانات حركة الاتصالات (التوجيه 2006/24/EC الصادر عن البرلمان الأوروبي ومجلس الاتحاد الأوروبي في ١٥ آذار/مارس ٢٠٠٦ بشأن الاحتفاظ بالبيانات التي يتم توليدها أو معالجتها في إطار توفير خدمات الاتصالات الإلكترونية المتاحة للجمهور أو شبكات الاتصالات العامة، الذي يعدِّل بموجبه التوجيه 2002/58/EC).[١٧٦] ويقر التوجيه 2006/24/EC بالتحديات الناشئة عن الاختلافات القانونية والتقنية بين الأحكام الوطنية فيما يخص أنواع البيانات التي يجب الاحتفاظ بها، وشروط الاحتفاظ بالبيانات ومدته.[١٧٧] ومن ثم فإنَّ التوجيه يسعى إلى تحقيق الاتساق فيما بين الحدود الدنيا للالتزامات المفروضة على مقدمي خدمات الاتصالات الإلكترونية العاملين في الدول الأعضاء في الاتحاد الأوروبي بشأن الاحتفاظ بالبيانات، بغرض منع الأفعال الجنائية والتحقيق فيها والكشف عنها والملاحقة القضائية بشأنها.

٤١١- ويُلزم التوجيه 2006/24/EC الدول الأعضاء باعتماد تشريعات[١٧٨] تُلزم مقدمي خدمات الاتصالات بالاحتفاظ ببيانات معينة حول حركة الاتصالات الإلكترونية،[١٧٩] لمدة تتراوح بين ستة أشهر وسنتين. وتتضمن هذه البيانات المعلومات اللازمة للوقوف على هوية المنشئ والمتلقي لرسائل البريد الإلكتروني والاتصالات الهاتفية، إلى جانب معلومات حول وقت هذه الاتصالات وتاريخها ومدتها، بيد أنَّها لا تشمل محتوى الاتصالات الإلكترونية.[١٨٠] ويجب إتاحة هذه البيانات في إطار التحقيق في الجرائم الخطيرة والكشف عنها والملاحقة القضائية لسلطات إنفاذ القانون الوطنية، ولنظيراتها في البلدان الأخرى الأعضاء في الاتحاد الأوروبي عبر السلطات الوطنية،[١٨١] كل وفقاً لمقتضيات قوانينه الوطنية.

---

(١٧٥) European Commission, "Report from the Commission to the Council and the European Parliament: evaluation report on the Data Retention Directive (Directive 2006/24/EC)", document COM(2011) 225 (Brussels, 18 April 2011), sect. 3.2.

(١٧٦) *Official Journal of the European Union,* L 105, 13 April 2006.

(١٧٧) المرجع نفسه، preamble, para. 6.

(١٧٨) كانت هناك، حتى نيسان/أبريل ٢٠١١، تشريعات سارية من هذا القبيل في ٢٢ دولة عضواً في الاتحاد الأوروبي.

(١٧٩) تتضمن هذه البيانات التي يولدها أو يعالجها مقدمو الخدمات في سياق أنشطتهم، مثل البيانات التي تولّد أو تعالَج بغرض إرسال رسالة، أو إرسال فواتير، أو الاتصال عبر الشبكي، أو السداد، أو التسويق، أو غير ذلك من خدمات القيمة المضافة.

(١٨٠) *Official Journal of the European Union,* L 105, 13 April 2006, art. 5.

(١٨١) المرجع نفسه، المادة ٤.

٤١٢- فعلى سبيل المثال، يجوز لسلطات إنفاذ القانون الوطنية فور إدماج التوجيه في التشريعات المحلية، ورهناً بالمتطلبات الإجرائية المنطبقة، أن تطلب من مقدمي الخدمات الوصول إلى البيانات للوقوف على هوية المشتركين الذين يستخدمون عنواناً معيناً من عناوين بروتوكول الإنترنت، والجهات التي كان هؤلاء الأشخاص يتصلون بها خلال فترة محددة من الزمن.[١٨٢] وعلاوة على ذلك، يجوز الاستناد في التحقيقات في الأعمال الإرهابية إلى ما يحتفظ به مقدمو الخدمات من بيانات تبين طول الفترة الزمنية التي استغرقها التخطيط للعمل الإرهابي للوقوف على أنماط السلوك الإجرامي والعلاقات فيما بين الشركاء في الجريمة وإثبات القصد الجنائي.[١٨٣] وقد أشار بعض الدول الأعضاء في الاتحاد الأوروبي[١٨٤] إلى أنَّ سجلات الاحتفاظ بالبيانات هي الوسيلة الوحيدة للتحقيق في بعض الجرائم التي تنطوي على اتصالات عبر الإنترنت، مثل المواد المنشورة في منتديات الدردشة، التي لا يمكن اقتفاء أثرها إلا عبر بيانات حركة المعلومات على الإنترنت.[١٨٥] كما أفاد العديد من الدول الأعضاء في الاتحاد الأوروبي[١٨٦] باستخدام البيانات التي يحتفظ بها مقدمو الخدمات لتبرئة أشخاص متهمين بجرائم دون اللجوء لأساليب أخرى، أكثر تطفلا، للمراقبة مثل اعتراض الاتصالات وتفتيش المنازل. كذلك فإنَّ البيانات المكانية مهمة أيضاً حين تستخدمها أجهزة إنفاذ القانون لاستبعاد وجود المشتبه بهم في مسرح الجريمة والتحقق من صحة حجج الغياب. كما أنَّ البيانات المحتفظ بها بموجب التشريعات الصادرة بشأن التوجيه تمكّن من اقتفاء أثر الأدلة وصولاً إلى العمل الإرهابي، بوسائل منها تيسير إحداث أو تدعيم أشكال أخرى من الأدلة على الأنشطة والصلات بين المشتبه بهم.[١٨٧]

٢- *المواقع الشبكية وغيرها من المنابر التي تستضيف محتويات من إعداد المستخدمين أنفسهم*

٤١٣- إنَّ لدى المحتويات ذات الصلة بالإرهاب التي يعدّها المستخدمون أنفسهم وتستضيفها مواقع شبكية ذات شعبية القدرةُ على الوصول إلى جمهور أكبر كثيراً من المحتويات الموجودة في المواقع التقليدية المتخصصة ولوحات الإعلان الإلكترونية والمنتديات الشبكية التي عادةً ما تجتذب مجموعة أفراد تتكوَّن تلقائيا. فوفقاً لموقع يوتيوب لنشر شرائط الفيديو، فإنَّ ٤٨ ساعة من شرائط الفيديو التي ينتجها المستخدمون أنفسهم تُحمَّل على الموقع كل دقيقة، أي أنَّ ما يعادل ثماني سنوات من المحتويات يُحمَّل كل يوم.[١٨٨] وكون المحتوى متاحاً لما يُقدَّر بـ ٨ ملايين من مستخدمي موقع يوتيوب كل شهر الذين يتفرد كل واحد منهم بخصائص معينة، يقلل كثيرا من الحواجز أمام الوصول إلى المحتويات ذات الصلة بالإرهاب. كما أنَّ الزيادة الهائلة في الإقبال على المحتويات التي يعدها المستخدمون أنفسهم في السنوات الأخيرة تزيد من الصعوبات اللوجستية أمام رصد المحتويات ذات الصلة بالإرهاب. وبالإضافة لذلك، قد يصادف مستخدمو مواقع استضافة الفيديو محتويات ذا صلة بالإرهاب عن غير قصد منهم نتيجة لبحثهم عن مواد أكثر اعتدالا أو مشاهدتهم لهذه المواد، بسبب إدماج آليات في هذه المواقع تقترح على المستخدم تلقائياً مشاهدة محتويات ذات صلة.

---

(١٨٢) European Commission, "Report from the Commission to the Council and the European Parliament: evaluation report on the Data Retention Directive (Directive 2006/24/EC)", sect. 5.2.

(١٨٣) المرجع نفسه، البندان ٣-١ و٥-٢.

(١٨٤) إيرلندا، وبلجيكا، والمملكة المتحدة.

(١٨٥) European Commission, "Report from the Commission to the Council and the European Parliament: evaluation report on the Data Retention Directive (Directive 2006/24/EC)", sect. 5.4.

(١٨٦) ألمانيا، وبولندا، وسلوفينيا، والمملكة المتحدة.

(١٨٧) European Commission, "Report from the Commission to the Council and the European Parliament: evaluation report on the Data Retention Directive (Directive 2006/24/EC)"sect. 5.4.

(١٨٨) إحصائيات من موقع يوتيوب، متاحة على الرابط التالي: www.youtube.com/t/press_statistics.

قضية فيليز غ

في هـذه القضيـة الألمانيـة، أدينت المدَّعى عليها، فيليـز غ.، في التهم المنسوبـة إليها بتجنيد أعضـاء أو مؤيدين لتنظيمـات إرهابية أجنبيـة (تنظيم القاعدة، واتحاد الجهـاد الإسلامي، ومجاهدي طالبـان الألمان) وبتقديم الدعم لهذه المنظمات.

ففـي آذار/مارس ٢٠٠٩، انضمـت المدَّعى عليها إلى منتدى على الإنترنت وبـدأت في نشر ترجمات إلى الألمانية لبيانـات من تنظيمـات إرهابية تشجب الجرائم المزعومة للقوات المسلحة الدوليـة في العراق وأفغانستان وتدعو المستخدمين للانضمام إلى الجهاد أو تقديم الدعم له. ولكون فيليز غ. زوجة إرهابي ألماني مسجون، سرعان ما نالت حقوق إدارة المنتدى. وبحلول الوقت الذي ألقي فيه القبض عليها في شباط/فبراير ٢٠١٠، كانت قد نشرت مـا يربـو علـى ١ ٠٠٠ مساهمة وتعليـق، في جزء من المنتدى متـاح للجمهور وفي قسم آخر مغلـق لا يتاح الدخول إليـه إلا للأعضـاء المسجلين. وقامت بفتح تسع قنوات فيديو على بوابة يوتيوب، ونشرت ١٠١ من أشرطة الفيديو علـى هـذه القنوات جميعها، بما في ذلك منشورات أعدتها تنظيمات إرهابية مثل تنظيم القاعدة واتحاد الجهاد الإسلامـي وأشرطة فيديـو أنتجتها هي نفسها. وكانت المدَّعى عليها تتعاون علـى نحو وثيق مع م.، "جهة الوصل الإعلاميـة" في اتحـاد الجهاد الإسلامي. وقـد اتصل م. بالمدَّعى عليها عبر الإنترنـت وطلب منها في البداية أن تقـوم بترجمة نصوص ذات محتوى ديني من التركيـة إلى الألمانية. ثم وافاها بروابـط لأشرطة فيديو نشرتها المدَّعى عليها على يوتيوب، كما طلب منها المساعدة في جمع تبرعات.

