الأمم المتحدة

A/CONF.222/12

Distr.: General
2 February 2015
Arabic
Original: English

مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية

الدوحة، ١٢-١٩ نيسان/أبريل ٢٠١٥

البند ٥ من جدول الأعمال المؤقَّت*

النُّهُج الشاملة المتوازنة لمنع ظهور أشكال جديدة ومستجدَّة للجريمة العابرة للحدود الوطنية والتصدِّي لها على نحو ملائم

حلقة العمل ٣: تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدِّي للأشكال المتطوِّرة للجريمة، مثل الجرائم الإلكترونية (السيبرانية) والاتجار بالممتلكات الثقافية، بما في ذلك الدروس المستفادة والتعاون الدولي**

ورقة معلومات أساسية

ملخَّص

تقدِّم ورقةُ المعلومات الأساسية هذه لمحةً مجملةً عن الجوانب العامة والخاصة لما تتَّخذه نُظم منع الجريمة والعدالة الجنائية من تدابير لمواجهة الجريمة السيبرانية والاتجار بالممتلكات الثقافية، وهما مثالان بارزان لأشكال الإجرام المتطوِّرة التي اكتسبت مزيداً من الأهمية بفعل العولمة وتطوُّر تكنولوجيا المعلومات. ومع أنَّ الجماعات الإجرامية قد استغلَّت الفرص التي أتاحتها هاتان الظاهرتان، فإنَّ هناك حاجةً إلى تدابير فعَّالة لزيادة المعارف عن نطاق الجرائم ذات الصلة وأسبابها الجذرية وأساليب العمل التي تُستخدَم في ارتكابها، من أجل استحداث استراتيجيات وقائية فعَّالة وتحسين تبادل المعلومات وتدعيم الأُطر الوطنية والتعاون الدولي بين الدول الأعضاء.

* A/CONF.222/1.

** تودُّ الأمانة العامة للأمم المتحدة أن تعرب عن تقديرها للمعاهد الأعضاء في شبكة برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية، وخصوصاً للمعهد الوطني للعدالة بالولايات المتحدة الأمريكية، والمجلس الاستشاري الدولي للشؤون العلمية والفنِّية، والمعهد الكوري لعلم الإجرام، والمعهد الأوروبي لمنع الجريمة ومكافحتها، المنتسب إلى الأمم المتحدة، لمدِّها يد المساعدة في التحضير لحلقة العمل وتنظيمها.

100215 V.15-00661 (A)

المحتويات

الصفحة

أولاً- مقدِّمة ٣

ثانياً- الجريمة السيبرانية ٧

ألف- استبانة التحدِّيات القائمة ٧

باء- قياس الجريمة السيبرانية ١٠

جيم- منع الجريمة السيبرانية ومكافحتها ١٤

ثالثاً- الاتجار بالممتلكات الثقافية ١٨

ألف- تحديد ماهية التحدِّي ١٨

باء- تدابير التصدِّي للاتجار بالممتلكات الثقافية ٢١

رابعاً- الاستنتاجات والتوصيات ٢٤

أولاً- مقدِّمة

١- أثناء اجتماعات آسيا والمحيط الهادئ وغربي آسيا وأفريقيا الإقليمية التحضيرية لمؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية، سَلَّمت الدول الأعضاء بأهمية استحداث تدابير شاملة لمواجهة الجريمة السيبرانية وجريمة الاتجار بالممتلكات الثقافية الناشئتين.[١] وكما هو الحال في كثير من الجرائم الأخرى، ثمة أساسان ضروريان لأيِّ استراتيجيات وقائية فعَّالة وأيِّ تدابير مضادة تتَّخذها نظم العدالة الجنائية لمكافحة أشكال الإجرام الناشئة هذه، ألا وهما وجود قاعدة معرفية مفصَّلة وفَهم واضح للعوامل الإجرامية المسهِّلة والأنماط السائدة.

٢- وفي ورقة العمل التي أعدَّتها الأمانة بشأن النُّهج الشاملة المتوازنة لمنع ظهور أشكال جديدة ومستجدَّة للجريمة العابرة للحدود الوطنية والتصدِّي لها على نحو ملائم،[٢] أُجريت محاولات استكشافية لتصنيف الأشكال الجديدة والمستجدَّة من الجرائم تصنيفاً متعدِّد المستويات، يستند إلى جذورها المحتملة ودوافعها وأساليب العمل الشائعة في ارتكابها. وذُكرت في تلك الورقة، كأسباب جذرية ودوافع محتملة لأشكال الإجرام المستجدَّة، عوامل مثل العولمة وقُرب أوضاع الفقر والنزاع وضَعف سيادة القانون من الأسواق العالية القيمة؛ وسرعة ظهور أشكال جديدة من التكنولوجيا الحديثة. كما ذَكرت الورقة ما جرى من تغيُّر في بنية الجماعات الإجرامية المنظَّمة واللجوء إلى الفساد لتسهيل الجرائم كأسلوبَي عمل رئيسيين.

٣- وإلى جانب أنواع أخرى من الجرائم، مثل القرصنة والتعدِّي على الأطفال واستغلالهم والاتجار بالحيوانات والنباتات البرِّية، يشيع ذِكر جريمة الاتجار بالممتلكات الثقافية والجريمة السيبرانية باعتبارهما تندرجان ضمن فئة الجرائم المستجدَّة أو الناشئة.[٣] ومثلما وَرد في الوثيقة A/CONF.222/8، قد لا تكون هاتان الجريمتان جديدتين كليًّا، بل يمكن أن تمثِّلا أيضاً عودة ظهورٍ أنواع تقليدية من الجرائم أو نشوء سبل ووسائل جديدة لارتكاب أفعال إجرامية مستحكمة.

---

(١) A/CONF.222/RPM.1/1، الفقرتان ٣٣ و٣٥؛ وA/CONF.222/RPM.2/1، الفقرتان ٣٨ و٤٠؛ وA/CONF.222/RPM.4/1، الفقرة ٧٠.

(٢) A/CONF.222/8.

(٣) انظر، على سبيل المثال، قرار الجمعية العامة ٦٦/١٨١، الفقرة ١٨.

٤- فعلى سبيل المثال، كانت سرقة الممتلكات الثقافية والاتجار بها محليًّا موجودةً منذ عدَّة قرون. غير أنَّ المجتمع الدولي لم يَسْعَ إلى تنظيم التجارة في الممتلكات الثقافية، وتحديداً إلى تجريم سرقة القطع الفنية والتُّحف التاريخية، إلاَّ في العقود القليلة الماضية. وفي الوقت نفسه، سَهَّلت العولمة تزايد ضلوع الجماعات الإجرامية المنظَّمة، مما أفضى إلى نشوء أسواق معولَمة غير مشروعة للممتلكات الثقافية المسروقة وإمكانية توليد أرباح كبيرة للجماعات الإجرامية المنظَّمة، وربما للجماعات الإرهابية. وعلى نحو مشابه، أخذ كثير من البلدان، منذ عام ١٩٦٠، يعترف بأنَّ بعض الأفعال المتصلة بالحواسيب، مثل الاستخدام غير المأذون به للنظم الحاسوبية والتلاعب بالبيانات الإلكترونية، هي أفعال إجرامية. غير أنَّ استخدام تكنولوجيا التواصُل المعلوماتي المعولمة في ارتكاب أفعال إجرامية ذات نطاق عابر للحدود الوطنية، في شكل الجريمة السيبرانية المعاصِرة، لم يأت إلاَّ مع ظهور الإنترنت.

٥- وبذلك، تمثِّل الجريمة السيبرانية والاتجار بالممتلكات الثقافية نموذجين لما يمكن أن يكون للأسباب الجذرية والدوافع، ومنها العولمة وظهور أشكال جديدة من التكنولوجيا، من تأثير في الابتكار الإجرامي. فعلى الرغم من أنَّ هذين النوعين من الجرائم يختلفان في جوانب شتَّى، مثل المستهدَف الرئيسي بالفعل الإجرامي، فإنهما يتشاطران عدداً من السمات المشتركة.

٦- والاتجار بالممتلكات الثقافية يتعلق بسرقة أشياء ملموسة تكتسب قيمتها من أهميتها الخاصة للتراث الثقافي وبالاتجار بتلك الأشياء وبيعها. ومع أنَّ الشيء المستهدَف بالجريمة السيبرانية كثيراً ما يكون غير ملموس، مثل البيانات الحاسوبية أو النظام الحاسوبي، فإنَّ جزءاً من أفعال الجريمة السيبرانية يتمحور حول السرقة وإعادة البيع. فالأفعال المتصلة بالحواسيب التي تُرتكَب للحصول على مكسب شخصي أو مالي أو لإلحاق ضرر شخصي أو مالي، مثلاً، قد تنطوي على سرقة معلومات مفصَّلة عن تعاملات مصرفية عبر الإنترنت أو بيانات مفصَّلة لبطاقات ائتمان، ثم إعادة بيعها لكي تُستخدَم في الاحتيال المالي أو السرقة. ومثلما هو حال الاتجار بالممتلكات الثقافية، قد يكون مكانا البائع والمشتري واقعين في ولايتين قضائيتين مختلفتين.

٧- وفيما يتعلق بدرجة التنظيم الإجرامي، قد يكون للجماعات الضالعة في الجرائم السيبرانية هيكل مائع نسبيًّا.[٤] غير أنَّ هناك شواهد متزايدة على أنَّ الجماعات ذات الهيكل

(٤) United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (2013, draft), p. 46; and Blythe Bowman Proulx, "Organized criminal involvement in the illicit antiquities trade", *Trends in Organized Crime*, vol. 14, No. 1 (March 2011).

التقليدي القائم على التراتب الهرمي تستفيد أيضاً من سوق الجريمة السيبرانية ذات الطابع الخدماتي لتنفيذ جرائم أكثر تَعقُّداً.(٥) وفي هذا الصدد، يمكن أن يتقاطع نطاقا جريمة الاتجار بالممتلكات الثقافية والجريمة السيبرانية على مستوى بيع الأشياء الثقافية بصورة غير مشروعة عبر الإنترنت. وقد اعترفت المنظَّمة الدولية للشرطة الجنائية (الإنتربول) ومنظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو) ومجلس المتاحف الدولي، على سبيل المثال، بأنَّ التجارة غير المشروعة في الأشياء الثقافية عبر الإنترنت هي مشكلة خطيرة ومتنامية، لبلدان المنشأ والمقصد على السواء.(٦) وتتناول المبادئ التوجيهية الدولية بشأن تدابير منع الجريمة والعدالة الجنائية فيما يتعلق بالاتجار بالممتلكات الثقافية وما يتصل به من جرائم أخرى(٧) هذه المشكلة إذ توصي بإنشاء آليات إبلاغ ورصد خاصة بالتجارة في الممتلكات الثقافية عبر الإنترنت.(٨)

٨- وإلى جانب طابع الجريمتين نفسيهما وتقاطعهما على النحو المبيَّن أعلاه، يمكن أن توجد أيضاً سمات مشتركة على مستوى التدابير الوقائية وجمع المعلومات لأغراض العدالة الجنائية. كما لا توجد معلومات مفصَّلة عن اتجاهات هذين النوعين من الجرائم ولا معلومات إحصائية عنهما. فحتى الآونة الأخيرة، كان الجانب الأكبر مما هو معروف عن الاتجار بالممتلكات الثقافية يأتي من دراسات حالة لأشكال خاصة من الجرائم، مثل سرقة القطع الفنِّية أو نهب التحف التاريخية. غير أنه بُذلت، من خلال دراسة الأمم المتحدة الاستقصائية لاتجاهات الجريمة وعمليات نظم العدالة الجنائية، جهود لتعزيز المعلومات المتاحة، بوسائل منها جمع إحصاءات شُرَطية وقضائية عن الاتجار بالممتلكات الثقافية وسرقتها وحيازتها ومناولتها واستخراجها بصورة غير مشروعة. وتؤكِّد النتائج أنَّ هناك حاجة إلى جمع المعلومات بصورة منهجية ومتواصلة، من أجل التوصُّل إلى استنتاجات ممثِّلة للواقع. ولكن ضخامة عدد الأفعال المختلفة التي يمكن أن تندرج تحت تعبير "الجريمة السيبرانية" العام تمثِّل تحدِّياً لعمليات جمع البيانات. غير أنه يمكن للمنهجيات المنطوية على استخدام مصادر متعدِّدة للبيانات أن توفِّر نهوجاً واعدةً في هذا الشأن.

