

Distr.: General  
23 January 2020  
Arabic  
Original: English

# مؤتمر الأمم المتحدة الرابع عشر لمنع الجريمة والعدالة الجنائية



كيوتو، اليابان، ٢٠-٢٧ نيسان/أبريل ٢٠٢٠

البند ٦ من جدول الأعمال المؤقت\*  
التعاون الدولي وتقديم المساعدة التقنية من أجل منع  
الجرائم بجميع أشكالها والتصدي لها

## حلقة العمل ٤ - الاتجاهات الراهنة للجريمة، والتطورات الأخيرة والحلول المستجدة، لا سيما التكنولوجيات الجديدة بوصفها وسائل لارتكاب الجريمة وأدوات لمكافحتها\*\*

ورقة معلومات أساسية أعدتها الأمانة

### ملخص

تبحث ورقة المعلومات الأساسية هذه آثار التكنولوجيا على الجريمة. والتكنولوجيا سلاح ذو حدين، فهي يمكن أن تساعد على ارتكاب الجرائم، لكنها تسهم أيضاً في منعها وكشفها وقمعها. وبناءً على ذلك، تتبع هذه الورقة نهجاً ذا شقين لشرح تلك الازدواجية الأساسية المستجدة، أي دور التكنولوجيا في إيجاد حلول تساعد على حفظ الأمن والملاحقة القضائية للمجرمين والنجاح في تطبيق العدالة الجنائية من ناحية؛ ودورها الأكثر قتامة المتمثل في تعزيز أساليب عمل المجرمين والجماعات الإجرامية المنظمة من ناحية أخرى. ويأخذ التحليل في الاعتبار التطورات الحاصلة في مجالات محددة، ويغطي جانبين من الجوانب الجامعة، أولهما هو أهمية توفير التدريب واتباع نهج متعددة التخصصات وتحقيق التعاون والتآزر في العمل بين أصحاب المصلحة المعنيين من أجل التوصل إلى فهم للفوائد الحالية للتكنولوجيات وما تنطوي عليه من إمكانات يمكن الاستفادة منها في التصدي لمخاطر الجريمة في المستقبل، أما الجانب الثاني فهو ضرورة إيلاء الاعتبار الواجب للمسائل الأخلاقية و ضمانات حقوق الإنسان في استخدام التكنولوجيات لمكافحة الجريمة.

\* A/CONF.234/1

\*\* تؤد الأمانة أن تُعرب عن تقديرها للمعاهد الأعضاء في شبكة برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية، ولا سيما المعهد الكوري لعلم الإحرام والمعهد الوطني للعدالة التابع لوزارة العدل بالولايات المتحدة، لما وفرته من مساعدة في إعداد وتنظيم حلقة العمل.



الرجاء إعادة استعمال الورق

060220 060220 V.20-00546 (A)



## أولاً - مقدمة

١ - عندما أُدمج في عام ١٩٩٧ برنامج الأمم المتحدة للمراقبة الدولية للمخدرات ومركز منع الجريمة الدولية لتشكيل مكتب مراقبة المخدرات ومنع الجريمة، الذي أعيدت تسميته في عام ٢٠٠٢ ليصبح مكتب الأمم المتحدة المعني بالمخدرات والجريمة (المكتب)، أصبحت نسخة محدّثة من حاسوب لعب الشطرنج اسمه "الأزرق العميق" أول نظام حاسوبي يهزم بطل العالم في ذلك الوقت في مباراة تخضع لضوابط الوقت المعيارية في دورات لعبة الشطرنج. وعلى الرغم من التقدم المطرد للتكنولوجيا في ذلك الوقت، كان استغلال التكنولوجيا في مجال الجريمة لا يزال محدوداً نسبياً، وكانت الإنترنت قد بدأت لتوها في التأثير على المجتمع بوصفها التكنولوجيا الحاسمة في "عصر المعلومات".

٢ - وفي غضون أكثر من عقدين بقليل، مكّن النمو السريع للإنترنت وتكنولوجيات المعلومات والاتصالات من تحقيق النمو الاقتصادي وتوسيع نطاق الوصول إلى الخدمات الحيوية، ولكنه هباً أيضاً فرصاً جديدة لممارسة الأنشطة الإجرامية. وأصبح المجرمون المستفيدين غير المقصودين من التكنولوجيا الجديدة والعولمة لأن تلك التطورات مكّنتهم من ارتكاب الجرائم والترُّب منها عن طريق استغلال الأنشطة عبر الوطنية، ومن توسيع نطاق أنشطتهم وأعمالهم غير المشروعة عبر المنصات الرقمية على نحو قلل من المخاطر، وخصوصاً خطر الانكشاف.<sup>(١)</sup>

٣ - ومن ناحية أخرى، تتيح التكنولوجيات الجديدة والحالية فرصاً جديدة لإنفاذ القانون والتحقيق الجنائي والملاحقة القضائية. وقد يكون لتحسين السلامة العامة وتمكين أجهزة إنفاذ القانون والعدالة الجنائية من منع الجريمة ومكافحتها من خلال التقدم التكنولوجي أثر إيجابي على تحقيق أهداف خطة التنمية المستدامة لعام ٢٠٣٠، ولا سيما الهدف ١٦ من تلك الأهداف.

٤ - وكانت هذه الازدواجية أيضاً موضع اهتمام الفريق الرفيع المستوى المعني بالتعاون الرقمي، الذي أنشأه الأمين العام في عام ٢٠١٨ لتعزيز التعاون الدولي والتعاون بين أصحاب المصلحة المتعددين والمساهمة في المناقشة العامة بشأن مستقبل رقمي آمن وشامل للجميع، والذي سلط عليها الضوء في تقريره المعنون "عصر الترابط الرقمي". وكما ذكر، أثبتت التكنولوجيات الرقمية أنها قادرة على ربط الأفراد عبر الحواجز الثقافية والجغرافية، مما يزيد التفاهم ويُحتمل أن يساعد المجتمعات على أن تصبح أكثر سلاماً وتماسكاً. ومع ذلك، هناك أيضاً أمثلة على تكنولوجيات رقمية تُستخدم لانتهاك الحقوق، وتقويض الخصوصية، واستقطاب المجتمعات، والتحرّض على العنف.<sup>(٢)</sup>

٥ - وتستند ورقة المعلومات الأساسية هذه إلى الإطار المواضيعي لحلقة العمل ٤، الوارد في دليل المناقشة الخاص بالمؤتمر الرابع عشر، وتوسع من نطاقه.<sup>(٣)</sup> وقد نُظِّمت ورقة المعلومات الأساسية هذه في أقسام منفصلة، يجسد كل منها زوايا مختلفة من نفس المسألة الأساسية، وهي أن

(١) Yury Fedotov, "In just two decades, technology has become a cornerstone of criminality", *Huffington Post* (١) .UK, 23 October 2017

(٢) انظر A/CONF.234/PM.1، الفقرات ١٦١-١٨٩.

(٣) A/CONF.234/PM.1، الفقرات ١٦١-١٨٩.

أجهزة إنفاذ القانون والعدالة الجنائية تقف عند مفترق طرق في ساحة التكنولوجيا، إذ إن الابتكارات التكنولوجية السريعة قد لا تفضي فحسب إلى حفظ الأمن بفعالية والنهوض بدور محوري في معالجة أوجه القصور التقليدية في الجهود الرامية إلى إنفاذ سيادة القانون إنفاذاً كاملاً، بل قد تكون عرضةً أيضاً للاستغلال الإجرامي في مجالات مختلفة.<sup>(٤)</sup>

## ثانياً - استخدام التكنولوجيا في ارتكاب الجرائم وفي مكافحتها

### ألف - العملات المشفرة والموجودات الافتراضية

٦- ظهرت في السنوات الأخيرة العملات المشفرة والموجودات الافتراضية وجذبت استثمارات لإقامة بني تحتية لنظم للدفع باستخدام بروتوكولات برمجية خاصة بتلك العملات والموجودات.<sup>(٥)</sup> وقد يستصوب البعض استعمال العملات المشفرة لمجموعة متنوعة من الأسباب، وربما يحتفظ بها في الوقت نفسه لاستثمارها في المضاربات. ويسعى البعض إلى الاستفادة من طابع السرية المرتبط بما توفره من مستويات عليا من حجب الهوية في المعاملات، في حين أن كل ما يريده آخرون هو تجنب خضوع معاملاته القانونية للإشراف و/أو المراقبة من جانب الدولة أو المصارف.<sup>(٦)</sup> ويشير مؤيدو العملات المشفرة إلى أن رسوم المعاملات بها تقل عن الرسوم التي تفرضها البنوك التقليدية على العملات الوطنية، وإن كان من المحتمل أن تقلل أي خسارة في أسعار الصرف وارتفاع الرسوم المرتبطة بمقدمي خدمات العملات المشفرة من وفورات التكلفة.<sup>(٧)</sup> وفي المواقع التي لا تتوافر فيها المصارف التقليدية، يمكن للعملات المشفرة أن توفر الوظائف المرتبطة بخدمات الدفع التقليدية.<sup>(٨)</sup> وأخيراً، فإن العملة المشفرة يمكن أن تسهل المعاملات العابرة للحدود لأنها ليست في العادة عملة مرتبطة بدولة معينة.<sup>(٩)</sup>

٧- ومع ذلك، فإن العديد من البلدان التي تسمح بتشغيل أسواق العملات المشفرة قد سنت قوانين لمنع استخدامها في غسل الأموال والجريمة المنظمة وتمويل الإرهاب،<sup>(١٠)</sup> على الرغم من أنه

(٤) تناول ورقة العمل التي أعدها الأمانة بشأن البند ٦ من جدول الأعمال (A/CONF.234/7) استخدام الإنترنت والتكنولوجيات الرقمية لأغراض إرهابية، وكذلك المسائل المتصلة بالجريمة السيبرانية.

(٥) Sesha Kethineni and Yin Cao, "The rise in popularity of cryptocurrency and associated criminal activity", *International Criminal Justice Review*, 6 February 2019; Stearns Broadhead, "The contemporary cybercrime ecosystem: a multi-disciplinary overview of the state of affairs and developments", *Computer Law and Security Review*, vol. 34, No. 6 (December 2018), pp. 1180-1196.

(٦) Geoff Goodell and Tomaso Aste, "Can cryptocurrencies preserve privacy and comply with regulations?", *Frontiers in Blockchain*, vol. 2, art. 4 (May 2019), pp. 1-20.

(٧) Angela S. M. Irwin and Adam B. Turner, "Illicit Bitcoin transactions: challenges in getting to the who, what, when and where", *Journal of Money Laundering Control*, vol. 21, No. 3 (July 2018), pp. 297-313.

(٨) المرجع نفسه.

(٩) Perri Reynolds and Angela S. M. Irwin, "Tracking digital footprints: anonymity within the bitcoin system", *Journal of Money Laundering Control*, vol. 20, No. 2 (May 2017), pp. 172-189.

(١٠) United States, Law Library of Congress, Global Legal Research Center, *Regulation of Cryptocurrency around the World* (Washington, D.C., 2018), June 2018.