وفي إحـدى المـرات، قامت المدَّعى عليهـا بترجمة مواد منشورة علـى صفحة شبكية باللغة التركيـة إلى الألمانية ونشرتها على صفحة شبكية ألمانية. وكانت المواد تناشد المتبرعين دعم "عائلات المجاهدين في أفغانستان الذين يقاومون الهجمات الشرسة التي تشنها الدول الصليبية". وكان النص مصحوباً بسبع صور، إحداها تُظهر عدداً من المواد الغذائية المختلفة فيما تُظهر الست الأخرى أطفالا مسلحين ببنادق هجومية وغيرها من الأسلحة.

وبالإضافة إلى نشر المدعى عليها مواد تستهدف جمع الأموال، كانت ضالعة كذلك في عملية جمع الأموال نفسها. وللحفـاظ علـى سرية هوية المتبرعـين، قامت بفتح صندوق بريـد، كان المتبرعون يُرسلـون إليه مظاريف تحمل أسمـاء استخـدام الإنترنت الخاصة بهم وتحتوي علـى نقود (مساهمات بمئات من اليـوروات عادةً). بعد ذلك كانـت تستعين بشركة ويسترن يونيون للخدمات المالية لتحويـل الأموال إلى وسيط في تركيا يقوم بدوره بإحالتها إلى م. في وزيرستـان. كمـا قامت المدَّعى عليها بنشر أشرطة فيديو علـى الإنترنت تشكر فيها المتبرعين (الذين أطلقت عليهم لهذا الغرض أسماء مستعارة مرتبطة بأسماء استخدام الإنترنت الخاصة بهم) وتبلغهم بتطورات حملة جمع الأموال.

وفي المحاكمـة، في آذار/مارس ٢٠١١، أقرَّت المدَّعى عليها بذنبها في التهـم المنسوبة إليها وحُكم عليها بالسجن سنتـين ونصـف. وورد في حيثيـات قرار المحكمة بإدانة المدعـى عليها أنها كانت على علم تام بـأنَّ مصدر المواد الدعائيـة التي كانت توزعهـا تنظيماتٌ إرهابية وأنَّ الهدف من الأموال التي جمعتهـا وحولتها كان شراء أسلحة وذخـيرة، إلى جانـب السلع الإنسانيـة، لحساب هذه التنظيمـات. وعلق القاضي الذي أصـدر الحكم قائلا، في معرض إشارته إلى أنَّ الجرائم قد وقعت بالأساس على الإنترنت:

> [...] إنَّ المحكمـة تـولي أهميـة كبيرة لما لنشر دعايـة جهادية على الإنترنت من خطـورة شديدة. فبمجرد تحميـل مـواد على الإنترنت يصبح من المستحيـل أو يكاد التحكم فيها أو إزالتها مـن الشبكة، إذ يستطيع المستخدمـون الآخـرون تنزيلها واستعمالها ونشرها مـرة أخرى. وبالنظر إلى استخـدام هذه الوسيلة في كل أنحـاء العالم تقريباً، والعدد الهائل والمتزايد من مستخدميهـا، فإنَّ الإنترنت منبر ذو أهمية متزايدة للتنظيمـات الإرهابيـة في نشر أهدافها ودعايتهـا وإشاعة الخوف في جميع أنحـاء العالم من وجود خطر الإرهاب في كل مكان. ومن ثم فإنَّ نشرِ مساهمات من قبيل المساهمات التي نشرتها المتهمة يعتبر في حكم "إشعـال حرائق فكرية عمداً"، وأثره أدْوَمُ، ومن ثـم أخطر، من نشر مواد دعائية عن طريق المنشورات أو غيرها من المطبوعات، بل لا وجه للمقارنة بينهما.

٤١٤- وتُعدُّ قضية *التاج البريطاني ضد روشانارا تشودري* مثالاً على تحوُّل شخص عصامي إلى التطرف المؤدي إلى ارتكاب عمل من أعمال العنف لسبب وحيد هو الاطلاع على مواد عبر الإنترنت، وبالأخص في مواقع استضافة مقاطع الفيديو. وقد لفتت قضية السيدة تشودري الاهتمام الدولي إلى سهولة تمكُّنِها من العثور على أشرطة فيديو ذات محتوى إسلامي متطرف ومشاهدة هذه الأشرطة في موقع استضافة مقاطع الفيديو الذي ينشر محتويات من إعداد المستخدمين أنفسهم، وإلى عملية التحوُّل التي طرأت عليها وانتهت بها إلى اتخاذ قرار بتنفيذ عمل إرهابي عبر المثابرة على مشاهدة هذا المحتوى على مدى عدة أشهر.

٤١٥- وفي عام ٢٠١٠، وعقب محادثات مع حكومتي المملكة المتحدة، ممثلة في وحدة تلقي الشكاوى المعنية بمكافحة الإرهاب، والولايات المتحدة، التي تقع فيها خوادیم يوتيوب، تطوعت الشركة الأم ليوتيوب، وهي شركة غوغل ذات المسؤولية غير المحدودة، بوضع نظام يُمكِّن مشاهدي المحتوى من الإبلاغ عن أي محتوى يمكن أن يكون ذا صلة بالإرهاب على موقع يوتيوب الشبكي. وتُعدُّ هذه الآلية أداة هامة للوقوف بصورة استباقية على المحتويات التي قد تروِّج لأعمال إرهابية.

٤١٦- كذلك فإنَّ بعض المواقع الشبكية ومنابر التواصل الاجتماعي تتضمَّن شروط استخدامها أحكاماً تحظر استغلال خدماتها للترويج للأنشطة الإرهابية، في جملة أمور أخرى. فعلى سبيل المثال، تحظر شروط الخدمة الخاصة بتويتر،[١٨٩] وهي شبكة معلومات آنية، استغلال الخدمة لنشر تهديدات مباشرة ومحددة بارتكاب العنف ضد آخرين أو لأي غرض غير قانوني أو دعماً لأنشطة غير قانونية.[١٩٠] وفي حالة الإخلال بهذه الشروط، يحتفظ مقدِّم الخدمة لنفسه بالحق في إزالة المحتوى الذي فيه إساءة أو رفض نشره أو في قطع الخدمة (دون أن يكون مُلزماً بأي من ذلك). وعلاوة على ذلك، فإنَّ مستخدمي تويتر لا يضمّون في صفوفهم الأشخاص الممنوعين من تلقي الخدمات بموجب قوانين الولايات المتحدة أو غيرها من الولايات القضائية المعنية، ومن ثم فالجماعات المسمَّاة تنظيمات إرهابية مستبعدةٌ من الاستفادة من خدماته. ومع ذلك، من الممكن، حتى حين وجود هذه الأحكام، أن تنشأ صعوبات فيما يخص تنفيذها، وهو ما يعود جزئياً إلى اتساع قاعدة المستخدمين وما ينتج عن ذلك من حجم هائل لما يتعين رصده من محتويات يعدها المستخدمون أنفسهم.

٤١٧- وتشير تقارير إخبارية حديثة إلى أن غوغل تقوم، في حالة وقوع انتهاك لحقوق التأليف والنشر، بإزالة المحتوى أو الروابط المعنية في غضون ست ساعات من تلقيها لطلب بذلك، بالرغم من تلقّيها سيلاً من الطلبات من هذا النوع بلغت ما يربو على خمسة ملايين طلب في عام ٢٠١١.[١٩١] ومن شأن الجمع بين آلية الإبلاغ عن المحتويات المسيئة واتباع نهج التصدي بجدية وفي الوقت المناسب للمحتويات المشتبه في صلتها بالإرهاب أن يكون خطوة إيجابية للغاية في طريق مكافحة استخدام الإنترنت للدفع باتجاه التطرف، والتجنيد للأعمال الإرهابية، والتدريب عليها، وتمجيدها، والتحريض عليها.

٤١٨- وكثيراً ما يُميَّز المحتوى الذي تنشره التنظيمات الإرهابية بعلامات معروفة تخص كل تنظيم.[١٩٢] ويمكن أن يؤدي رصد هذه المحتويات التي يسهل التعرف عليها وإزالتها من قبل المواقع الشبكية المستضيفة لها إلى

---

[١٨٩] انظر الرابط التالي: https://twitter.com/tos.

[١٩٠] انظر الرابط التالي: http://support.twitter.com/articles/18311-the-twitter-rules#.

[١٩١] Jenna Wortham, "A political coming of age for the tech industry", The New York Times, 17 January 2012. انظر الرابط التالي: www.nytimes.com/2012/01/18/technology/web-wide-protest-over-two-antipiracy-bills.html?hp.

[١٩٢] "Jihadist use of social media: how to prevent terrorism and preserve innovation", testimony of A. Aaron Weisburd, Director, Society for Internet Research, before the United States House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence, 6 December 2011.

مكاسب كبيرة في مجال مكافحة نشر الدعاية الإرهابية غير القانونية. وعلاوة على ذلك، فإنَّ استخدام آليات إبلاغ مماثلة للآليات التي استحدثت على موقع يوتيوب كخاصية ثابتة في جميع وسائط التواصل الاجتماعي الأخرى ومحركات البحث على الإنترنت قد يزيد من احتمال إزالة المواد الدعائية المستهدفة لدعم الأغراض الإرهابية في الوقت المناسب. ومن شأن زيادة التدابير الهادفة للوقوف على المحتويات ذات الصلة بالإرهاب، إذا ما تم الجمع بينها وبين شراكات أفضل، رسمية وغير رسمية، لتبادل المعلومات بين الدولة وجهات القطاع الخاص المعنية، أن تساعد كثيراً في الوقوف على الأنشطة الإرهابية التي تُستخدم فيها الإنترنت ومكافحتها.

٤١٩- وتبادل المعلومات أهمٌّ في سياق التمييز بين محتويات الإنترنت التي قد تعتبر تجريحية والمحتويات التي قد تكون غير قانونية (انظر المناقشة الواردة في القسم أولا-باء-١). فعلى سبيل المثال، إذا كان نظام الإبلاغ المعمول به في يوتيوب قد يساعد على إيلاء الأولوية لمحتويات بعينها بغرض المراجعة، فلا بد بعد ذلك من تقرير ما إذا كانت هذه المحتويات تبلغ المبلغ الذي يلزم عنده إزالتها أو حجبها. وقد يسهِّل الحوار غير الرسمي، بين مقدمي خدمات الإنترنت ومواقع الاستضافة من جهة ومسؤولي العدالة الجنائية من جهة أخرى، من هذه العملية. وتحقيقاً لهذه الغاية، يمكن تشجيع جهات القطاع الخاص المعنية على التعاون مع سلطات إنفاذ القانون من خلال الإبلاغ عن المحتوى التجريحي المشتبه في كونه ذا صلة بأي مستخدم منتسب لتنظيم إرهابي معروف أو يروِّج لأنشطة هذا التنظيم.

