مكافحة الإجرام المنظم عبر شبكة الإنترنت المظلمة:
دراسة تحليلية فى التشريع المصرى

رامى متولى القاضى*

تسعى التنظيمات الإجرامية والإرهابية إلى الاستفادة من مزايا استخدام شبكة الإنترنت المظلمة، وبصفة خاصة طابعها السرى وصعوبة تعقب مستخدميها، بما يحقق لها مباشرة أنشطتها الإجرامية بعيدًا عن أية رقابة أو مسائلة قانونية، حيث يوجد على هذه الشبكة مواقع لبيع الوثائق المزورة والمسروقة وبيانات البطاقات الائتمانية والحسابات الشخصية، بالشكل الذى أصبحت به هذه الشبكة سوقًا سوداء لكل الأنشطة غير المشروعة، ويهدف البحث إلى تسليط الضوء على الأنشطة الإجرامية غير المشروعة عبر شبكة الإنترنت المظلمة، وبحث سبل مكافحتها فى ضوء التحديات التقنية والقانونية ذات الصلة، ودور التشريعات الوطنية فى الحد من هذه الأنشطة، ودور أجهزة الشرطة الدولية فى تعقبها، والتصور الأمثل للتعامل معها.

الكلمات الدالة:
شبكة الإنترنت المظلمة- الجماعات الإجرامية المنظمة- غسل الأموال- تمويل الإرهاب- الاتجار بالمخدرات- الاتجار بالأسلحة النارية- الاتجار بالبشر.

مقدمة

أصبحت التكنولوجيا سلاحًا ذا حدين، تعمل التنظيمات الإجرامية على توظيفها فى أنشطتها غير المشروعة، وعلى الجانب الآخر تعمل أجهزة إنفاذ القانون على توظيفها فى تعقب هذه الأنشطة الإجرامية وضبط مرتكبيها، ومن ثم فإن التكنولوجيا كما يمكن أن تساعد على ارتكاب الجرائم، يمكن أيضًا أن تسهم فى مكافحتها، وهى لها دور فى إيجاد حلول تساعد أجهزة إنفاذ القانون على حفظ الأمن والملاحقة القضائية للمجرمين والنجاح فى تطبيق العدالة الجنائية من ناحية؛ كما أن لها دورها فى تعزيز أساليب عمل المجرمين والجماعات

* عقيد دكتور، رئيس قسم القانون الجنائى بكلية الشرطة والأستاذ المشارك.

الإجرامية المنظمة من ناحية أخرى، ففى خضم التطورات التكنولوجية المتسارعة ظهر جليًا استغلال التنظيمات الإجرامية المنظمة والإرهابية لشبكة الإنترنت[1]، حيث تهيئ الإنترنت فرصًا جديدة لبيع السلع وشرائها بصورة غير مشروعة، سواء عبر الشبكة الواضحة أو الشبكة المظلمة "الداركنت".

وتسعى التنظيمات الإجرامية والإرهابية إلى الاستفادة من مزايا استخدام شبكة الإنترنت المظلمة، وبصفة خاصة طابعها السرى وصعوبة تعقب مستخدميها، بما يحقق لها مباشرة أنشطتها الإجرامية بعيدًا عن أية رقابة أو مسائلة قانونية، حيث يوجد على هذه الشبكة مواقع لبيع الوثائق المزورة والمسروقة وبيانات البطاقات الائتمانية والحسابات الشخصية، بالشكل الذى أصبحت به هذه الشبكة سوقًا سوداء لكافة الأنشطة غير المشروعة، ومرتعًا للمجرمين والقراصنة المعلوماتيين، والقتلة المأجورين والمزورين وتجار البشر إلى غير ذلك، بحيث يقوم أى مستخدم على الشبكة بالتواصل معهم للحصول على هذه الخدمات فى سرية تامة من دون أن يتعرض لأية رقابة رسمية.

وقد أشارت التقارير والدراسات إلى خطورة الأنشطة الإجرامية التى تتم عبر الشبكة المظلمة، حيث إن تداول المصنفات الفنية والبرامج من خلال الشبكة السوداء فى عام ٢٠٠٥ قد خلف خسائر للشركات التجارية- آنذاك- قدرت بنحو ٣٤ مليار دولار أمريكى على مستوى العالم، فضلًا عما أشارت إليه تقارير أخرى من أن أرباح موقع طريق الحرير الذى أنشأ فى عام ٢٠١١ واُستخدم لترويج المخدرات عبر الشبكة السوداء قد قدرت بـ١,٢ مليار دولار خلال أعوام ٢٠١١ و٢٠١٣، كما أظهرت إحدى الدراسات أن تكلفة التزوير الإلكترونى الذى يعتمد على الشبكات السوداء يكلف الاقتصاد البريطانى عشرات المليارات سنويًا، ناهيك عما أعلنت عنه إحدى شركات الأمن الإلكترونى من أن الشبكة السوداء فى عام ٢٠١٠ أضحت تضم أكثر من ٥٠ ألف موقع إلكترونى للفكر المتطرف وأكثر من ٣٠٠ منتدى افتراضى للجماعات الإرهابية، علاوة على استخدام هذه التنظيمات لأرباح بيع

البرامج المسروقة فى تمويل العمليات الإرهابية، أضف إلى ذلك استخدام هذه الشبكة بين إجراء اتصالات بين عناصر التنظيمات الإرهابية المتطرفة[٢].

وجدير بالذكر أن ممارسة هذه الأنشطة الإجرامية عن طريق تنظيمات إجرامية تحترف الجريمة، وتتسم بالثبات والدوام فى تكوينها، وتستهدف تحقيق الربح، وتعمل على نطاق دولى واسع، يشمل العديد من الدول، فضلًا عن استخدامها من قبل العناصر الإرهابية المتطرفة، لا شك فى أن ذلك يشكل خطرًا كبيرًا على أمن المجتمعات كافة، ويتطلب ضرورة تضافر جميع الجهود الدولية فى مواجهتها[٣]، وذلك فى ضوء ما يوفره استخدام شبكة الإنترنت من فرص للمجرمين المعلوماتيين من ارتكاب جرائمهم خارج نطاق دولهم، فضلًا عن تسهيلها لعملية التواصل وتبادل المعلومات فيما بينهم، مما يمكنهم من الالتقاء فى العالم الافتراضى، والتخطيط والإعداد لارتكاب جرائهم، والتى يمتد نطاقها إلى أكثر من دولة، وبل فى بعض الأحيان قد تستهدف هذه الجماعات الإجرامية المنظمة دولًا أو مؤسسات تجارية أو اقتصادية بعينها، مما قد يؤدى إلى وقوع أضرار اقتصادية جسيمة لهذه الدول أو المؤسسات.

٢- أهداف البحث: يهدف هذا البحث إلى تحقيق هدف رئيسى، يتمثل فى إلقاء الضوء على استخدام شبكة الإنترنت المظلمة من جانب التنظيمات الإجرامية والإرهابية، وهو ما يمكن تحقيقه من خلال مجموعة من الأهداف الفرعية، من أبرزها: تسليط الضوء على الأنشطة الإجرامية غير المشروعة عبر شبكة الإنترنت المظلمة، وبحث سبل مكافحتها فى ضوء التحديات التقنية والقانونية ذات الصلة، ودور التشريعات الوطنية فى الحد من هذه الأنشطة، ودور أجهزة الشرطة الدولية فى تعقبها، والتصور الأمثل للتعامل معها.

٣- صعوبات وإشكاليات البحث: تتبلور أبرز صعوبات البحث فيما يتطلبه التعامل مع هذه الشبكة المظلمة من طابع تقني خاص للدخول عليها، ورصد ومتابعة أنشطتها غير المشروعة، نتيجة صعوبة الوصول إليها من خلال محركات البحث التقليدية، واستخدام

تقنيات التشفير المعقدة، التى تعمل على تجهيل هوية مستخدميها وصعوبة التعرف عليهم وتتبعهم، وضبطهم.

٤- منهج البحث: يعد المنهج الوصفى التحليلى هو أنسب مناهج البحث لدراسة الظواهر الاجتماعية والقانونية، ويعرف بأنه: "دراسة الظاهرة كما توجد فى الواقع ووصفها وصفًا وثيقًا ويعبر عنها تعبيرًا كيفيًا أو كميًا بغية الوصول إلى استنتاجات تسهم فى فهم هذا الواقع وتطويره"[١]، كما أن موضوع البحث وطابعه عبر الوطنى يفرض على الباحث استخدام المنهج المقارن، من خلال الإشارة إلى بعض الوقائع والحوادث ذات الصلة بأنشطة الإجرام المنظم عبر الشبكة المظلمة، مع التركيز على موقف المشرع المصرى من مواجهة هذه الظواهر الإجرامية الخطيرة.

وتتمثل أدوات البحث التى سوف يستعين بها الباحث كمصادر علمية فى إعداد هذا البحث فى المؤلفات القانونية العربية والأجنبية ذات الصلة بموضوع البحث فى مجال القانون الجنائى، فضلًا عن المؤلفات المُتخصصة ذات الصلة، سواء أكانت مؤلفات أم أوراق عمل أم غير ذلك أو الرسائل الجامعية من أطروحات دكتوراه أو ماجستير أو مقالات قانونية منشورة بالدوريات العلمية حول موضوع البحث، فضلًا عن المقالات والأخبار المنشورة فى وسائل الإعلام المُختلفة وشبكة الإنترنت.

٥- خطة البحث: نتناول موضوع البحث فى مطلبين، نعرض فى الأول استخدام التنظيمات الإجرامية لشبكة الإنترنت المظلمة، ونتطرق فى الثانى لأبرز الأنشطة الإجرامية التى تتم عبر هذه الشبكة السوداء.