---

(٥) European Police Office, *The Internet Organised Crime Threat Assessment 2014* (The Hague, 2014), p. 10.

(٦) UNESCO, INTERPOL and International Council of Museums, "Basic actions concerning cultural objects being offered for sale over the Internet". متاحة في الموقع الشبكي www.unesco.org/new/en/culture/themes/illicit-trafficking-of-cultural-property.

(٧) مرفق قرار الجمعية العامة ٦٩/١٩٦.

(٨) المبدآن التوجيهيان ٣ (د) و١٠.

٩- ومع أنَّ ارتكاب الجرم يمكن أن يحدث، في كلتا الحالتين، في ولاية قضائية واحدة، يشترك الاتجار بالممتلكات الثقافية والجريمة السيبرانية أيضاً في عنصر آخر هو طابعهما العابر للحدود الوطنية، مما يجعل التعاون الدولي عاملاً محوريًّا في فعالية تدابير التصدِّي المتَّخَذة. وقد أُبرزت أهمية تعزيز التعاون في هذا الشأن في جميع الاتجاهات الإقليمية التحضيرية للمؤتمر الثالث عشر.[٩] ففيما يتعلق بالجريمة السيبرانية، يشير أحد التقديرات إلى أنَّ ما بين ٣٠ و٧٠ في المائة من الجرائم السيبرانية ينطوي على بُعد عبر وطني.[١٠] كما أنَّ جرائم الاتجار بالممتلكات الثقافية يَغلُب عليها الطابع عبر الوطني.[١١] ويتطلَّب التحرِّي عن الأفعال الإجرامية التي تمسُّ ولايات قضائية متعدِّدة أوسع نطاق ممكن من المساعدة القانونية المتبادلة في التحرِّيات والتحقيقات والملاحقات والدعاوى القضائية، بغية تعزيز فعالية الإجراءات وتسريعها.

١٠- ومما يسهِّل التعاون الدولي وجودُ أُطر قانونية وطنية تتضمَّنُ تجريماً لنفس أنماط السلوك الجوهرية الأصلية. ففي حالة الاتجار بالممتلكات الثقافية، هناك جرائم معيَّنة يمكن أن تشتمل على الاتجار بتلك الممتلكات وتصديرها واستيرادها بصورة غير مشروعة وسرقتها، وكذلك نهب المواقع الأثرية والثقافية وإجراء عمليات تنقيب غير مشروعة فيها.[١٢] أمَّا في حالة الجريمة السيبرانية، فيلزم عادة وجود أحكام معيَّنة في القانون الجنائي لتجريم السلوك الموجَّه ضد البيانات أو النظم الحاسوبية، مثل جرم اقتحام نظام حاسوبي أو الاطِّلاع على بيانات حاسوبية بصورة غير مشروعة.

١١- وأخيراً، يُرجَّح أن تَبلُغ تدابير التصدِّي لكلا الشكلين من الجرائم أقصى درجات الفعالية عندما تنطوي على نهج يتَّسم بتعدُّد الجهات ذات المصلحة. إذ إنَّ القطاع الخاص يمتلك ويُشغِّل جانباً كبيراً من البنى التحتية للإنترنت التي يعتمد عليها الكثير من أشكال الجريمة السيبرانية. أمَّا الأشياء ذات القيمة الثقافية فقد تكون مملوكةً لجهات واسعة التنوُّع، منها الدولة والأفراد والمتاحف والصناديق الاستئمانية وغيرها من الرابطات غير الحكومية. ويُعتبَر إشراك جميع الجهات المعنية، بما في ذلك من خلال شراكات بين القطاعين العام والخاص، أمراً بالغ الأهمية لزيادة الوعي بالمخاطر الإجرامية ولترويج ممارسات جيدة لدرء

---

(٩) A/CONF.222/RPM.1/1، الفقرة ٣٤؛ وA/CONF.222/RPM.2/1، الفقرة ٤٠؛ وA/CONF.222/RPM.3/1، الفقرة ٦١؛ وA/CONF.222/RPM.4/1، الفقرة ٧١.

(١٠) UNODC, *Comprehensive Study on Cybercrime*, p. 183.

(١١) CTOC/COP/2010/12، الفقرة ٣٣.

(١٢) انظر المبدأ التوجيهي ١٦ من المبادئ التوجيهية الدولية بشأن تدابير منع الجريمة والعدالة الجنائية فيما يتعلق بالاتجار بالممتلكات الثقافية وما يتصل به من جرائم أخرى.

تلك المخاطر، وكذلك لتسهيل التحرِّيات والتحقيقات واتخاذ الترتيبات اللازمة للتعويض على الضحايا أو جبر الأضرار الواقعة عليهم.

١٢- وتهدف ورقة المعلومات الأساسية هذه إلى اتخاذ الإطار المبيَّن في الوثيقة A/CONF.222/8 مُرتَكَزاً لتبيان الدروس المستفادة والنهوج المتَّبعة في التعاون الدولي بشأن الأنواع الناشئة من الجريمة السيبرانية والاتجار بالممتلكات الثقافية. وتتناول هذه الورقة بالبحث قاعدة المعارف المتعلقة بكل نوع من هاتين الجريمتين وماهية التحدِّيات القائمة والممارسات المتَّبعة في النهوج التشريعية الوطنية وطرائق التحرِّي والتحقيق وأشكال التعاون الدولي. وتحدِّد الورقة، عند الاقتضاء، نقاط الانطلاق المحتملة لمنع تلك الجرائم. كما تنظر في ماهية التدابير التي يمكن أن تتَّخذها الدول، والمجتمع الدولي ككل، تدعيماً لتدابير التصدِّي العالمية في مجالَيْ منع الجريمة والعدالة الجنائية.

ثانياً- الجريمة السيبرانية

ألف- استبانة التحدِّيات القائمة

١٣- في عام ١٩٩٤، ذُكر في دليل الأمم المتحدة لمنع الجريمة المتصلة بالحواسيب ومكافحتها أنَّ مدى انتشار الجرائم الحاسوبية قد يكون واسعاً بقدر اتِّساع نظم الاتصالات الدولية.[١٣] ومع أنَّ كلمة "الإنترنت" لم تُستخدَم في الدليل سوى مرة واحدة وأنَّ عبارة "الجريمة السيبرانية" لم تُستخدَم فيه بتاتاً، وهذا قد لا يكون أمراً مُستغرَباً، فقد انطوت استنتاجاته على قدر عظيم من الاستبصار. كما أنه بالرغم من تركيز الدليل على مفهوم "الجريمة الحاسوبية" فإنَّ من المسلَّم به أنَّ الجريمة السيبرانية بشكلها الحالي تعتمد بالفعل على تكنولوجيا التواصل المعلوماتي المعولمة، وخصوصاً الإنترنت، في ارتكاب أفعال إجرامية ذات نطاق دولي.

١٤- ومع تطوُّر المصطلحات المستخدَمة، جرى بذل جهود أكاديمية لتعريف تعبير "الجريمة السيبرانية".[١٤] ولا بدَّ لأيِّ نهج عصري في هذا الشأن أن يُسلِّم بأنَّ تعبير "الجريمة السيبرانية" ليس مصطلحاً قانونيًّا قائماً بذاته، بل هو تعبير جامع يشمل مجموعة أفعال مرتكَبة ضد

---

(١٣) *United Nations Manual on the Prevention and Control of Computer-related Crime*, International Review of Criminal Policy, Series M, Nos. 43-44 (United Nations publication, Sales No. E.94.IV.5), para. 12.

(١٤) انظر على سبيل المثال David Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Cambridge, Polity Press, 2007).

بيانات أو نظم حاسوبية أو باستخدامها. وثمة نهوج أخرى تركِّز على الجرائم المرتكَبة بحقِّ المعلومات الحاسوبية أو على استخدام موارد المعلومات لأغراض غير مشروعة.(١٥)

١٥- وتشمل الأفعال التي تندرج عادةً ضمن فئة "الجريمة السيبرانية"، تلك التي تكون فيها البيانات أو النظم الحاسوبية هي الشيء المستهدَف بالجرم، وكذلك الأفعال التي تشكِّل فيها النظم أو المعلومات الحاسوبية جزءاً أساسيًّا من وسائط ارتكاب الجرم. ومن أمثلة النوع الأول ما يُرتكَب من جرائم بحقِّ سرِّية البيانات أو النظم الحاسوبية وسلامتها وتَوافُرها، مثل أفعال الاقتحام غير المشروع للبيانات أو النظم الحاسوبية (والتي يشار إليها أحياناً بالجرائم السيبرانية "الصَّميمية"). ومن أمثلة النوع الثاني استخدام البيانات أو النظم الحاسوبية لأغراض الاحتيال أو السرقة أو إلحاق الأذى بالآخرين، وكذلك الجرائم المتصلة بالحاسوب ومحتوى الإنترنت، بما فيها جرائم الحضِّ على الكراهية واستخدام الأطفال في إنتاج مواد خلاعية والجرائم المتعلقة بالهوية وبيع السلع غير المشروعة بالاتصال الحاسوبي المباشر.(١٦)

١٦- غير أنَّ الحدَّ الفاصل بين الجريمة السيبرانية والجريمة التقليدية أخذ يزداد انطماساً على وجه الإجمال. فمع التزايد المطَّرد في انتشار الأجهزة الإلكترونية والتواصُلية العالمية في الحياة اليومية، أخذت الأدلة الإلكترونية، ومنها رسائل البيانات ورسائل البريد الإلكتروني وبيانات تَصفُّح الإنترنت وبيانات مواقع شبكات التواصُل الاجتماعي، تصبح شيئاً معتاداً في كثير من التحريات والتحقيقات الجنائية التقليدية. إذ إنَّ ما يُستخدَم في تلك الحالات من أدوات استدلال جنائي رقمية ومن طلبات إلى مقدِّمي الخدمات الإلكترونية، وكذلك الكثير من التحدِّيات المواجَهة وممارسات التحرِّي والتحقيق الجيِّدة كثيراً ما تكون هي نفس ما يُستخدَم في حالات الجريمة السيبرانية. وبذلك، ومع أنَّ هذه الورقة تركِّز على الأفعال التي يُرى عادةً أنها تشكِّل جريمةً سيبرانيةً فإنَّ لكثير من الآراء والاستنتاجات الواردة فيها مجال تطبيق أوسع نطاقاً فيما يتعلق بالأدلة الإلكترونية بصفة عامة.