٣- *محركات البحث على الإنترنت*

٤٢٠- محركات البحث على الإنترنت هي بمثابة جسر ما بين محتويات الإنترنت والمستخدم النهائي. وللمحتويات المستبعدة من هذه المحركات جمهور أقل كثيراً. وتتطوع بعض هذه المحركات، مثل غوغل وياهو، بفرض رقابة على المحتويات التي تُعتبر حساسة أو ضارة بمصالحها. فعلى سبيل المثال، قام العديد من محركات البحث على الإنترنت في أعقاب هجمات ١١ أيلول/سبتمبر ٢٠٠١ في الولايات المتحدة بإزالة نتائج البحث المتعلقة بالتنظيمات الإرهابية المحتملة.[١٩٣] وقد شجَّع مقررو السياسات العامة ومسؤولو إنفاذ القانون في العديد من الدول الأعضاء على اتخاذ مبادرات طوعية مماثلة لتصعيب الوصول عبر محركات البحث على الإنترنت إلى محتويات تروِّج لأعمال عنف. كذلك قد يكون من المفيد أن تطبِّق محركات البحث نظاماً للإبلاغ عن المحتويات ذات الصلة بالإرهاب شبيهاً بالنظام المستخدم على يوتيوب.

٤- *خدمات الرصد*

٤٢١- في هذا السياق أيضا، تتبع بعض الجهات الخاصة نهجاً أكثر تنظيماً إزاء مكافحة الأنشطة الإرهابية على الإنترنت. فخدمات الرصد مثل خدمتي "SITE" (البحث عن كيانات إرهابية دولية) و"شبكة الهاغانا على الإنترنت" اللتين تتخذان من الولايات المتحدة مقراً لهما تقوم برصد المعلومات ذات المصدر العلني المتعلقة بالتنظيمات الإرهابية وتجمعها.[١٩٤] وتحصل خدمة "البحث عن كيانات إرهابية دولية"، التي تعمل على جمع المعلومات الاستخبارية، على عوائد ذات شأن من الاشتراكات المدفوعة. لذا فقد تكون هي ومثيلاتها من المنظمات أقدر على الحصول على الموارد التي تُمكِّن من الوقوف بسرعة على الأنشطة التي تروِّج لأعمال إرهابية على الإنترنت وترجمتها، حسب الاقتضاء. أمَّا "شبكة الهاغانا على الإنترنت" فترصد الأنشطة التي تقوم بها

[١٩٣] Conway, "Terrorism and Internet governance: core issues", p. 30.

[١٩٤] المرجع نفسه، الصفحة ٣١.

الجماعات الإسلامية المتطرفة على الإنترنت بهدف الوقوف على المحتويات ذات الصلة بالإرهاب وحجبها. وتُموَّل "شبكة الهاغانا على الإنترنت" جزئياً من التبرعات وتعمل بالأساس استناداً إلى إسهامات شبكة من المتطوعين. وتبادر خدمة الرصد هذه إلى البحث والكشف عن محتويات الإنترنت التي تُعتبر ذات صلة بالإرهاب والمواقع التي تستضيفها. وقد يجري مشاطرة هذه المعلومات مع سلطات إنفاذ القانون أو عامة الجمهور أو استخدامها للاتصال بالموقع الشبكي المستضيف لحثّه على إزالة المحتوى المعني أو عرقلة الوصول إليه.[١٩٥] ولئن اختلفت أغراض هاتين الخدمتين وطرائق عملهما، فإنَّ ما تقوم به كل منهما من أعمال يشجِّع على الوقوف بسرعة على المحتويات ذات الصلة بالإرهاب على الإنترنت، وهو ما قد يكون مفيداً في جمع المعلومات الاستخبارية عن هذه الأنشطة والتحقيق فيها والملاحقة القضائية بشأنها.

باء- الشراكة بين القطاعين العام والخاص

٤٢٢- ثمة العديد من الفوائد المرجوَّة من إقامة شراكات بين الجهات المعنية ذات المصلحة في القطاعين العام والخاص في مجال مكافحة استخدام الإنترنت في أغراض إرهابية. ومن التحديات التي يكثر الحديث عنها فيما يتعلق بالتعاون بين القطاعين العام والخاص بشأن الجرائم السيبرانية عموماً عدم التواصل بين أجهزة إنفاذ القانون ومقدِّمي الخدمات فيما يتعلق بجمع الأدلة على نحو فعَّال، والصعوبات التي تطرحها ضرورة تحقيق التوازن بين احترام الخصوصية من جهة والحاجة للاحتفاظ بالبيانات لأغراض قانونية من جهة أخرى. ومن شأن إنشاء منتدى للحوار الرسمي وغير الرسمي بين النظراء في القطاعين العام والخاص أن يخفف من حدة هذه المخاوف كثيراً. فبالإضافة إلى الفرص التي تتيحها الاجتماعات الدورية بين الشركاء المعنيين، يمكن أن تساعد أنشطة من قبيل برامج التدريب المشتركة على كسر حواجز التواصل وتعزيز الثقة بين المشاركين من الجانبين.[١٩٦]

٤٢٣- وقد تحقق تقدم كبير في إقامة الشراكات ما بين القطاعين العام والخاص في المسائل الأمنية التي تتعلق باحتمالات شن هجمات إرهابية على أهداف غير محصّنة أو على البنية التحتية، أو فيما يتعلق بالجرائم السيبرانية عموماً من حيث منعها والملاحقة القضائية بشأنها. وسوف يكون من المفيد أن تُقام شراكات مماثلة في مجال التنظيم الرقابي لاستخدام الإنترنت في أغراض إرهابية. ومن بين الأمثلة على الشراكات الناجحة بين القطاعين العام والخاص في المجال الأمني المجلسُ الاستشاري للأمن الخارجي، الذي أنشئ بالاشتراك ما بين وزارة الخارجية في الولايات المتحدة ومنظمات أمريكية خاصة تعمل خارج البلاد. ويتيح المجلس منتدى لتبادل الممارسات المثلى وتبادل المعلومات تبادلا دوريا في الوقت المناسب بين القطاع الخاص وحكومة الولايات المتحدة الأمريكية فيما يخص التطورات في الوضع الأمني خارج البلد، بما في ذلك التطورات المتعلقة بالإرهاب، فضلاً عن العوامل السياسية والاقتصادية والاجتماعية التي قد يكون لها تأثير على الوضع الأمني عالمياً وفي كل بلد على حدة.[١٩٧]

---

[١٩٥] Ariana Eunjung Cha, "Watchdogs seek out the web's bad side", *Washington Post*, 25 April 2005. انظر الرابط التالي: www.washingtonpost.com/wp-dyn/content/article/2005/04/24/AR2005042401473.html.

[١٩٦] United Nations Interregional Crime and Justice Research Institute, "Public-private partnerships for the protection of vulnerable targets against terrorist attacks: review of activities and findings" (January 2009), para. 23.

[١٩٧] المرجع نفسه، الفقرة ٩.

٤٢٤- وهنـاك مثـال آخر على مبادرات الشراكة بين القطاعين العام والخاص التي تتمحور حول المسائل الأمنية هـو فريق التصدي للحـوادث الأمنية على البنية التحتية للإنترنت في إندونيسيـا. فالفريق يجمع بين ممثلين عن خدمـات البريد والاتصالات، والشرطة الوطنيـة، ومكتب النائب العام، وبنك إندونيسيا، ورابطة مقدِّمي خدمات الإنترنـت الإندونيسيـين، ورابطـة مقاهي الإنترنـت في إندونيسيـا، ورابطة مقدِّمـي خدمات بطاقـات الائتمان الإندونيسيـين، والجمعيـة الإندونيسيـة لتكنولوجيـا الاتصـالات والمعلومـات (MASTEL). ويتعـاون الأعضاء علـى رصد التهديـدات والانقطاعات في شبكات الاتصـالات العاملة ببروتوكول الإنترنـت والكشف عنها والإنذار المبكـر بشأنها؛ والقيام بالبحوث والتطوير؛ وتوفير مختـبرات للمحاكاة والتدريب على الاستخدام الآمن لشبكات الاتصـالات العاملة ببروتوكـول الإنترنت؛ وتقديم الخدمـات الاستشارية والدعم التقني للأجهـزة أو المؤسسات ذات الطابـع الاستراتيجـي؛ والعمل بمثابة مركز للتنسيـق بين الأجهزة والمؤسسات المعنية، سـواء المحلي منها أو الدولي،[١٩٨] ضمن أمور أخرى.

٤٢٥- وفي تشريـن الثاني/نوفمـبر ٢٠٠٦، انعقد المنتـدى العالمي للشراكات بين الدول وقطـاع الأعمال من أجل مكافحـة الإرهـاب في موسكـو. وأسفر المنتدى عـن اعتماد مجموعة البلـدان الثمانيـة[١٩٩] استراتيجية من أجل الشـراكات بـين الدول والأوساط التجارية لمكافحة الإرهاب،[٢٠٠] تشجِّع علـى أمور في جملتها التعاون بين مقدِّمي خدمات الإنترنت وغيرهم من المشتغلين بالأعمال التجارية من جهة والسلطات الحكومية من جهة أخرى لمكافحة إسـاءة استخـدام الإنترنت من قِبَل الإرهابيين وعرقلـة الخطوات النهائية التي تقود مـن التطرف إلى الإرهاب. وتحث هذه الاستراتيجية الحكومات على إقامة وتوثيق شراكات وطنية ودولية طوعية مع مقدِّمي خدمات الإنترنت بغيـة التصـدِّي لاستخـدام الإنترنت لأنشطـة من قبيل التجنيـد والتدريب لارتـكاب أعمال إرهابيـة والتحريض على ذلك.

٤٢٦- وتشمل مبادرات الشراكة الأخرى بين القطاعين العام والخاص الفريق العامل الذي أسسه مجلس أوروبا في عـام ٢٠٠٧، والذي يضم مشاركين من أجهزة إنفاذ القانون، والقطاعات المعنية، ورابطات مقدمي الخدمات، ليتنـاول المسائـل المتعلقة بالجرائم السيبرانية بصفة عامة. وتهدف هذه المبـادرة إلى تعزيز التعاون بين سلطات إنفاذ القانون والقطاع الخاص بغية تحقيق مزيد من الكفاءة في التصدي للجرائم السيبرانية.

٤٢٧- وفي عام ٢٠١٠، وافقت المفوضية الأوروبية على مشروع تعاون بين المؤسسات الأكاديمية والقطاعات المعنية وأجهـزة إنفـاذ القانون، ووفَّرت له التمويل، بغرض إنشاء شبكة من المراكـز المتميِّزة للتدريب والبحوث والتثقيف في مجـال مكافحة الجرائم السيبرانية (2CENTRE) في أوروبا. وتوفِّـر هذه الشبكة في الوقت الراهن التدريب عبر مركزين وطنيين متميزين في إيرلندا وفرنسا. ويقوم كل مركز وطني على الشراكة بين ممثلين لأجهزة إنفاذ القانـون، والقطاعات المعنيـة، والمؤسسات الأكاديمية، يتعاونـون على وضع البرامج التدريبيـة والأدوات اللازمة لاستخدامها في مكافحة الجرائم السيبرانية (انظر القسم رابعاً-زاي).