المطلب الأول

استخدام التنظيمات الإجرامية لشبكات الإنترنت المظلمة

أولًا: تعريف شبكة الإنترنت المظلمة:

يمكن تقسيم الإنترنت إلى ثلاثة أقسام:

- القسم الأول: الشبكة السطحية، التى يتم استخدامها حاليًا، والتى يوجد بها المواقع والمعلومات والبيانات التى يمكن للأفراد الوصول إليها عن طريق محركات البحث التقليدية المتعارف عليها، ولا تمثل سوى (٠,٠٣٪) من المعلومات المتعلقة بها على الإنترنت.
- القسم الثانى: الشبكة العميقة، التى تحتوى على قواعد البيانات الأكاديمية والسجلات الحكومية، وقواعد بيانات الشركات والبنوك التجارية، ومحتوى رسائل البريد الإلكترونى وخدمات البث التليفزيونى، والتى تعتبر غير مخالفة للقانون.
- القسم الثالث: الشبكة المظلمة، والتى لا يمكن الوصول إليها بالطرق العادية، وهى مجال خصب للعديد من الأنشطة الإجرامية غير المشروعة، فليس كل ما هو موجود على شبكة الإنترنت يمكن رؤيته أو الوصول إليه من قبل المستخدمين، فقد ظهر ما يعرف بالشبكات السوداء، والتى يتسم جزء كبير من محتوياتها بطابع السرية، بحيث توفر الخصوصية لمستخدميها بعيداً عن أى نوع من الرقابة[٢]، حيث يتم فيها تقديم خدمات وتبادل معلومات بشكل سرى بين أعضائها، ولا يمكن لأى مستخدم خارج الشبكة رؤية محتواها، أو البحث عنها بالطرق التقليدية.

وعلى عكس الشبكة الواضحة التى تسمى أيضًا "الشبكة السطحية"، التى تحيل إلى معلومات متاحة للجمهور وتفهرسها محركات البحث التقليدية، فإن الشبكة الخفية تتكون من شبكات خفية مشفَّرة، مما يسمح لمالك الموقع ومستخدميه على السواء بإبقاء هويتهم مجهولة مع صعوبة تعقبها نسبيًّا[٣]، وهو ما يجعلها الشبكة المفضلة لدى كل المجرمين وأصحاب

الأنشطة الإجرامية لما توفره من بيئة آمنة لأنشطتهم غير المشروعة التى يرتكبونها بعيدًا عن أيادى سلطات العدالة الجنائية.

ومن جانب آخر، تشير الشبكة السوداء إلى المجتمعات المغلقة على الإنترنت التى يكون الدخول إليها مسموحًا فقط لأعضائها بشكل خاص، ويتم تشفيرها وتشفير المعاملات والأنشطة كافة التى تتم عليها بحيث يستحيل ترقبها، ويتم الدخول عليها من خلال تحميل برامج معينة على جهاز الحاسب الآلى تمكن المستخدم من تبادل كلمات السر مع الأجهزة الأخرى المتصلة على الشبكة نفسها، ويتم نقل المعلومات بين هذه الأجهزة بشكل مشفر تمامًا؛ كالمعاملات البنكية الإلكترونية، وهو ما يجعل الشبكات السوداء أكثر أماناً من الشبكات الداخلية التى تستخدمها الشركات، والتى لا يتم فيها تشفير الاتصالات بين الأجهزة(٤).

وخلاصة القول إن شبكة الإنترنت المظلمة يمكن تعريفها بأنها: جزء من شبكة الإنترنت، يسمح بإصدار المواقع الإلكترونية ونشر المعلومات بدون الكشف عن هوية الناشر أو موقعه، ويحتاج إلى برمجيات وضبط وتفويض خاص للولوج إليه، وهى جزء من الويب لا تفهرسه محركات البحث، ويمكن الوصول إلى الإنترنت المظلم من خلال خدمات معينة مثل خدمة Tor(٥).

وتتشابه المواقع الإلكترونية الموجودة فى الدارك ويب مع مثيلاتها فى الويب السطحى surface web الذى نستخدم مواقعه فى حياتنا العادية، إلا أن الاختلاف الأكبر هو بنوع اللاحقة التى ينتهي بها الموقع الإلكترونى، حيث تتعدد أنواع اللاحقات التى تنتهى بها المواقع الإلكترونية العادية مثل "com وorg وedu"، بينما تنتهى المواقع فى الدارك ويب بلاحقة "onion"، يسمح استخدام هذه اللاحقة للمتصفحات الخاصة بالدارك ويب فقط الوصول إلى هذه المواقع الإلكترونية.

وتبرز خطورة استخدام الشبكة المظلمة فى أنها تشكل بيئة خصبة وعالمًا خاصًا للمجرمين المعلوماتيين، لا يخضعون فيه لأى رقابة (لتعذر وصول السلطات واستحالة تعقبه أو تعقب مستخدميه إذا استعملوه بطريقة صحيحة)، فهو يستخدم كسوق سوداء وكمكان لتبادل المعلومات الممنوعة التى يعاقب عليها القانون، ومن بين هذه الأمور: (تعليم صناعة واستخدام الأسلحه والمتفجرات وحتى الأسلحه البيولوجية منها- تعليم الاختراق وتبادل البرمجيات الممنوعة كالفيروسات والثغرات والتطبيقات الخبيثة- مواقع بيع وشراء المخدرات وهى أكثر ما تنشط التجارة فيها عبر الإنترنت المظلم- مواقع مختصة بالتزوير والمعاملات الرسمية المزيفة- مواقع تبادل الكتب والفيديوهات المسروقة.

ولا تستغرب من وجود مواقع للتواصل الاجتماعى بين مستخدمى هذا الإنترنت، بالإضافة إلى محركات بحث خاصة بالإنترنت العميق، وقد ذكر موقع ويكيبيديا فى دراسة أن (١٥,٤٪) من محتوى الإنترنت المظلم يتعلق بالمخدرات، و(٩٪) للمتاجر الإلكترونية الموجودة فيه، بالإضافة إلى (٦,٢٪) لتبادل ومقايضة العملة الافتراضية المشفرة Bit Coin.

وفى إنفوجرافيك[٦] نشره مركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء المصرى، تناول فيه "أسواق الإنترنت المظلمة Dark web marketplaces"؛ أشار فيه إلى أن عائدات التعاملات على مواقع الإنترنت المظلم قد شهدت ارتفاعًا ملحوظًا لتصل إلى ١,٥ مليار دولار وفقًا لآخر بيانات فى ٢٠٢٠، مقابل ١,٣ مليار دولار فى ٢٠١٩، وأن عمليات الشراء على تلك المواقع تتم عن طريق "العملات المشفرة"، و"البيتكوين" هى العملة الأولى عالميا عليه، وأنه من أبرز أنواع المعاملات على تلك الشبكة: الاتجار بالمخدرات، والأسلحة، وترويج البرمجيات الخبيثة كبرامج الفيروسات، والسلع المزيفة غير الأصلية، وأدوات للجرائم الإلكترونية، وأدوات للمراقبة، كما يوفر أماكن لتخزين البيانات المسروقة، وتتم التعاملات على تلك الشبكة دون الكشف عن هوية أى من أطراف المعاملة، والوسيط هو المسئول عن التسليم، وتظل نقود المشترى تحت تصرفه حتى يتم تأكيد الاستلام.

وقد أضاف إلى ذلك إنه رغم محاولات الحكومات لحظر تلك المواقع، فإن ذلك لا يحد كثيرًا من تجارة السلع غير المشروعة، بل يتحول المشترون والبائعون إلى مواقع أخرى، لما تحققه الشبكة المظلمة لهم من قدر كبير من الخصوصية وإخفاء الهوية، وأن تلك الأسواق لم تكن بمنأى عن تداعيات فيروس كورونا؛ حيث شهدت عمليات احتيال، منها بيع مجموعة من المنتجات من أقنعة وأدوية وأمصال غير أصلية لمواجهة فيروس كورونا؛ مما تسبب فى الاستيلاء على بيانات العديد من الأشخاص ووقوعهم ضحايا للاستغلال المالى، وقد سبق أن قدرت السلطات الأوروبية مبيعات الأدوية فى السوق المظلمة بما يقرب من ٤٤ مليون دولار أمريكى سنويًا بين عامى ٢٠١١ و٢٠١٥.

ثانياً: **الفرق بين الديب ويب** (deep web) **والدارك ويب** (dark web):

تحدث مغالطاتٌ كثيرةٌ عند الحديث عن الدارك ويب والديب ويب، حيث يعتقد معظم الناس أن المصطلحين يشيران إلى نفس الموضوع، ولكن هناك اختلافًا هائلًا بين معنى المصطلحين، وما يمثلان من الشبكة العنكبوتية العالمية، وذلك على النحو التالى:

- يتألف الدارك ويب (dark web) من مجموعةٍ من المواقع الإلكترونية التى تقوم بإخفاء عنوان الـ IP الخاصة بها، بحيث يحتاج المستخدم لبرمجياتٍ خاصةٍ للوصول إليها، كما يشكل الدارك ويب نسبةً ضئيلةً جدًا مقارنةً بالديب ويب، ما يقارب (٠,٠١٪) من حجم الشبكة العنكبوتية فى العالم.
- تتألف شبكة الدارك ويب من عددٍ قليلٍ جدًا من المواقع الإلكترونية يقدر بالآلاف فقط، وتقوم هذه المواقع باستخدام وسائل وطرق تشفير عديدة، بهدف حجب هوية مالكي الموقع وأماكن تواجدهم.
- يشمل الديب ويب جزءًا كبيرًا من الشبكة العنكبوتية العالمية، حيث يشمل جميع المعلومات والمعطيات والمواقع الإلكترونية التى لا يمكن الوصول إليها عن طريق محركات البحث المشهورة مثل جوجل أو بينج، ويطلق على نتائج البحث التى تتمكن

محركات البحث من إيجادها بالويب السطحى (surface web)، الذى يشكل ٠,٠٣٪ فقط من المحتوى الموجود على شبكة الإنترنت.