١٧- ومن أهمِّ الدوافع الأساسية للجريمة السيبرانية المعاصرة ولازدياد استخدام الأدلة الإلكترونية تَطوُّرُ التواصُلية الإلكترونية على النطاق العالمي. ففي الوقت الحاضر، هناك قرابة ٣ بلايين مستعمل للإنترنت، وهذا يمثِّل نحو ٤٠ في المائة من سكان العالم. وغالبية هؤلاء يَصِلون إلى الإنترنت بواسطة أجهزة محمولة ذات نطاق تردُّدي عريض، بنسبة وُلوج قدرها

---

(١٥) انظر، مثلاً، الاتفاق المتعلق بالتعاون بين الدول الأعضاء في كومنولث الدول المستقلة لمكافحة الجرائم في مجال المعلومات الحاسوبية (لعام ٢٠٠١).

(١٦) UNODC, *Comprehensive Study on Cybercrime*, p. 16.

٣٢ في المائة من سكان العالم، أيْ أكثر بأربع مرات مما كانت عليها في عام ٢٠٠٩.[١٧] ويُتوقَّع أن يبلغ عدد الأجهزة الموصولة بشبكات بروتوكول الإنترنت بحلول عام ٢٠١٨ قُرابة ضعفي عدد سكان العالم.[١٨]

١٨- ومع أنَّ هذا النمو السريع في تكنولوجيا الإنترنت والحواسيب أتاح نموًّا اقتصاديًّا ووَسَّع سبل الوصول إلى خدمات حيوية مثل التعليم والرعاية الصحية والحوكمة الإلكترونية فقد فتح أيضاً إمكانيات جديدة للنشاط الإجرامي. فثمة أدوات للجريمة السيبرانية مثل شبكات "البوتْنت" (وهو تعبير مشتق من كلمتي "robot" و"network" الإنكليزيتين) يمكن أن تتألَّف، مثلاً، من شبكات عالمية تضمُّ عشرات الألوف أو مئات الألوف من الأجهزة الضحايا، كل منها موبوء ببرامجيات خبيثة يمكن أن يتحكَّم بها المجرمون عن بُعد. كما يمكن استخدام مواقع التواصُل الاجتماعي في المضايقة الإجرامية أو الحضِّ على الكراهية أو التهديد بالعنف أو الابتزاز أو نشر معلومات شخصية تخصُّ الأفراد على نطاق عالمي في غضون ثوان قليلة. وبما أنَّ المجرمين يسعون أيضاً إلى استهداف "إنترنت الأشياء" فإنَّ الإمكانيات العالمية المتاحة للنشاط الإجرامي يمكن أن تستمر في التزايد.

١٩- وإلى جانب الطابع العالمي لهذا التحدِّي، شهد العقد الأخير أيضاً تفاوتات دورية في مدى ما توفِّره الإنترنت من إخفاء للهوية، مع ما ترتَّب على ذلك من إمكانية استخدامها في ارتكاب أفعال إجرامية. ففي أيام الإنترنت الأولى، كان هناك افتراض واسع النطاق بأنَّ الإنترنت توفِّر درجةً عاليةً من إخفاء الهوية، على الأقل ما دام المستعملون لا يفهمون الإمكانيات التقنية التي تتيح تعقُّب النشاط التواصُلي عبر الإنترنت وصولاً إلى الأفراد القائمين به. غير أنَّ نظم العدالة الجنائية أصبحت في السنوات الأخيرة أكثر اعتياداً على مفهومَي عناوين بروتوكول الإنترنت وسجلات الاتصال، وعلى استخدام أوامر المحاكم للحصول على بيانات من مقدِّمي الخدمات الإلكترونية. ونتيجةً لذلك، أصبح المحقِّقون أكثر قدرةً على الوصول إلى الآثار الإلكترونية التي يُخلِّفها مستعملو الإنترنت، مع أنَّ الحصول على بيانات الإنترنت قد يتطلَّب كثيراً من الوقت والجهد. وعلى نحو مماثل، كان لأوجه التقدُّم في أدوات الاستدلال الجنائي الرقمية، ومنها الأدوات السهلة التركيب على الحاسوب والمسمَّاة بالإنكليزية "plug-and-play"، وهي أدوات يَسهُل استعمالها، دور في تيسير التحليل الروتيني للبيانات المخزونة في أجهزة رقمية مثل الحواسيب والهواتف الذكية المحمولة.

(١٧) International Telecommunication Union, “The World in 2014: ICT facts and figures” (Geneva, 2014).

(١٨) Cisco, “The zettabyte era: trends and analysis”, Cisco Visual Networking Index (San Jose, California, 2014).

٢٠- ونظراً لأنَّ التكنولوجيا تتقدَّم باستمرار، تواجه أدوات الاستدلال الجنائي والنهوج المتَّبعة حاليًّا في التحرِّي عن الجرائم السيبرانية تحدِّيات ما كان يمكن تَوقُّعها قبل عقد من الزمن. فالبرامجيات المجَّانية والمتيسِّرة على نطاق واسع، مثلاً، تتيح تشفيراً لملفَّات منفردة أو لأدوات تخزين بيانات كاملة بحجم تشفير قدره ٢٥٦ بِتًّا. وبدون كلمة سر أو مفتاح، يكون الوصول إلى البيانات المشفَّرة على هذا النحو أمراً مستعصياً تقريباً على أجهزة إنفاذ القانون. أمَّا التشفير الأكثر تقدُّماً، القائم على استخدام تشفير بحجم ٢٠٤٨ بِتًّا، فيمثِّل حتى الآن من الناحية النظرية عقبةً يتعذَّر تخطِّيها. وتعمل الشبكات اللامركزية الجديدة لإخفاء الهوية، التي كثيراً ما يشار إليها بـ "الشبكة المُعتِمة"، جنباً إلى جنب مع الإنترنت التقليدية. وثمة خدمات مثل برنامج إخفاء الهوية ("Onion Router" المعروف باسم "تور" (Tor)) تجعل تحديد منشأ الخطابات الإلكترونية، أو استبانة المواقع الشبكية التي تَستخدِم "خدمة خَفِيَّة"، أمراً بالغ الصعوبة على كثير من سلطات إنفاذ القانون. فهذه الخدمات الخفيَّة يمكن أن تُستخدَم لاستضافة أسواق إنترنت غير مشروعة للاتجار بالمخدِّرات أو الأسلحة أو المواد الخلاعية المستغِلَّة للأطفال دون كشف هوية القائمين عليها. كما يتيح بعض تلك الشبكات إمكانية تخزين البيانات المشفَّرة تخزيناً لامركزيًّا في "عُقَد" خاصة بالشبكات المشاركة. والوصول إلى الوثائق أو الصور الإلكترونية المخزَّنة على هذا النحو يكاد يكون، مرة أخرى، أمراً مستعصياً على أجهزة إنفاذ القانون. ولاستخدام تكنولوجيا من هذا القبيل تداعيات عميقة على أجهزة إنفاذ القانون تطرح مسألة الكيفية الفضلى التي يمكن بها لتدابير التصدِّي التي تتَّخذها تلك الأجهزة أن تواكب إيقاع الابتكارات في مجال الجريمة السيبرانية.

باء- قياس الجريمة السيبرانية

٢١- ثمة نهج لقياس الأشكال والأبعاد الجديدة للجريمة، بما فيها الجريمة السيبرانية، يتطلَّب توليفةً من المقاييس، مثل المعلومات المتعلقة بالمرتكبين والمعلومات المتعلقة بالتدفُّقات داخل الأسواق غير المشروعة والمعلومات المتعلقة بأعداد الأحداث الإجرامية وما تسبِّبه من أضرار وخسائر وما ينتج عنها من تدفُّقات مالية غير مشروعة. وفي حالة الجريمة السيبرانية، يمكن في هذا الشأن استخدام عدد من مصادر البيانات، منها إحصاءات الجرائم المسجَّلة لدى الشرطة والاستقصاءات الخاصة بالسكان والمنشآت التجارية والمبادرات الخاصة ببلاغات الضحايا والمعلومات الخاصة بالأمن السيبراني القائم على التكنولوجيا. وثمة مصادر أخر تشمل أيضاً أساليب مثل الزحف على عناوين الموارد الموحَّدة (URL crawling) وانتزاع السيطرة على شبكات البوتنت (botnet takeover).

٢٢- ومع أنه لا ينبغي صرف النظر عن إحصاءات الجرائم السيبرانية المسجَّلة لدى الشرطة فمن الواضح أنَّ فيها عيوباً ذات شأن، لأنَّ معظم حالات الإيذاء لا تُبلَّغ إلى الشرطة. ففي استقصاء شمل ٢٠ ٠٠٠ مستعمل للإنترنت في ٢٤ بلداً، كانت نسبة الأشخاص الذين أبلغوا الشرطة ممن قالوا إنهم وقعوا ضحيةً لجريمة سيبرانية لا تزيد على ٢١ في المائة من المستجيبين.[١٩] وعلى الصعيد العالمي، قد تَستخدم أجهزة إنفاذ القانون منهجيات وأساليب إحصائية مختلفة، مما يجعل المقارنات الدولية أمراً صعباً. وإلى جانب ذلك، يرتبط المقدار الإجمالي للجرائم السيبرانية المسجَّلة لدى الشرطة ارتباطاً شديداً بعدد وحدات الشرطة المتخصِّصة، وهذا يدلُّ على أنَّ تلك الإحصاءات يمكن أن تكون مؤشِّراً لأنشطة التحرِّي التي تقوم بها الشرطة، لا إلى مقدار حالات الإيذاء الناشئة عن الجرائم السيبرانية.[٢٠]

٢٣- وتوفِّر استقصاءات الإيذاء الخاصة بالأفراد والمنشآت التجارية والتي تتناول فئات محدَّدة من عامة السكان مصدراً بديلاً مهمًّا للمعلومات. وتدلُّ تلك الإحصاءات على أنَّ حالات تَأَذِّي عامة السكان بالجريمة السيبرانية هي أكثر بكثير من تَأَذِّيهم بأشكال الجرائم "التقليدية". إذ إنَّ نسب التأذِّي من الاحتيال المتعلق ببطاقات الائتمان عبر الإنترنت وسرقة الهوية والاستجابة لمحاولات التصيُّد الاحتيالي والتعرُّض لحالات نفاذ غير مأذون به إلى حساب البريد الإلكتروني تتراوح بين ١ و١٧ في المائة من إجمالي مستعملي الإنترنت في ٢١ بلداً من مختلف أنحاء العالم، في حين أنَّ نسبة المتأذِّين بالجرائم المعتادة، مثل السطو والسلب وسرقة السيارات تقلُّ عن ٥ في المائة في البلدان ذاتها.[٢١] وتفيد منشآت القطاع الخاص أيضاً عن نسب إيذاء مماثلة. ففي أوروبا، مثلاً، تفيد المنشآت عن نسب تعرُّض للإيذاء تتراوح بين ٢ و١٦ في المائة نتيجةً لأفعال مثل انتهاك البيانات الناشئ عن الاقتحام أو التصيُّد الاحتيالي.[٢٢] وتَبيَّن من دراسة أُجريت في عام ٢٠١٢ أنَّ عدد ضحايا الاحتيال المتعلق بالهوية ازداد بما يزيد على ١ مليون ضحية، سرق فيها الجناة ما يزيد على ٢١ بليون

(١٩) Symantec, “Norton Cybercrime Report”, 2012. متاح في الموقع الشبكي http://us.norton.com/cybercrimereport.