٤٢٨- وقد تكون الشراكات بين القطاعين العام والخاص التي تستهدف خصيصا استخدام الإنترنت في أغراض إرهابيـة وسيلةً للترويج لمبادئ توجيهيـة واضحة فيما يخص تبادل المعلومات بـين القطاعين العام والخاص، بما

[١٩٨] مذكرة مكتوبة قدَّمها الخبير الإندونيسي.

[١٩٩] منتـدى غـير رسمي لقـادة الـدول الصناعية الآتية: الاتحـاد الروسـي، ألمانيا، إيطاليـا، فرنسا، كنـدا، المملكة المتحـدة، الولايات المتحدة، اليابان.

[٢٠٠] A/61/606-S/2006/936، المرفق.

يتفـق وما هو مطبَّـق من القواعد المنظمة لحماية البيانات. وتتيح المبادئ التوجيهية، الصادرة عن مجلس أوروبا، الخاصة بالتعاون بين أجهزة إنفاذ القانون ومقدِّمي خدمات الإنترنت من أجل مكافحة جرائم الفضاء الحاسوبي أساسـاً جيـداً للمبادئ التوجيهية لتبادل المعلومـات.[٢٠١] وتركِّز هذه المبادئ التوجيهيـة على إقامة علاقات تقوم علـى الثقة المتبادلـة والتعاون بين الجهات المعنية في القطاعين العام والخاص أساسـاً للتعاون. كما تشدِّد المبادئ التوجيهية على ضرورة تشجيع الكفاءة وفعالية التكلفة في إجراءات التعاون، وتحث مسؤولي إنفاذ القانون ومقدمي خدمـات الإنترنت علـى تبادل المعلومات لتعزيز قدراتهـم على الوقوف على الجرائـم السيبرانية ومكافحتها من خـلال اجتماعات دورية ومشاطرة الممارسات الجيدة والتقييم. كما تشجِّع المبادئ التوجيهية على إقامة شراكات رسمية وإجراءات مكتوبة أساساً لعلاقات طويلة الأمد، لضمان أمور في جملتها وضع ضمانات كافية حتى لا تنتهك الشراكة الحقوق القانونية للمشاركين من القطاعات المعنية أو الصلاحيات القانونية لسلطات إنفاذ القانون.[٢٠٢]

٤٢٩- ومن بين التدابير التي توصَى سلطات إنفاذ القانون باتباعها وفقاً للمبادئ التوجيهية ما يلي:

- التعاون الاستراتيجي الموسَّع مع مقدِّمي خدمات الإنترنت، بوسائل منها عقد حلقات دراسية للتدريب التقني والقانوني، إلى جانب التزويد بمعلومات عن التحقيقات التي أجريت أو المعلومات الاستخبارية التي جُمعت، استناداً إلى تقارير مقدِّمي خدمات الإنترنت أو شكاواهم
- تزويد مقدِّمي خدمات الإنترنت بشروح ومساعدات فيما يخص تقنيات التحقيق غير المرتبطة مباشرة بالقضية قيد التحقيق، حتى يتأتى لهم فهم كيف يؤدي تعاونهم إلى مزيد من الكفاءة في التحقيقات
- إيـلاء الأولوية للطلبات على كميـات كبيرة من البيانات مع تلافي التكاليـف التي لا داعي لها وتعطيل الأعمال.[٢٠٣]

٤٣٠- ومن بين التدابير التي يوصَى مقدمو خدمات الإنترنت باتباعها وفقا للمبادئ التوجيهية ما يلي:

- التعاون لتقليل استخدام الخدمات في أغراض غير قانونية إلى أدنى حد
- إبلاغ سلطات إنفاذ القانون بالأنشطة الإجرامية
- وضـع قائمـة إذا أمكن عند الطلب، بأنواع البيانات المتعلقة بكل نوع من أنواع الخدمات على حدة التي يمكن إتاحتها لسلطات إنفاذ القانون، عند تلقي طلب سليم بالكشف عن المعلومات.[٢٠٤]

٤٣١- كما أنَّ الشراكات بين القطاعين العام والخاص قد تتيح منتدىً للترويج لمعايير دنيا فيما يخص الاحتفاظ الآمـن بالبيانـات من قِبَل جهات القطاع الخاص المعنية وتحسين قنوات الاتصال بما يمكِّن جهات القطاع الخاص المعنية من تقديم ما لديها من معلومات متعلقة بالأنشطة المشبوهة.

---

(٢٠١) Council of Europe, Economic Crime Division, "Guidelines for the cooperation between law enforcement and Internet service providers against cybercrime" (Strasbourg, 2 April 2008). متاح على الرابط التالي:
www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/567_prov-d-guidelines_provisional2%20_3%20April%202008_final_arabic.pdf.

(٢٠٢) المرجع نفسه، الفقرات ١٠-١٣.

(٢٠٣) المرجع نفسه، الفقرات ١٧، ٢٩، ٣٠، ٣٣.

(٢٠٤) المرجع نفسه، الفقرات ٤١، ٤٢، ٥٠.

ثامناً- الخلاصة

ألف- استخدام الإنترنت في أغراض إرهابية

٤٣٢- قدَّمت الفصول الأولى من هذا المنشور لمحةً عامةً، من منظور عملي، للطرائق التي كثيراً ما تُستخدم بها شبكة الإنترنت للترويج للأعمال الإرهابية ودعمها، ولا سيما فيما يتعلق بالدعاية (لأغراض منها التجنيد، والدفع باتجاه التطرف، والتحريض على الإرهاب)، والتدريب والتمويل، والتخطيط لهذه الأعمال وتنفيذها. كما ينصب التركيز على الفرص التي تُتيحها الإنترنت لمنع الأعمال الإرهابية والكشف عنها وردعها، بما قد يشمل جمع المعلومات الاستخبارية وغير ذلك من الأنشطة التي تهدف إلى منع الأعمال الإرهابية ومكافحتها، إلى جانب جمع الأدلة بغرض ملاحقة مرتكبي هذه الأعمال قضائياً.

٤٣٣- ومن الممكن أن تكون الأفكار المضادة وغيرها من أشكال التواصل الاستراتيجية وسيلةً فعَّالةً لعرقلة عملية الدفع باتجاه التطرف واعتناق مبادئ متطرفة، وهو ما قد يتجلى في أعمال إرهابية. كذلك من الأهمية بمكان الوصول إلى فهم واضح للمسائل الأعم التي تكمن وراء التحول إلى التطرف حتى يتأتى الانخراط في حوار بنَّاء مع الأشخاص الذين يحتمل تجنيدهم دفاعاً عن القضايا الإرهابية، والتشجيع على إيجاد وسائل قانونية بديلة للسعي وراء تحقيق التطلعات السياسية والاجتماعية والدينية المشروعة.

٤٣٤- كما أنَّ احترام حقوق الإنسان وسيادة القانون جزء لا يتجزأ من مكافحة الإرهاب. ويشار بالأخص إلى أنَّ الدول الأعضاء قد أكَّدت هذه الالتزامات في استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب، وأقرَّت فيها بأنَّ "اتخاذ تدابير فعَّالة لمكافحة الإرهاب وحماية حقوق الإنسان هدفان لا يتعارضان، بل متكاملان ويعزز كل منهما الآخر". ولا بد من تقييم مدى الفعالية في تنفيذ النهج القائم على سيادة القانون في مكافحة استخدام الإنترنت في أغراض إرهابية تقييماً مستمراً في جميع مراحل مبادرات مكافحة الإرهاب، بدءاً بجمع المعلومات الاستخبارية من باب التحوط وانتهاءً بضمان مراعاة الأصول القانونية في الملاحقة القضائية للمشتبه بهم.

باء- السياق الدولي

٤٣٥- لا توجد في الوقت الراهن معاهدة شاملة للأمم المتحدة بشأن الإرهاب، كما لا يوجد تعريف رسمي لمصطلح "الإرهاب". إلا أنَّ الدول الأعضاء في الأمم المتحدة تعكف على صوغ اتفاقية شاملة بشأن الإرهاب الدولي من شأنها أن تستكمل الإطار القانوني الدولي القائم فيما يخص مكافحة الإرهاب. ويُستقى هذا الإطار من مجموعة من المصادر، بما في ذلك قرارات الجمعية العامة ومجلس الأمن، والمعاهدات، والسوابق القضائية، والقانون الدولي العرفي. كما أنَّ العديد من الصكوك الإقليمية ودون الإقليمية تتيح معايير موضوعية وإجرائية قيِّمة لتجريم الأعمال الإرهابية التي قد تُرتكب عن طريق الإنترنت.

٤٣٦- وقد قرَّرت الدول الأعضاء، عملا بالاستراتيجية العالمية لمكافحة الإرهاب، أن تتخذ إجراءات عاجلة لمنع ومكافحة الإرهاب بجميع أشكاله ومظاهره، وبوجه خاص:

(أ) النظر في الانضمام، دون تأخير، إلى الاتفاقيات والبروتوكولات الدولية القائمة حالياً بشأن مكافحة الإرهاب، وتنفيذها، وبذل قصارى جهودها من أجل التوصل إلى اتفاق بشأن اتفاقية شاملة بشأن الإرهاب الدولي وإبرامها؛

(ب) تنفيذ جميع قرارات الجمعية العامة المتعلقة بالتدابير الرامية إلى القضاء على الإرهاب الدولي، وقرارات الجمعية العامة ذات الصلة بحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب؛

(ج) تنفيذ جميع قرارات مجلس الأمن المتعلقة بالإرهاب الدولي والتعاون التام مع هيئات مجلس الأمن الفرعية المعنية بمكافحة الإرهاب في اضطلاعها بالمهام المسندة إليها.

جيم- أطر السياسات العامة والتشريعات

١- *السياسات العامة*

٤٣٧- يتعين على الحكومات، ليتسنى التصدِّي على مستوى العدالة الجنائية لمخاطر استخدام الإنترنت في أغراض إرهابية، أن تضع سياسات وقوانين وطنية واضحة تتناول أموراً في جملتها: *(أ)* تجريم الأفعال غير القانونية التي يقوم بها الإرهابيون على الإنترنت أو الخدمات ذات الصلة؛ *(ب)* تخويل صلاحيات التحقيق لأجهزة إنفاذ القانون المشاركة في التحقيقات ذات الصلة بالإرهاب؛ *(ج)* التنظيم الرقابي للخدمات المتصلة بالإنترنت (مثل مقدِّمي خدمات الإنترنت)، ومراقبة المحتويات؛ *(د)* تيسير التعاون الدولي؛ *(هـ)* استحداث إجراءات قضائية وإجراءات إثبات متخصصة؛ *(و)* الحفاظ على المعايير الدولية لحقوق الإنسان.