- لا تشكل أغلب مواقع الإنترنت الموجودة ضمن الديب ويب أى مشاكل أمنية على عكس مواقع الدارك ويب، حيث تحتوى المواقع الإلكترونية فيه على محتويات حسابات البريد الإلكترونى المحمى بكلمات سرٍّ، بالإضافة للاشتراكات الرقمية فى خدمات مثل نيتفلكس وغيرها، ويحمى تواجد هذه المواقع والخدمات مستخدميها من إمكانية الوصول لمحتوياتها عبر عملية البحث البسيطة على أحد محركات البحث، فلو توفرت هذه المعلومات والمواقع على الويب السطحى أو الـ (surface web)، لتمكن أى شخصٍ من الوصول للرسائل الإلكترونية الخاصة بالمستخدمين بمجرد البحث عنها.

ثالثاً: خصائص شبكة الإنترنت المظلمة:

تتميز شبكة الإنترنت المظلمة ببعض الخصائص المميزة، من أبرزها:

١- السرية: تتسم شبكة الدارك ويب بالسرية التامة التى يتمتع بها مستخدموها نتيجة التشفير الحاصل لأى بياناتٍ تدخل إليها.

٢- الخصوصية: يحافظ مستخدمو شبكة الدارك ويب على خصوصيتهم بشكلٍ كبيرٍ نتيجة تعطيل أنظمة التشفير المستخدمة ضمنها لأى محاولات تعقبٍ إلكترونيةٍ لبيانات ومعلومات المستخدمين، حيث تساعد شبكة التحويلات التى تمر عبرها الإشارة فى حماية المستخدم من وصول معلوماتهم الشخصية إلى أصحاب المواقع الإلكترونية المتواجدة على الدارك ويب، كما يتواجد متصفحٌ يحمل نفس اسم TOR يستخدم للوصول إليها، بالإضافة إلى إمكانية استخدامه كمتصفحٍ عادى لباقى أجزاء الشبكة العنكبوتية.

رابعاً: مخاطر استخدام شبكة الإنترنت المظلمة: ومن أبرزها:

- تشجع السرية والخصوصية العالية لمستخدمى الدارك ويب على القيام بالكثير من الأنشطة غير المشروعة؛ كبيع المخدرات والأسلحة والأجهزة الإلكترونية المسروقة، وتزوير الهويات الشخصية وجوازات السفر، بسبب صعوبة تعقب المستخدمين وكشف هويتهم وأماكن تواجدهم، فأغلب تجارة المخدرات فى الوقت الراهن تتم عبر الإنترنت المظلم، وأشهر موقع كان يقوم بهذا هو موقع Silk Road الذى قبضت الشرطة الأمريكية على القائمين عليه عام ٢٠١٣.
- توفر بعض مواقع الدارك ويب خدماتٍ لتوظيف مخترقين، ومزورين وحتى قتلة مأجورين، فهناك قتلة مأجورون، يعملون بإرسال صورة الضحية إلى القاتل والاتفاق على سعر معين، وبعد إرسال صورة الضحية مقتولًا يتسلم نقوده من مشترى هذه الخدمة، علاوة على استئجار مخترقى حسابات البنوك والحسابات الشخصية، أو حتى إن أردت سرقة شىء ثمين، فهناك لصوص محترفون يتقاضون أجرًا مقابل عمليات السطو، كما أن هناك مواقع خاصة لبيع المسروقات على الإنترنت.
- تقدم الكثير من مواقع الدارك ويب خدماتٍ مزيفةً، بهدف جذب المستخدمين المبتدئين الذين ليسوا على درايةٍ كافيةٍ بتفاصيل هذه المواقع والخدمات الموجودة فيها، مستغلين الخصوصية والسرية التى يتمتع بها أصحاب المواقع وصعوبة تعقبهم.
- يواجه مستخدمو الدارك ويب خطرًا كبيرًا لإصابة أجهزة الكمبيوتر الخاصة بهم بواسطة البرمجيات الخبيثة (Malware)[٧].

خامساً: استغلال التنظيمات الإجرامية لشبكة الإنترنت المظلمة:

يمكن التمييز فى ارتكاب الجرائم ما بين جرائم بسيطة ترتكب من أفراد عاديين، وجرائم منظمة ترتكب من جماعات إجرامية منظمة تتسم بمجموعة من الخصائص التى تضفى على الجريمة طابع من الخطورة [٨]، ومن ثم حينما ترتكب الجرائم ذات الطابع المنظم مقترنة

بوسائل التقنية الحديثة باستخدام وسائل كشبكة الإنترنت، التى توفر عنصر الانتشار وسهولة وصول هذه العناصر لأهدافها بسهولة، فلا شك فى أن ذلك يشكل خطورة حقيقية على أمن المجتمعات.

ويثار التساؤل حول استخدام التنظيمات الإجرامية المنظمة لشبكة الإنترنت فى ارتكاب جرائمها، حيث يرى البعض[٩] أنه على الرغم من أن بعض السمات التقليدية للجريمة المنظمة؛ كاستخدام العنف- على سبيل المثال- من الصعب الأخذ بها فى توصيف النشاط الإجرامى السيبرانى، إلا إنه ما يستطيع الأفراد فعله، يمكن للمنظمات أيضًا فعله، وربما بشكل أفضل، فى ضوء ما تحققه شبكة الإنترنت من تواصل وتنسيق أفضل بين الأفراد فى منطقة جغرافية مترامية الأطراف، وبما توفره من إمكانية للتواصل بين مجموعات من الأفراد ومجموعات قائمة على التسلسل الهرمى، وهو ما يشير إلى تحول بعض الجرائم السيبرانية إلى جرائم منظمة[١٠]، حيث تتطلب العديد من الجرائم السيبرانية درجة عالية من التنظيم والتخصص، ومن ثم يكون من المرجح أن يكون مستوى ضلوع الجماعات الإجرامية المنظمة التقليدية فى ارتكاب جريمة سيبرانية عاليًا، وبصفة خاصة فى الجرائم التى تنطوى على دوافع مالية، مثل: جرائم الاحتيال المالى والتزوير وجرائم انتحال الهوية، وهو ما أكدت عليه بعض التقارير، والتى أجرت استعراضًا لعينة من ٥٠٠ جريمة سيبرانية مسجلة لدى أجهزة الشرطة، أن ما يزيد على (٨٠٪) من الجريمة السيبرانية تستلزم بعضًا من أشكال النشاط المنظم[١١]، وقد تبلغ نسبة الجريمة المنظمة التى تنطوى على جريمة سيبرانية (٩٠٪)، كتقدير أعلى[١٢]، وعلى نحوٍ مواز، يرى البعض الآخر[١٣] أن غالبية الجرائم السيبرانية هى جريمة فرد، وليست جريمة منظمة.

وتحليلًا لبعض الجرائم السيبرانية ذات الدافع المالى، مثل: سرقة بيانات البطاقات المصرفية وبطاقات الائتمان، فقد وجد أن هذه الجرائم ترتكب بأسواق سوداء من خلال جماعات وأفراد، يؤدون أدوارًا مختلفة، ففيهم المبرمجون والموزعون والخبراء التقنيون

والقراصنة والمحتالون والمستضيفون والصرافون ونقلة الأموال والزعماء[١٤]، علاوة على أن هذه الجماعات والأفراد تتفاعل مع عدة عمليات، منها: إعداد البرمجيات الخبيثة، والتحكم فى شبكات معلوماتية مصابة من خلال رسائل التصيد الاحتيالى، وإدارة شبكات الروبوت، والحصول على البيانات الشخصية والمالية والمتاجرة بالبيانات المالية[١٥]، ومن ثم فإن سوق الجريمة السيبرانية فى هذا السياق يمكن تعريفها بأنها "شبكات تواصل اجتماعى تتألف من أفراد ضالعين فى نشاط إجرامى منظم"، وليست منشأة مؤلفة من جماعة إجرامية وحيدة[١٦]، وأنه يمكن التمييز بين طائفتين من الأفراد، الأولى تضم المبرمجين الأصليين للبرمجيات الخبيثة، وأصحاب شبكة روبوت قائمة على تكنولوجيا المعلومات، وهم يمثلون اللاعبين الأساسيين داخل السوق، والطائفة الثانية تشمل الموزعين المركزيين، وبعض الأفراد الآخرون، والأسراب الذين يحومون حولهم، فمن الواضح أن هؤلاء الضالعين بإعداد وإدارة عناصر السوق الرئيسية، مثل شبكات الروبوت، يباشرون أفعالهم الإجرامية فى شكل جماعات صغيرة نسبيًا، أو حتى بشكل منفرد[١٧].

ويتضح من الدراسة التى أعدتها إحدى شركات الأمن السيبرانى (BAE Detica/ LMU)، بشأن المجموعات التى حددتها، أن أغلب النماذج التنظيمية الأكثر شيوعًا تتألف من٣–٥ أفراد قد عملوا سويًا لما يقرب من سنة، ووفقًا لذلك؛ تتكون نصف المجموعات من ٦ أفراد أو أكثر، ويضم الربع ١١فردًا أو أكثر، حيث عملت ربع المجموعات النشطة لمدة أقل من ستة أشهر، وبالرغم من هذا لا يرتبط حجم المجـموعة، أو مدة تكوينها بمدى تأثير العمل الإجرامى، حيث يمكن للمجموعات الصغيرة إحداث ضرر جسيم خلال فترة قصيرة[١٨].