(٢٠) UNODC, *Comprehensive Study on Cybercrime*, annex 2.

(٢١) الدراسة الاستقصائية وفَّرتها شركة "سيمانتك" (Symantec).

(٢٢) Eurostat, Information society statistics, Community survey on ICT usage and e-commerce in enterprises, 2011. متاح في الموقع الشبكي http://ec.europa.eu/eurostat/web/informationsociety/data/database.

دولار، وهذا أكبر مبلغ منذ عام ٢٠٠٩، وإن كان أدنى بكثير من الخسائر في عام ٢٠٠٤، والتي قُدِّرت بنحو ٤٧ بليون دولار.[٢٣]

٢٤- ويمكن استخدام البيانات المستمدَّة من الاستقصاءات، والتي تتضمَّن معلومات عن الخسائر المالية المتكبَّدة بسبب الجرائم السيبرانية، لوضع تقديرات لآثار الجريمة السيبرانية. ففي أحد الاستقصاءات، أفاد المستهلكون الضحايا في ٢٤ بلداً من مختلف أنحاء العالم عن خسائر مباشرة يتراوح متوسطها بين ٥٠ و٨٥٠ دولاراً في سنة واحدة نتيجةً للوقوع ضحية لجريمة سيبرانية واحدة أو أكثر.[٢٤] وتفيد تقديرات دراسة أخرى، استَخدَمت بيانات مستمدَّة من عدَّة استقصاءات، بأنَّ الحجم الإجمالي للتكاليف المباشرة وغير المباشرة والدفاعية المرتبطة بعدد من أشكال الجريمة السيبرانية، بما فيها الاحتيال المصرفي عبر الإنترنت والاحتيال بواسطة بطاقات الدفع عبر الإنترنت والاحتيال باشتراط دفع الرسوم مسبقاً، يبلغ مئات الملايين، إن لم يكن آلاف الملايين، من الدولارات سنويًّا.[٢٥]

٢٥- ويتيح تحليل أسواق الجريمة السيبرانية أيضاً إمكانيات لتقدير طبيعة ونطاق بعض أشكال الجريمة السيبرانية. ويركِّز أحد تلك النهوج على تحليل منتديات الإنترنت التي تعمل في صورة "شبكات تواصُل اجتماعي" إجرامية من أجل بيع وشراء سلع اجتماعية وتقاسم معلومات إجرامية.

٢٦- وثمة دراسة أُجريت في عام ٢٠١١ واستَخدمت بيانات مستمدَّة من ستة منتديات شبكية سرِّية، احتوت على ما يزيد على ٢ ٥٠٠ ٠٠٠ رسالة عامة و٩٠٠ ٠٠٠ رسالة خاصة من ١٠٠ ٠٠٠ مستعمل. وكان من أشيع البضائع المتاجَر بها بطاقات ائتمان وبيانات حسابات مصرفية وأدوات تُستخدَم في ارتكاب أفعال احتيالية.[٢٦] ويدلُّ تحليل أُجري أخيراً لخيوط مأخوذة من ١٣ منتدىً شبكيًّا على أنَّ قوائم بيانات بطاقات الائتمان المسروقة تُعرَض على الإنترنت بسعر وسطي يقارب ١٠٠ دولار، وأنه يمكن شراء أدوات إجرامية،

---

(٢٣) Javelin Strategy and Research, “2013 Identity Fraud Report: Data Breaches becoming a treasure trove for fraudsters”. متاح على الرابط الشبكي www.javelinstrategy.com/brochure/276.

(٢٤) الدراسة الاستقصائية وفَّرتها شركة "سيمانتك" (Symantec).

(٢٥) Ross Anderson and others, “Measuring the cost of cybercrime”, in *The Economics of Information Security and Privacy*, Rainer Böhme, ed. (Springer Berlin Heidelberg, Berlin, 2013).

(٢٦) Marti Motoyama and others, “An analysis of underground forums”, in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (New York, ACM, 2011).

مثل "مَقاشِد" بطاقات الائتمان بسعر وسطي قدره ٤٠٠ ٢ دولار.[٢٧] وهناك أيضاً تكنولوجيات بحثية جديدة تتيح إمكانية الزحف الشبكي لخدمات Tor الخفيَّة. وهذا يمكن أن يسهِّل التحديد والتصنيف المنهجي لأعداد وأنواع المواقع الشبكية الخفيَّة ذات الصلة بمواضيع مثل بيع المخدِّرات غير المشروعة واستغلال الأطفال في إنتاج مواد خلاعية وبيع الأسلحة وأدوات الجريمة السيبرانية.[٢٨]

٢٧- وأخيراً، من شأن تحديد سمات الجناة أن يساعد على فهم طبيعة التنظيمات الإجرامية التي تقف خلف تلك الأفعال وعلى كشف أساليب عملها. ومن المرجَّح ألاَّ تكون لها سمات نمطية في هذا الشأن. إذ يمكن لعدد صغير نسبيًّا من المبرمجين والقراصنة ذوي المهارة العالية أن يدفعوا خطى الابتكار في مجال الجريمة السيبرانية ويعرضوا مهاراتهم في شكل خدمة إجرامية. غير أنَّ توافر عُدد الأدوات والبرامجيات الخبيثة يعني أنَّ كثيراً من الجناة لا يعودون في حاجة إلى معارف متقدِّمة. كما أنَّ أشكال الجريمة السيبرانية يمكن أن تتطلَّب، بصورة متزايدة، أعداداً كبيرةً من "الجنود المشاة" ذوي المستوى المنخفض. ففي أحد مخطَّطات الاحتيال ببطاقات الخصم المسبقة الدفع التي اكتُشفت أخيراً، جنَّدت الجماعة الإجرامية المنظَّمة مئات من الأشخاص في ٢٦ بلداً، مما أفضى إلى ما يزيد على ٠٠٠ ٤٠ عملية سحب متزامنة من آلات صرف نقود في مناسبتين منفصلتين. وبذلك سُرق مبلغ يُقدَّر بنحو ٤٥ مليون دولار.[٢٩] ومع أنَّ ما يزيد على ٨٠ في المائة من الجرائم السيبرانية يمكن أن يكون منشؤها في أوساط الجريمة المنظَّمة،[٣٠] فمن الواضح أنَّ التنوُّع الواسع لهياكل تلك المجموعات، بما فيها الرابطات الإجرامية ذات التنظيم الأقل إحكاماً، يمكن أن يمثِّل تحدِّياً أمام أيِّ تحديد مباشر لسمات مرتكبي الجرائم السيبرانية.

---

(٢٧) Thomas Holt and Olga Smirnova, “Examining the structure, organization, and processes of the international market for stolen data”, research paper prepared for the National Institute of Justice, Rockville, Maryland, United States of America, March 2014.

(٢٨) Martijn Spitters and others, “Towards a comprehensive insight into the thematic organization of the ToR hidden services”, paper presented at the IEEE Joint Intelligence and Security Informatics Conference, The Hague, September 2014.

(٢٩) INTERPOL, “Criminal network involved in payment card fraud dismantled with INTERPOL support”, 30 April 2014. متاحة على الرابط الشبكي www.interpol.int/News-and-media/News/2014/N2014-074.

(٣٠) BAE Systems Detica and the John Grieve Centre for Policing and Community Safety, *Organised Crime in the Digital Age* (London Metropolitan University, 2012).

جيم- منع الجريمة السيبرانية ومكافحتها

٢٨- تمثِّل المعلومات المتعلقة بطبيعة الجريمة السيبرانية ونطاقها عنصراً مهمًّا في صوغ استراتيجيات فعَّالة لمنع تلك الجرائم والتحرِّي عنها. فاستراتيجيات التوعية الرامية إلى منع الاحتيال الاستهلاكي عبر الإنترنت، مثلاً، قد يتطلَّب اتِّباع نهج مغاير لتدابير التوعية في مجال حماية الأطفال من الجرائم المرتكَبة عبر الإنترنت. وفي هذا الصدد، أُوصي في الاجتماعات الإقليمية التحضيرية للمؤتمر الثالث عشر باستحداث أدوات وبرامج يمكن أن تسهِّل التوعية بالجريمة السيبرانية ومنعها. كما أنَّ المعلومات عن أخطار الجريمة السيبرانية واتجاهاتها يمكن أن يُسترشد بها في تدابير التحرِّي المضادة. إذ إنَّ التحرِّي عن بيع المخدِّرات غير المشروعة عبر الإنترنت، مثلاً، يتطلَّب مهارات وتقنيات مغايرة لتلك المستخدَمة في فحص الأجهزة الحاسوبية لأغراض الاستدلال الجنائي. ومع أنَّ البيانات المتاحة عن الجريمة السيبرانية يمكن أن تساعد على تركيز الجهود من أجل التصدِّي للاتجاهات المستجدَّة، فإنَّ تنوُّع الجرائم السيبرانية المحتملة يتطلَّب من البلدان أن تنمِّي قدرات تشمل طائفةً واسعةً من تدابير المنع والتحرِّي المضادة.

٢٩- وإلى جانب قدرات قياس الجريمة السيبرانية، ينبغي اتخاذ تدابير وطنية مضادة لها ضمن مجالَي الإطارين التشريعي والسياساتي، بما فيها التجريم ومنح الصلاحيات الإجرائية؛ وبناء قدرات أجهزة إنفاذ القانون ونظم العدالة الجنائية في مجال التحرِّي عن الجرائم السيبرانية والتحقيق فيها، وعمليات الاستدلال الجنائي الرقمية، وكيفية التعامل مع الأدلة الإلكترونية؛ وآليات التعاون الدولي في المسائل الجنائية؛ ومنع الجريمة السيبرانية.