٤٣٨- ويتيح التصنيف العام للنُّهُج الاستراتيجية، الذي أعده الفريق العامل المعني بمكافحة استخدام الإنترنت في أغراض إرهابية التابع لفرقة العمل المعنية بتنفيذ تدابير مكافحة الإرهاب، والذي يشمل استخدام تشريعات عامة لمكافحة الجرائم السيبرانية، وتشريعات عامة (أي غير مخصصة للإنترنت) لمكافحة الإرهاب، وتشريعات مكافحة الإرهاب المخصصة للإنترنت، إطاراً مفاهيمياً مفيداً لمقرري السياسات العامة والمشرعين. وليس هناك في الوقت الراهن سوى عدد قليل من الدول التي وضعت تشريعات تستهدف على وجه التحديد الأعمال التي يقوم بها الإرهابيون على الإنترنت، فيما تستخدم معظم البلدان القوانين الجنائية العامة أو التشريعات المتعلقة بمكافحة الجرائم السيبرانية أو بمكافحة الإرهاب أو مزيج مما سبق لتجريم هذه الأعمال وملاحقة مرتكبيها قضائياً.

٢- *التشريعات*

٤٣٩- بالإضافة إلى استخدام الإرهابيين للإنترنت في إطار الأعمال التي يقومون بها لتنفيذ الجرائم الموضوعية (مثل التفجيرات)، يمكن لهم أن يستخدموا الإنترنت لتنفيذ أنشطة دعم أخرى (مثل نشر الدعاية أو تجنيد الأعضاء وتدريبهم). وتتبع البلدان مختلف النُّهُج في تجريم التصرفات غير القانونية المرتبطة بالإرهاب والتي تنفَّذ باستخدام الإنترنت.

٤٤٠- ودعا مجلس الأمن الدول في قراره ١٦٢٤ (٢٠٠٥) إلى تجريم التحريض على الأعمال الإرهابية، ضمن أمور أخرى. والدول مُلزَمة، بموجب القرار وغيره من الصكوك الدولية، بضمان اتفاق التدابير المستهدِفة للأعمال التي تحرض على الإرهاب تمام الاتفاق والتزاماتها الدولية بموجب قانون حقوق الإنسان، وقانون اللاجئين، والقانون الإنساني.

٤٤١- وما زال وضع القوانين التي تجرِّم التحريض على الأعمال الإرهابية وتنفيذُ تلك القوانين مع توفير الحماية الكاملة لحقوق الإنسان (مثل الحق في حرية التعبير) من التحديات المطروحة على مقرِّري السياسات العامة، والمشرعين، وأجهزة إنفاذ القانون، وأعضاء النيابة العامة في جميع البلدان. وتعتمد البلدان نُهُجاً مختلفة لتجريم أعمال التحريض على الإرهاب. فقد جرَّمت بعض الدول أعمال التحريض على الأعمال الإرهابية أو تمجيد هذه الأعمال على وجه التحديد، فيما يعتمد البعض الآخر على الجرائم غير الكاملة مثل التحريض أو التآمر.

٤٤٢- وكثيراً ما يستلزم التحقيق في قضايا الإرهاب التي تنطوي على استخدام الإنترنت أو خدمات أخرى ذات صلة من قِبَل الإرهابيين المشتبه بهم استخدامَ أجهزة إنفاذ القانون لأنواع متخصصة من صلاحيات التحقيق. وقد اعتمدت معظم الحكومات تشريعات تسمح لأجهزة إنفاذ القانون بالقيام بهذه الأنشطة في التحقيقات المتعلقة بالإرهاب. وينبغي أن يصدر إذن صحيح باستخدام تقنيات التحقيق هذه بموجب القوانين الوطنية، وأنْ تنفَّذ بطريقة تحترم حقوق الإنسان الأساسية التي يحميها القانون الدولي لحقوق الإنسان.

٤٤٣- وتحتاج السلطات إلى تعاون مشغِّلي خدمات الاتصالات عند القيام بالمراقبة الإلكترونية، والتنصت على المكالمات الهاتفية، ونحو ذلك من تقنيات التحقيق الإلكترونية. ومن المستصوب أن توضح الحكومات الأساس القانوني للالتزامات الواقعة على كاهل جهات القطاع الخاص، بما في ذلك المواصفات التقنية المطلوب توافرها في شبكاتها وكيفية تغطية التكلفة اللازمة للوفاء بهذه المواصفات.

٤٤٤- وثمة أدلة على أنَّ الإرهابيين قد استخدموا مقاهي الإنترنت للقيام بأنشطتهم، إلا أنَّ مدى هذه المشكلة غير معروف. وقد فرضت بعض الحكومات واجبات محددة على مشغِّلي مقاهي الإنترنت بغرض إنفاذ القانون (بما في ذلك مكافحة الإرهاب) تشمل الحصول على وثيقة هوية تحمل صورة فوتوغرافية لزبائنهم، إضافة إلى عناوين إقامتهم، وبيانات الاستخدام والاتصال الخاصة بهم، والاحتفاظ بكل ما سبق وتقديمه إلى جهات إنفاذ القانون عند الطلب. وثمة بعض الشك بشأن جدوى استهداف مقاهي الإنترنت وحدها بهذه التدابير في حين أنَّ أشكالاً أخرى من الوصول إلى الإنترنت في الأماكن العامة (في المطارات، والمكتبات العامة، ونقاط الاتصال اللاسلكي بالإنترنت (واي فاي) على سبيل المثال) تتيح للمجرمين (بمن فيهم الإرهابيون) نفس الفرص للدخول إلى الإنترنت ولا تخضع للتنظيم الرقابي.

٤٤٥- وتُعدُّ مسألة المدى الذي ينبغي على الحكومات أن تذهب إليه في التنظيم الرقابي لمحتويات الإنترنت المتعلقة بالإرهاب مسألة محفوفة بالمصاعب، تتطلب تحقيق التوازن بين إنفاذ القانون واعتبارات حقوق الإنسان (مثل الحق في حرية التعبير). وتتعدَّد نُهُج التنظيم الرقابي للمحتويات ذات الصلة بالإرهاب، حيث تفرض بعض الدول ضوابط تنظيمية صارمة على مقدِّمي خدمات الإنترنت وغيرها من الخدمات ذات الصلة، بما في ذلك في بعض الحالات استخدام التكنولوجيا لفرز بعض المحتويات أو عرقلة الوصول إليها، فيما تعتمد دول أخرى نهجاً تنظيمياً أخف وطأة، معتمدة بصورة أكبر على التنظيم الرقابي الذاتي الذي يفرضه قطاع المعلومات على المنتمين إليه. فلدى معظم مقدِّمي خدمات الإنترنت، وشركات الاستضافة الشبكية، ومواقع تبادل الملفات، ومواقع التواصل الاجتماعي، اتفاقات لشروط الخدمة تحظر محتويات معينة، وقد يكون بعض المحتويات ذات الصلة بالإرهاب مخالفاً لهذه القيود التعاقدية.

دال- التحقيقات وجمع المعلومات الاستخبارية

٤٤٦- تستند التحقيقات الفعَّالة في أنشطة الإنترنت إلى مزيج من أساليب التحقيق التقليدية، والمعرفة بالأدوات المتاحة للقيام بأنشطة غير مشروعة عبر الإنترنت، واستحداث ممارسات تستهدف الوقوف على هوية مرتكبي هذه الأعمال وإلقاء القبض عليهم وملاحقتهم قضائياً. ويمكِّن اتباعُ نهج استباقي إزاء استراتيجيات التحقيق، بدعم من الأدوات المتخصصة التي يستفاد فيها من موارد الإنترنت المتطوِّرة دوماً، من الفعالية في تحديد البيانات والخدمات التي يُرجَّح أن تعود على التحقيق بفائدة عظيمة.

٤٤٧- وثمة مجموعة كبيرة من الأدوات والأجهزة المتخصصة المتاحة أمام المحققين الذين لديهم المؤهلات التقنية المناسبة. وينبغي إيلاء العناية الواجبة، متى أمكن ذلك، في القضايا التي تتطلب الحصول على أدلة رقمية إلى إعمال إجراءات موحَّدة لاسترداد البيانات لتعزيز إمكانية استرجاع أكبر قدر ممكن من الأدلة المتاحة وحفظ سلامة مصدر البيانات وتسلسل العهدة لضمان مقبولية الأدلة في المحكمة. ونظراً لهشاشة الأدلة الرقمية، فإنَّ عمليات تقييمها والحصول عليها وفحصها تكون أكثر فعالية إذا تولاّها خبراء تحليل جنائي مدرَّبون خصيصاً لهذا الغرض.

هاء- التعاون الدولي

٤٤٨- إنَّ التعاون الدولي الفعَّال عامل هام في العديد من الملاحقات القضائية بشأن قضايا الإرهاب، بما في ذلك القضايا التي تنطوي على جانب من جوانب استخدام الإنترنت من قِبَل الجناة. والدول مُلزَمة، بموجب العديد من مختلف الصكوك الدولية والإقليمية والثنائية والمتعددة الأطراف المتعلقة بالإرهاب والجريمة المنظمة العابرة للحدود الوطنية، بوضع سياسات عامة وأطر تشريعية لتيسير التعاون الدولي الفعَّال في التحقيق في الأعمال الإرهابية أو ما يتصل بها من الجرائم المنظمة الخطيرة وملاحقة مرتكبيها قضائياً. ولا يوجد في الوقت الراهن صك عالمي بشأن الجرائم السيبرانية أو الإرهاب يفرض التزامات محددة على الدول فيما يخص التعاون الدولي. ويُعدُّ هذا الأمر عقبة في سبيل التعاون الدولي الفعَّال في بعض التحقيقات والملاحقات القضائية المتعلقة بالإرهاب.

٤٤٩- وفيما تظل القنوات الرسمية للتعاون الدولي ذات أهمية حيوية، فالقنوات غير الرسمية قد صارت على نفس القدر من الأهمية في الممارسة العملية. وبصرف النظر عن طريقة التعاون، فالثقة بين السلطات الوطنية في مختلف البلدان ركن رئيسي في تحقيق التعاون الدولي الفعَّال في كثير من الحالات. وبالإضافة إلى التعاون بموجب المعاهدات الرسمية أو ما شابهها من الصكوك القانونية، فالمبادرات الإقليمية أو دون الإقليمية التي لا تستند إلى معاهدات وتستهدف تعزيز التعاون في مجال إنفاذ القانون مهمة أيضاً. وقد تضع البلدان التي لها مصالح أمنية مشتركة في مجالات معينة ترتيبات جماعية تتيح أساساً لتبادل المعلومات ومشاطرة المعلومات الاستخبارية.

٤٥٠- ويعد وجود إطار تشريعي وطني يتيح أساساً للتعاون الدولي الفعَّال ركناً رئيسياً من أركان إطار عمل فعَّال لتيسير التعاون الدولي في التحقيقات والملاحقات القضائية في قضايا الإرهاب. وينبغي أن تُدرِج هذه التشريعات في القانون الوطني لبلد من البلدان المبادئَ التي اعتمدتها الصكوك العالمية لمكافحة الإرهاب فيما يخص التعاون وما يتصل بذلك في شأن الجريمة المنظمة العابرة للحدود الوطنية.