لا يبدو حتى الآن أن الإرهابيين يستخدمون العملات المشفرة على نطاق واسع.<sup>(١١)</sup> وقد ظهر هذا الاتجاه التنظيمي الرقابي كرد فعل على الاستخدام المتكرر للعملات المشفرة لإجراء عمليات شراء غير قانونية في السوق السوداء عبر الإنترنت،<sup>(١٢)</sup> وكوسيلة للدفع في عمليات غسل الأموال ومخططات الاحتيال الهرمي (بونزي) والابتزاز (بما فيه التهديد بأسلوب الهجمات الموزعة للحرمان من الخدمة (DDOS)) والاحتيال.

٨- ويمكن أن تنطبق أيضاً على عمليات غسل الأموال باستخدام العملات المشفرة نفس المفاهيم المنطبقة على غسل الأموال باستخدام النقد.<sup>(١٣)</sup> وتتشابه عمليات غسل الأموال باستخدام عملة مشفرة مع عمليات غسل الأموال التقليدية لكنها تستغل التكنولوجيا في عملها.<sup>(١٤)</sup> وإضافة إلى ذلك، قد تُستخدم العملات المشفرة لتسهيل التهرب الضريبي.<sup>(١٥)</sup>

٩- وسرقة العملات المشفرة هي أيضاً مصدر قلق متزايد،<sup>(١٦)</sup> إذ يمكن لمستخدمي العملة المشفرة أن يقعوا فريسة لعمليات الاحتيال المصممة لسرقة العملة المشفرة.<sup>(١٧)</sup> وعلاوة على ذلك، فإن مدبري الهجمات الفيروسية المعطلة لأجهزة الأفراد أو الشركات أو الحكومات بغرض طلب الفدية كثيراً ما يطلبون دفع الفدية بالعملات المشفرة.

١٠- وييسر ارتكاب الجرائم المتعلقة باستخدام عملات مشفرة في البيئات التي تكون فيها اللوائح التنظيمية غير كافية للسماح بتحديد هوية المستخدمين أو فرض عقوبات، وحيث يمكن استغلال الثغرات التنظيمية. واختلاف اللوائح التنظيمية للعملات المشفرة من بلد إلى آخر يتيح لمن يستعمل تلك العملات القيام في أي بلد بأنشطة لا تعد قانونية في أماكن أخرى.<sup>(١٨)</sup>

١١- وينبغي النظر في عدد من الإجراءات لمنع استخدام العملات المشفرة لأغراض إجرامية والعمل على تطبيقها، مثل نهج منع تجهيل هوية أطراف المعاملات التي من شأنها أن تساعد على ردع الجناة والتحقيق معهم. وقد يشمل ذلك تطبيق لوائح تنظيمية تشترط تقديم معلومات لتبيان

(١١) Cynthia Dion-Schwarz, David Manheim and Patrick B. Johnson, *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats* (Santa Monica, California, RAND Corporation, 2019)

(١٢) Reynolds and Irwin, "Tracking digital footprints"; Monica J. Barratt, Jason A. Ferris and Adam R. Winstock, "Safer scoring? Cryptomarkets, social supply and drug market violence", *International Journal of Drug Policy*, vol. 35 (September 2016), pp. 24-31

(١٣) Chad Albrecht and others, "The use of cryptocurrencies in the money laundering process", *Journal of Money Laundering Control*, vol. 22, No. 2 (May 2019), pp. 210-216; Rolf van Wegberg, Jan-Jaap Oerlemans and Oskar van Deventer, "Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin", *Journal of Financial Crime*, vol. 25, No. 2 (June 2018), pp. 419-435

(١٤) Denis B. Desmond, David Lacey and Paul Salmon, "Evaluating cryptocurrency laundering as a complex socio-technical system: a systematic literature review", *Journal of Money Laundering Control*, vol. 22, No. 3 (July 2019), pp. 480-497

(١٥) Albrecht and others, "The use of cryptocurrencies in the money laundering process"; Saman Jafari and others, "Cryptocurrency: a challenge to legal system", 10 May 2018

(١٦) Garrick Hileman and Michel Rauchs, *Global Cryptocurrency Benchmarking Study* (Cambridge, United Kingdom of Great Britain and Northern Ireland, Cambridge Centre for Alternative Finance, 2017)

(١٧) Desmond and others, "Evaluating cryptocurrency laundering as a complex socio-technical system"

(١٨) Angela S. M. Irwin and Caitlin Dawson, "Following the cyber money trail: global challenges when investigating ransomware attacks and how regulation can help", *Journal of Money Laundering Control*, vol. 22, No. 1 (January 2019), pp. 110-131

الهوية (قواعد "اعرف زبونك")<sup>(١٩)</sup> أو تحليل المعاملات باستخدام تقنيات التعلم الآلي أو غيرها من تقنيات المراقبة لاستبانة المعاملات غير القانونية.<sup>(٢٠)</sup>

١٢- ولما كانت قلة الحصيلة المتوفرة من المعارف والمهارات اللازمة لاستبانة مخططات العملات المشفرة أو التحقيق فيها بفعالية تفسح الطريق أمام استخدام العملات المشفرة لأغراض غير مشروعة وتزيد من فرصه،<sup>(٢١)</sup> فإن الجهود المبذولة من جانب الأمم المتحدة وغيرها من أجل توفير التدريب للمحققين على التعامل مع جرائم العملات المشفرة تساهم في منع تلك الأنشطة واستبانتها.<sup>(٢٢)</sup>

١٣- ومن الجهات التي يمكن أن تنهض بدور رئيسي في إعاقه استخدام العملات المشفرة لتسهيل ارتكاب الجرائم الجهات المصدرة لتلك العملات وهيئات التنظيم الرقابي وأجهزة إنفاذ القانون. ومن المهم استحداث مجموعة مُحكمة من تقنيات الوقاية والتحقيق، التي يمكن تكييفها مع التغيرات في التكنولوجيا ومختلف تطبيقات العملات المشفرة، بغية التقليل إلى أدنى حد من التهديدات المرتبطة باستغلالها الإجرامي.

## باء- التكنولوجيا وأسواق الشبكة الخفية، بما في ذلك أسواق المخدرات

١٤- تهيئ الإنترنت فرصاً جديدة لبيع السلع وشراؤها بصورة غير مشروعة، سواء عبر الشبكة الواضحة أو الشبكة الخفية ("الداركنت"). وعلى عكس الشبكة الواضحة (التي تسمى أيضاً "الشبكة السطحية")، التي تحيل إلى معلومات متاحة للجمهور وتفهرسها محركات البحث الشائعة التوافر، فإن الشبكة الخفية تتكون من شبكات خفية مشفرة، مما يسمح لمالك الموقع ومستخدميه على السواء بإبقاء هويتهم مجهولة مع صعوبة تعقبها نسبياً.<sup>(٢٣)</sup>

١٥- وتتيح أسواق الشبكة الخفية (التي توصف أيضاً باسم "الأسواق المشفرة")<sup>(٢٤)</sup> للمشتريين والبائعين عدم الكشف عن هويتهم، وفي تلك الأسواق، تُستخدم العملات المشفرة أساساً لدفع ثمن المشتريات لتيسير بيع وتداول سلع من قبيل الأسلحة والمخدرات غير المشروعة.

١٦- وقد أشارت وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون (اليوروبول) إلى أن البيانات الشخصية والطبية والمالية المسروقة سلعة رئيسية في أسواق الشبكة الخفية، وهي تضطلع بدور حاسم في أنشطة مثل الاحتيال، والتصيد الاحتيالي، وسرقة الهوية، والاستيلاء على الحسابات. ورغم أن أسواق الشبكة الخفية تقدم طائفة من السلع المقلدة والمقرصنة للبيع، فإن

(١٩) Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: the FATF Recommendations* (Paris, 2012).

(٢٠) Irwin and Turner, "Illicit Bitcoin transactions"; Goodell and Aste, "Can cryptocurrencies preserve privacy and comply with regulations?"

(٢١) Sessa Kethineni, Yin Cao and Cassandra Dodge, "Use of Bitcoin in darknet markets: examining facilitative factors on Bitcoin-related crimes", *American Journal of Criminal Justice*, vol. 43, No. 2 (June 2018), pp. 141-157.

(٢٢) United Nations Office on Drugs and Crime (UNODC), "UNODC launches training to tackle cryptocurrency-enabled organized crime", 8 May 2017.

(٢٣) Darren Guccione, "What is the dark web? How to access it and what you'll find", *The State of Cybersecurity*, 4 July 2019.

(٢٤) Julian Broseus and others, "Studying illicit drug trafficking on Darknet markets: structure and organization from a Canadian perspective", *Forensic Science International*, vol. 264, 5 March 2016, p. 7.

أنشطة التجارة غير المشروعة لا تزال تجري في معظمها عبر الشبكة السطحية.<sup>(٢٥)</sup> ويتزايد استخدام الشبكة الخفية في عمليات التلاعب بنتائج المباريات وأنشطة القمار لدعم دروب غسل الأموال، ولا سيما من جانب الجماعات الإجرامية المنظمة عبر الوطنية.<sup>(٢٦)</sup> وقد شدد أيضاً الاجتماع الإقليمي الأوروبي التحضيري للمؤتمر الرابع عشر على ضرورة التصدي لاستخدام الشبكة الخفية في ارتكاب جرائم الكراهية.<sup>(٢٧)</sup>

١٧- وفي مجال المخدرات، ذكر تقرير المخدرات العالمي ٢٠١٩ أن مشتريات المخدرات عبر الشبكة الخفية آخذة في الازدياد على المدى الطويل، على الرغم من أنها ربما تكون قد انخفضت من عام ٢٠١٨ إلى عام ٢٠١٩. وتشير البيانات المستمدة من الدراسة الاستقصائية العالمية للمخدرات لعام ٢٠١٩ إلى أن شراء المخدرات عن طريق الشبكة الخفية لا يزال ظاهرة حديثة جداً، حيث إن ٤٨ في المائة من الأشخاص الذين أبلغوا عن شراء المخدرات عن طريق الشبكة الخفية في عام ٢٠١٩ بدأوا في استخدامها لتلك الأغراض في العامين السابقين، وإن نسبة ٢٩ في المائة أخرى بدأت في ذلك في العامين السابقين عليهما.<sup>(٢٨)</sup>

١٨- وقد يكون بوسع أسواق المخدرات الكائنة على الشبكة الخفية أن تدخل تغييرات في أنماط تعاطي المخدرات ومدى انتشاره،<sup>(٢٩)</sup> فاستخدامها يمكن أن يقلل بعض المخاطر بالنسبة للمشتريين والبائعين، مثل التعرض لمواجهات عنيفة في الأحياء التي تباع فيها المخدرات والإكراه<sup>(٣٠)</sup> والتوقيف.<sup>(٣١)</sup> ومع ذلك، فإن مبيعات المخدرات، التي تيسرها الإنترنت، لها مخاطرها. ومن المرجح أن تحدث أكبر تلك المخاطر أثناء أنشطة تتم خارج دائرة الاتصال بالإنترنت.<sup>(٣٢)</sup> وقد تكون مبيعات المخدرات التي تيسرها الإنترنت مرتبطة أيضاً بالزيادات في الجرعات المفرطة إذا كانت تيسر على المتعاطين تجربة عقاقير جديدة وتتيح لهم الحصول على مخدرات أقوى مفعولاً.<sup>(٣٣)</sup>

(٢٥) European Union Agency for Law Enforcement Cooperation (Europol), European Cybercrime Centre, *Internet Organised Crime Threat Assessment (IOCTA) 2018* (The Hague, 2018), p. 49

(٢٦) Robin Cartwright and France Cleland Bones, *Transnational Organized Crime and the Impact on the Private Sector: The Hidden Battalions* (Geneva, Global Initiative against Transnational Organized Crime, 2017), p. 29

(٢٧) انظر الفقرة ٣٦ (ز) من الوثيقة A/CONF.234/RPM.5/1.