٣٠- وتمثِّل السياسات والاستراتيجيات والتشريعات الوطنية الخاصة بالجريمة السيبرانية نقطة انطلاق في إرساء إطار وأولويات تدابير التصدِّي للجريمة السيبرانية. وسوف يحتوي مستودع مكتب المخدِّرات والجريمة الإلكتروني الخاص بالجريمة السيبرانية (الذي سيصدر في عام ٢٠١٥) معلومات مفصَّلة عن الاستراتيجيات الوطنية المستبانة في نحو ٥٠ بلداً، تشمل مجالات مثل التوعية بالجريمة السيبرانية، والتعاون الدولي، وقدرات إنفاذ القانون، والتشريعات، وتدابير المنع، والشراكات بين القطاعين العام والخاص. كما أنَّ التشريعات الوطنية الخاصة بالجريمة السيبرانية كثيراً ما تشمل مجالات عدَّة، منها التجريم والصلاحيات الإجرائية، والولاية القضائية، والأدلة الإلكترونية، والتعاون الدولي. ويَتبيَّن من استعراض القوانين الوطنية المتعلقة بالجريمة السيبرانية أنَّ تلك الجريمة مجرَّمة من خلال توليفة من الأحكام التي تتناول الأفعال الإجرامية الخاصة بالفضاء الحاسوبي والأفعال الإجرامية العامة. فالأفعال التي تُعتبر جرائم سيبرانية "صميمية"، مثل النفاذ غير المشروع إلى البيانات والنظم الحاسوبية، قد تكون مجرَّمةً من خلال أحكام قانونية خاصة، أمَّا الأفعال المتصلة بالحاسوب والمرتَكَبة

للحصول على مكسب شخصي أو مالي أو لإحداث ضرر فمن الأشيع أن تجرَّم بأحكام تتناول الأفعال الإجرامية العامة (غير الخاصة بالحاسوب).[٣١]

٣١- وفي بعض الحالات، تكون الأُطر القانونية الوطنية مشترَعة بمقتضى صكوك متعدِّدة الأطراف، ملزمةً أو غير ملزمة، أو مستوحاة منها. وتشمل تلك الصكوك: اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية؛ والاتفاق المتعلق بالتعاون بين الدول الأعضاء في كومنولث الدول المستقلة بشأن مكافحة الجرائم المتعلقة بالمعلومات الحاسوبية؛ واتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية؛ والإيعاز 2013/40/EU الصادر عن البرلمان الأوروبي والمجلس الأوروبي بشأن الهجمات على نظم المعلومات؛ والاتفاقية العربية لمكافحة جرائم تقنية المعلومات؛ واتفاق منظمة شانغهاي للتعاون في ميدان أمن المعلومات على الصعيد الدولي. وفيما يتعلق بإمكانية استحداث أُطر أخرى متعدِّدة الأطراف، أوصى اجتماع أفريقيا الإقليمي التحضيري للمؤتمر الثالث عشر بأن تنظر الدول في وضع اتفاقية بشأن الجريمة السيبرانية ضمن سياق المؤتمر الثالث عشر.

٣٢- وإلى جانب الأحكام المتعلقة بالتجريم والصلاحيات الإجرائية، يمكن أن تتضمَّن الصكوك الموجودة أيضاً آليات للتعاون الدولي في التحرِّي عن الجرائم السيبرانية وملاحقتها قضائيًّا عبر الحدود. ويمثِّل هذا المجال تحدِّياً متنامياً أمام سلطات إنفاذ القانون. ويعني ظهور الحوسبة السحابية وتقاسم البيانات وتخزينها بين النظراء أنه على الرغم من أنَّ مكان وجود بيانات حاسوبية معيَّنة قد يكون من الناحية النظرية قابلاً للتحديد في نقطة زمنية معيَّنة، يمكن أن تكون البيانات موجودةً في نسخ متعدِّدة وأن تكون موزَّعةً في أجهزة وأماكن متعدِّدة، كما يمكن أن تُنقَل إلى موقع جغرافي آخر في غضون ثوان قليلة.

٣٣- وقد يكون بعض مقدِّمي خدمات تخزين البيانات، مثل مقدِّمي الخدمات الإلكترونية أو خدمات الحوسبة السحابية التابعين للقطاع الخاص، ملزمين قانوناً بأن يحتفظوا بنسخ من البيانات لفترة زمنية معيَّنة ومن شأنهم عادةً أن يقدِّموا تلك البيانات إلى سلطات إنفاذ القانون عملاً بأمر من محكمة أو بمقتضى عملية قانونية ملائمة أخرى. غير أنه عندما يكون أيٌّ من مقدِّم الخدمة أو البيانات نفسها موجوداً خارج الولاية القضائية القائمة بالتحرِّيات، كثيراً ما تكون تلك العملية القانونية منطويةً على استخدام إجراءات رسمية مطوَّلة لتبادل المساعدة القانونية بين الدول. وفي حال استخدام وسائط أخرى لتخزين البيانات، كما في حالة التخزين من جانب الأفراد في شبكة حاسوبية بين نظراء، قد يَصعُب في المقام الأول

(٣١) UNODC, *Comprehensive Study on Cybercrime*, p. 78.

استبانة البيانات لأنها كثيراً ما تكون مخزَّنةً في شكل مُشفَّر. وقد يلزم اتخاذ تدابير قسرية ضد الفرد المعني من أجل تأمين البيانات والإفراج عنها.

٣٤- ويجري على الصعيد الدولي نقاش متعدِّد المستويات حول المذهب المتَّبع حاليًّا، الذي يقوم أساساً على فكرة التبعية الإقليمية، بشأن التحرِّي عن الجرائم السيبرانية وتيسير الوصول إلى البيانات عبر الحدود الوطنية.[٣٢] فبعض الصكوك الموجودة المتعدِّدة الأطراف ترسي آليات تهدف إلى تيسير الوصول إلى البيانات أمام أجهزة إنفاذ القانون، مثل نقاط اتصال متاحة على مدار الساعة تُعنى بالتحرِّيات عن الجرائم السيبرانية، وتعجيل عمليات حفظ البيانات، وتيسير الوصول المأذون عبر الحدود الوطنية إلى البيانات الحاسوبية المخزَّنة أو حيثما تكون متاحةً لعامة الناس، وإمكانية توجيه طلبات عاجلة للمساعدة المتبادلة. أمَّا من الناحية العملية، فمن الواضح أنَّ كثيراً من أجهزة إنفاذ القانون تُواجِه، حتى مع وجود تلك الآليات، صعوبات كبيرة في اكتساب إمكانية الوصول في الوقت المناسب إلى البيانات الموجودة خارج نطاق إقليمها أثناء التحرِّي عن الجرائم السيبرانية. وفي الوقت نفسه، يجب أن تكون ضمانات حقوق الإنسان وسيادة القانون وصون الحرمة الشخصية كافيةً لضمان أن يكون ذلك الوصول إلى البيانات من جانب أجهزة إنفاذ القانون محدَّداً وقابلاً للتنبُّؤ ومتناسباً وخاضعاً لرقابة وافية.

٣٥- ومن شأن ابتكارات مثل إدراج نميطة الأدلة الرقمية في الصيغة الجديدة لأداة كتابة طلبات المساعدة القانونية المتبادلة، التي استحدثها مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة، أن تساعد على تبسيط عمليات تبادل المساعدة القانونية المتعلقة بالأدلة الإلكترونية. ولكنْ، في موازاة ذلك، قد يتعيَّن على أجهزة إنفاذ القانون، بصورة متزايدة، أن تعثر على سبل ريادية للتعاون في التحرِّيات عبر الوطنية عن الجرائم السيبرانية. وربما كان إشراك كيانات مثل المجمَّع العالمي للابتكار، التابع للإنتربول، والمركز الأوروبي لشؤون الجريمة السيبرانية، التابع لمكتب الشرطة الأوروبي (اليوروبول)، في تنسيق التحرِّيات عبر الوطنية ودعمها، بوسائل منها تسهيل تقاسم المعلومات بين سلطات إنفاذ القانون الوطنية، ذا أهمية بالغة في هذا الشأن. وثمة محافل ومبادرات أخرى، مثل المؤتمر العالمي المعني بالفضاء السيبراني،

(٣٢) انظر، مثلاً، Council of Europe, “Cybercrime Convention Committee assessment report: the mutual legal assistance provisions of the Budapest Convention on Cybercrime”, document T-CY(2013)17rev, and “Transborder access to data and jurisdiction: options for further action by the Cybercrime Convention Committee”, document T-CY(2014)16, and Albert Rees, “International cooperation in cybercrime investigations”, presentation prepared for the Organization of American States Regional Cyber Crime Workshop, April 2007.

قد أتاحت أيضاً للبلدان فرصة النظر في تدابير مبتكرة في مجال التعاون الدولي على مكافحة الجريمة السيبرانية.

٣٦- ويجب أيضاً أن يكون القطاع الخاص طرفاً في الشراكات الرامية إلى منع الجريمة السيبرانية ومكافحتها، سواء أعُقدت على صعيد متعدِّد الأطراف أم على صعيد وطني. ويمكن لمقدِّمي خدمات الإنترنت وخدمات الاستضافة أن يقوموا بدور محوري في منع الجريمة السيبرانية. إذ إنَّ بوسعهم أن يحتفظوا بسجلات يمكن استخدامها في التحرِّي عن النشاط الإجرامي، وأن يساعدوا الزبائن على اعتماد ممارسات آمنة في استخدام الإنترنت وعلى استبانة الحواسيب المعبوث بها، وأن يحجبوا بعض أنواع المحتويات الخبيثة، وأن يساعدوا، بصفة عامة، على توفير بيئة اتصالات آمنة لزبائنهم. وهناك عدَّة نماذج للشراكات بين القطاعين العام والخاص، منها مثلاً الشراكات بين أجهزة إنفاذ القانون ومقدِّمي الخدمات الإلكترونية. ويقوم كثير من تلك الشراكات على تقاسم المعلومات استناداً إلى قواعد واضحة، وعلى الثقة ومحدودية العضوية وتشجيع المنفعة والتجاوبية المتبادلتين. وفي بعض الحالات، توفِّر هيئات الصناعة ذات العضوية الحصرية، مثل التحالف البيئي في مجال الأمن السيبراني، منصَّات لكي تنخرط الصناعة مع الحكومات في مجالي الأمن السيبراني ومكافحة الجريمة السيبرانية.

٣٧- وأخيراً، من الهام جدًّا بناء القدرات على صعيد أجهزة إنفاذ القانون ونظم العدالة الجنائية الوطنية. ومع أنَّ غالبية البلدان قد شَرَعت في إنشاء هياكل متخصِّصة للتحرِّي عن الجرائم السيبرانية والجرائم المنطوية على أدلة إلكترونية، فإنَّ هذه الهياكل في كثير من البلدان تعاني من نقص التمويل والقدرات. ونظراً لأنَّ الأدلة الرقمية أخذت تزداد انتشاراً في التحرِّي عن الجرائم "التقليدية"، فقد يتعيَّن على سلطات إنفاذ القانون أن تميِّز بوضوح بين الجهات التي تتولَّى التحقيق في الجرائم السيبرانية والجهات المسؤولة عن مختبرات الاستدلال الجنائي الرقمي، وأن تحدِّد موضوع مهام كلٍّ من تلك الجهات. وقد يحتاج موظفو الخطوط الأمامية في أجهزة إنفاذ القانون، بصورة متزايدة، إلى اكتساب واستخدام مهارات أساسية مثل تلك التي تُستخدَم في إنتاج صورة لأداة التخزين الإلكترونية تَصلُح للاستدلال الجنائي.

٣٨- ونظراً لأنَّ التطوُّرات التكنولوجية الجديدة، مثل الشبكات المُخفية للهوية والتشفير العالي الدرجة والعملات الافتراضية أخذت تصبح شيئاً معتاداً في الجرائم السيبرانية، فسوف يتعيَّن أيضاً على المحقِّقين أن يعتمدوا استراتيجيات جديدة. إذ يمكن لسلطات إنفاذ القانون، مثلاً، أن يعملوا على تدعيم الشراكات مع أفرقة البحث الأكاديمي التي تركِّز على استحداث منهجيات تقنية في مجالات مثل تحديد سمات المعاملات التي تُجرى بالعملات الافتراضية

والتحرِّي عنها.[٣٣] وربما يتعيَّن أيضاً على المحقِّقين أن ينظروا في الكيفية التي يمكن بها استخدام أساليب التحرِّي الخاصة، مثل المراقبة والعمليات المستترة واستخدام المُخبرين والتسليم المراقب، في حالة بيع سلع غير مشروعة عبر الإنترنت جنباً إلى جنب مع التحرِّيات الخاصة بالإنترنت وتقنيات الاستدلال الجنائي الرقمي. ومن الواضح إجمالاً أنَّ بناء قدرات الجهات المعنية بإنفاذ القانون والعدالة الجنائية في مجال مكافحة الجريمة السيبرانية سيكون عمليةً جاريةً ومتواصلةً، مع استمرار ظهور الابتكارات التكنولوجية والإجرامية بإيقاع سريع.