٤٥١- ولئن كانت التشريعات مكوِّناً رئيسياً من مكوِّنات أي نظام فعَّال للتعاون الدولي، فإنها ليست، في حد ذاتها، هي الحل. فمن الأهمية بمكان كذلك وجودُ سلطة مركزية لديها موارد كافية وقادرة على أخذ زمام المبادرة بحيث تستطيع تيسير المساعدة القانونية المتبادلة، باستخدام كل القنوات المتاحة. ومن المهم كذلك إقامة علاقات تقوم على الثقة بالنظراء الأجانب المتعاونين في التحقيقات الجنائية العابرة للحدود والحفاظ على هذه العلاقات.

٤٥٢- وبالإضافة إلى قنوات التعاون الرسمية، يتعيَّن على السلطات أن تستخدم وتطوِّر قنوات التعاون الثنائي غير الرسمية القائمة. ويدير كثير من أجهزة إنفاذ القانون الوطنية شبكة من نقاط الاتصال الدولية، الأمر الذي يساعد كثيراً في تيسير طلبات التعاون الدولي. وليس ثمة إشارة صريحة إلى استخدام فرق التحقيق المشتركة في الصكوك العالمية لمكافحة الإرهاب، بيد أنَّ استراتيجية التعاون هذه تتفق تمام الاتفاق والمبادئ والروح الكامنتين وراء الجوانب المتعلقة بالتعاون الدولي في هذه الصكوك. وقد اعتمد بعض البلدان، وبالأخص في أوروبا، هذا النهج بنجاح في عدد من التحقيقات المتعلقة بالإرهاب.

٤٥٣- وبالرغم من التحسن في إجراءات المساعدة القانونية المتبادلة الرسمية في القضايا الجنائية، فقد تستغرق هذه الإجراءات حتى الآن وقتاً طويلاً وتتطلب قدراً كبيراً من البيروقراطية. وفي القضايا التي تتطلب حفظ البيانات المتعلقة بالإنترنت الموجودة لدى مقدِّمي خدمات الإنترنت في ولاية قضائية أخرى، قد يكون من الممكن أن تتعاون السلطات مع مقدِّمي خدمات الإنترنت تعاونا مباشرا غير رسمي لحفظ هذه البيانات بغرض التحقيق في جريمة أو ملاحقة مرتكبيها قضائياً. وفي حالات أخرى، قد يكون اللجوء للسلطة الجبرية والإذن القضائي أمراً لازماً، فيما يخص حفظ بيانات الإنترنت وتفتيشها وضبطها لتقديمها واستخدامها كأدلة في دعوى جنائية على سبيل المثال.

٤٥٤- وينبغي أن يدرك المحققون وأعضاء النيابة العامة تمام الإدراك ما قد تكون عليه هذه البيانات من أهمية والحاجة لاتخاذ خطوات بأسرع ما يمكن لحفظها بطريقة تضمن مقبوليتها كأدلة يمكن الاستعانة بها في أية دعاوى لاحقة. وينبغي ما أمكن لأجهزة إنفاذ القانون الوطنية أن تضع، إما مباشرة مع مقدِّمي خدمات الإنترنت أو مع نظيراتها في البلدان الأخرى، إجراءات واضحة، تتضمن عناصر رسمية وغير رسمية على حد سواء، وتستهدف ضمان الاحتفاظ ببيانات استخدام الإنترنت المطلوبة لتحقيق جنائي وتقديمها بأسرع ما يمكن.

٤٥٥- وقد سلَّط بعض المشاركين في اجتماع فريق الخبراء الضوء على أنَّ حاجة السلطات الوطنية إلى حماية المواد الاستخبارية الحساسة كثيراً ما تمثِّل عقبة أمام مشاطرة المعلومات.

٤٥٦- وعند النظر في اتخاذ إجراءات تحقيق في ولايات قضائية أخرى تتعلق بجمع أدلة رقمية، ينبغي للسلطات أن تأخذ في حسبانها ما قد يكون لهذه الإجراءات من آثار على سيادة دول أخرى. وينبغي للسلطات التي تنظر في اتخاذ إجراءات تحقيق تتصل بشخص أو شيء موجود في ولاية قضائية أخرى أن تخطر، متى أمكن ذلك، نظيراتها الأجنبية في البلدان المعنية بهذه الإجراءات وتنسِّقها معها.

٤٥٧- وكثيرا ما تكون البيانات المتعلقة بالإنترنت (مثل بيانات الاستخدام الخاصة بالعملاء) أدلةً هامةً في العديد من قضايا الإرهاب. وينبغي للسلطات أن تضمن في هذه القضايا حفظ البيانات المعنية لاستخدامها لاحقاً كأدلة في الدعوى. ومن المهم الإشارة في هذا الصدد إلى التمييز بين "الاحتفاظ" بالبيانات (البيانات التي

يحتفظ بها مقدِّمو خدمات الإنترنت بموجب التزام تفرضه عليهم اللوائح المنظمة لعملهم) وبين "حفظ" البيانات (البيانات التي تُحفظ بناءً على أمر أو تفويض قضائي). وفي العديد من البلدان، يُلزِم القانون مقدِّمي خدمات الإنترنت بالاحتفاظ بأنواع معينة من البيانات المتعلقة بالاتصالات لمدة زمنية محددة. ومع ذلك، وبالرغم من بعض الجهود المبذولة على هذا الصعيد (كما هو الحال على المستوى الإقليمي في أوروبا)، فليس هناك اتفاق دولي بشأن نوع البيانات التي ينبغي لمقدِّمي خدمات الإنترنت الاحتفاظ بها أو مدة الاحتفاظ بها. ونتيجة لذلك، ثمة تفاوت كبير على المستوى الدولي في نوعية البيانات التي يحتفظ بها مقدِّمو خدمات الإنترنت وفي المدة التي يبقون فيها عليها. ومن الممكن أن يطرح هذا الأمر مشاكل في القضايا التي تحتاج فيها السلطات إلى بينات متعلقة بالاتصالات موجودة في أحد البلدان لاستخدامها أدلةً في دعوى جنائية مقامة في بلد آخر.

٤٥٨- ومن شأن وضع إطار تنظيمي متفق عليه عالمياً يفرض التزامات موحَّدة على كل مقدِّمي خدمات الإنترنت بشأن نوع بيانات الاستخدام الخاصة بالعميل التي يُحتفظ بها ومدة الاحتفاظ بها أن يكون ذا فائدة جمة لأجهزة إنفاذ القانون والاستخبارات التي تقوم بالتحقيق في قضايا الإرهاب. وفي ظل عدم وجود إطار عالمي متفق عليه للاحتفاظ بالبيانات من قِبَل مقدِّمي خدمات الإنترنت، ينبغي للسلطات أن تحدد، بأسرع ما يمكن، وجود بيانات مقدِّم خدمات الإنترنت المتصلة بالتحقيق من عدمه ومكان وجودها، وتبدأ في اتخاذ خطوات بأسرع ما يمكن لحفظها لاحتمال استخدامها كأدلة.

٤٥٩- وينبغي للسلطات أن تقيم قدر الإمكان علاقات أو اتفاقات غير رسمية مع مقدِّمي خدمات الإنترنت (المحليين والأجانب على حد سواء) الذين قد تكون لديهم بيانات هامة في مجال إنفاذ القانون بشأن الإجراءات اللازمة لإتاحة هذه البيانات في التحقيقات التي تقوم بها أجهزة إنفاذ القانون. فإن لم توجد إجراءات غير رسمية من هذا القبيل، فينبغي للسلطات أن تتواصل بأسرع ما يمكن أثناء اضطلاعها بالتحقيقات مع نظيراتها الأجنبية، عبر القنوات الرسمية ووفقاً لإذن قضائي صحيح إن لزم الأمر، بشأن حفظ هذه البيانات.

٤٦٠- وفيما يتعلق بالأدلة، فإنَّ قضايا الإرهاب التي تتطلب تحقيقات عابرة للحدود تزيد من صعوبة مهمة المحققين وأعضاء النيابة العامة المعقدة أصلاً، بما يقتضي منهم كفالة اتفاق الأساليب المستخدمة في الحصول على الأدلة (في بلد واحد أو أكثر) وتقديمها ضمن الأدلة في ملاحقة قضائية تجرى في ولاية قضائية أخرى تمام الاتفاق والقوانين والمبادئ المطبَّقة في جميع الولايات القضائية المعنية.

٤٦١- ويمكن أن يؤدي اشتراط ازدواجية التجريم (أي أن تشكِّل الأفعال التي تتعلق بها طلبات تسليم المطلوبين والمساعدة القانونية المتبادلة جريمة في الدولتين المعنيتين)، والشائع وروده في العديد من الصكوك الثنائية والمتعددة الأطراف المتعلقة بالإرهاب والجريمة المنظمة العابرة للحدود الوطنية، إلى صعوبات في القضايا الجنائية، بما في ذلك قضايا الإرهاب، التي تنطوي على عنصر من عناصر التعاون الدولي.

٤٦٢- وقد تثير قضايا الإرهاب التي تكون الأفعال المكوِّنة للجريمة فيها قد نُفِّذت على الإنترنت مسائل معقدة فيما يتعلق بالاختصاص، ولا سيما في القضايا التي يكون فيها أحد من يشتبه في كونهم مجرمين موجوداً في بلد ما في حين يستخدم مواقع أو خدمات على الإنترنت يستضيفها مقدِّمو خدمات في بلد آخر لتنفيذ الأفعال المكوِّنة للجريمة. ففي هذه الحالات، كان الأشخاص يقيمون في بلد ما، ويقومون في الوقت نفسه بإنشاء وإدارة مواقع شبكية مستضافة في بلد آخر تُستخدم للترويج للجهاد وغيره من أعمال العنف المتعلقة بالإرهاب.

٤٦٣- وليس ثمة قواعد ملزمة بموجب القانون الدولي تتناول مسألة كيفية تعامل الدول مع القضايا التي قد تدعي فيها أكثر من دولة واحدة اختصاصها بالملاحقة القضائية في جريمة ارتكبها نفس المشتبه به. وعادة ما تقوم السلطات الوطنية بموازنة العوامل ذات الصلة، بما فيها مدى الصلة بين مختلف الولايات القضائية من جهة والجريمة المزعومة من جهة أخرى، في سعيها لتقرير ما إذا كانت سوف تؤكد اختصاصها وتمارسه في القضية المعنية. وفي حالات التنازع على الاختصاص، من المهم الإسراع بالتواصل القائم على التعاون فيما بين السلطات المركزية المعنية (أجهزة النيابة العامة الوطنية في الأغلب) لحل هذه المسائل.

٤٦٤- وكثيراً ما تحد التشريعات الوطنية بشأن حماية البيانات أو الخصوصية من قدرة أجهزة إنفاذ القانون وأجهزة الاستخبارات على مشاطرة المعلومات مع نظيراتها المحلية والأجنبية على حد سواء. ومن التحديات التي تواجهها الحكومات دوما وتثير الانشغال في بعض الحالات، ومنها تدابير التصدّي للإرهاب، تحقيقُ توازن معقول بين حق الإنسان في الخصوصية والمصلحة المشروعة للدولة في التحقيق في الجرائم وملاحقة مرتكبيها قضائياً على نحو فعَّال.