وفى السياق ذاته، تشير التقديرات إلى أن مثل هذه الأسواق الإجرامية السيبرانية تضم عددًا كبيرًا من الأفراد، والمنظمات التى قد تكون عابرة، ولاسيما فى حالة مهربى الأموال والأعمال والمعاملات التجارية المشبوهة، مثل: استئجار الروبوتات من فرد واحد أو مجموعة

إلى أخرى، هذا، وتستخدم شبكات الروبوت فى ارتكاب الهجمات ضد نظم المعلومات وسرقة البيانات، وتُعرض بتكلفة منخفضة نسبيًا، مستفيدة من تقلب حركة الأموال على أساس عدد العملاء [١٩].

ومن جانب آخر، تتيح أسواق الشبكة الخفية، التى توصف أيضًا باسم "الأسواق المشفَّرة[٢٠]، للمشترين والبائعين عدم الكشف عن هويتهم، وتعتبر المنتديات أو غرف الدردشة السرية أحد الأساليب التى تستخدمها الجماعات الإجرامية داخل أسواق الشبكة المظلمة المسيرة غالبًا بخدمات إخفاء الهوية، لتبادل المعلومات والتوسط فى بيع الخدمات الاستشارية، وخدمات الانتشار والفيروس، وتأجير شبكة الروبوت، وخدمات البريد الإلكترونى الطفيلى والاستضافة وقوائم البريد الإلكترونى والتفاصيل المالية[٢١]، ويضرب المثل فى ذلك بالمنتديات التى أنشأها قراصنة بطاقات الائتمان لتيسير تبادل بيانات بطاقات الائتمان المسروقة، والتى بدأت غالبًا على شكل مجموعات أنشأت على شبكة الإنترنت للالتقاء لتبادل الخبرات وتقديم الخدمات غير المشروعة، ثم بدأت هذه المجموعات فى التطور لتتميز بدرجات أعلى من التنظيم الإجرامى[٢٢].

وفى تلك الأسواق السوداء الرقمية، تُستخدم العملات المشفَّرة أساسًا لدفع ثمن المشتريات لتيسير بيع وتداول سلع من قبيل الأسلحة والمخدِّرات غير المشروعة، وقد أشارت وكالة الاتحاد الأوروبى للتعاون فى مجال إنفاذ القانون (اليوروبول) إلى أن البيانات الشخصية والطبية والمالية المسروقة سلعة رئيسية فى أسواق الشبكة الخفية، وهى تضطلع بدور حاسم فى أنشطة مثل: الاحتيال، والتصيد الاحتيالى، وسرقة الهوية، والاستيلاء على الحسابات، ورغم أن أسواق الشبكة الخفية تقدم طائفة من السلع المقلدة والمقرصنة للبيع، فإن أنشطة التجارة غير المشروعة لا تزال تجرى فى معظمها عبر الشبكة السطحية[٢٣]، ويتزايد استخدام الشبكة الخفية فى عمليات التلاعب بنتائج المباريات وأنشطة القمار لدعم دروب غسل الأموال، ولا سيما من جانب الجماعات الإجرامية المنظمة عبر الوطنية[٢٤]، وقد شدد

أيضًا الاجتماع الإقليمى الأوروبى التحضيرى للمؤتمر الرابع عشر على ضرورة التصدى لاستخدام الشبكة الخفية فى ارتكاب جرائم الكراهية[٢٥].

سادساً: موقف التشريع المصرى من تجريم الأنشطة الإجرامية عبر الشبكة المظلمة:

تنص المادة (٢٧) من قانون مكافحة جرائم تقنية المعلومات رقم (١٧٥) لسنة ٢٠١٨ على أنه: "فى غير الأحوال المنصوص عليها فى هذا القانون، يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنيه، ولا تزيد على ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أنشأ أو أدار أو استخدم موقعًا أو حسابًا خاصًا على شبكة معلوماتية يهدف إلى ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانونًا"، وتتمثل على التجريم فى مواجهة السلوك الإجرامى الضار المرتكب على شبكة الإنترنت أيا كانت صورتها شبكة عميقة أو سطحية أو مظلمة، والمتمثل فى إنشاء أو إدارة أو استخدام المواقع الإلكترونية والحسابات الخاصة فى ارتكاب الجرائم أو تسهيل ارتكابها، ومن ثم فإن هذا النص يشكل إطارًا لتجريم لاستخدام المعلوماتية أو المواقع الإلكترونية كوسيلة لارتكاب الجريمة أيا كانت صورتها، فقد حرص المشرع المصرى على إدراج نص واحد، يشمل تجريم إنشاء المواقع الإلكترونية الحسابات الخاصة لغرض ارتكاب أو تسهيل الجرائم أيا كانت صورتها، وهو نهج محمود من جانب المشرع المصرى.

سابعاً: العملات المشفرة كأداة دفع على شبكة الإنترنت المظلمة:

تعمل التنظيمات الإجرامية على توظيف العملات الرقمية المشفرة كأحد أشكال الدفع المقبولة على شبكة الإنترنت المظلمة[٢٦]، واستخدامها فى أنشطة الإجرام المنظم المختلفة وعمليات غسل الأموال وتمويل الإرهاب، فقد واكبت عمليات التطور التكنولوجى نحو التحول الرقمى اتجاه غالبية المؤسسات والهيئات والدول لرقمنة مختلف أنظمتها وتحولها للاقتصاد الرقمى ونظم الشمول المالى، ومن ثم ظهرت الحاجة لاستحداث أدوات جديدة تحمل الصفة الرقمية للتعامل داخل هذا العالم، حيث كانت العملات المشفرة والبلوكتشين إحدى أدوات التعامل

المالى على شبكة الإنترنت، والتى تضم الملايين من التعاملات المالية، وقد تعددت أسماء هذه العملات منذ بدأت تحت مسمى العملات الرقمية المشفرة Cryptocurrencies، وقد خلصت العديد من الدراسات إلى خطورة العملات المشفرة على الأمن الاقتصادى للدول[٢٧]، نتيجة صعوبة تعقبها، وهذا ما قد تستغله التنظيمات الإرهابية لتسهيل عمليات تمويلها، الأمر الذى من شأنه أن يمثل تهديدًا حقيقيًا للأمن القومى للدول.

وقد عرف البنك المركزى الأوروبى العملات الإلكترونية بأنّها: التمثيل الرقمى للقيمة، التى لا تخضع للبنوك المركزية والسلطة العامة، ولا ترتبط بالعملات الورقية، ويقبلها الأشخاص العاديون، أو الاعتباريون، كوسيلةً للدفع بها، ويمكن تحويلها، أو ادّخارها، وتداولها إلكترونياً[٢٨]، كما عرف التشريع المصرى العملات المشفرة بأنها:"عملات مخزنة إلكترونيًا غير مقومة بأى من العملات الصادرة عن سلطات النقد الرسمية، ويتم تدولها عبر شبكة الإنترنت" (م١ من قانون البنك المركزى والجهاز المصرفى رقم ١٩٤ لسنة ٢٠٢٠).

ومن ثم يمكن القول بأنها: عملة رقمية افتراضية ليس لها كيان مادى ملموس أو وجود فيزيائى، مُنتجة بواسطة برامج حاسوبية، ولا تخضع للسيطرة أو التحكم فيها من جانب بنك مركزى أو أى إدارة رسمية دولية، كما أنها لا تحمل رقمًا مسلسلًا، يتم استخدامها عن طريق الإنترنت فى عمليات الشراء والبيع أو تحويلها إلى عملات أخرى، وتلقى قبولاً اختياريًا لدى المتعاملين فيها [٢٩].

وكانت طريقة عمل العملة الرقمية فى بادئ الأمر عملية سهلة، يمكن لأى فرد وفى أى مكان مراجعة الشفرة، والبدء فى إنتاج عملات رقمية من خلال برامج مجانية خاصة، تعمل على حل مسائل حسابية معقدة، أو القيام بعملية التعدين أو التنقيب، ولكن مع التطور السريع، وبزيادة الطلب على العملة الرقمية، أصبح الأمر معقدًا وصعبًا على الأشخاص العاديين، لكونها عملية مكلفة، تحتاج إلى وسائل متطورة، واستهلاك كهرباء عالٍ، لذلك اتجه

المستثمرون إلى توظيف أموالهم فى شركات التعدين، والتى تقوم بدورها فى التنقيب عن العملات الرقمية، وتقديمها للأفراد للتداول والاستثمار.

وتسهل تطبيقات بتكوين الإلكترونية للمستخدمين التعامل على الإنترنت، حيث تسمح بإنشاء وحفظ مفاتيح خاصة بالمستخدم للاتصال بشبكتها، وتتم مدفوعات بتكوين من خلال تطبيقات محفظة بتكوين عبر الكمبيوتر الشخصى أو الهاتف الذكى، عن طريق إدخال عنوان المستلم والمبلغ المدفوع، ويمكن أن تستعمل كخادم لاستقبال تلك المدفوعات ولخدمات أخرى متعلقة بالدفع؛ كالشراء الإلكترونى[٣٠]، وليست البتكوين هى العملة الرقمية الوحيدة، فقد ظهرت عملات رقمية أخرى، من أبرزها: الريبل والتى ظهرت فى عام ٢٠١٢، واللايتكوين والمونرو التى ظهرت فى عام ٢٠١٤، عملة نيو الصينية التى أطلقت الحكومة الصينية فى العام ذاته من أجل تدعيم الاقتصاد الصينى، والإيثريوم التى ظهرت فى عام ٢٠١٥[٣١]، وأخيرًا وليس بآخر عملة البتكوين فولت، التى ظهرت فى عام ٢٠١٩، وعملة الليبرا التى يعزم مارك زوكر بيرج مؤسس فيسبوك إطلاقها.