(٢٨) تقرير المخدرات العالمي ٢٠١٩: لمحة عامة عن الطلب على المخدرات وعرضها على الصعيد العالمي (منشورات الأمم المتحدة (الكتيب الثاني)).

(٢٩) Judith Aldridge and David Décary-Hétu, "Hidden wholesale: the drug diffusing capacity of online drug cryptomarkets", *International Journal of Drug Policy*, vol. 35, September 2016, p. 12

(٣٠) Julia Buxton and Tim Bingham, *The Rise and Challenge of Dark Net Drug Markets*, Policy brief, No. 7 (Swansea, United Kingdom, Global Drug Policy Observatory, January 2015), pp. 1-24

(٣١) David Décary-Hétu, و انظر أيضاً Buxton and Bingham, *The Rise and Challenge of Dark Net Drug Markets* Masarah Paquet-Clouston and Judith Aldridge, "Going international? Risk taking by cryptomarket drug vendors", *International Journal of Drug Policy*, vol. 35, September 2016, p. 71

(٣٢) Judith Aldridge and Rebecca Askew, "Delivery dilemmas: how drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement", *International Journal of Drug Policy*, vol. 41, March 2017, pp. 101-109

(٣٣) Nathaniel Popper, "Opioid dealers embrace the dark web to send deadly drugs by mail", *New York Times*, 10 June 2017

١٩- وقد تحقق نجاح ملحوظ في تفكيك أسواق كبيرة على الشبكة الخفية. غير أن المجرمين، وفقاً لما ذكره اليوروبول، يستكشفون وسائل بديلة للتحايل على إجراءات إنفاذ القانون. ويتمثل أحد الاتجاهات الجديدة في ظهور نماذج تجارية يستخدم فيها المجرمون هويات متعددة، من خلال استخدام ملفات تعريف متعددة، على منصات مختلفة على الإنترنت، مما ييسر بدوره العمليات التي يقوم بها أفراد مختلفون بدلاً من شخص واحد.<sup>(٣٤)</sup>

٢٠- وهناك عدد من التحديات التي تعترض التحري عن أنشطة الشبكة الخفية، ومن أهمها عدم فهرسة المعلومات الموجودة بها، مما يجعل من محاولة تحديد موقع تلك المعلومات باستخدام محركات البحث أو الكلمات الرئيسية أمراً غير يسير للمحققين. وعلاوة على ذلك، يستخدم المجرمون منصات لامركزية لاستضافة خوادمهم الشبكية، مما يتيح انتشار خدمات قد يكون من الصعب اكتشافها.<sup>(٣٥)</sup>

٢١- ومن ناحية أخرى، هناك فرص متاحة أمام أجهزة إنفاذ القانون لرصد أسواق الشبكة الخفية وإجراء تحريات بالاتصال الحاسوبي المباشر،<sup>(٣٦)</sup> وهناك طائفة من الأدوات، التي يمكن أن تتيح في هذا السياق حلولاً فعالة، منها مثلاً الزواحف الشبكية التي يمكن استخدامها لأتمتة فهرسة البيانات عبر الإنترنت على نحو متكرر، وأدوات التنقيب عن البيانات للبحث في مجموعات البيانات الضخمة، والأدوات التحليلية للعمليات المشفرة لتعقب مسار المدفوعات، وبرمجيات سلاسل كتل البيانات المشفرة المستخدمة لتعقب الأدلة.<sup>(٣٧)</sup> وللمساعدة التقنية أهميتها في هذا الشأن، ولذا يعمل المكتب مجد على توفير أنشطة للتدريب تركز على أساليب التحري المتعلقة بالشبكة الخفية.

## جيم- الأسلحة النارية: المخاطر الأمنية المتصلة بالتكنولوجيا

### ١- البوليمرات الصناعية في صنع الأسلحة النارية

٢٢- من المقدر حتماً أن تلعب البوليمرات الصناعية دوراً بارزاً متزايد الأهمية في صناعة الأسلحة، مما يطرح تحديات أمام التنفيذ الفعال للأحكام المتعلقة بتعقب الأسلحة النارية وحفظ سجلاتها الواردة في بروتوكول مكافحة صنع الأسلحة النارية وأجزائها ومكوناتها والذخيرة والاتجار بها بصورة غير مشروعة، المكمل لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية. واستخدام البوليمرات الصناعية على هذا النحو يهدد قدرة السلطات المختصة على الكشف عن الجرائم ذات الصلة والتحقيق فيها وملاحقة مرتكبيها على النحو الملائم.

٢٣- ومن الممكن للبلدان أن تجد في مجموعة وحدات تدابير التنفيذ المتعلقة بتحديد الأسلحة الصغيرة ذات التصميم التجميعي ما يساعدها على التغلب على المشاكل المتعلقة بالهياكل أو علب

(٣٤) Europol, European Cybercrime Centre, *Internet Organised Crime Threat Assessment (IOCTA) 2019* (The Hague, 2019), p. 45.

(٣٥) International Criminal Police Organization (INTERPOL) "Innovation report: anonymous networks and darknet" (September 2018), pp. 12-13.

(٣٦) European Monitoring Centre for Drugs and Drug Addiction and Europol, *Drugs and the Darknet: Perspectives for Enforcement, Research and Policy* (Luxembourg, 2017), p. 60 ff.

(٣٧) Shira Stein, "Law enforcement adapts to using cryptocurrency to catch criminals", *Securities Regulation and Law Report*, 49 SRLR 1029 (Arlington, Virginia, Bureau of National Affairs, 2017).

المغلاق المصنوعة من البوليمر، فهذا المنشور يضم مجموعة من الممارسات الجيدة غير الملزمة بشأن مراقبة الأسلحة الصغيرة تستند إلى الأحكام المتراكمة في الصكوك الدولية ذات الصلة، وهي: بروتوكول الأسلحة النارية، وبرنامج العمل المتعلق بالأسلحة الصغيرة والصك الدولي للتعقب المرتبط به، ومعاهدة تجارة الأسلحة.

## ٢- الأسلحة المصنوعة الطيبة التشكيل (الأسلحة ذات التصميم التجميعي)

٢٤- أدت التكنولوجيات الجديدة والثغرات التشريعية القائمة إلى إغراق الأسواق المشروعة وغير المشروعة على حد سواء بمجموعات من أدوات التعديل والتحويل والصنع التي تمكن مالكي الأسلحة النارية من تطوير أسلحتهم النارية، بل وإنتاج أسلحة مؤدية للغرض بالكامل، بأدنى قدر من المعرفة التقنية.

٢٥- وينطبق بروتوكول الأسلحة النارية على "الأجزاء والمكونات"، بيد أن شروط الوسم الواردة فيه (المادة ٨) لا تنطبق إلا على "الأسلحة النارية". ويمكن أن ينطوي ذلك على إشكالية كبيرة فيما يتعلق بالأسلحة المصنوعة من وحدات قابلة لإعادة التشكيل.<sup>(٣٨)</sup> وقد يتطلب التغلب على هذا التحدي اتخاذ تدابير من قبيل تحديد عنصر معين يمكن استخدامه لمراقبة جميع الأسلحة النارية، سواء كانت عادية أو مجمعة، في عمليات الوسم وحفظ السجلات والتعقب؛ وتحديد المعلومات التي ينبغي تدوينها على عنصر المراقبة لتجنب الازدواجية في الأرقام المسلسلة؛ وتقديم إرشادات بشأن المحددات الفريدة للهوية لأغراض التعقب، ولا سيما فيما يخص الأسلحة المصنوعة.<sup>(٣٩)</sup>

## ٣- الأسلحة المصنوعة بتكنولوجيا الصنع بالإضافة (الطباعة المجسمة)

٢٦- تكنولوجيا الصنع بالإضافة (additive manufacturing) المعروفة عامة باسم الطباعة المجسمة أو الطباعة الثلاثية الأبعاد هي تكنولوجيا ناشئة قد تكون لها آثار على الأمن المحلي والوطني والدولي على المدينين القريب والبعيد. ويمكن لتطويرها وانتشارها أن يعجلاً إلى حد كبير بانتشار الأسلحة، وقد تكون لهما عواقب وخيمة على الجرائم اليومية. وعلاوة على ذلك، قد يكون للأسلحة النارية المصنوعة بأسلوب الطباعة المجسمة أثر سلبي على فعالية نظم تسجيل الأسلحة النارية وترخيصها وقواعد بيانات المقذوفات النارية المستخدمة في تحقيقات الشرطة.

٢٧- وأحكام المادة ٣ (د) والفقرة ١ (أ) من المادة ٥ من بروتوكول الأسلحة النارية المتعلقة بالصنع غير المشروع للأسلحة النارية تنطبق على الأسلحة النارية المصنوعة بالطباعة المجسمة مثلما تنطبق على الأسلحة النارية المصنوعة بالأساليب التقليدية، لكن تنزيل الملفات الرقمية من أجل صنع الأسلحة النارية بأسلوب الطباعة المجسمة غير مشمول فيما يبدو بالبروتوكول، مما يتطلب اتخاذ تدابير تشريعية عاجلة لتدارك الأمر.

(٣٨) Giacomo Persi Paoli, "From firearms to weapon systems: challenges and implications of modular design for marking, record-keeping, and tracing", in *Behind the Curve: New Technologies, New Control Challenges*, Occasional paper of the Small Arms Survey, No. 32, Benjamin King and Glenn McDonald, eds. (Geneva, Small Arms Survey, 2015), p. 23

(٣٩) المرجع نفسه، الصفحة ٤٠.