واو- الملاحقة القضائية

٤٦٥- يعدُّ الالتزام المفروض على الدول بالامتناع عن توفير الملاذ الآمن لمرتكبي الأعمال الإرهابية وتقديمهم للعدالة، أينما كان مكان وقوع هذه الأعمال، جزءاً لا يتجزأ من الإطار القانوني العالمي لمكافحة الإرهاب، ومن استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب. وإلى جانب وجود الإطار التشريعي اللازم، فإنَّ القدرة المؤسسية لأجهزة النيابة العامة الوطنية على احترام سيادة القانون أثناء الملاحقة القضائية بشأن قضايا الإرهاب، بما يتفق وحقوق المشتبه بهم والأشخاص المتهمين بموجب القانون الدولي لحقوق الإنسان، جزءٌ لا يتجزأ من تدابير التصدّي للإرهاب بفعالية في مجال العدالة الجنائية.

٤٦٦- وفي كثير من الأحيان، لا يقتصر دور أعضاء النيابة العامة على ما يقومون به في مرحلة الملاحقة القضائية من قضايا الإرهاب، وإنما يؤدون كذلك دوراً مباشراً في مرحلة التحقيق، بما يقدمونه من مشورة قانونية واستراتيجية في المسائل التي من شأنها أن تؤثّر على نتيجة أي ملاحقة قضائية يتمخَّض عنها التحقيق. وعادة ما يقوم أعضاء النيابة العامة بهذا الدور في إطار فريق متعدد التخصصات أو متعدد الولايات القضائية. وكما يعدُّ وجود مستوى مرتفع من الثقة والتنسيق والتواصل عنصراً حيوياً في التعاون الفعَّال على المستوى الدولي، فيتعيَّن أن يكون موجوداً كذلك فيما بين الأجهزة الوطنية لإنفاذ القانون، والاستخبارات، والنيابة العامة.

٤٦٧- ولئن عزَّزت تقنيات التحقيق الجديدة الفرص المتاحة أمام السلطات لاستهداف الأنشطة الإرهابية على الإنترنت، فإنَّها تحمل في طياتها مخاطر قانونية لا بد لأعضاء النيابة العامة أن ينتبَّهوا لها. والاختلافات في القوانين الوطنية المتعلقة بجمع الأدلة ومقبوليتها تعني أنَّ هذه المخاطر تشتد حين تكون الأعمال التي تُستقى منها هذه الأدلة قد وقعت في ولاية قضائية غير الولاية التي ستُجرى فيها المحاكمة.

٤٦٨- وفي معظم البلدان، يمارس أعضاء النيابة العامة سلطة تقديرية واسعة فيما يخص رفع الدعوى الجنائية من عدمه، والتهم التي سوف يوجِّهونها لرفع الدعوى. وكثيراً ما تُتَّخذ هذه القرارات وفقاً لمبادئ توجيهية أو مدونات الغرض منها ضمان الممارسة العادلة والشفافة والمتسقة لهذه السلطة التقديرية الهامة، وغالباً ما تفرض هذه المبادئ أو المدوّنات الحدود الدنيا لرفع الدعاوى على أساس كفاية الأدلة والمصلحة العامة.

٤٦٩- إنَّ الهدف الرئيسي للتحقيقات المتعلقة بالإرهاب هو السلامة العامة. وفي بعض الحالات، يتعيَّن على السلطات التدخل للحيلولة دون ارتكاب أعمال إرهابية قبل توافر أدلة كافية للشروع في الملاحقة القضائية بشأن الأعمال التي تشتبه السلطات في كونها قيد التخطيط.

٤٧٠- وفي هذه المواقف، قد يتعيَّن على السلطات أن تعتمد على جرائم أخرى لإتاحة الأساس القانوني لإجراءاتها، بما في ذلك جرائم من قبيل التحريض، والتآمر، والتواطؤ الإجرامي، وتوفير الدعم المادي للإرهابيين، عوضاً عن الجرائم المتعلقة في حد ذاتها بالأعمال الإرهابية التي يجري التخطيط لها. كما يمكن استخدام أحكام جنائية عامة أخرى تتعلق بالاحتيال أو حيازة مواد غير قانونية أو استخدامها (مثل وثائق الهوية أو السفر المزورة أو الأسلحة) لعرقلة أنشطة الجماعات الإرهابية أو إحباطها قبل تنفيذ هذه الجماعات لما تخطط له من هجمات أو أنشطة.

٤٧١- وفي العديد من قضايا الإرهاب، تكون الأدلة التي تستعين بها النيابة العامة مستندة إلى معلومات استخبارية. ولا يزال إدماج الأنشطة الاستخبارية في نظم العدالة الجنائية مشكلةً جوهريةً تواجه السلطات في تعاملها مع الإرهاب، بمعنى: كيف يمكن للسلطات أن تحمي المعلومات الاستخبارية الحسَّاسة التي تُستمد منها الأدلة مع الوفاء بالتزاماتها بضمان محاكمة عادلة ودفاع فعَّال للأشخاص المتهمين في الوقت نفسه، بما في ذلك الالتزام بالكشف للدفاع عن جميع الأجزاء الجوهرية من دفوع النيابة العامة؟

٤٧٢- وفي قضايا الإرهاب التي تستخدم فيها أجهزة الحاسوب أو الإنترنت، تكون الأدلة الرقمية جزءاً هاماً من دفوع النيابة العامة. وفي جميع الأحوال يؤدي استخدام هذا النوع من الأدلة إلى إثارة مسائل تتعلق بالمقبولية. لذا فمن المهم للغاية أن يُتوخى الكثير من الحذر في جميع مراحل التحقيق والملاحقة القضائية للتأكد من أنَّ الأساليب المستخدمة للحصول على الأدلة الرقمية، وحفظها، وتحليلها، وتقديمها، تتفق تمام الاتفاق وقواعد الإثبات المعنية أو الإجراءات وتسير وفق الممارسات الجيدة المتعارف عليها.

٤٧٣- ويتعيَّن على السلطات القائمة على الملاحقة القضائية أن تُقنع المحكمة بموثوقية الأدلة الرقمية، بما يشمل أساليب الحصول عليها وتحليلها وتقديمها. وتُعرف إجراءات حفظ سلامة الأدلة بـ"تسلسل العهدة" أو "تسلسل الأدلة". وحين يكون الحصول على هذه الأدلة قد تم في إحدى الولايات القضائية لتُستخدم في محاكمة تجرى في ولاية قضائية أخرى، يغدو الموقف أكثر تعقيداً ويتطلب من المحققين وأعضاء النيابة العامة توخي الحذر الكافي. وفي الحالات التي تقف فيها السلطات على وجود أدلة رقمية ذات صلة أو على مكان وجود هذه الأدلة أو كليهما معاً، فينبغي لها أن تستكشف الوسائل (الرسمي منها وغير الرسمي) التي تمكِّنها من الحصول على هذه الأدلة وحفظها بغرض استخدامها. وينبغي أن تضمن القناة التي يقع عليها الاختيار مقبولية الأدلة في البلد الذي ستُجرى فيه المحاكمة.

٤٧٤- وكثيراً ما تختلف المبادئ والإجراءات القانونية المتعلقة بجمع الأدلة ومقبوليتها في الدعاوى الجنائية باختلاف الولايات القضائية. وينطوي جزء كبير من عمل السلطات في التحقيقات العابرة للحدود على "الوساطة" فيما يتعلق بمختلف جوانب الأدلة. ومن الممكن أن تكون هذه العملية معقدة وأن تستغرق وقتاً طويلاً، إلا أنها تُعدُّ عاملاً حاسماً في نجاح الملاحقات القضائية. ومن شبه المؤكد أن يطعن الدفاع في أي قصور قانوني في وسائل الحصول على الأدلة التي تُستخدم في المحاكمة في نهاية المطاف أو حفظ هذه الأدلة أو إرسالها أو تقديمها.

٤٧٥- وكثيراً ما يَلزم النيابة العامة أن تستعين بشهادة الخبراء لإثبات جانب متخصص أو جوانب متخصصة من قضايا الإرهاب. وتشمل المجالات التي كثيراً ما تُطلب فيها شهادة الخبراء التكنولوجيا والاتصالات، والمعتقدات الإيديولوجية التي تحملها الجماعات الإرهابية وأنشطتها وهياكلها التنظيمية. وهناك إمكانية حقيقية لأن يحتاج أعضاء النيابة العامة الاستعانة بعدة شهود خبراء. وعادة ما تتكوَّن القضايا التي تتطلب الاستعانة بشهادة الخبراء من ثلاث خطوات أو مراحل هي: *(أ)* تحديد المسائل التي تحتاج إلى رأي خبير (ونطاق هذه المسائل) بوضوح؛ *(ب)* اختيار خبراء مؤهلين؛ *(ج)* ضمان استخدام الخبراء المؤهلين لوسائل يمكن قبولها في المحكمة.

٤٧٦- وينبغي لأعضاء النيابة العامة أن يحدِّدوا بأسرع ما يمكن المسائل التي يُرجَّح أنهم سيحتاجون فيها إلى شهادة الخبراء، وأن يستعينوا بالخبراء ليضطلعوا بالتحليل اللازم، مع توفير إرشادات واضحة بشأن القواعد الأساسية للإجراءات أو الإثبات إذا لزم الأمر. وعلى النيابة العامة النظر، عند اختيار الشهود الخبراء، فيما إذا كان ينبغي الاستعانة بخبراء حكوميين أو غير حكوميين. ولئن كان للاستعانة بالخبراء الحكوميين مزايا، فقد تكون الاستعانة بخبراء غير حكوميين أمراً مستصوباً في القضايا التي تستمد فيها الأدلة بالاستعانة بمصادر أو أساليب استخبارية حساسة. ومن الممكن أن يكون إيجاد الخبير المناسب، ولا سيما في التخصصات الدقيقة، مشكلة كبيرة في الولايات القضائية الأقل تطوراً. وينبغي للشهود الخبراء حسب الاقتضاء أن يتبعوا الممارسات الجيدة المتعارف عليها ويطبِّقوها في المجال الذي يدلون فيه بشهاداتهم. ونظراً لتعقيد بعض الشهادات التي يدلي بها الخبراء، فينبغي أن تؤخذ في الاعتبار الوسائل المبتكرة في عرض الأدلة المعقَّدة على القضاة أو هيئات المحلفين أو غيرهم من متقصِّي الحقائق في المحاكمة بطريق يسهل فهمها. ومن المهم أن يكون لدى أعضاء النيابة العامة معرفة عملية جيدة بالموضوع المعني.