ثالثاً- الاتجار بالممتلكات الثقافية

ألف- تحديد ماهية التحدِّي

٣٩- تُعتبَر حماية الممتلكات الثقافية واحداً من أكبر التحدِّيات القائمة أمام سياسات العدالة الجنائية المعاصرة. فقد أصبح يُنظَر إلى الممتلكات الثقافية لا بصفتها مجرَّد موجودات قيِّمة تخصُّ "بلدان المنشأ" بل هي قَيِّمة أيضاً للجنس البشري كله وتستحقُّ أن تُحمى وتُصان، لكونها مورداً لزيادة المعارف التاريخية ولإسهامها في تشكيل الهوية الثقافية ولما لها من دور في الأعراف الاجتماعية. ومن هنا يأتي الاهتمام المتزايد الذي تُوليه الأمم المتحدة وكثير من المنظمات الدولية لهذه الظاهرة، والتزام الدول بصوغ وتنفيذ صكوك قانونية دولية تستهدف حماية الممتلكات الثقافية.

٤٠- وقد يكون السلوك المحدِّد الذي يمكن أن يُنسَب إلى الاتجار بالممتلكات الثقافية أكثر جلاءً منه في حالة الجرائم السيبرانية، ولكنْ ثمة تحدِّيات كبيرة في البحث في نطاق هذه المسألة وحجمها. وهذه التحدِّيات لها صلة بالتحرِّي عن أنواع كثيرة من الجرائم المنظَّمة؛ إذ تشمل تَعقُّد العمليات غير المشروعة، ونقص القدرات والوعي لدى أجهزة إنفاذ القانون، والفساد. كما أنَّ تَجاوُر الأنشطة غير المشروعة المتعلقة بتصدير الممتلكات الثقافية المسروقة مع عناصر من السوق المشروعة للقطع الفنِّية والتحف التاريخية وطرائق عملها في كثير من البلدان يتطلَّب جهوداً إضافيةً. وتتفاقم هذه الصعوبات عندما يتعلق الأمر بممتلكات ثقافية مهرَّبة من عمليات تنقيب غير مشروعة في مواقع أثرية، إذ قد يكون تحديد منشأ القطع الأثرية أمراً بالغ الصعوبة.

---

(٣٣) انظر، مثلاً، Sarah Meiklejohn and others, “A fistful of bitcoins: characterizing payments among men with no names”, in *Proceedings of the 2013 ACM SIGCOMM conference on Internet measurement conference* (New York, ACM, 2013).

٤١- وقد بُذلت جهود لجمع بيانات عن الاتجار بالممتلكات الثقافية ولكشف الطرائق التي تستخدمها الجماعات الإجرامية. فعلى سبيل المثال، أُجريت في عام ٢٠٠٩ دراسة استخدمت بيانات مستمدَّة من قاعدة بيانات البنك الدولي الخاصة بالحل العالمي المتكامل لمسائل التجارة، التي تتضمَّن بيانات عن أشياء يزيد عمرها على ١٠٠ سنة، من أجل وضع نماذج تجريبية تُوضِّح كيفية تهريب القطع الفنِّية والتحف التاريخية.[٣٤] ودَلَّت تلك الدراسة على وجود صلة قوية بين الفساد واحتمالات نقص الإبلاغ عن صادرات التحف التاريخية، وهو مؤشِّر قوي على حدوث تهريب.

٤٢- وثمة نهج آخر تَمثَّل في التركيز على رسم خرائط للأسواق غير المشروعة للممتلكات الثقافية وقياس أحجامها. وتناولت بعض الدراسات الجانب المتعلق بالطلب من تلك الأسواق، بأن رَكَّزت على عمليات بيع القطع الفنِّية والتحف التاريخية في بيوت المزادات وحاولت تحديد مصدر تلك القطع والسجل التاريخي لملكيتها. فعلى سبيل المثال، ثمة دراسة أُجريت في عام ٢٠٠٢ ركَّزت على أكثر من ١٨ ٠٠٠ قطعة من الخزفيات اليونانية بِيعت في بيوت المزادات في الولايات المتحدة الأمريكية والمملكة المتحدة لبريطانيا العظمى وإيرلندا الشمالية بين عامي ١٩٥٤ و١٩٩٨، فتَبَيَّن منها أنَّ ما بين ٨٠ و٩٠ في المائة من تلك القطع ليس لها سجل نَشأة (أيْ أنه قد تَعَذَّر تَعقُّب سلسلة ملكيتها الشرعية إلى اللُّقْيَة الأصلية).[٣٥] وعدم وجود سجل نشأة ليس في حدِّ ذاته دليلاً على التهريب، بل يمثِّل عاملَ اشتباه مُهمًّا. وثمة دراسات أخرى للأسواق غير المشروعة تُركِّز على العرض، وغالباً ما يجري ذلك من خلال فحص المواقع الأثرية المنهوبة وتوثيقها. وبعض هذه الدراسات تتَّبع المنهجيات التقليدية لعلم الاجتماع والسلوك، والتي تشمل إجراء بحوث ميدانية تهدف إلى توثيق حالة المواقع الأثرية في بلدان معيَّنة. وفي الآونة الأخيرة، أتاح استخدام سواتل تجارية عالية القدرة إجراء مسوح أكثر تواتراً وأوسع نطاقاً لتلك المواقع بحثاً عن علامات دالة على النهب. فعلى سبيل المثال، أُجريت في عام ٢٠٠٨ سلسلة دراسات استُخدمت فيها تقنيات التصوير الرقمي من أجل توثيق مدى النهب الذي تعرَّضت له المواقع الأثرية في العراق.[٣٦]

---

(٣٤) Raymond Fisman and Shang-Jin Wei, “The Smuggling of Art, and the Art of Smuggling: Uncovering the Illicit Trade in Cultural Property and Antiques”, *American Economic Journal: Applied Economics*, vol. 1, No. 3 (July 2009), pp. 82-96.

(٣٥) Vinnie Nørskov, *Greek Vases in New Contexts* (Aarhus, Denmark, Aarhus University Press, 2002).

(٣٦) Elizabeth Stone, “Patterns of looting in southern Iraq”, *Antiquity*, vol. 82, No. 315 (March 2008), pp. 125-138.

٤٣- وتناولت بعض الدراسات أيضاً مختلف مراحل سلسلة التوريد غير المشروع للممتلكات الثقافية المتَّجَر بها. فَركَّز بعضها على أولئك الذين ينهبون المواقع الأثرية، مثل الدراسة التي أُجريت في عام ٢٠٠٥ لـ٤٠٠ فرد من هذا القبيل في بليز، والتي خلصت إلى أنَّ الدافع الرئيسي لأولئك الجناة لم يكن خبيثاً بل كان إيجاد مصدر للرزق.[٣٧] وثمة دراسة أخرى لعمليات النهب في العراق أُجريت في عامي ٢٠٠٣ و٢٠٠٤ وخلصت إلى أنَّ النهب كانت له دوافع اقتصادية مشابهة، ولكنها أشارت أيضاً إلى وجود أشكال إجرامية أكثر تنظيماً، اتَّسمت بالسيطرة على منافذ الوصول إلى المواقع الأثرية وقتل موظفي الجمارك العراقيين الذين حاولوا مكافحة ذلك النهب.[٣٨] وثمة دراسة تجريبية أحدث عهداً لشبكة اتِّجار بالتماثيل، استُخدمت فيها مقابلات شخصية مع رواةٍ للتاريخ المتناقَل أُجريت أثناء بحث ميداني خاص بالجرائم الإثنية في كمبوديا وتايلند وشملت درجات تنظيم الأنشطة غير المشروعة ذات الصلة.[٣٩]

٤٤- وناقشت بعض الدراسات ضلوع أوساط الإجرام المنظَّم أو الإجرام المنظَّم عبر الوطني في أنشطة الأسواق غير المشروعة للممتلكات الثقافية. فأجرت إحدى الدراسات تحليلاً إجماليًّا لما نُشر سابقاً من دراسات عن الاتجار بالممتلكات الثقافية، وخلصت إلى أنَّ النهج المتمثِّل في رسم خرائط لكيفية حدوث الاتجار وتحديد ما لمختلف الجناة في كل شبكة من أدوار وعلاقات هو أفضل من افتراض أنَّ جميع أنواع الاتجار بالممتلكات الثقافية تندرج ضمن فئة الجريمة المنظَّمة.[٤٠] وثمة دراسة أخرى طبَّقت المفهوم الشبكي لتوضيح المرونة النسبية لهيكل التجارة غير المشروعة في الممتلكات الثقافية، وشجَّعت على إجراء مزيد من الدراسات للهيكل التنظيمي لذلك النوع من الاتجار.[٤١] وقامت دراسة أخرى، ضمن إطار

(٣٧) David Matsuda, “Subsistence Diggers”, in *Who Owns the Past? Cultural Policy, Cultural Property, and the Law*, Kate Fitz Gibbon, ed. (New Brunswick, New Jersey, Rutgers University Press, 2005), pp. 255-268.

(٣٨) Joanne Farchakh-Bajjaly, “Who are the Looters at Archaeological Sites in Iraq?”, in *Antiquities Under Siege: Cultural Heritage Protection After the Iraq War*, Lawrence Rothfield, ed. (Washington, D.C., AltaMira Press, 2008), pp. 49-56.

(٣٩) Simon Mackenzie and Tess Davis, “Temple looting in Cambodia: anatomy of a statue trafficking network”, *British Journal of Criminology*, vol. 54, No. 5 (September 2014), pp. 722-740.

(٤٠) Jessica Dietzler, “On ‘organized crime’ in the illicit antiquities trade: moving beyond the definitional debate”, *Trends in Organized Crime*, vol. 16, No. 3 (September 2013), pp. 329-342.

(٤١) Peter B. Campbell, “The illicit antiquities trade as a transnational criminal network: characterizing and anticipating trafficking of cultural heritage”, *International Journal of Cultural Property*, vol. 20, No. 2 (May 2013), pp. 113-153.