٢٨- والأسلحة النارية المصنوعة بأسلوب الطباعة المجسمة مشمولة بالعديد من القوانين والجرائم الحالية المتعلقة بصنع الأسلحة النارية وتكوينها وحيازتها دون ترخيص، ولكن تلك القوانين والجرائم لا تتعلق بالضرورة بجائزة ملفات التصميم أو توزيعها.<sup>(٤٠)</sup> وقد يلزم أن تحدد القوانين المتعلقة بالصنع غير المشروع للأسلحة النارية جوانب مسؤولية الأطراف الثالثة عندما تتيح آلات الطباعة المجسمة لأشخاص يرغبون في استعمالها لإنتاج أسلحة نارية.<sup>(٤١)</sup>

٢٩- ويتعين أن يشمل أي نهج تنظيمي شامل الجهات الفاعلة المحلية والدولية، وكذلك القطاعين العام والخاص على السواء. ولما كانت تكنولوجيا الطباعة المجسمة قابلة للاستعمال المزدوج، فإن من المستحيل الحد من انتشارها دون الحد أيضاً من فوائدها العديدة.<sup>(٤٢)</sup> وكما هو الحال بالنسبة لأي تكنولوجيا ناشئة، سيكون من المهم توفير برامج للتدريب والتعليم لموظفي إنفاذ القانون.

#### ٤- الاتجار بالأسلحة النارية على الشبكة الخفية

٣٠- يمكن أن تتحول الشبكة الخفية إلى ساحة مفضلة لأعضاء الجماعات الإجرامية المنظمة والأفراد الذين يريدون شراء أسلحة نارية دون الكشف عن هويتهم أو لأغراض غير مشروعة.<sup>(٤٣)</sup> وفي ضوء دراسة أعدتها مكتب الأمم المتحدة لشؤون نزع السلاح على أساس مشروع بحثي أكبر أجرته مؤسسة RAND Europe في عام ٢٠١٧،<sup>(٤٤)</sup> وقدمها إلى اللجنة الأولى للجمعية العامة في عام ٢٠١٨، لوحظ أن هناك حاجة ماسة إلى تعاون دولي جديد لمكافحة مبيعات الأسلحة غير المشروعة التي أصبحت ممكنة من خلال حجب الهوية في الشبكة الخفية.<sup>(٤٥)</sup>

٣١- ويبدو أن حجم مبيعات الأسلحة عبر الشبكة الخفية أقل من حجم مبيعات غيرها من البضائع غير المشروعة.<sup>(٤٦)</sup> وتبين دراسة حديثة تركز فقط على قوائم السلع المتصلة بالأسلحة المعروضة على الشبكة الخفية أن قوائم الأسلحة النارية هي الأكثر شيوعاً، حيث تشكل نسبة ٤٢ في المائة من جميع القوائم على الشبكة الخفية، تليها المنتجات الرقمية المتصلة بالأسلحة بنسبة ٢٧ في المائة، ومنتجات أخرى مثل الذخيرة بنسبة ٢٢ في المائة.<sup>(٤٧)</sup>

(٤٠) INTERPOL Innovation Paper, "3D and 4D printing", INTERPOL Global Complex for Innovation, 2018, p. 6

(٤١) N. R. Jenzen-Jones, "Small arms and additive manufacturing: An assessment of 3D-printed firearms, components, and accessories", in *Behind the Curve: New Technologies, New Control Challenges*, Occasional paper of the Small Arms Survey, No. 32, Benjamin King and Glenn McDonald, eds. (Geneva, Small Arms Survey, 2015), pp. 63-64

(٤٢) Trevor Johnston, Troy D. Smith and J. Luke Irwin, "Additive manufacturing in 2040: powerful enabler, disruptive threat", document No. PE-283-RC (Santa Monica, California, RAND Corporation, 2018), p. 17

(٤٣) RAND Europe, "International arms trade on the dark web" (2019), Findings section, para. 8

(٤٤) Giacomo Persi Paoli and others, *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web* (Santa Monica, California, RAND Corporation, 2017)

(٤٥) Giacomo Persi Paoli, *The Trade in Small Arms and Light Weapons on the Dark Web*, United Nations Office for Disarmament Affairs (UNODA) Occasional Papers, No. 32 (United Nations publications, Sales No. E.19.XI.1), p. ix

(٤٦) Damien Rhumorbarbe and others, "Characterising the online weapons trafficking on cryptomarkets", *Forensic Science International*, vol. 283, December 2018, pp. 16-20

(٤٧) RAND Europe, "International arms trade on the dark web" (2019), Findings section, para. 4

٣٢- ولا غنى عن السعي لمعرفة حجم ونطاق تجارة الأسلحة غير المشروعة عبر الشبكة الخفية من أجل التوصل إلى فهم أفضل لدى أجهزة إنفاذ القانون لما تمثله تلك التجارة من خطر وما يترتب عليها من آثار. فعلى الصعيد الوطني، ينبغي لوضعي السياسات الحرص على تزويد أجهزة إنفاذ القانون بما يكفي من الموظفين والمعدات والتدريب للتصدي للتحديات ذات الصلة. وقد توفر الأطر القانونية الدولية القائمة، ولا سيما اتفاقية الجريمة المنظمة وبروتوكولها الخاص بالأسلحة النارية، أساساً لاعتماد نهج شاملة للتصدي لهذه الظاهرة. ويلزم إجراء تحليل متعمق لما إذا كانت تسري عليها لوائح السمسرة القائمة، المنصوص عليها في بروتوكول الأسلحة النارية (المادة ١٥) ومعاهدة تجارة الأسلحة (المادة ١٠).<sup>(٤٨)</sup>

#### ٥- الأسلحة الفتاكة الذاتية التشغيل

٣٣- على الرغم من عدم وجود اعتراف رسمي بوجود أسلحة ذاتية التشغيل بالكامل، فإن فكرة استخدام الذكاء الاصطناعي للتحكم في أسلحة من هذا القبيل توجب مناقشات حادة. ففي عام ٢٠١٦، أنشأ المؤتمر الاستعراضي الخامس للأطراف المتعاقدة السامية في اتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر فريق الخبراء الحكوميين المعني بالتكنولوجيات الناشئة في مجال منظومات الأسلحة الفتاكة الذاتية التشغيل. وأوصى الفريق، في دورته لعام ٢٠١٩، بأن تؤيد الأطراف المتعاقدة السامية المبادئ التوجيهية التي أكدها الفريق.<sup>(٤٩)</sup>

#### دال- الاتجار بالأشخاص

٣٤- تبين البحوث التي أجريت على مدى السنوات الماضية والأدلة المباشرة أن المتجرين بالبشر يستخدمون التكنولوجيا خلال جميع مراحل الجريمة، بما في ذلك تصيد الضحايا ومراقبتهم واستغلالهم.

٣٥- وأحد الأسباب التي تجعل المتجرين يستخدمون التكنولوجيا في عملهم هو أنها تمكنهم من العمل دون الكشف عن هويتهم، كما أن العملة المشفرة تسمح لهم بإجراء معاملات مالية ونقل العائدات الإجرامية دون الكشف عن هويتهم. أما السبب الثاني، فهو أن التكنولوجيا تيسر لهم تصيد الضحايا واستغلالهم، حيث يمكن استخدام مواقع الإعلانات المبوبة على الإنترنت وشبكات التواصل الاجتماعي كقنوات للاتجار بالبشر.<sup>(٥٠)</sup>

٣٦- وعلاوة على ذلك، فإن إساءة استخدام التكنولوجيا يمكن أن تيسر على المتجرين إبرام معاملات مع زبائنهم، ودخول أسواق جديدة، وتوسيع نطاق العمليات الإجرامية. ويمكن

(٤٨) Simonetta Grassi and Mareike Buettner, "Annex: overview of international legal instruments and their applicability to illicit firearms trafficking on the dark web", in Paoli and others, *Behind the Curtain*, p. 101.

(٤٩) الوثيقة CCW/GGE.1/2019/3، المرفق الرابع.

(٥٠) Mark Latonero, *Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds*, Centre on Communication Leadership and Policy Research Series (Los Angeles, University of Southern California, September 2011), p. 8.

للمتجّرين استخدام تطبيقات البث المباشر للوصول إلى سوق أوسع لزبائن ربما لم يسبق لهم قط أي اتصال فعلي بالضحية.<sup>(٥١)</sup>

٣٧- وعلاوة على ذلك، فإن إساءة استخدام التكنولوجيات يمكن أن تساعد المتّجرين على مراقبة الضحايا وإكراههم. ويمكن للمتجّرين أن يستفيدوا من تطبيقات تتبع الحركة وتحديد المكان لتيسير استغلال الضحايا. وحتى بعد أن يفلت الضحايا من قبضة المتّجرين، يظل من الممكن تعقبهم حيث يكتشف الجناة أماكن وجود ضحاياهم باستخدام تطبيقات تتبع الحركة وتحديد المكان الموجودة في الهواتف النقالة للضحايا.

٣٨- وفي الوقت نفسه، تستخدم أجهزة إنفاذ القانون بالفعل تطبيقات تتبع الحركة وتحديد المكان للكشف عن مكان وجود المتّجرين المشتبه فيهم أو غيرهم من الأفراد المشاركين في شبكة الاتّجار. واستعمال بيانات تتبع الحركة وتحديد المكان الخاصة بالضحايا على هذا النحو هو الوجه الآخر للعملة نفسها، حيث يمكن استخدام الضحايا كقواعد بيانات متحركة لجمع الأدلة.<sup>(٥٢)</sup>

٣٩- واستخدام التكنولوجيا في جهود مكافحة الاتّجار أمر يتطلب التعاون على نطاق قطاعات مختلفة. وقد أقامت دوائر صناعة تكنولوجيات المعلومات والاتصالات والمنظمات الدولية شراكة لاستكشاف كيفية تسخير التكنولوجيات لأغراض منع الاتّجار بالأشخاص والمساعدة على إعادة تأهيل الضحايا. ويقدم ائتلاف التكنولوجيا ضد الاتّجار (Tech Against Trafficking)، الذي يضم شركات تكنولوجيا بارزة ومؤسسات أكاديمية والمنظمة الدولية للهجرة، قائمة بحلول تكنولوجية لمكافحة الاتّجار بالبشر.<sup>(٥٣)</sup>

٤٠- والعمل على بناء قدرات جميع الجهات الفاعلة المعنية مقوم محوري للتغلب على تحديات استخدام التكنولوجيا في الاتّجار بالأشخاص. ويجب إجراء دراسات دقيقة من أجل تطوير التكنولوجيا التي يستخدمها الممارسون من أجل مكافحة الاتّجار بالأشخاص وتعهده هذه التكنولوجيا ورصدها وتقييمها،<sup>(٥٤)</sup> على أن يُراعى في تطوير تلك الأدوات، التي يمكن أن يستعين بها الأشخاص المعرضون لخطر الاتّجار بهم في حماية أنفسهم، التحسب للاختلافات القائمة بينهم واستيعاب تلك الاختلافات.<sup>(٥٥)</sup>

(٥١) Inter-Agency Coordination Group against Trafficking in Persons, "Human trafficking and technology: trends, challenges and opportunities", Issue brief, No. 7 (2019), pp. 1-2.

(٥٢) Felicity Gerry, Julia Muraszkiwicz and Niowi Vavoula, "The role of technology in the fight against human trafficking: reflections on privacy and data protection concerns", *Computer Law and Security Review*, vol. 32, No. 2 (April 2016), pp. 210-211.

(٥٣) Business for Social Responsibility, "List of technology tools and initiatives identified by tech against trafficking", 15 January 2019.