ويشير جانب من الفقه الجنائى [٣٢] إلى اتساع نطاق استخدام العملات الرقمية المشفرة فى أنشطة إجرامية متنوعة، وعدم اقتصارها على أنشطة غسل الأموال وتمويل الإرهاب فحسب؛ إذ يضيف الرأى السابق إلى هاتين الجريمتين أنشطة أخرى للإجرام المنظم كجرائم المخدرات والأسلحة والاتجار بالبشر والأعضاء البشرية، وجرائم الاحتيال المالى وجرائم المساس بالأسواق المالية والمقامرة، وجرائم الابتزاز والتهديد فى الفضاء الإلكترونى، وجرائم التزييف والتزوير وتقلبات أسعار العملات الورقية، والتهرب الضريبى.

وعلى الرغم من اعتراف بعض الدول بالعملات المشفرة كوسيلة للدفع، فإن غالبية الدول تتحفظ على استخدامها، فقد قامت السلطات الأميركية بمصادرة نحو (٢٨) مليون دولار من عملة البتكوين من جهاز حاسب آلى ينتمى إلى صاحب موقع "طريق الحرير" الإلكترونى، الذى يعد بمثابة سوق مزدهرة لتجارة المخدرات وغسل الأموال والأنشطة غير

القانونيـة إلكترونيًـا، بينمـا اتخـذ وزراء ماليـة الاتحـاد الأوروبـى خـلال اجتماعـات مجموعـة السـبعة فـى عـام ٢٠١٥م، قـرارًا بتـشديد القـوانين المتعلقـة باسـتخدام عملـة البتكـوين، لمنـع التنظيمـات الإرهابيـة والتنظيمـات الإجراميـة مـن اسـتغلال هـذه العملـة فـى تمويـل أنـشطتها، وحـذر المـصرف المركـزى الروسـى مـن اسـتخدام عملـة البتكـوين، وأشـار إلـى إنـه يمكـن اسـتخدامها فـى غـسل الأمـوال أو تمويـل الإرهـاب وأن التعامـل بهـا كعملـة موازيـة مخـالف للقـانون، كمـا أن هـذه العمـلات لا تملـك سـندًا قانونيًـا لإصـدارها، وتعتمـد علـى المراهنـة فـى تحديد سعرها، الأمر الذى يشكل خطرًا كبيرًا لفقدان نسبة كبيرة من قيمتها، كما ألقت الشرطة اليابانيـة القـبض علـى "مـارك كـاربيليز"، الـرئيس التنفيـذى لـشركة "MTGox" المتعثـرة، التـى كانـت تعـد أكبـر شـركة صـرافة لعملـة البتكـوين، وذلـك لعلاقتـه بخـسارة عمـلات بتكـوين تقـدر قيمتها بـ (٣٨٧) مليون دولار فى فبراير عام ٢٠١٤م، بينما فرضت فيتنام حظرًا على عملة البتكـوين، مـستندة إلـى سـهولة اسـتخدامها لأغـراض جنائيـة، ومخاطرهـا الكبيـرة علـى المستثمرين، وقال البنك المركزي فى بيانه: "إن المعاملات بالعملة الإلكترونية مجهولة بشكل كبير، ومن ثم يمكن أن تصبح أداة لتنفيذ جرائم كغسل الأموال وتهريب المخدرات والتهرب مـن الـضرائب"، ومـن الـدول العربيـة، أصـدر البنـك الأردنـى المركـزى بيانًـا رسـميًا، محـذرًا مواطنيه من تجربة العملة الرقمية التى تفتقد الدعم من أى مؤسسة مالية فى العالم.

ثامناً: موقف التشريع المصرى من العملات المشفرة:

وضع القانون رقم ١٩٤ لسنة ٢٠٢٠، الخاص بإصدار قانون البنك المركزى والجهاز المصرفى، ضوابط جديدة لإصدار وتداول العملات المُشفرة والنقود الإلكترونية، فقد حظرت المادة (٢٠٦) من قانون البنك المركزى والجهاز المصرفى، إنشاء أو تشغيل منصات لإصدار أو تداول العملات المُشفرة أو النقود الرقمية، أو الترويج لها بدون الحصول على ترخيص من مجلس إدارة البنك المركزى المصرى، وفقًا للقواعد والإجراءات التى يُحددها[٣٣].

المطلب الثانى

أبرز أنشطة الإجرام المنظم عبر شبكة الإنترنت المظلمة.

نتناول فيما يلى أبرز أنشطة الإجرام المنظم المرتكبة عبر شبكة الإنترنت المظلمة، وذلك على النحو التالى:

أولاً: عمليات غسل الأموال:

يتفق الباحثون[٣٤] على أن عمليات غسل الأموال وتمويل الإرهاب وأنشطة الجريمة المنظمة يمكن أن ترتكب باستعمال النقود المشفرة فى إطار شبكة الإنترنت المظلمة، حيث تعمل التنظيمات الإجرامية والإرهابية على استخدام هذا النوع من العملات المستحدثة والتعامل بها من خلال مواقع أو تطبيقات إلكترونية، بالشكل الذى يصعب معه على السلطات الرسمية من تتبع هذه العمليات، بسبب وجود معظم الخوادم الخاصة بهذه المواقع خارج سيطرة الدول، حيث تجذب العملات الافتراضية غاسلى الأموال، بسبب غموضها، وسهولة تحويلها إلى مبالغ مالية بشكل سريع عبر شبكة الإنترنت[٣٥]، وهو ما دفع المشرعون الجنائيون إلى حظر التعامل بها، وتجريم استخدامها فى الأنشطة الإجرامية المختلفة[٣٦].

وعلى الرغم من أن النظام المصرفى العالمى يخضع للوائح التنظيمية الصارمة المتعلقة بغسل الأموال وتمويل الإرهاب وتحديد هوية العميل، علاوة على تعزيز الحكومات الوطنية هذه القواعد بشكل كبير فى أعقاب أحداث ١١ سبتمبر ٢٠٠١، إلا أن العملات الافتراضية– ونظرًا لاعتمادها على معاملات نظير إلى نظير مستقلة عن المؤسسات المالية الخاضعة للتنظيم– قد أزالت مصدرًا مهمًا للرقابة على مختلف الأنشطة غير المشروعة، فقد أضحت العملات المشفرة مثل: البتكوين وزكاش وغيرها مصدرًا ووسيلة لتمويل الإرهاب، بالنظر إلى مزاياها المتعددة التى يأتى فى مقدمتها القدرة على إخفاء هويات المتعاملين بها، وانتشار معاملاتها فى جميع أنحاء العالم.

موقف التشريع المصرى:

حرص المشرع المصرى على مواجهة إساءة استخدام العملات المشفرة من خلال التوسع فى مدلول الأموال لتشمل الأموال والأصول الافتراضية التى يتم تداولها على شبكة الإنترنت، حيث عدل المشرع مدلول الأموال فى قوانين مكافحة الإرهاب وغسل الأموال وتنظيم قوائم الكيانات الإرهابية والإرهابيين، فقد عرفت المادة الأولى (بند/أ) من قانون غسل الأموال المعدل بالقانون رقم (١٧) لسنة ٢٠٢٠ الأموال أو الأصول بأنها: "جميع الأصول المادية والافتراضية... والممتلكات والعملات الوطنية أو الأجنبية والأوراق المالية أو التجارية... أيًا كان شكلها بما فى ذلك الشكل الرقمى أو الإلكترونى...، كما تشمل الأصول الافتراضية التى لها قيمة رقمية يمكن تداولها أو نقلها أو تحويلها رقميًا ويمكن استخدامها كأداة للدفع أو الاستثمار"، بينما عرفت المادة الأولى من القانون رقم ١٤ لسنة ٢٠٢٠ بتعديل بعض أحكام القانون رقم ٨ لسنة ٢٠١٥ بشأن تنظيم قوائم الكيانات الإرهابية والإرهابيين الأموال أو الأصول الأخرى بأنها: "جميع الأصول المالية والموارد الاقتصادية... والعملات...، بما فى ذلك الشكل الرقمى أو الإلكترونى..." ، كما عرفت المادة الأولى بند/ و من القانون رقم ١٥ لسنة ٢٠٢٠ بتعديل بعض أحكام قانون مكافحة الإرهاب الصادر بالقانون رقم ٩٤ لسنة ٢٠١٥ الأموال أو الأصول بأنها: "جميع الأصول المادية والافتراضية... بما فى ذلك المستندات والعملات الوطنية أو الأجنبية... أيًا كان شكلها، بما فى ذلك الشكل الرقمى أو الإلكترونى ... كما تشمل الأصول الافتراضية التى لها قيمة رقمية يمكن تداولها أو نقلها أو تحويلها لشكل رقمى وتستخدم كأداة للدفع أو للاستثمار"، ويحسب للمشرع المصرى تعديله لأحكام القوانين المشار إليه ليشمل الأخذ بمدلول موسع للأموال يشمل العملات المشفرة والأصول الافتراضية[٣٧].

ويقصد بمفهوم غسل الأموال عملية إضفاء الشرعية على الأموال المشبوهة المتحصلة من ارتكاب جرائم محددة[٣٨]، وهى تتمثل فى عمليات إدخال أموال الناجمة عن الجرائم فى

مشروعات أخرى بهدف إضفاء صفة شرعية عليها، وقد عرف القانون المصرى رقم ٨٠ لسنة ٢٠٠٢ غسل الأموال بأنه: "كل سلوك ينطوى على اكتساب أموال أو حيازتها أو التصرف فيها أو إدارتها أو حفظها أو استبدالها أو إيداعها أو ضمانها أو استثمارها أو نقلها أو تحويلها أو التلاعب فى قيمتها إذا كانت متحصلة من جريمة من الجرائم المنصوص عليها فى المادة (٢) من هذا القانون مع العلم بذلك متى كان القصد من هذا السلوك إخفاء المال أو تمويه طبيعته أو مصدره أو مكانه أو صاحب الحق فيه أو تغير حقيقته أو الحيلولة دون اكتشاف ذلك أو عرقلة التوصل إلى شخص من ارتكب الجريمة المتحصل منها المال"، فالمشرع أراد أن يكافح كل صور التربح غير المشروع من خلال تجريم جميع الأفعال التى تهدف إلى تحويل أو دمج الأموال المتحصلة من ارتكاب الجرائم فى أموال لها أصول مشروعة، بالشكل الذى يصعب معه تعقبها أو الوصول إليها.