دراسة حالة عن الاتجار بالممتلكات الثقافية، برسم خريطة لسلسلة الجناة المشاركين، محدِّدةً دورَ كل منهم والعلاقات فيما بينهم وتصرُّفاتهم المهيكلة جزئيًّا في شكل مُتراتِب هرميًّا.[٤٢]

باء- تدابير التصدِّي للاتجار بالممتلكات الثقافية

٤٥- لقد اعتُمدت صكوك دولية عدَّة من أجل التصدِّي للاتجار بالممتلكات الثقافية. وكان منع الأضرار التي تلحق بالممتلكات الثقافية أثناء الحروب ومعاقبة المتسبِّبين فيها هو أول هدف ابتغته اتفاقية حماية الممتلكات الثقافية في حال نزاع مسلَّح والبروتوكولات الإضافية لها. وثمة صكوك دولية أخرى تتناول استيراد الممتلكات الثقافية وتصديرها ونقل ملكيتها بصورة غير مشروعة تحت أيِّ ظرف من الظروف. وتشمل تلك الصكوك الاتفاقية المتعلقة بوسائل حظر ومنع استيراد الممتلكات الثقافية وتصديرها ونقل ملكيتها بصورة غير مشروعة والاتفاقية المتعلقة بالأشياء الثقافية المسروقة أو المصدَّرة بصورة غير مشروعة. كما أنَّ هناك التزاماً دوليًّا بصون التراث الثقافي موجود في اتفاقية حماية المياه الجوفية والتراث الثقافي. أمَّا على الصعيد الإقليمي فقد فُتح باب التوقيع على الاتفاقية الأوروبية المتعلقة بالجرائم المتصلة بالممتلكات الثقافية في عام ١٩٨٥ ولكنها لم تدخل حيِّز النفاذ بعد.

٤٦- وتمثِّل المعاهدة النموذجية لمنع الجرائم التي تمسُّ بالتراث الثقافي للشعوب في شكل ممتلكات منقولة[٤٣] واحداً من الصكوك القانونية "الناعمة" التي تحظى باهتمام في سياق القانون الجنائي. وربما توفِّر بعض أحكام تلك المعاهدة النموذجية أساساً لوضع أحكام معيارية بشأن مكافحة الاتجار بالممتلكات الثقافية. وقد شجَّع المجلسُ الاقتصادي والاجتماعي، في قراره ٢٠٠٣/٢٩، الدولَ الأعضاءَ على أخذ المعاهدة النموذجية في الاعتبار، عند الاقتضاء وبما يتوافق مع قانونها الوطني، لدى إبرامها اتفاقات بهذا الشأن مع دول أخرى.[٤٤]

---

(٤٢) Mackenzie and Davis, “Temple looting in Cambodia: anatomy of a statue trafficking network”.

(٤٣) مؤتمر الأمم المتحدة الثامن بشأن منع الجريمة والعدالة الجنائية، هافانا، ٢٧ آب/أغسطس – ٧ أيلول/سبتمبر ١٩٩٠: تقرير من إعداد الأمانة (منشورات الأمم المتحدة، رقم المبيع A.91.IV.2)، الفصل الأول، الباب باء-١، المرفق.

(٤٤) انظر أيضاً المبدأ التوجيهي ١٤ من المبادئ التوجيهية الدولية بشأن تدابير منع الجريمة والعدالة الجنائية فيما يتعلق بالاتجار بالممتلكات الثقافية وما يتصل به من جرائم أخرى. وتجدر الإشارة أيضاً إلى أنَّ الجمعية العامة، في قرارها ٦٨/١٨٦، طلبت إلى مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة أن يواصل استعراضه للمعاهدة النموذجية، آخذاً في اعتباره ما أبدته الدول الأعضاء من آراء وتعليقات، وطلبت إلى

٤٧- وقد أصبح تفشّي الاتجار بالممتلكات الثقافية وما له من سمات معقَّدة في هذه الأيام مسألةً تحظى باعتراف متزايد على الصعيدين الدولي والوطني. إذ يُعتقَد أنَّ الاتجار بالممتلكات الثقافية وما يتصل به من جرائم هو واحد من قطاعات الإجرام المتنامية على الدوام، كما تتزايد جاذبيته لدى التنظيمات الإجرامية الوطنية والدولية. وهذه العوامل أفضت بالدول الأعضاء إلى التفاوض على صكٍّ قانوني "ناعم" آخر واعتماده، وهو المبادئ التوجيهية الدولية بشأن تدابير منع الجريمة والعدالة الجنائية فيما يتعلق بالاتجار بالممتلكات الثقافية وما يتصل به من جرائم أخرى، بصفته إطاراً مفيداً لتوجيه الدول الأعضاء لدى استحداث وتدعيم سياساتها الخاصة بالعدالة الجنائية واستراتيجياتها وتشريعاتها وآلياتها التعاونية في مجال مكافحة الاتجار بالممتلكات الثقافية وما يتصل به من جرائم أخرى.

٤٨- وقد أعربت الهيئات الحكومية الدولية، منذ عام ٢٠٠٠، عن قلقها المتزايد إزاء الاتجار بالممتلكات الثقافية. فلدى اعتماد اتفاقية الأمم المتحدة لمكافحة الجريمة المنظَّمة عبر الوطنية، أعلنت الجمعية العامة، في ديباجة قرارها ٥٥/٢٥، عن اقتناعها الشديد بأنَّ اتفاقية الجريمة المنظَّمة ستمثِّل أداةً فعَّالةً، والإطار القانوني الضروري، للتعاون الدولي على مكافحة جرائم مختلفة، منها الجرائم المرتكَبة بحقِّ التراث الثقافي.[٤٥]

٤٩- وفي وقت لاحق، أعرب المجلس الاقتصادي والاجتماعي، في قراريه ٢٠٠٤/٣٤ و٢٠٠٨/٢٣، عن جزعه إزاء انخراط الجماعات الإجرامية المنظَّمة في الاتجار بالممتلكات الثقافية المسروقة وأكَّد ضرورة التعاون الدولي لمكافحة ذلك الاتجار. وفي قراره ٢٠١٠/١٩، رأى المجلس الاقتصادي والاجتماعي أنَّ اتفاقية الجريمة المنظَّمة واتفاقية الأمم المتحدة لمكافحة الفساد ينبغي أن يستفاد منهما استفادةً كاملةً لتدعيم مكافحة الاتجار بالممتلكات الثقافية، بما في ذلك باستكشاف وسائط أخرى محتملة لتطوير المعايير، عند الاقتضاء. واعتمد مؤتمر الأطراف في اتفاقية الجريمة المنظَّمة، في دورته الخامسة المعقودة في عام ٢٠١٠، قراره ٥/٧ الذي حثَّ فيه الدول الأطراف على استخدام الاتفاقية في إقامة تعاون واسع النطاق على منع ومكافحة الأفعال الإجرامية بحقِّ الممتلكات الثقافية، وخصوصاً على إعادة تلك العائدات الإجرامية أو تلك الممتلكات إلى مالكيها الشرعيين، وفقاً للفقرة ٢ من المادة ١٤ من الاتفاقية. وإلى جانب ذلك، دعت الجمعية العامة، في قرارها ١٨٠/٦٦ و١٨٦/٦٨، الدول الأعضاء إلى النظر، عند الاقتضاء، في مراجعة أُطرها القانونية بهدف توفير أوسع نطاق ممكن من التعاون

الدول الأعضاء والمنظمات الدولية ذات الصلة التي لم تقدِّم بعدُ إلى الأمانة العامة تعليقاتها على المعاهدة النموذجية أن تفعل ذلك.

(٤٥) تحتوي الوثيقة CTOC/COP/2010/12 على تحليل للعناصر المتصلة بانطباق الاتفاقية في هذا الميدان.

الدولي لمعالجة مشكلة الاتجار بالممتلكات الثقافية معالجةً تامةً، كما دعتها إلى جعل الاتجار بالممتلكات الثقافية، بما فيه السرقة والنهب في المواقع الأثرية وسائر المواقع الثقافية، جريمةً خطيرةً حسب التعريف الوارد في المادة ٢ من اتفاقية الجريمة المنظَّمة، بغية الاستفادة التامة من تلك الاتفاقية بغرض إقامة تعاون دولي واسع النطاق على مكافحة جميع أشكال وجوانب الاتجار بالممتلكات الثقافية وما يتصل به من جرائم. وعملاً بتلك القرارات، وضعت الدول الأعضاء المبادئ التوجيهية الدولية المذكورة أعلاه.

٥٠- وتتضمَّن المبادئ التوجيهية الدولية بشأن تدابير منع الجريمة والعدالة الجنائية فيما يتعلق بالاتجار بالممتلكات الثقافية وما يتصل به من جرائم أخرى فصولاً تتعلق بالمواضيع التالية: (أ) استراتيجيات منع الجريمة (تشمل جمع المعلومات والبيانات، ودور المؤسسات الثقافية والقطاع الخاص، ورصد سوق الممتلكات الثقافية والواردات والصادرات والمواقع الأثرية، والتعليم وتوعية الناس)؛ و(ب) سياسات العدالة الجنائية (تشمل الانضمام إلى المعاهدات الدولية ذات الصلة وتنفيذها، وتجريم أنواع معيَّنة من السلوك الضار أو تجريم تصرُّفات إدارية معيَّنة، ومسؤولية الشركات، والحجز والمصادرة، وتدابير التحرِّي والتحقيق)؛ و(ج) التعاون الدولي (بما في ذلك الأمور المتعلقة بأساس الولاية القضائية وتسليم المطلوبين والحجز والمصادرة والتعاون بين سلطات إنفاذ القانون وسلطات التحقيق، وإعادة الممتلكات الثقافية أو ردُّها أو إعادتها إلى مواطنها)؛ و(د) نطاق انطباق المبادئ على أية حالة، بما فيها أيُّ ظروف استثنائية، تساعد على الاتجار بالممتلكات الثقافية وما يتصل به من جرائم.

٥١- وتَعتمد تدابير التصدِّي للاتجار بالممتلكات الثقافية بصفة عامة على وجود تعاون وتنسيق بين الدول وشراكات تضمُّ القطاعين العام والخاص فيها. ويمكن أن يشمل ذلك التعاون وتلك الشراكات، مثلاً، إدراج معلومات شاملة في قوائم الجرد وقواعد البيانات التي قد تمثِّل أدوات مهمَّة لبذل الحرص الواجب بشأن نشأة القطعة الفنِّية ذات القيمة الثقافية قبل بيعها في السوق المشروعة، بما في ذلك في بيوت المزادات، وللمساعدة في التحرِّي عن احتمال حدوث سرقة أو اتِّجار. وإلى جانب إنشاء قوائم الجرد وقواعد البيانات الوطنية، تجمع قاعدة بيانات الإنتربول الخاصة بالأعمال الفنِّية المسروقة[٤٦] بين الوصف الدقيق والصور الفوتوغرافية لنحو ٤٣ ٠٠٠ قطعة، مما قد يفيد كثيراً في الحالات عبر الوطنية. وتحتوي "القوائم الحمراء" الثلاث عشرة[٤٧] التي أصدرها المجلس الدولي للمتاحف، وهو

(٤٦) متاحة على الرابط الشبكي www.interpol.int/Crime-areas/Works-of-art/Database.

(٤٧) متاحة على الرابط الشبكي http://icom.museum/programmes/fighting-illicit-traffic/red-list.

منظمة دولية غير حكومية، على تصنيف للقطع الأثرية أو الأعمال الفنِّية الموجودة في مناطق العالم الأضعف مَنَعةً، مثل أفغانستان والجمهورية العربية السورية وهايتي، من أجل الحيلولة دون بيعها أو تصديرها بصورة غير مشروعة. ويمثِّل سجل المفقودات الفنِّية[٤٨] قاعدة بيانات خاصة ضخمة للقطع الفنِّية والتحف التاريخية والمقتنيات المفقودة والمسروقة. كما يحتوي السجل على أوصاف تفصيلية لأعمال فنِّية غير مسروقة، مما قد يكون له مفعول رادع للُّصُوص المحتملين ويساعد على استرجاع تلك الأعمال[٤٩] في حال سرقتها.