(٥٤) Inter-Agency Coordination Group against Trafficking in Persons, "Human trafficking and technology", p. 4.

(٥٥) انظر Mark Latonero, Bronwyn Wex and Meredith Dank, *Technology and Labor Trafficking in a Networked Society: General Overview, Emerging Innovations, and Philippines Case Study* (Los Angeles, University of Southern California, Annenberg Center on Communication Leadership and Policy, 2015), p. 11.

## هاء- تهريب المهاجرين

٤١- أصبحت تكنولوجيا المعلومات والاتصالات أداة مهمة يستخدمها المهاجرون ومن يوقعون بهم على حد سواء على نطاق واسع لنقل المعلومات عن الدروب والخدمات والأسعار.<sup>(٥٦)</sup> وعلاوةً على ذلك، زادت وسائط التواصل الاجتماعي من قدرة المهريين على تغيير الدروب للإفلات من التدابير التي تتخذها أجهزة إنفاذ القانون في بلدان العبور للتصدي لهم، مما زاد من فعالية عمليات التهريب وعرقل التحقيق في مثل هذه الجرائم وملاحقة مرتكبيها قضائياً.<sup>(٥٧)</sup>

٤٢- ويمكن أن تترتب على التطور السريع في تكنولوجيا الأجهزة المحمولة آثار على العلاقة بين المهاجرين والمهريين. ففي العديد من مجموعات الفيسبوك، يمكن للمهاجرين التحقق من موثوقية بعض المهريين وتبادل المعلومات حول أفضل الأشخاص الذين يمكن أن يتصل بهم. وقد وُصفت عمليات الاستيثار تلك بأنها "سلم الجدارة بالثقة".<sup>(٥٨)</sup>

٤٣- ويمكن أيضاً استخدام التكنولوجيا في الدفع المالي، لأن المدفوعات للمهريين تتم أساساً من خلال نظم الدفع عبر الإنترنت. وقد تزيد العملات المشفرة من السهولة التي يتمكن بها المهربون من تلقي الأموال وإخفائها ونقلها. ويمكن لهذه العملات أن تساعد على غسل الأموال وأن تعين المهريين على تجنب التعرض للتحقيق أو التوقيف من خلال حجب هويتهم والحد من الحاجة إلى حمل مبالغ نقدية كبيرة.

٤٤- وتضطلع التكنولوجيا كذلك بدور رئيسي في إتاحة وثائق السفر أو الهوية المزورة التي تيسر تهريب المهاجرين. وتستخدم أنواع مختلفة من المعدات لتزييف جوازات السفر أو تزويرها أو نسخها بطرائق احتيالية. وفي بعض الحالات، تستخدم أدوات متقدمة تكنولوجياً لتنفيذ عمليات تزييف عالية الجودة (إعداد جوازات سفر مطابقة تماماً للجوازات الصحيحة).<sup>(٥٩)</sup>

٤٥- بيد أنه يمكن النظر إلى الابتكارات التكنولوجية من زوايا متعددة وليس فقط من منظور الفوائد التي تعود بها على المهريين. وتقلل الرقمنة أيضاً الفجوات في المعلومات التي يمكن للمهريين استغلالها. ويمكن أن تكون الإنترنت وسيلة مفيدة لمساعدة المهاجرين على التواصل مع الشبكات الاجتماعية للدعم والمعلومات. ويتمثل أحد الاتجاهات الأخيرة المنبثقة عن التحول القائم على التكنولوجيا في أن عدداً متزايداً من المهاجرين يتمتعون بالاكتماء الذاتي طوال عملية الهجرة ويعتمدون بدرجة أقل على المهريين. ويعطي هذا المهاجرين قدراً أكبر من الاستقلالية ويقلل من تعرضهم للاستغلال.<sup>(٦٠)</sup>

(٥٦) Europol and INTERPOL, "Migrant smuggling networks: executive summary" (May 2016), p. 8

(٥٧) الوثيقة CT0C/COP/WG.7/2018/2، الفقرة ٢٥.

(٥٨) Judith Zijlstra and Ilse van Liempt, "Smart(phone) travelling: understanding the use and impact of mobile technology on irregular migration journeys", *International Journal of Migration and Border Studies*, vol. 3, Nos. 2 and 3 (March 2017), pp. 176-177

(٥٩) UNODC Regional Office for South-East Asia and the Pacific, *Facilitators of Smuggling of Migrants in Southeast Asia: Fraudulent Documents, Money Laundering, and Corruption* (Bangkok, 2019), p. 26

(٦٠) مكتب الأمم المتحدة المعني بالمخدرات والجريمة، إعلان الدوحة، التعليم الجامعي، النمائط الجامعية لمبادرة "التعليم من أجل العدالة"، تهريب المهاجرين والاتجار بالأشخاص، النميطه ١٤: أوجه الترابط بين الجريمة السيبرانية

٤٦ - وتختلف كيفية استخدام المهاجرين لوسائل التواصل الاجتماعي باختلاف جنسيتهم وانتمائهم العرقي وموطنهم الأصلي وخلفيتهم التعليمية، وكذلك بمدى قدرتهم على الوصول إلى الإنترنت واستعمالها.<sup>(٦١)</sup> وقد أظهرت الأدلة أن هناك فجوة رقمية بين مجموعات المهاجرين تقوم على تفاوت قدرتهم الفعلية على الوصول إلى التكنولوجيا الرقمية واستخدامها، والمهارات اللازمة لاستخدام مختلف التكنولوجيات بفعالية، والقدرة على دفع تكاليف الخدمات.<sup>(٦٢)</sup>

٤٧ - ومن منظور إنفاذ القانون، هناك اهتمام متزايد بإيجاد سبل لاستغلال التكنولوجيا لتعطيل شبكات تهريب المهاجرين. كما أن الأدلة المتحصّل عليها من وسائط التواصل الاجتماعي و/أو من خلال استخدام التكنولوجيا قد تدعم شهادات المهاجرين المهرّبين في الإجراءات الجنائية ذات الصلة.

٤٨ - ويساعد الاستخدام المناسب للتكنولوجيا الحكومات والقطاع الخاص والمنظمات غير الحكومية على منع تهريب المهاجرين والتخفيف من حدته، كلٌّ في مجالات اختصاصه. ولذلك، فإنه من المهم للغاية زيادة فعالية تدابير العدالة الجنائية وتقديم حوافز تشجع مقدمي خدمات الإنترنت على تحسين عمليات رصد المحتويات المتصلة بجرائم التهريب وكشفها والإبلاغ عنها وتكوين شراكات معهم لهذا الغرض.

## واو- الاعتداء على الأطفال واستغلالهم باستخدام الإنترنت

٤٩ - على الرغم من أن جرائم الاعتداء على الأطفال واستغلالهم جنسيا موجودة من قبل ظهور الإنترنت، فإن البعد الإلكتروني لهذه الجرائم قد مكّن الجناة من التفاعل فيما بينهم والحصول على مواد الاستغلال الجنسي للأطفال عبر الإنترنت. وعلاوة على ذلك، فإن العدد المتزايد من الأطفال الصغار الذين يمكنهم الوصول إلى الإنترنت قد منح الجناة فرصة للوصول إلى الأطفال بسهولة أكبر - مقارنةً بالبيئة غير المتصلة بالإنترنت - وكان لذلك بدوره آثار كبيرة على طريقة عمل مرتكبي الجرائم ذات الصلة.

٥٠ - وأصبح التقدم في التكنولوجيا محورياً في الاستغلال الجنسي التجاري للأطفال. ويمكن للسياح الذين يمارسون الجنس مع الأطفال الاستفادة من تطبيقات الحوسبة السحابية لتخزين الصور أو مقاطع الفيديو، ومن ثمّ تجنب المخاطرة بالنقل الفعلي لمواد تصور اعتداءات جنسية على الأطفال. وعلاوة على ذلك، تربط تكنولوجيا الهاتف المحمول بين منظّمي عمليات استغلال الأطفال والاعتداء عليهم جنسياً والضحايا والمستهلكين، ومن ثمّ، تقل حاجة المنتجين والموزعين إلى الحضور شخصياً أثناء المعاملات، مما يؤدي بدوره إلى تحسين فرصهم في تحاشي كشف أمرهم.

وتهريب المهاجرين والاتجار بالأشخاص - التكنولوجيا في تهريب المهاجرين (links between cybercrime, trafficking in persons and smuggling of migrants - Technology in smuggling of migrants). متاحة في:

[www.unodc.org/e4j/](http://www.unodc.org/e4j/)

(٦١) European Commission, "The use of social media in the fight against migrant smuggling", European Migration Network (EMN) Inform (September 2016).

(٦٢) Alam Khorshed and Sophia Imran, "The digital divide and social inclusion among refugee migrants: a case in regional Australia", *Information Technology and People*, vol. 28, No. 2 (June 2015), pp. 344 ff.

٥١ - وتشمل الأشكال الرئيسية للاعتداء على الأطفال واستغلالهم، التي تيسرها تكنولوجيات المعلومات والاتصالات، تعريضهم لمشاهدة مواد إباحية، واستخدام الإنترنت في إغوائهم أو محاولة استمالتهم لأغراض جنسية غير مرغوبة، والكثير من أفعال الاستغلال تلك ينطوي على أنشطة جنسية غير لائقة مع الأطفال. وتلفت دراسة ذات صلة أجراها المكتب الانتباه إلى الأشكال الجديدة للاعتداء على الأطفال واستغلالهم، مثل استغلالهم في الصور واللقطات التي يأخذها لهم مستعمل الإنترنت (المحتوى الذي ينتجه المستعمل) أو الصور واللقطات الذاتية (المحتوى الذاتي الإنتاج)، بما في ذلك تبادل الرسائل الجنسية، وبث لقطات حية للاعتداء الجنسي على الأطفال، ومواد معدة حسب الطلب تصور اعتداءات جنسية على الأطفال.<sup>(٦٣)</sup>

٥٢ - ووفقاً لليوروبول، أصبح بث اللقطات الحية للاعتداءات الجنسية خطراً حقيقياً، ويتم بث تلك اللقطات من خلال تطبيقات وسائل التواصل الاجتماعي وتطبيقات الدردشة المرئية ومنصات الألعاب وغرف الدردشة على الإنترنت. وعلاوة على ذلك، يبدو أن هناك انتقالاً من استخدام الحاسوب إلى استخدام الهواتف الذكية والأجهزة اللوحية، ومن الإنترنت الكابلي إلى الاتصال بالإنترنت لاسلكياً (Wi-Fi) والإنترنت المحمول.<sup>(٦٤)</sup>

٥٣ - ومن أهم المخاطر في توزيع مواد الاستغلال الجنسي للأطفال عبر الإنترنت الزيادة المستمرة في استخدام الشبكة الخفية، حيث أشارت مؤسسة رصد الإنترنت (Internet Watch Foundation) إلى أن المواقع الشبكية المقتنعة، التي تستخدم طريقة "المسار الرقمي" لإخفاء صور الاعتداء الجنسي على الأطفال، لا تزال تمثل مشكلة كبيرة. وعلاوة على ذلك، لاحظت المؤسسة حدوث زيادة مطردة في عدد عناوين المواقع الشبكية للاعتداء الجنسي على الأطفال في السنوات الأخيرة: من ٦٨ ٠٩٢ عنواناً في عام ٢٠١٥ إلى ١٠٥ ٠٤٧ عنواناً في عام ٢٠١٨.<sup>(٦٥)</sup>

٥٤ - وعلاوة على ذلك، فإن الأشخاص الذين يسعون إلى الاعتداء على الأطفال جنسياً باستخدام الإنترنت سوف يواصلون البحث عن سبل جديدة لتجنب الانكشاف كلما ازدادت مهارتهم التقنية. وفي الآونة الأخيرة، حدث تحول من استخدام المنتديات الكبيرة إلى تشكيل مجموعات صغيرة من المستعملين، وهو ما تيسره تطبيقات التراسل بالأجهزة المحمولة مع تشفير عمليات التراسل من بدايتها إلى نهايتها.