وتفترض جريمة غسل الأموال وقوع جريمة أصلية- جناية أو جنحة- وأن يتحصل الجانى من ورائها على أموال أو عائدات يتم غسلها، وإضفاء صفة المشروعية عليها من خلال القيام بعمليات تجارية ومصرفية كغطاء مشروع لإخفاء أو تمويه الصفة غير المشروعة للمال، والركن المادى فى جريمة غسل الأموال قد يتخذ صور: أفعال الإخفاء أو الحيازة أو النقل للأموال، أو التعامل أو التحويل أو الإيداع إلى غير ذلك من صور السلوك التى تقع على الأموال، ومن ثم تقوم الجريمة بكل نشاط أو عمل مادي استخدمت فيه هذه الأموال غير المشروعة؛ كعمليات البيع والشراء للعقارات كالأراضى والمبانى والمنقولات كالسيارات والمشغولات الذهبية، وشراء شهادات الاستثمار، والتحويلات البنكية والحوالات البريدية وتحرير الشيكات المصرفية، وعمليات المضاربة بالبورصة إلى غير ذلك من الأنشطة التجارية والمصرفية، ويجب أن يستخدم الجانى الأموال والعائدات المتحصلة من الجرائم المنصوص عليها فى القانون فى العمليات والأنشطة التجارية والمصرفية المشار إليها، حتى تتحقق جريمة غسل الأموال، فعدم وجود أموال متحصلة من مصدر غير مشروع

تنتفى معه جريمة غسل الأموال، وجريمة غسل الأموال من الجرائم العمدية، وهى من جرائم القصد الخاص، فالقصد الجنائى فى جريمة غسل الأموال يقتضى توافر عنصرين: القصد العام، وهو علم الجانى وقت ارتكابها بتوافر أركانها، والقصد الخاص، وهو نية إخفاء المال أو تمويه طبيعته أو مصدره أو مكانه أو صاحب الحق فيه أو تغيير حقيقته، حيث يتطلب القانون أن يكون القصد من هذا السلوك إخفاء هذا المال أو تمويه طبيعته أو مصدره دون اكتشاف ذلك أو عرقلة التوصل إلى شخص من ارتكب الجريمة المتحصل منها المال.

عقوبة غسل الأموال فى التشريع المصرى: تنص المادة (١٤) من قانون مكافحة غسل الأموال رقم (٨٠) لسنة ٢٠٠٢ على أنه: "يعاقب بالسجن مدة لا تجاوز سبع سنوات وبغرامة تعادل مثلى الأموال محل الجريمة، كل من ارتكب أو شرع فى ارتكاب جريمة غسل الأموال المنصوص عليها فى المادة (٢) من هذا القانون. ويحكم فى جميع الأحوال بمصادرة الأموال المضبوطة، أو بغرامة إضافية تعادل قيمتها فى حالة تعذر ضبطها أو فى حالة التصرف فيها إلى الغير حسن النية"، ومن ثم فإن العقوبات المقررة فى حال غسل الأموال هى السجن والمصادرة والغرامة النسبية.

ثانياً: عمليات تمويل الإرهاب:

تدرك الجماعات الإرهابية والمتطرفة التى تنتهج العنف سبيلًا، أنّ الحفاظ على قوتها وبقائها، يتطلب توفير مواردٍ ماليةٍ ثابتةٍ، يصعب ملاحقتها ومصادرتها من قبل المصارف والبنوك، أو السلطات العامة فى الدول والحكومات؛ لذا فإنّها تسعى، بشكلٍ قويٍّ، إلى استغلال التقنيات والآليات الحديثة فى إخفاء مواردها المالية للحفاظ عليها، وتشفير عمليات نقل الأموال، وشراء المعدات والأجهزة اللازمة لها، ويمكن القول: إنّ العديد من المؤشرات والظواهر تشير بوضوح إلى إلمام العديد من الحركات والجماعات المتطرفة والإرهابية، بتلك الأوعية الجديدة، كما تشير المؤشرات إلى وجود القدرات العلمية والتقنية اللازمة لاستخدام هذه الأوعية واستثمارها، ما دفع العديد من الدول والمنظمات إلى الاهتمام بتلك الأوعية، والعمل

على إيجاد وسائل حديثةٍ، وآلياتٍ متقدمةٍ، لرصد وتتبّع تلك العملات، وفرض رقابةٍ عليها، وعلى حركتها عبر الدول.

ويمكن إيجاز هذا الاهتمام المتزايد بالعملة الافتراضية فى أنه فى نوفمبر من عام ٢٠١٥م؛ قررت دول الاتحاد الأوروبى، فرض قيود على التعاملات المالية التى تتم بعملة (بتكوين)، إلى جانب التحويلات النقدية الشائعة، بهدف تجفيف منابع تمويل الإرهاب، ومحاربة غسل الأموال، وذلك بعد تداول الإعلام الفرنسى بيانًا لقراصنة يطلقون على أنفسهم "جوست سيك"، ويقولون إنّهم تابعون لمجموعة قراصنة الكمبيوتر الشهيرة "أنونيموس"، بشأن امتلاك تنظيم داعش حسابًا بهذه العملة الافتراضية، يناهز (٩٢٩٨) بتكوين، أى ما يعادل(٣) ملايين دولار، وهو ما أجّج المخاوف من إمكانية إقدام التنظيم على استخدام هذا الحساب لتكون عملة آمنة للحصول على تمويل سرى ومُشفر لتمويل هجمات إرهابية جديدة سواء فى أوروبا، أو فى مناطق أخرى من العالم، وهو مؤشر قوى على إدراك تنظيم داعش أهمية البتكوين، وخصائصه الجاذبة للجماعات والتنظيمات المتطرفة والإرهابية.

وفى السياق ذاته، أصدر أحد مناصرى تنظيم داعش، وثيقة بعنوان: "بتكوين وصدقة الجهاد"، من تأليف تقى الدين المنذر، والذى حدّد فيها الأحكام الشرعية لاستعمال البتكوين، مشدداً على ضرورة استعمال تلك العملة الافتراضية لتمويل الأنشطة الجهادية، وقد لجأت بعض الجماعات والحركات الإرهابية لطلب تبرعات لها عبر الإنترنت بعملة البتكوين مُعلنة عن محفظة إلكترونية للتبرع من خلالها للحصول علي التمويل اللازم للعمليات الإرهابية، نذكر منها على سبيل المثال الحملة التى أُطلقت بعنوان "جهزونا"، بل إنها تقوم أيضًا بشراء الأسلحة والمتفجرات من خلال الإنترنت العميق بواسطة العملة الرقمية البتكوين، ويمكن القول: إنّ طبيعة البتكوين كعملة مشفرة، لا تخضع لسلطة مركزية أو هيئة مالية، جعلت منها عملة جاذبة وحافزة لكافة التنظيمات غير الشرعية للتداول من خلالها، والتعامل بها فى شتى المعاملات المالية التى تتطلب السرية والخصوصية.

ويقصد بتمويل الإرهاب: (كل جمع أو تلق أو حيازة أو إمداد أو نقل أو توفير أموال أو أصول أخرى... أيًا كان مصدره وبأى وسيلة كانت بما فيها الشكل الرقمى أو الإلكترونى) (م٣ من قانون الإرهاب رقم ٩٤ لسنة ٢٠١٥ المعدلة بالقانون رقم ١٥ لسنة ٢٠٢٠)، حيث تسهل خدمات الدفع عبر الإنترنت المتاحة عبر المواقع الشبكية المخصصة، أو عبر منصات الاتصالات، تحويل الأموال إلكترونيًا بين الأطراف المعنية، وكثيرًا ما تحول الأموال عن طريق التحويلات البرقية الإلكترونية، أو بطاقات الائتمان، أو خدمات الدفع البديلة، مثل: باى بال أو سكايب[٣٩]، ويتجه غالبية الفقه والتشريعات إلى دمج كل من جريمتى غسل الأموال وتمويل الإرهاب فى جريمة واحدة، بالنظر إلى التقارب الشديد فى مدلولها، وانتهاج كل من الجماعات الإجرامية والتنظيمات الإرهابية لذات الوسائل والطرق لإخفاء الأموال عن أعين السلطات الرسمية، سواء أكان ذلك بشكل تقليدى أو عبر شبكة الإنترنت المظلمة.

وترجع علة تجريم تمويل الإرهاب إلى ما تبين من أن قوة الإرهاب ترجع إلى حد كبير إلى القدرة المالية للإرهابيين، بحسب أن التخطيط للعمليات الإرهابية وتنفيذها، بما يتضمنه من تعقد الكيانات الإرهابية وشبكات العملاء الإرهابيين – تتطلب بالضرورة الاعتماد على الموارد المالية[٤٠].

ويقوم الركن المادى لتمويل الإرهاب بإحدى صورتين: (الأولى) جمع أو تلقى أو حيازة أو إمداد أو نقل أو توفير أموال أو أسلحة أو ذخائر أو مفرقعات أو مهمات أو آلات أو بيانات أو معلومات أو مواد أو غيرها، سواء تم ذلك مباشرة أو بطريق غير مباشر، وأيًا كانت الوسيلة المتبعة بما فى ذلك الوسيلة التى تخذ الشكل الرقمى أو الإلكترونى، و(الثانية) توفير ملاذ آمن لإرهابى أو أكثر، أو لمن يقوم بتمويله بأى من طرق التمويل السالف الإشارة إليها[٤١].