٤٧٧- إنَّ التعقيد الذي يتسم به الكثير من المحاكمات المتعلقة بالإرهاب، ولا سيما المحاكمات التي تتطلب التعاون الدولي أو تتضمن عناصر تقنية معقدة، تجعل من المستصوب للغاية أن يتولى فريق من أعضاء النيابة العامة تسيير القضايا. وحتى يتأتى ضمانُ اتباع نهج متكامل يقوم على سيادة القانون والحفاظُ على اكتمال تدابير التصدي للإرهاب في مجال العدالة الجنائية، من الضروري أن يكون لدى البلدان آليات قوية ودائمة لتعزيز قدرة النيابة العامة على تنفيذ التشريعات الوطنية لمكافحة الإرهاب والتزامات التعاون الدولي ذات الصلة. وفي البلدان التي يكون فيها احتمال وقوع أنشطة إرهابية قويا، مع تدنٍّ في القدرات المؤسسية لأجهزة النيابة العامة وغيرها من أجهزة العدالة الجنائية، ينبغي إيلاء أولوية قصوى لاستحداث قدرات متخصصة داخل هذه الأجهزة، ليس فيما يتعلق بالملاحقة القضائية فحسب وإنما كذلك فيما يخص آليات التعاون الدولي ذات الصلة.

زاي- التعاون مع القطاع الخاص

٤٧٨- لئن كانت مسؤولية مكافحة استخدام الإنترنت في أغراض إرهابية تقع في نهاية المطاف على عاتق الدول الأعضاء، فإنَّ التعاون مع أهم جهات القطاع الخاص المعنية له أهمية حاسمة في فعالية التنفيذ. فالمبادرة إلى التواصل مع جهات القطاع الخاص المعنية مثل مقدِّمي الخدمات، ومواقع استضافة المحتويات التي يعدها المستخدمون أنفسهم، ومحركات البحث، ستظل ذات أهمية في التحكم في مدى توافر المحتويات ذات الصلة بالإرهاب المنشورة عبر الإنترنت.

٤٧٩- وسيكون من المفيد إقامة شراكات بين القطاعين العام والخاص فيما يتعلق بالرقابة على استخدام الإنترنت في أغراض إرهابية. وقد اتُّخذت مبادرات من هذا القبيل بنجاح فيما يتعلق بجوانب أخرى لمكافحة الإرهاب، ولمكافحة الجرائم السيبرانية بصفة عامة. وتتيح هذه المبادرات منتدى للحوار الرسمي وغير الرسمي بين النظراء من القطاعين العام والخاص، كما تدعم أنشطة من قبيل برامج التدريب المشتركة، مما قد يسهم في كسر حواجز التواصل وتعزيز الثقة والتفاهم واستحداث ممارسات متجانسة بين أعضاء الشراكات الذين يؤدون دورا فاعلا في هذه المبادرات.

المرفق
قائمة بأسماء المساهمين في هذا المنشور

الاتحاد الروسي

السيد أليكسي يودينتسيف
نائب مدير إدارة التحدِّيات والأخطار الجديدة
وزارة الخارجية

السيد أليكسي درونوف
رئيس قسم، مستشار أول
البعثة الدائمة للاتحاد الروسي لدى المنظمات الدولية في فيينا

السيد أندري فاسيلينكو
سكرتير ثان
البعثة الدائمة للاتحاد الروسي لدى المنظمات الدولية في فيينا

إسبانيا

السيد ألفونسو إستيفيز أوتشوا
كبير مفتشي مكتب الاستخبارات
قوة الشرطة المدنية الوطنية لإسبانيا

السيد إسماعيل روميرو راموس
ملازم أول
رئيس مكتب الاستخبارات
الحرس المدني

السيد سيرخيو دي فروتوس باريينتي
مكتب الاستخبارات
وزارة الداخلية

إسرائيل

السيد حاييم فيسمونسكي
المشرف الوطني على شؤون القانون والتكنولوجيا
مكتب المدعي العام لدولة إسرائيل

ألمانيا

السيد كريستيان مونكا
مدع عام أول

د. أوفه إي كيميزيس
رئيس وحدة بحوث الإرهاب/التطرف
المكتب الاتحادي للشرطة الجنائية

السيد فلوريان تورنر
البعثة الدائمة لألمانيا، فيينا

إندونيسيا

السيد بيتروس جولوس
مدير العمليات
وكالة مكافحة الإرهاب الوطنية

السيد أريس موناندار
مستشار
البعثة الدائمة لإندونيسيا، فيينا

إيطاليا

السيد جورجيو روجيري
مجموعة العمليات الخاصة التابعة لقوات الدرك الإيطالية (كارابينييري)
إدارة التحقيقات التقنية

باكستان

السيد ياسر محمود
مدير مساعد
وزارة الخارجية

البرازيل

السيد روموالو دانتاس
مدير إدارة مكافحة الإرهاب
مجلس الأمن المؤسسي/وكالة الاستخبارات البرازيلية

الجزائر

السيد بشير سعيد
محافظ شرطة
المديرية العامة للأمن الوطني

جمهورية كوريا

السيد مينوو يون
أستاذ مساعد
قسم علوم الشرطة، جامعة هانساي

رومانيا

السيد رازفان أفراميسكو
وكالة الاستخبارات الرومانية

الصين

السيد بن هو
مستشار
البعثة الدائمة لجمهورية الصين الشعبية، فيينا

السيدة شوينا لو
نائبة رئيس شعبة
مكتب الأمن الشبكي، وزارة الأمن العام

فرنسا

السيد أوليفييه كريستن
نائب المدعي العام
رئيس القسم C1: مكافحة الإرهاب وانتهاكات الأمن الوطني

السيد غيوم بورتانسيني
نائب المدعي العام

كندا

السيد دومينيك دودمين
كبير محامين
دائرة النيابة العامة في كندا

كولومبيا

النقيب لويس فرناندو أتويستا زاراتي
فريق تحقيقات التكنولوجيا
مديرية التحقيقات الجنائية والمنظمة الدولية للشرطة الجنائية (الإنتربول)
الشرطة الوطنية

الملازم نادريس برناردو مولينا فيفاس
فريق تحقيقات التكنولوجيا
مديرية التحقيقات الجنائية والمنظمة الدولية للشرطة الجنائية (الإنتربول)
الشرطة الوطنية

ماوريسيو أغيري باتينيو
مدع عام متخصص
النيابة الوطنية لمكافحة الإرهاب

ماليزيا
السيد توماس كوروث صاموئيل
مدير البحوث والمنشورات
المركز الإقليمي لجنوب شرقي آسيا لمكافحة الإرهاب
وزارة الخارجية

مصر
د. إيهاب ماهر السنباطي
قاض بالمحاكم العليا

المغرب
السيد عبد الرحيم حنين
رئيس قسم القضايا الجنائية الخاصة
وزارة العدل

المملكة المتحدة
السيدة مويرا ماكميلان
محامية متخصصة بمكافحة الإرهاب
النيابة العامة للتاج البريطاني

النمسا
السيد ديفيد بلوم
وزارة الداخلية الاتحادية
الوكالة الاتحادية لحماية الدولة ومكافحة الإرهاب
السيد هانز شنايدر

نيجيريا
السيد أكين أكينتيوي
نائب مدير النيابة العامة
وزارة العدل

الهند
د. رافي شانكار أيانار
وكالة التحقيقات الوطنية، حيدر أباد
السيد أبهيجيت هادلر
مستشار
البعثة الدائمة للهند، فيينا

الولايات المتحدة
السيد مايكل مولاني
رئيس قسم مكافحة الإرهاب
وزارة العدل

السيد مايكل كيغان
النائب الأول لرئيس قسم مكافحة الإرهاب
وزارة العدل

اليابان
السيد ماساو كواهارا
مدير شعبة مكافحة الإرهاب، إدارة الشؤون الخارجية والاستخبارات
مكتب الأمن، وكالة الشرطة الوطنية

السيد ساتوشي هاناشيما
مفتش شرطة
شعبة مكافحة الإرهاب، إدارة الشؤون الخارجية والاستخبارات
مكتب الأمن، وكالة الشرطة الوطنية

السيد ماساو سوميتا
مفتش شرطة مساعد
شعبة مكافحة الإرهاب الدولي، إدارة الشؤون الخارجية والاستخبارات
مكتب الأمن، وكالة الشرطة الوطنية

مجلس أوروبا
السيدة غرتراوده كابلكا
ممثلة النمسا
لجنة خبراء الإرهاب

المديرية التنفيذية للجنة مكافحة الإرهاب
السيدة نورها ريستريبو
مسؤولة الإعلام

فرقة العمل المعنية بتنفيذ تدابير مكافحة الإرهاب
السيد كاسبر إيغه
إدارة الشؤون السياسية

وحدة التعاون القضائي التابعة للاتحاد الأوروبي (يوروجوست)
السيدة ماريا غارثيا إسكوميل
فريق مكافحة الإرهاب

منظمة الأمن والتعاون في أوروبا
السيد بن هيلر
مسؤول برامج مساعد/وحدة إجراءات مكافحة الإرهاب التابعة لإدارة المخاطر العابرة للحدود الوطنية بمنظمة الأمن والتعاون في أوروبا

السيد نيمانيا ماليسيفتش
المسؤول عن الأمن السيبراني
خلية التنسيق التابعة لإدارة المخاطر العابرة للحدود الوطنية

برايس ووترهاوس كوبرز

السيد نيل بولارد

جامعة دبلن

البروفيسور جو كارثي
مدير مركز الأمن السيبراني والتحقيق في الجرائم السيبرانية

مفوضية الأمم المتحدة لحقوق الإنسان

السيدة ليزا أولدرينغ
وحدة سيادة القانون والديمقراطية

مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة[٢٠٥]

السيدة مارتا ريكينا
رئيسة فرع منع الإرهاب

السيدة جيليان موراي
رئيسة قسم دعم المؤتمر
الفرع المعني بالجريمة المنظمة والاتجار غير المشروع

السيد ماورو ميديكو
رئيس الوحدة المتخصصة في منع الإرهاب
فرع منع الإرهاب

السيد فيليب ديفيت
مسؤول برامج، الوحدة المتخصصة في منع الإرهاب
فرع منع الإرهاب

السيد ستيفن مالبي
الموظف المعني بمراقبة المخدِّرات ومنع الجريمة، قسم دعم المؤتمر
الفرع المعني بالجريمة المنظمة والاتجار غير المشروع

السيد يوجين غالاغر
مستشار
فرع منع الإرهاب

السيدة كيري داليب
مستشارة
فرع منع الإرهاب

[٢٠٥] يودُّ مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة أن يعبِّر عن تقديره للمتدربين الداخليين التالية أسماؤهم الذين أسهموا في إعداد هذا المنشور: توم لينغوروفسكي، ولوسيانا نياغو، وأندريه بينيا توريس، وستانيسلاو تسيبلياكو.

UNODC
مكتب الأمم المتحدة المعني بالمخدرات والجريمة

Vienna International Centre, PO Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-5866, www.unodc.org

V.12-57351—June 2013