٥٢- وتتجلَّى أهمية تدابير التصدِّي المنسَّقة بمزيد من الوضوح في مبادرة إذكاء الوعي المشتركة بين مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة ومنظمة الأمم المتحدة العالمية للسياحة واليونسكو، والتي تحثُّ المسافرين على دعم مكافحة عدد من أشكال الاتجار، منها الاتجار بالممتلكات الثقافية.[٥٠] وثمة مثال مفيد آخر للتعاون المهم بين المنظمات الحكومية الدولية والأجهزة الوطنية والقطاع الخاص، هو إنشاء المجلس الدولي للمتاحف المِرصدَ الدولي المعني بالاتجار غير المشروع بالسلع الثقافية،[٥١] وهو منصَّة تعاونية توفِّر المعلومات والموارد المرجعية للمعنيين من الأفراد والمنظمات.

رابعاً- الاستنتاجات والتوصيات

٥٣- على الرغم من أنَّ الجريمة السيبرانية والاتجار قد يختلفان من حيث الشيء المستهدَف بالجرم في المقام الأول، فمن الواضح أنَّ للدوافع الأساسية الجديدة، بما فيها العولمة وظهور تكنولوجيات جديدة، أهمية محورية في نشوء أسواق غير مشروعة في كلا المجالين. ومع تطوُّر تلك الأسباب الجذرية والدوافع، يمكن أن تتطوَّر أيضاً الفرص المتاحة لتوسُّع هذين النوعين

(٤٨) متاح على الرابط الشبكي www.artloss.com/en.

(٤٩) تجدر الإشارة إلى أنَّ المادة ٥ (ب) من الاتفاقية المتعلقة بوسائل حظر ومنع استيراد الممتلكات الثقافية وتصديرها ونقل ملكيتها بصورة غير مشروعة تتضمَّن حكماً يُلزم الدول الأطراف بأن تضع وتُحدِّث باستمرار، بالاستناد إلى جرد للممتلكات الخاضعة للحماية على المستوى الوطني، قائمةً بالممتلكات الثقافية العامة والخاصة المهمَّة التي يشكِّل تصديرها إفقاراً جسيماً للتراث الثقافي الوطني. كما أن المبدأ التوجيهي ١ من المبادئ التوجيهية الدولية بشأن تدابير منع الجريمة والعدالة الجنائية فيما يتعلق بالاتجار بالممتلكات الثقافية وما يتصل به من جرائم أخرى ينصُّ على أنه "ينبغي للدول أن تنظر في إنشاء وتطوير قوائم جرد أو قواعد بيانات، حسب الاقتضاء، للممتلكات الثقافية بغرض حمايتها من الاتجار بها. ولا يجوز، بأيِّ حال من الأحوال، أن يفضي عدم تسجيل الممتلكات الثقافية في تلك القوائم إلى استبعادها من الحماية".

(٥٠) يتوافر مزيد من المعلومات بهذا الشأن على الرابط الشبكي www.bearesponsibletraveller.org.

(٥١) متاح على الرابط الشبكي http://obs-traffic.museum.

من الجرائم وتسبُّبهما في مزيد من الخسائر والأضرار. وفيما يتعلق بالجريمة السيبرانية على وجه الخصوص، يتوسَّع الحجم المحتمل للسوق الإجرامية، في مجالات مثل استخدام الإنترنت في الابتزاز أو البيع غير المشروع أو انتهاك البيانات وبيعها، نتيجةً للتزايد المطَّرد في نسبة الموصولين بشبكة الإنترنت بين سكان العالم. ولذلك، يمثِّل ارتقاب التطوُّر المستقبلي للأسواق غير المشروعة في مجالَي الجريمة السيبرانية والاتجار بالممتلكات الثقافية والاستعداد لذلك التطوُّر أمرين بالغَي الأهمية في صوغ تدابير مضادة فعَّالة.

٥٤- ويجب أن تبدأ هذه العملية بإجراء بحوث منهجية وإنتاج إحصاءات موقوتة وموثوقة وميسورة المنال عن هذين النوعين من الجرائم. وحسبما ذُكر في تقرير فريق الخبراء المستقلين الاستشاري المعني بإحداث ثورة بيانات من أجل التنمية المستدامة،[٥٢] يلزم وجود "توافق عالمي بشأن البيانات" يجري في إطاره تقاسم التكنولوجيات والابتكارات واستخدامها لخير الجميع، بوسائل منها إنشاء شبكة عالمية للابتكار في مجال البيانات. وهذا ينطبق على فهمنا للتحدِّيات الإجرامية العالمية المستجدَّة، مثل الجريمة السيبرانية والاتجار بالممتلكات الثقافية، وكذلك على كيفية قياسنا لتلك التحدِّيات.

٥٥- ويمكن أن تشمل التدابير الإضافية اللازمة للتصدِّي للجريمة السيبرانية والاتجار بالممتلكات الثقافية ما يلي:

(أ) يمكن للدول الأعضاء أن تنظر في تدعيم قدرتها على حفظ سجلات للجرائم ذات الصلة، وفي تبادل المعلومات على الصعيدين الإقليمي والدولي عن ضلوع الجماعات الإجرامية المنظَّمة فيها وعن أساليب عمل تلك الجماعات وعن التقنيات المستخدَمة في كشف أشكال الجريمة السيبرانية والاتجار بالممتلكات الثقافية؛

(ب) ينبغي المضي في تعزيز التفاعل بين منشآت القطاع الخاص، سواء أكانت جهات مقدِّمة لخدمات الإنترنت أَم مصارف أَم منشآت عاملة في مجال اللوجستيات وخدمات التوصيل على الصعيد العالمي أَم متاحف أَم بيوت مزادات، والمؤسسات العمومية، مثل الجهات الفاعلة في مجالَي إنفاذ القانون والعدالة الجنائية، من خلال شراكات بين القطاعين العام والخاص يمكن فيها تعزيز الثقة والتحاور. وعلى وجه الإجمال، قد تكون تدابير التصدِّي الرقابية الحكومية التي تتجاوز نطاق إنفاذ القانون وتُوفِّر حوافز لانخراط

(٥٢) *A World that Counts: Mobilising the Data Revolution for Sustainable Development* (November 2014). متاح على الرابط الشبكي www.undatarevolution.org.

القطاع الخاص على نحو فعَّال في منع الجريمة، مفيدةً في توفير بيئة تتحسَّس للأخطار المستجدَّة وتساعد على استبانة تلك الأخطار ومواجهتها؛

(ج) يمكن للدول الأعضاء أن تنظر في مراجعة أُطرها الوطنية لمنع الاتجار بالممتلكات الثقافية ومكافحته، بما في ذلك في الأحوال التي قد تكون فيها تلك الممتلكات شديدة التعرُّض لخطر الاتجار، وفي تدعيم تلك الأُطر بوسائل مثل استخدام المبادئ التوجيهية الدولية بشأن تدابير منع الجريمة والعدالة الجنائية فيما يتعلق بالاتجار بالممتلكات الثقافية وما يتصل به من جرائم أخرى. وفي مجال الجريمة السيبرانية، يمكن للدول الأعضاء أن تنظر في ضمان اتِّباع نهج قانوني متوازن يستفيد من تجريم أفعال معيَّنة في تجريم أفعال أساسية تمسُّ بسرِّية البيانات الحاسوبية وسلامتها وتوافرها، مع إعادة النظر في انسحاب جرائم عامة أخرى، مثل السرقة والاحتيال والتزوير والإضرار الشخصي، على الأفعال المرتكبة عبر الإنترنت؛

(د) قد يكون من الضروري أن تبحث الدول الأعضاء في السبل والوسائل الكفيلة بتعزيز التعاون الدولي في المسائل الجنائية. ففي مجال الجريمة السيبرانية، يمكن أن يشمل ذلك، على وجه الخصوص، دراسة إمكانيات تعجيل الإجراءات الرسمية المتعلقة بتبادل المساعدة القانونية، وتدعيم التعاون بين أجهزة إنفاذ القانون، ومواصلة الحوار المتعدِّد الأطراف في مجال تيسير الوصول إلى البيانات الحاسوبية عبر الحدود الوطنية. أمَّا في مجال الاتجار بالممتلكات الثقافية، فقد يتطلَّب ذلك زيادة التركيز على التحرِّي عن الشبكات الإجرامية وملاحقتها قضائيًّا، من خلال تبادل المعلومات فيما بين هيئات التحقيق الوطنية المتخصِّصة؛

(هـ) يجب تدعيم ركائز البحوث والإحصاءات والشراكات بين القطاعين العام والخاص والأُطر التشريعية وآليات التعاون الدولي بتوفير قدرات فعَّالة على الصعيد الوطني. وللمساعدة التقنية والتعاون التقني أهمية في إتاحة إمكانية تقاسم ممارسات التحرِّي والتحقيق الجيِّدة والتجارب المكتسبة وتعميم الأساليب الجديدة. ففي مجال الجريمة السيبرانية، لعلَّ الدول الأعضاء تودُّ تعزيز تقاسم النهوج الجديدة في التحرِّي عن جرائم معقَّدة، مثل الاحتيال المالي بواسطة الإنترنت أو الاتجار بالمخدِّرات عبر الإنترنت أو استخدام العملات الافتراضية في غسل الأموال، مما يتيح لسلطات إنفاذ القانون في بلدان متعدِّدة سرعة اكتساب المهارات الضرورية لمواجهة الأخطار المستجدَّة. أمَّا بشأن الاتجار بالممتلكات الثقافية، فلعلَّ الدول الأعضاء تودُّ تعزيز قدرة الأجهزة المعنية بالحدود والجمارك على كشف الممتلكات الثقافية المتَّجَر بها، واستكشاف العلاقات بين الأُطر الوطنية الخاصة بمكافحة غسل

الأموال والاتجار بالممتلكات الثقافية، واستبانة وتبادل الممارسات الجيِّدة في مجالَي منع الجريمة وتدابير العدالة الجنائية الرامية إلى مكافحة ذلك الاتجار؛

(و) ينبغي لمكتب المخدِّرات والجريمة أن يواصل تزويد الدول الأعضاء بمساعدة تقنية تهدف إلى تدعيم قدرة نظم منع الجريمة والعدالة الجنائية على التصدِّي لأشكال الجرائم الجديدة والمستجدَّة، بما فيها الجريمة السيبرانية والاتجار بالممتلكات الثقافية وما يتصل بهما من جرائم، عند الطلب وبالتنسيق مع المنظمات الدولية ذات الصلة. ولعلَّ الدول الأعضاء تودُّ النظر، على وجه الأولوية، في توفير التمويل اللازم لذلك الغرض؛

(ز) لعلَّ الدول الأعضاء تودُّ أن تعتمد، في التصدِّي للجريمة السيبرانية والاتجار بالممتلكات الثقافية، نهجاً شموليًّا يأخذ في الاعتبار أساليب العمل والأخطار الإجرامية الراهنة وكذلك تطوُّرات الإجرام المستقبلية المحتملة. وينبغي لتدابير التصدِّي أن ترتكز بصورة متزايدة على التعاون العالمي وانخراط جهات معنية متعدِّدة واستعمال تكنولوجيات مثل قواعد البيانات ومنصَّات التواصُل الآمنة.