ويستوى أن تكون مصادر تمويل الإرهاب أموالًا مشروعة أو غير مشروعة، مادام الغرض من تقديمها استخدامها فى عمل إرهابى، وهو ما يميز جريمة تمويل الإرهاب عن جريمة غسل الأموال التى تقع عندما يكون مصدر الأموال القذرة المراد غسلها ارتكاب جناية أو جنحة، وهو ما لا يشترط فى تجريم تمويل الإرهاب، فقد يكون مصدر التمويل معاملات مشروعة، فإذا وقعت جريمة تمويل الإرهاب فإن الحصول على هذا التمويل فى حد ذاته يجعله متحصلا من جريمة، فإذا قام من تلقى التمويل بإخفاء مصدره الإجرامى عن طريق غسل هذه الأموال، وقعت منه أيضًا جناية غسل الأموال، وهو ما يلجأ إليه كثير من ممولى الإرهاب، الأمر الذى ضاعف من خطورة جريمة غسل الأموال(٤٢).

وجريمة تمويل الإرهاب جريمة عمدية، تقوم بالقصد الجنائى العام بعنصريه الإرادة والعلم، كما يجب أن تتجه الإرادة لا إلى مجرد التمويل، بل إلى تحقيق غرض معين هو استخدام التمويل فى ارتكاب أية جريمة إرهابية، أو العلم بأنه سيستخدم فى ذلك، ويلاحظ أن قصد ارتكاب أية جريمة إرهابية ليس قصدًا خاصًا فى الجريمة، لأن التمويل وحده ليس محل التجريم، بل لابد أن يكون مشفوعاً بغرض ارتكاب أية جريمة إرهابية، وقد أكد المشرع هذا المعنى حين جعل العلم بأن التمويل سيستخدم لتحقيق لتحقيق هذا الغرض، ويجب أن يكون العلم مؤكدًا، فإذا كان احتماليًا مشفوعًا بقبول الممول تحقيق هذا الاحتمال توافر القصد الجنائى الاحتمالى الذى يعد من أشكال القصد الجنائى.

ويتعين توافر هذا القصد الجنائى فى الصورة الثانية للركن المادى، فلا تقع هذه الجريمة إذا كان التمويل بقصد إفلات الإرهابى من الوقوع فى قبضة العدالة، دون إخلال بوقوع جريمة تمكين مرتكب جريمة إرهابية من الهرب قبل أو بعد القبض عليه المنصوص عليها فى المادة ٧ من قانون مكافحة الإرهاب، فضلًا عن ارتكاب الجريمة المنصوص عليها فى المادة ١٤٢ من قانون العقوبات إذا كان الإرهابى مقبوضًا عليه وسهل التمويل هروبه(٤٣).

عقوبة تمويل الإرهاب فى التشريع المصرى:

تنص المادة (١٣) من قانون مكافحة الإرهاب المعدلة بالقانون رقم ١٥ لسنة ٢٠٢٠ على بأنه: "يعاقب بالسجن المؤبد كل من ارتكب جريمة من جرائم تمويل الإرهاب إذا كان التمويل لإرهابى، وتكون العقوبة الإعدام إذا كان التمويل لجماعة إرهابية أو لعمل إرهابى. ويعاقب بالعقوبة ذاتها المنصوص عليها بالفقرة الأولى من هذه المادة إذا كان تمويل الإرهاب بقصد سفر أفراد إلى دولة غير دولة إقامتهم أو جنسيتهم بغرض ارتكاب عمل إرهابى أو التخطيط له أو إعداده أو المشاركة فيه أو تقديم العون أيًا كان شكله. وفى الأحوال التى ترتكب فيها الجريمة بواسطة جماعة إرهابية أو شخص اعتبارى، يعاقب المسئول عن الإدارة الفعلية لهذه الجماعة أو ذلك الشخص بالعقوبة المقررة فى الفقرة الأولى من هذه المادة. كما تعاقب الجماعة الإرهابية أو الشخص الاعتبارى بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثة ملايين جنيه، وتكون مسئولة بالتضامن عن الوفاء بما يحكم به من عقوبات مالية أو تعويضات"، ويلاحظ على هذا النص أنه ميز فى العقوبة بين التمويل لإرهابى والتمويل لعمل إرهابى، بينما هذا العمل يعد جزءًا فى معظم الجرائم الإرهابية التى تقع بالنظر إلى الوسيلة الإرهابية والغرض الإرهابى، باعتبار أن هذين الأمرين يتمثلان فى العمل الإرهابى نفسه، ووفقًا لتعريف الإرهابى فى المادة الأولى (ب) فإنه من يرتكب أو يشرع فى ارتكاب أو يحرض أو يهدد أو يخطط فى الداخل أو الخارج لجريمة إرهابية بأية وسيلة كانت[٤٤]، كما يلاحظ أن الحكم على الجماعة بالغرامة لا يتأتى إلا إذا كانت تتخفى فى شكل قانونى، بحسب أن الغرامة لا تفرض إلا على شخص قانونى، فإذا لم يكن للجماعة شكل قانونى قضى بالغرامة على جميع أعضائها بالتضامن فيما بينهم[٤٥].

كما تبرز الإشارة إلى أن النص الأخير يتضمن المعاقبة على عمليات تمويل الإرهاب التى تستهدف تمويل المقاتلين الإرهابيين الأجانب، من خلال تمويل سفر الأفراد إلى دولة

غير دولة إقامتهم أو جنسيتهم بغرض ارتكاب عمل إرهابى أو التخطيط له أو إعداده أو المشاركة فيه أو تقديم العون أيًا كان شكله.

كما تنص الفقرة الأولى من المادة (٢٠) من قانون مكافحة الإرهاب على تجريم إخفاء أو التعامل فى أشياء استعملت أو أعدت للاستعمال فى ارتكاب جريمة إرهابية أو الأموال التى تحصلت عنها، حيث تقضى المادة المذكورة بأنه: "يعاقب بالسجن المشدد مدة لا تقل عن عشر سنين كل من:

١- أخفى أو تعامل فى أشياء استعملت أو أعدت للاستعمال فى ارتكاب جريمة إرهابية أو الأموال التى تحصلت عنها"، ومن ثم فإن المشرع المصرى يجرم عمليات إخفاء الأموال المتحصلة ولو كانت تتخذ الشكل الرقمى أو الإلكترونى، وقد تضمنت المادة (٣٩) من قانون مكافحة الإرهاب النص على عقوبة المصادرة للأموال المتحصلة من ارتكاب جرائم إرهابية وكل مال خُصص للصرف على جرائم إرهابية، حيث تقضى المادة المذكورة بأنه: "مع عدم الإخلال بحقوق الغير حسنة النية تقضى المحكمة فى كل حكم يصدر بالإدانة فى جريمة إرهابية فضلًا عن العقوبة المقررة للجريمة بمصادرة الأموال والأمتعة والأسلحة والأدوات والمستندات وغيرها مما استخدم فى ارتكاب الجريمة أو تحصل عنها وبحل الجماعة الإرهابية وإغلاق مقارها وأمكنتها فى الداخل والخارج فضلًا عن إغلاق أى مكان تم فيه تصنيع أو تصميم الأسلحة بمختلف أنواعها المستخدمة فى ارتكاب أية جريمة إرهابية وغيرها مما يكون قد استعمل أو أعد للاستعمال من قبل الإرهابى أو الجماعة الإرهابية. كما تقضى المحكمة عند الحكم بالإدانة بمصادرة كل مال متى ثبت أنه كان مخصصاً للصرف منه على الأعمال الإرهابية".

فضلًا عن تقرير سلطة النيابة العامة فى التحفظ على الأموال المشار إليها وتجميدها والمنع من التصرف فيها أو إدارتها، حيث تنص المادة (٤٨) من قانون مكافحة الإرهاب على سريان القواعد الخاصة بالتحفظ على أموال المتهم فى قانون الإجراءات الجنائية على

المتهم بالجريمة الإرهابية، حيث تقضى المادة المذكورة بأنه: "تسرى أحكام المواد ٢٠٨ مكررًا (أ) و٢٠٨ مكررًا (ب) و٢٠٨ مكررًا (ج) و٢٠٨ مكررًا (د) من قانون الإجراءات الجنائية فى الأحوال التى يظهر فيها من الاستدلال أو التحقيق دلائل كافية على الاتهام بارتكاب أى جريمة إرهابية. وللسلطات المختصة اتخاذ التدابير التحفظية اللازمة بما فى ذلك تجميد الأموال والمنع من التصرف فيها أو إدارتها أو المنع من السفر على أن تلتزم بالأحكام والإجراءات المنصوص عليها فى المواد المذكورة بالفقرة الأولى من هذه المادة"، ويتضح لنا من العرض السابق أن التشريعات سارعت إلى مواجهة إساءة استخدام العملات الرقمية المشفرة، من خلال توسعها فى مدلول الأموال لتشمل كل من الأموال التقليدية والرقمية، وبما يحقق مواجهة شاملة لإساءة استخدام مثل هذه الأموال، على الرغم من أن هذه التشريعات لا تعترف بمثل هذه العملات، ومن ثم فإن هذه العملات لا تقرر لها هذه التشريعات حماية جنائية لها كما هو مقرر للعملات التقليدية.