٥٥ - ومما يثير مشاكل كبيرة تعرقل محاولات كشف الجناة والتحقيق معهم وملاحقتهم قضائياً وتقلل من فرص نجاحها افتقار عدد من البلدان لأحكام قانونية واجبة التطبيق من أجل تنظيم التعامل مع الأشكال المستجدة للاعتداء على الأطفال والاختلافات القائمة في القوانين التي تحمي الأطفال وتحدد السن التي يمكن فيها إبداء الرضا.

(٦٣) UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* (Vienna, 2015), pp. 21 ff

(٦٤) Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2018*, p. 35

(٦٥) Internet Watch Foundation, *Once Upon a Year* (Cambridge, United Kingdom, 2018), pp. 19 and 43

٥٦- لكن التكنولوجيا تتيح أيضاً لأجهزة إنفاذ القانون سبباً للتصدي للمشاكل ذات الصلة.<sup>(٦٦)</sup> فالأساليب والتقنيات المتكررة، مثل تقنيات التنقيب في البيانات (data mining) وتحليلها الحاسوبي المنهجي (analytics)، تحسن عمليات الاستدلال العلمي الجنائي على نحو يفيد التحقيقات. وينبغي أن يُراعى في تطبيق التقنيات، التي تستخدم تكنولوجيا المعلومات، احترام حقوق الإنسان وعدم تجاوز الحدود التي تحميها، وذلك بسبب الطبيعة الصادمة للجرائم الاستغلال الجنسي للأطفال وصغر سن الشهود من الأطفال وضعفهم.

٥٧- وقد أنشئت أيضاً قواعد بيانات خاصة لتحليل المواد التي تصور الاعتداءات الجنسية على الأطفال لاستخدامها كأدلة في التحقيقات، مثل قاعدة البيانات الدولية للاستغلال الجنسي للأطفال التابعة للمنظمة الدولية للشرطة الجنائية. وفي الولايات المتحدة الأمريكية، تستخدم قاعدة بيانات المركز الوطني للأطفال المفقودين والمستغلين كمستودع مركزي لتخزين المواد المتعلقة بالاعتداءات الجنسية على الأطفال.<sup>(٦٧)</sup>

٥٨- وتتطلب الجهود الرامية إلى مكافحة الفعالة لضروب الاعتداء على الأطفال واستغلالهم التي تيسرها تكنولوجيا المعلومات والاتصالات الأخذ بنهج قائم على تعدد أصحاب المصلحة، يشمل ويُشرك بنشاط الأطفال والأسر والمجتمعات المحلية والحكومات والمجتمع المدني والقطاع الخاص في التصدي لتلك الجرائم.<sup>(٦٨)</sup>

## زاي- الذكاء الاصطناعي والروبوتيات

٥٩- بعد أن أفضت الإنترنت وتكنولوجيا الأجهزة المحمولة إلى "الثورة الصناعية الثالثة"، تُوَجِّح تكنولوجيايات الذكاء الاصطناعي، التي تستند إلى البيانات الضخمة،<sup>(٦٩)</sup> "الثورة الصناعية الرابعة". وفي حين أن ذلك يمكن أن يكون مفيداً للتنمية العالمية والتغير المجتمعي، من خلال الإسهام في تحقيق أهداف التنمية المستدامة، تنشأ أيضاً شواغل وتحديات قانونية وأخلاقية ومجتمعية. وفي مجال إنفاذ القانون، يمكن أن يؤدي التقدم في مجال الذكاء الاصطناعي إلى إتاحة فرص وإثارة مخاطر على حد سواء، ولذا يلزم اتباع نهج استراتيجي والاستثمار في الجهود والموارد.<sup>(٧٠)</sup>

٦٠- وشددت جميع الاجتماعات الإقليمية التحضيرية للمؤتمر الرابع عشر تقريباً على ضرورة وأهمية استكشاف السبل والوسائل الكفيلة بتمكين العاملين في مجال العدالة الجنائية وإنفاذ القانون

(٦٦) Victoria Brains, "Online child sexual exploitation: towards an optimal international response", *SSRN Electronic Journal*, 29 August 2018.

(٦٧) مكتب الأمم المتحدة المعني بالمخدرات والجريمة، إعلان الدوحة، التعليم الجامعي، النماذج الجامعية لمبادرة "التعليم من أجل العدالة"، الجريمة السيبرانية، النميطة ١٢: الجريمة السيبرانية المرتكبة في أوساط الأشخاص - الاستغلال الجنسي للأطفال والاعتداء عليهم جنسياً عبر الإنترنت (interpersonal cybercrime-online child sexual exploitation and abuse). متاحة في: [www.unodc.org/e4j/](http://www.unodc.org/e4j/).

(٦٨) UNODC, *Study on the Effects of New Information Technologies*.

(٦٩) Victor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution that Will Transform How We Live, Work and Think* (London, John Murray, 2013).

(٧٠) أنشأ معهد الأمم المتحدة الأقليمي لبحوث الجريمة والعدالة مركزاً معنياً بالذكاء الاصطناعي والروبوتيات في لاهاي ليكون جهة مرجعية دولية في المسائل المتصلة بالذكاء الاصطناعي والروبوتيات.

من توظيف التكنولوجيات المتطورة، مثل الذكاء الاصطناعي وتكنولوجيات المعلومات والاتصالات، بما في ذلك البيانات الضخمة، والاستفادة الكاملة منها في مكافحة الجريمة.<sup>(٧١)</sup>

٦١- ومن المسائل المطروحة للنقاش في هذا الشأن، استخدام الذكاء الاصطناعي لإجراء عمليات تشريح افتراضية، وإيجاد نُظُم تساعد الشرطة على التنبؤ بالجريمة من أجل تحسين الاستفادة من الموارد على النحو الأمثل، وأدوات للكشف عن السلوك، ونُهَجٍ للتتبع تستند إلى تقنية سلاسل كتل البيانات المشفرة وتحترم الخصوصية، ومركبات للدورية ذاتية القيادة.<sup>(٧٢)</sup> وعلاوة على ذلك، فإن التقدم المحرز في ميدان الذكاء الاصطناعي، الذي زاد من ذكاء الروبوتيات وجعلها قادرة على أن تقوم بالعديد من الوظائف والمهام بدلا من البشر، قد شجع عدداً متزايداً من أجهزة إنفاذ القانون على الاستفادة من أوجه التقدم التكنولوجي تلك في مجموعة متنوعة من عملياتها. لكن مستوى استخدام الروبوتيات ليس واحداً بين جميع البلدان في ضوء التفاوتات القائمة بينها في التقدم في مجالات البحث في تلك التكنولوجيات واستخدامها.<sup>(٧٣)</sup>

٦٢- ويبدو أن تكنولوجيات الذكاء الاصطناعي والتعلم الآلي توفر سبباً متزايداً للوقاية من غسل الأموال. فعلى غرار الخوارزميات التي تساعد تجار التجزئة عبر الإنترنت على استهداف الزبائن، يمكن لتكنولوجيات الذكاء الاصطناعي والتعلم الآلي أن تدعم سياسات لتوحيي العناية الواجبة أكثر تبصراً بالنشاط الإجرامي ودقة في استشعاره من خلال تفسير علاماته الدالة عليه وتحليل كميات أكبر بكثير من البيانات، وأن تقوم بذلك على نحو أكثر موثوقية. وعلاوة على ذلك، توظف منصات وسائل التواصل الاجتماعي تقنيات التعلم الآلي بشكل متزايد لمنع المواد ذات المحتوى غير المشروع والأخبار الزائفة. وتستخدم المنشآت التجارية الذكاء الاصطناعي لإدارة المخاطر الأعلى وكشف الاحتيال والتصدي له من أجل منع الجرائم والتنبؤ بها.

٦٣- بيد أن الذكاء الاصطناعي هو إلى حد كبير جدا سلاح ذو حدين، لأنه يمكن أن يؤدي إلى تغيرات كبيرة في الطريقة التي تتعامل بها أجهزة إنفاذ القانون مع مهمة حفظ الأمن، ولكنه يعزز أيضاً أساليب عمل الجماعات الإجرامية والإرهابية، بل ويمكن أن يبسر ظهور أشكال جديدة من الجريمة.<sup>(٧٤)</sup> والأولوية في ذلك الصراع، الذي يمكن تشبيهه استعارياً بمعركة بين خصمين سيكتب فيها "البقاء للأقوى"،<sup>(٧٥)</sup> هي عبارة موجزة تعزز حفظ الأمن بالاستعانة بتقنيات الذكاء الاصطناعي لمكافحة الجرائم القائمة على الذكاء الاصطناعي.

(٧١) الوثيقة A/CONF.234/RPM.1/1، الفقرة ٦١ (ي)؛ والوثيقة A/CONF.234/RPM.2/1، الفقرة ٧٩ (ك)؛ والوثيقة A/CONF.234/RPM.3/1، الفقرة ٥٦ (و)؛ والوثيقة A/CONF.234/RPM.4/1، الفقرة ٥٧ (هـ).

(٧٢) INTERPOL and UNICRI, "Artificial intelligence and robotics for law enforcement" (Turin, Italy, 2019), p. v

(٧٣) المرجع نفسه، الصفحة ٦.

(٧٤) فحص تقرير صادر في عام ٢٠١٨ التهديدات المتعلقة بإساءة استخدام الذكاء الاصطناعي للأغراض الإجرامية، وحدد منها ثلاث فئات رئيسية: (أ) التهديدات المرتبطة بالأمن الرقمي؛ و(ب) التهديدات المرتبطة بالأمن المادي؛ و(ج) التهديدات المتعلقة بالأمن السياسي (نشر الأخبار الزائفة والتضليل الآلي أو التأثير على الحملات على نحو يمس سلامة سلوكيات التصويت وربما تقويض القدرة على الحفاظ على صدق النقاش العام). انظر Miles Brundage and others, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* (February 2018)

(٧٥) INTERPOL Innovation Paper, "Artificial intelligence", INTERPOL Global Complex for Innovation, 2018, p. 2



## حاء- التعاون الدولي في المسائل الجنائية واستخدام التكنولوجيا

٦٤- يدور نقاش في ميدان التعاون الدولي في المسائل الجنائية حول كيفية الاستفادة الكاملة من التكنولوجيا الحديثة في عمل السلطات المركزية. ومن منظور السياسات العامة، شجّع مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية الدول الأطراف في عام ٢٠١٦ على الاستفادة التامة على خير وجه من التكنولوجيات المتاحة لتيسير التعاون بين السلطات المركزية.<sup>(٧٦)</sup>

٦٥- وتلبية الحاجة المتزايدة لتعزيز التعاون الدولي مسألة مرهونة بتوافر الموارد اللازمة، بما في ذلك "الموارد التكنولوجية"، مثل شبكات الإرسال الآمن للمعلومات، والمعدات التي تيسر الاتصال (مثل التداول عن بعد والتداول بالفيديو)، ونظم إدارة القضايا لتتبع الطلبات الواردة والصادرة. ويمكن أيضاً ربط الحاجة المتزايدة إلى الموارد بزيادة الكفاءة في معالجة طلبات المساعدة القانونية المتبادلة بأدلة الإثبات الإلكترونية (مثلاً، من خلال إنشاء وحدات متخصصة داخل السلطات المركزية).

٦٦- ومن الواضح أن أساليب إدارة القضايا في السلطات المركزية تجسد أوجه التقدم أو القصور في جميع الآليات المؤسسية للعدالة الجنائية في الدول الأعضاء، وفقاً لتفاوت مستويات القدرة. ففي كثير من البلدان، التي لا تزال تحفظ القيود في سجلات ورقية، يمكن أن يغدو البحث في تلك السجلات وتقديم الوثائق ذات الصلة إلى البلد الطالب مهمة شاقة، أما في البلدان التي تصدر المشهد التكنولوجي، فإن التكنولوجيا الحديثة تتيح لها استخدام المنصات الإلكترونية لإدارة طلبات المساعدة القانونية المتبادلة الواردة والصادرة أو تجميع البيانات الإحصائية عن القضايا والاتجاهات.<sup>(٧٧)</sup>

٦٧- وفي إطار استعراض سبل إحالة طلبات المساعدة القانونية المتبادلة، ناقش اجتماع أمريكا اللاتينية والكاريبي الإقليمي التحضيري للمؤتمر الرابع عشر استخدام الوسائل الإلكترونية لهذا الغرض، وسلط الضوء عليها باعتبارها من الممارسات الجيدة في بعض البلدان في المنطقة.<sup>(٧٨)</sup> وأوصى الاجتماع التحضيري بالتشجيع على استخدام التكنولوجيا لزيادة كفاءة التعاون الدولي في المسائل الجنائية، مع مراعاة جملة أمور منها الاتفاقات المبرمة بين السلطات المركزية فيما يتعلق بإرسال طلبات التعاون الدولي إلكترونياً وفقاً للتشريعات الوطنية.<sup>(٧٩)</sup>

٦٨- وقد اتخذ المكتب إجراءات لتعزيز التعاون الدولي بوسائل مختلفة، منها توفير أدوات وابتكارات تكنولوجية معدة خصيصاً لهذا الغرض، مثل بوابة إدارة المعرفة المعروفة باسم بوابة الموارد الإلكترونية والقوانين المتعلقة بالجريمة (بوابة "شيرلوك")، ودليل السلطات الوطنية المختصة، والنسخة المطورة من أداة كتابة طلبات المساعدة القانونية المتبادلة.<sup>(٨٠)</sup>

(٧٦) قرار المؤتمر ١/٨.

(٧٧) Asian Development Bank and Organization for Economic Cooperation and Development, *Mutual Legal Assistance in Asia and the Pacific: Experiences in 31 Jurisdictions* (2017), p. 31.

(٧٨) الوثيقة A/CONF.234/RPM.3/1، الفقرة ٧٢.

(٧٩) المرجع نفسه، الفقرة ٧٩ (ن).

(٨٠) متاحة في: [www.unodc.org/mla/en/index.html](http://www.unodc.org/mla/en/index.html).

٦٩- ويوفر المكتب دعماً نشطاً للعمليات الحكومية الدولية التي برز فيها التعاون الدولي في المجالات المتعلقة بأدلة الإثبات الإلكترونية كأولوية سياساتية وقانونية. ومن الأمثلة على هذه العمليات تأسيس فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن مشكلة الجريمة السيبرانية،<sup>(٨١)</sup> وتنظيم مناقشة مواضيعية حول الجريمة السيبرانية في الدورة السابعة والعشرين للجنة منع الجريمة والعدالة الجنائية، المعقودة في أيار/مايو ٢٠١٨،<sup>(٨٢)</sup> والأعمال ذات الصلة التي يضطلع بها الفريق العامل المعني بالتعاون الدولي التابع لمؤتمر الأطراف في اتفاقية الجريمة المنظمة.

## طاء- الاعتبارات الأخلاقية: الضمانات الإجرائية والضمانات المتعلقة بحقوق الإنسان

٧٠- يمكن أن تكون الأدوات القائمة على التكنولوجيا مداخل مفيدة للتصدي للتهديدات المتصلة بالجريمة. ومع ذلك، هناك حاجة إلى توجيح الحذر في التطبيق المحدد لهذه الأدوات لضمان الاستخدام المسؤول والأخلاقي وتجنّب العواقب غير المقصودة. ويكتسي هذا الأمر أهمية بالغة بالنظر إلى أن العديد من التكنولوجيات الحالية والمقبلة قد تكون لها آثار خطيرة على الخصوصية الشخصية والحريات المدنية.

٧١- فعلى سبيل المثال، يستخدم موظفو إنفاذ القانون المهنيون برمجيات التعرف على الوجوه لتحديد المشتبه فيهم بسرعة أكبر بكثير. ومع ذلك، يخشى النقاد من أن يؤدي هذا إلى ضروب من المراقبة الحكومية التعسفية والتلاعب المؤسسي والقضاء على الخصوصية. كما أن خاصية الاحتفاظ بالبيانات في النظم البيومترية قد تقوض الخصوصية من خلال احتمال إساءة استخدام البيانات.<sup>(٨٣)</sup>

٧٢- ومن الأمثلة الأخرى استخدام أساليب التحليل التنبؤي للبيانات في حفظ الأمن. فقد شهدت السنوات الماضية تزايداً في عدد أجهزة إنفاذ القانون التي تستخدم برمجيات لتحليل البيانات الإحصائية وإدراك الصلات بين مختلف الأنشطة والحالات، بل حتى التنبؤ بالمكان الذي سينشأ فيه التهديد المقبل. غير أن الخطر يكمن في أن استخدام أجهزة الأمن لأساليب التحليل التنبؤي في توصيف سمات المجرمين قد يؤدي إلى وصم أفراد وجماعات، ومن ثمّ إلى أشكال من التمييز القائم على الخوارزميات.<sup>(٨٤)</sup>

٧٣- وفي مجال مكافحة الاتجار بالأشخاص واستكشاف أوجه التفاعل بين استخدام التكنولوجيا وحقوق الإنسان وحماية البيانات،<sup>(٨٥)</sup> من الضروري ضمان الحماية المعززة للضحايا. وينبغي تصميم

(٨١) يمكن الاطلاع على اجتماعات فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن مشكلة الجريمة السيبرانية في: [www.unodc.org](http://www.unodc.org).

(٨٢) انظر الدليل فيما يخص تلك المناقشة المواضيعية (E/CN.15/2018/6).

(٨٣) Max Snijder, *Biometrics, Surveillance and Privacy* (Ispra, Italy, European Reference Network for Critical Infrastructure Protection (ERNICIP) Thematic Group Applied Biometrics for the Security of Critical Infrastructure, 2016), pp. 4 ff.

(٨٤) انظر Eva Schlehahn and others, "Benefits and pitfalls of predictive policing", in *2015 European Intelligence and Security Informatics Conference: EISIC 2015*, Joel Brynielsson and Moi Hoon Yap, eds. (Piscataway, New Jersey, Institute of Electrical and Electronics Engineers, Inc, 2015), pp. 145-148; Albert Meijer and Martijn Wessels, "Predictive policing: review of benefits and drawbacks", *International Journal of Public Administration*, vol. 42, No. 12 (February 2019).

(٨٥) انظر 5، Inter-Agency Coordination Group Against Trafficking in Persons, "Human trafficking and technology".

حلول مكافحة الاتجار تحت إشراف دقيق حتى لا تفتتت على الحق في الخصوصية أو تستهدف فئات معينة دون مبرر،<sup>(٨٦)</sup> مع ضمان حصول الضحايا أيضاً على التكنولوجيا بأمان.<sup>(٨٧)</sup>

٧٤- وثمة عامل مهم آخر هو الامتثال للضمانات الإجرائية لمقبولية الأدلة المتحصّل عليها بأساليب التحري الخاصة في المحاكم، بما في ذلك الأدلة التي تتطلب استخدام التكنولوجيا. ويخضع إجراء أساليب التحري الخاصة للأحكام ذات الصلة من القوانين المحلية والصكوك المتعددة الأطراف المنطبقة.<sup>(٨٨)</sup> وفي معظم الولايات القضائية، يتطلب جمع الأدلة التقيد الصارم بالضمانات لمواجهة إمكانية إساءة استخدام السلطة، بما في ذلك الإشراف القضائي أو المستقل على استخدام هذه التقنيات ومراعاة مبادئ الشرعية والضرورة والتناسب.<sup>(٨٩)</sup> وينبغي للأدلة الإلكترونية أن تمثل للإجراءات المعمول بها حتى تكون مقبولة.<sup>(٩٠)</sup> وتطبيق المبادئ العامة للقوانين الإجرائية المحلية والاجتهادات القانونية الوطنية بشأن مقبولية الأدلة المتحصّل عليها في تحقيقات الاستدلال الجنائي بشأن العملات المشفرة هو مجال جديد ينطوي على تحديات ويتطلب المزيد من الدراسة وتبادل الخبرات.<sup>(٩١)</sup>

٧٥- ومع تزايد انتشار استخدام تقنيات الذكاء الاصطناعي والروبوتيات لدى أجهزة إنفاذ القانون، تزداد أهمية ضمان أخلاقية ذلك الاستخدام. وقد اتُّخذت مبادرات ذات طابع طوعي غير ملزم من الناحية القانونية للتقليل إلى أدنى حد من مخاطر انتهاك الحقوق الأساسية من جراء استخدام أجهزة إنفاذ القانون لنظم الذكاء الاصطناعي وللتخفيف من غموض المسؤولية القانونية المحيطة باستخدام الأخلاقي للذكاء الاصطناعي والروبوتيات بشكل عام.<sup>(٩٢)</sup>

٧٦- ومع هذا، هناك سؤال أساسي يتعين الإجابة عليه، وهو هل المجتمع بوجه عام جاهز ومستعد تماماً لقبول ممارسات من قبيل إنشاء شبكة واسعة من أجهزة المراقبة، أم قد يَأْبَى ذلك حتى وإن كان في مصلحة السلامة العامة والأمن العام؟<sup>(٩٣)</sup> وينبغي أن تستند القرارات المتعلقة باستخدام الأساليب التكنولوجية إلى حوار اجتماعي واسع النطاق بشأن تكاليفها وفوائدها

(٨٦) Mark Latonero and others, *The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking*, (٨٦) .Research Series on Technology and Human Trafficking (November 2012), p. 38

(٨٧) Gerry, Muraszkiwicz and Vavoula, "The role of technology in the fight against human trafficking", p. 211

(٨٨) انظر المادة ٢٠ من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والمادة ٥٠ من اتفاقية الأمم المتحدة لمكافحة الفساد.

(٨٩) للاطلاع على الاجتهادات القانونية ذات الصلة للمحكمة الأوروبية لحقوق الإنسان، انظر Dimosthenis Chrysikos, "Article 50: special investigative techniques", in *The United Nations Convention against Corruption. A Commentary*, Cecily Rose, Michael Kubiciel and Oliver Landwehr, eds., Oxford Commentaries on International Law Series (Oxford, Oxford University Press, 2019), pp. 507 ff

(٩٠) الوثيقة E/CN.15/2018/6، الفقرة ٣٠.

(٩١) Michael Fröwis and others, "Safeguarding the evidential value of forensic cryptocurrency investigations" (2019)

(٩٢) أصدر معهد المهندسين الكهربائيين والإلكترونيين أطروحة عالمية تتعلق بأخلاقيات النظم المستقلة والذكية (التصميم المتوائم على نحو أخلاقي) لمواكبة التقنيات مع القيم والمبادئ الأخلاقية. انظر IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems* (Pascataway, New Jersey, 2019)

(٩٣) INTERPOL and UNICRI, "Artificial intelligence and robotics for law enforcement", p. 14

والقواعد المنطبقة عليها. وإقناع الجمهور العام بفوائد التكنولوجيا في إنفاذ القانون وتطبيق العدالة الجنائية هو مسألة تدرج في إطار النقاش العام الذي ينبغي أن تجري باستمرار من أجل ضمان عدم فقدان السلطات المختصة ثقة المجتمعات المحلية والمواطنين المكلفة بحمايتهم. وينبغي لهذا النقاش أن يتطرق أيضاً إلى "الوجه الآخر من العملة"، وهو انتقاد زيادة الاعتماد على التكنولوجيا التي يرى أنها قد تفضي أيضاً إلى زيادة الاعتماد على استراتيجيات المراقبة القسرية والتحكم القسري على السواء.<sup>(٩٤)</sup>

٧٧- وأوصى الفريق الرفيع المستوى المعني بالتعاون الرقمي بأن يُجري الأمين العام استعراضاً على نطاق الوكالات لكيفية انطباق الاتفاقات والمعايير الدولية القائمة في مجال حقوق الإنسان على التكنولوجيات الرقمية الجديدة والناشئة. وينبغي دعوة المجتمع المدني والحكومات والقطاع الخاص والجمهور العام إلى إبداء الرأي حول كيفية تطبيق صكوك حقوق الإنسان القائمة في العصر الرقمي في إطار عملية استباقية وشفافة.<sup>(٩٥)</sup>

٧٨- ويلزم تطبيق نهج متوازن لإيجاد حلول لما قد يتبدى من حالات تعارض في تطبيق التكنولوجيا واحترام الخصوصية أو غيرها من حقوق الإنسان. ولتفادي استخدام التكنولوجيات للتحايل على انتهاك الحقوق الأساسية كما لو كانت "حصان طروادة"، فلا بد من رصد تطور التكنولوجيا وتقييم آثاره على نحو مستمر.

### ثالثاً - الاستنتاجات والتوصيات

٧٩- يمكن للمرء استلهام أساطير الإغريق القديمة لعرض المشكلة على النحو التالي: هل التكنولوجيا هي الترياق السحري الشافي لكل الأمراض (الذي كان يدعو الإغريق بـ "الباناسيا" على اسم ابنة الإله أسكليبيوس) الذي يمكن أن يقي المجتمع من الجريمة؟ أم هي وعاء للشورور يمكن أن تكون لها آثار خطيرة من حيث توسيع فرص ارتكاب الجريمة مثل صندوق باندورا (الذي تروي الأسطورة أن باندورا قد فتحتة وخرجت منه كل الشرور لتسكن العالم)؟

٨٠- إن الحقيقة تكمن في المنتصف، بعيداً عن ثنائية الخير المطلق والشر الكامل. والتكنولوجيا هي حتماً نعمة ونقمة في آن واحد. ذلك أن أجهزة إنفاذ القانون والعدالة الجنائية تستفيد من أوجه التقدم في التكنولوجيا. وفي الوقت نفسه، توفر طفرة الابتكارات التكنولوجية تربة خصبة لازدهار الجريمة. وتشهد "ساحة الجريمة" تغيراً جذرياً بسبب مختلف تطبيقات التكنولوجيا الحديثة، ويتعين على السلطات المختصة أن تلحق بالركب.

٨١- والصراع القائم بين المجرمين والمدافعين عن سيادة القانون سوف تتوقف نتائجه إلى حد كبير على مدى الاستثمار في مجالات التدريب ومدى تكييف استراتيجيات منع الجريمة والعدالة

(٩٤) James Byrne and Gary Marx, "Technological innovations in crime prevention and policing: a review of the research on implementation and impact", *Cahiers Politistudies*, vol. 20, No. 3 (2011), p. 30

(٩٥) United Nations, *The Age of Digital Interdependence: Report of the Secretary-General's High-level Panel on Digital Cooperation* (June 2019), recommendation 3A

الجنائية باستمرار مع تطور التحديات المستجدة من أجل التصدي لها ومع مراعاة الاعتبارات الأخلاقية واعتبارات حقوق الإنسان.

٨٢- ولعلّ مؤتمر الأمم المتحدة الرابع عشر لمنع الجريمة والعدالة الجنائية يودُّ أن ينظر في التوصيات الآتية:

(أ) ينبغي للدول الأعضاء أن تحدد وتعالج الثغرات القائمة في نظمها القانونية لضمان التحقيق الفعال في الجرائم التي تيسرها التكنولوجيا وملاحقة مرتكبيها قضائياً، بما يشمل اعتماد قوانين جديدة و/أو تحديث القوانين القائمة بصياغة محايدة تكنولوجياً، وتعزيز التعاون الدولي؛

(ب) ينبغي للدول الأعضاء أن تعزز وتوسّع نطاق الشراكات وأوجه التآزر مع مختلف أصحاب المصلحة، بمن فيهم المنظمات الدولية والإقليمية والمجتمع المدني والقطاع الخاص والأوساط الأكاديمية، من أجل تعزيز البحث والابتكار والتطوير واستخدام التكنولوجيا في مجالي إنفاذ القانون والعدالة الجنائية؛

(ج) ينبغي للدول الأعضاء أن تحدد وتقيم مخاطر غسل الأموال وتمويل الإرهاب الناشئة عن الأنشطة أو العمليات التي يَضَلَعُ فيها مقدمو خدمات الموجودات الافتراضية؛ وأن تطبق نهجاً قائماً على المخاطر لضمان أن تكون التدابير الرامية إلى منع غسل الأموال وتمويل الإرهاب أو الحد من مخاطرها متناسبة مع المخاطر المستبانة؛ وأن تُلزِم مقدمي خدمات الموجودات الافتراضية بتحديد وتقييم واتخاذ إجراءات فعالة للحد من مخاطر غسل الأموال وتمويل الإرهاب؛

(د) ينبغي للدول الأعضاء أن تستثمر على نحو متزايد في توفير برامج مناسبة للتدريب تحسن من قدرة المحققين على معالجة المشاكل التي تثيرها العملات المشفرة أثناء التحقيقات معالجة فعالة؛

(هـ) ينبغي للدول الأعضاء أن تدرج في تشريعاتها أحكاماً تتناول حيازة ونشر وتوزيع المواد الرقمية التي يمكن استخدامها في صنع الأسلحة النارية في نهاية المطاف، وأن تعمل على توفير أنشطة لبناء القدرات من أجل زيادة المهارات اللازمة لمنع تلك الأفعال وعمليات الاتجار بالأسلحة النارية عبر الشبكة الخفية وكشفها والتحقيق فيها وملاحقة مرتكبيها؛

(و) ينبغي للمكتب أن يواصل الترويج لعقد اجتماعات منتظمة للممارسين لضمان اطلاع المحققين على أساليب العمل الجديدة لصنع الأسلحة النارية ونقلها، وكذلك على أساليب التحري المقابلة؛

(ز) ينبغي للدول الأعضاء أن تولي اهتماماً خاصاً لبناء الخبرات والقدرات اللازمة لدى السلطات المختصة في جميع القطاعات ذات الصلة للسماح بالاستخدام الأمثل للتكنولوجيا لمكافحة الاتجار بالأشخاص مع حماية حقوق الضحايا في الوقت نفسه؛

(ح) ينبغي للمكتب أن يواصل تطوير إرشاداته التقنية ودعمه للدول الأعضاء من أجل تحديد وتنفيذ تدابير تكنولوجية لتطبيق نظام العدالة الجنائية على نحو أكثر فعالية لمنع الاتجار بالأشخاص وتهريب المهاجرين والتحقيق مع الجناة وملاحقتهم قضائياً؛

- (ط) ينبغي للدول الأعضاء أن تتخذ تدابير تشريعية وغير تشريعية تيسر على مقدمي خدمات الإنترنت وخدمات الوصول إليها وسائر الكيانات المعنية الكشف عن المواد المتعلقة باستغلال الأطفال والاعتداء عليهم جنسياً وتضمن الإبلاغ عن تلك المواد وإزالتها؛
- (ي) ينبغي للدول الأعضاء أن تنفذ سياسات من أجل حماية الأطفال من الاستغلال والاعتداء الجنسيين وأن تتبادل الممارسات الفضلى في هذا الشأن، بما يشمل توفير برامج لدعم الضحايا وتعميم مراعاة المنظور الجنساني؛
- (ك) ينبغي للدول الأعضاء أن تعزز فهم المخاطر التي يشكلها الاستخدام الخبيث للذكاء الاصطناعي، وأن ترصد باستمرار التطورات في التكنولوجيات الجديدة لضمان التأهب لمعالجة مشاكلها وكفالة المساءلة والشفافية والنزاهة في هذا الشأن؛ وأن تروج لتطبيق المعايير الأخلاقية في استخدام تلك التكنولوجيات؛ وأن تكتسب ثقة المواطنين والمجتمعات المحلية في هذا الاستخدام؛
- (ل) ينبغي للدول الأعضاء أن تعزز أنشطة المساعدة التقنية والتدريب، بالتعاون مع المكتب وسائر المنظمات الدولية، بهدف تعزيز مهارات الممارسين والسلطات المركزية في استخدام التكنولوجيا لتعجيل إجراءات التعاون الدولي.