ثالثاً: **عمليات الاتجار بالمخدرات**:

تعمل عصابات المخدرات على استغلال شبكة الإنترنت الخفية فى ترويج المواد المخدرة، حيث ذكر تقرير المخدِّرات العالمى لعام ٢٠١٩ أن مشتريات المخدِّرات عبر الشبكة الخفية آخذة فى 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 للمخدِّرات لعام ٢٠١٩ إلى أن شراء المخدِّرات عن طريق الشبكة الخفية لا يزال ظاهرة حديثة جدًا، حيث إن ٤٨ فى المائة من الأشخاص الذين أبلغوا عن شراء المخدِّرات عن طريق الشبكة الخفية فى عام ٢٠١٩ بدأوا فى استخدامها لتلك الأغراض فى العامين السابقين، وأن نسبة ٢٩ فى المائة أخرى بدأت فى ذلك فى العامين السابقين عليهما[٤٦].

وقد يكون بوسع أسواق المخدِّرات الكائنة على الشبكة الخفية أن تدخل تغييرات فى أنماط تعاطى المخدِّرات ومدى انتشاره[٤٧]، فاستخدامها يمكن أن يقلِّل بعض المخاطر

بالنسبة للمشترين والبائعين، مثل التعرض لمواجهات عنيفة فى المناطق التى تباع فيها المخدِّرات[٤٨]، ومع ذلك، فإن مبيعات المخدِّرات، التى تيسِّرها الإنترنت، لها مخاطرها، ومن المرجح أن تحدث أكبر تلك المخاطر أثناء أنشطة تتم خارج دائرة الاتصال بالإنترنت[٤٩]، وقد تكون مبيعات المخدِّرات التى تيسرها الإنترنت مرتبطة أيضًا بالزيادات فى الجرعات المفرطة إذا كانت تيسر على المتعاطين تجربة عقاقير جديدة، وتتيح لهم الحصول على مخدِّرات أقوى مفعولاً[٥٠]، وقد أشار أحد التقارير الصادر عن اليوروبول إلى تحقيق نجاح ملحوظ فى تفكيك أسواق كبيرة على الشبكة الخفية، غير أن المجرمين، يستكشفون وسائل بديلة للتحايل على إجراءات إنفاذ القانون، ويتمثل أحد الاتجاهات الجديدة فى ظهور نماذج تجارية يستخدم فيها المجرمون هويات متعددة، من خلال استخدام ملفات تعريف متعددة، على منصات مختلفة على الإنترنت، مما ييسر بدوره العمليات التى يقوم بها أفراد مختلفون بدلًا من شخص واحد[٥١].

ومن أبرز الأمثلة على استخدام الشبكة المظمة فى ترويج المواد المخدرة موقع طريق الحرير، والذى كان أكبر موقع لتجارة المخدرات على الشبكة السوداء، وكان مكتب التحقيقات الفيدرالى الأمريكى قد أعلن أن هذا الموقع قد حقق منذ إنشائه عمولات مالية تقدر بحوالى ٨٠ مليار دولار، وأن السلطات الأمريكية قد تمكنت بعد إغلاقه من التوصل إلى العديد من تجار المخدرات من مستخدمى هذا الموقع من العديد من البلدان، من بينها الولايات المتحدة الأمريكية، وبريطانيا، وأستراليا، والسويد.

وعلى الرغم من هذا النجاح للسلطات الأمريكية فى غلق هذا الموقع، فقد أعاد أحد معاونى صاحب الموقع الأصلى إطلاق موقع طريق الحرير ٢ بعد شهر واحد من إغلاق الموقع السابق، بحيث تضمن الموقع الجديد بعد إطلاقه أكثر من ٥٠٠ قائمة من المخدرات [٥٢].

موقف التشريع المصرى:

تخضع عمليات الاتجار بالمخدرات عبر شبكة الإنترنت لأحكام قانون مُكافحة الاتجار بالمُخدرات رقم (١٨٢) لسنة ١٩٦٠، وقد أخذ هذا القانون بنهج تشريعىّ مُشدد تجاه جميع صور التعامل فى المواد المُخدرة من زراعة وإنتاج وجلب وتصدير واتجار وتعاطى، حيث نصت المادة الثانية من القانون على أنه: "يحظر على أى شخص أن يجلب أو يُصدر أو يُنتج أو يملك أو يُحرز أو يشترى أو يبيع جواهر مُخدرة أو يتبادل عليها أو ينزل عنها بأىّ صفة أو أن يتدخل بصفته وسيطًا فى شىء من ذلك إلا فى الأحوال المنصوص عليها فى هذا القانون وبالشروط المبينة به"، بينما نصت المادة (٣٣) من القانون ذاته على أنه: "يعاقب بالإعدام وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه. (أ) كل من صدر أو جلب جوهرًا مُخدرًا قبل الحصول على الترخيص المنصوص عليه فى المادة (٣). (ب) كل من أنتج أو استخرج أو فصل أو صنع جوهرًا مخدرًا وكان ذلك بقصد الاتجار. (ج) كل من زرع نباتًا من النباتات الواردة فى الجدول رقم (٥) أو صدره أو جلبه أو حازه أو أحرزه أو اشتراه أو باعه أو سلمه أو نقله أيًّا كان طور نموه، وكذلك بذوره، وكان ذلك بقصد الاتجار أو اتجر فيه بأيّة صورة، وذلك فى غير الأحوال المصرح بها قانونا... (د)...".

كما أدخل المُشرع المصرى عدة تعديلات على هذا القانون لتدعيم السياسة الجنائيّة لمُكافحة انتشار هذه الظاهرة، وجرم كل صور الأفعال التى لها صلة بالمواد المُخدرة والتى تندرج فى إطار الجريمة المُنظمة، حيث نصت المادة (٣٣/د) من قانون المُخدرات على أنّه: "(د) كل من قام ولو فى الخارج بتأليف عصابة، أو إدارتها أو التداخل فى إدارتها أو فى تنظيمها أو الانضمام إليها أو الاشتراك فيها وكان من أغراضها الاتجار فى الجواهر المُخدرة أو تقديمها للتعاطىّ أو ارتكاب أى من الجرائم المنصوص عليها فى هذه المادة داخل البلاد..."[٥٣]، فقد راعى المُشرع فى ذلك انتقال نشاط الاتجار بالمُخدرات من النشاط الفردى إلى دائرة المُنظمات الإجرامية التى تمتد شبكاتها فى مُعظم الأحوال إلى العديد من

دول العالم، فجعل تأليفها والانضمام إليها بأيّة صورة من الصور التى عددها النص ولو فى خارج البلاد هو محل التأثيم طالما كان من أغراضها مُمارسة أى من الأنشطة المُشار إليها داخل البلاد[٥٤]، ويقصد بتأليف العصابة تكوينها من شخصين أو أكثر، ويتخذ هذا النشاط صورة الاتفاق الجنائىّ على جرائم يكون من بينها الاتجار بالمُخدرات أو تقديمها للتعاطىّ أو ارتكاب إحدى الجرائم المنصوص عليها فى المادة (٣٣) من قانون مُكافحة المُخدرات داخل البلاد، أما إدارة العصابة فيقصد بها تنظيم العمل بها وتحديد الجرائم التى تهدف إلى ارتكابها وتوزيع الأدوار على المُشاركين فيها، وأما التداخل فى إدارة العصابة أو تنظيمها فيقصد به مُعاونة القائم على الإدارة فى القيام بمُهمته والمُعاونة على سير العمل فى العصابة. أما الانضمام إلى العصابة أو الاشتراك فيها فيقصد به قبول العضوية فيها بحيث يُسند إليه أى عمل من الأعمال التى تستهدفها [٥٥].

رابعاً: عمليات الاتجار بالبشر والغرف الحمراء:

تنتشر عبر شبكة الإنترنت المظلمة مواقع تستغل النساء والأطفال جنسيًا[٥٦]، فيما يعرف بالغرف الحمراء، تعمل عليها عصابات الاتجار بالبشر، فضلًا عن انتشار عمليات بيع الأعضاء البشرية كذلك، حيث تشير بعض التقارير إلى وجود مواقع على الشبكة المظلمة لإجراء تجارب على البشر، يعمل روادها بخطف المتشردين من الشوارع واستخدامهم بالتجارب العلمية، ويضعون معلوماتهم فى قوائم للمهتمين بهذه التجارب، فهناك مواقع إتجار بالنساء، ترسل قوائم بكل المواصفات التى يطلبها الزبون ليختار كما يشاء، والمفجع أكثر سوق الأطفال على الإنترنت المظلم، وهو الأكثر انتشارًا بحسب دراسة قامت بها جامعة بورتموث البريطانية فى كانون الأول ٢٠٠٤، كشفت أن أكثر المحتوى المتبادل على شبكة Torهو إباحية الأطفال، يليها الأسواق السوداء التى تبيع المخدرات والأسلحة بأنواعها، وحتى الإتجار بالبشر وبالأعضاء البشرية، ولجودة الخدمة فى السوق السوداء هناك ميزة التقييمات، إذ يقيم كل بائع من قبل المشترين لزيادة الثقة بينه وبين المشترين الجدد، هذا كله

غير تزوير الأوراق الرسمية كالهويات وجوازات السفر، وأكدت دراسة أخرى قامت بها جامعة كينجز كوليج البريطانية العام الحالى، هذه المعلومات وأن معظم استخدام شبكة Tor وبلاحقته onion، تتبادل محتوى غير شرعى، وقد تذهب الأمور أبعد من ذلك، فى موقع مخصص لمشاركة تجارب أكل لحوم البشر، حيث يعلق الناس ويكتبون عن تجاربهم بأكل لحم البشر لأول مرة.

كما تبيِّن البحوث التى أجريت والأدلة المباشرة أن المتَّجرين بالبشر يستخدمون التكنولوجيا خلال جميع مراحل الجريمة، بما فى ذلك تصيُّد الضحايا ومراقبتهم واستغلالهم، وأحد الأسباب التى تجعل المتَّجرين يستخدمون التكنولوجيا فى عملهم هو أنها تمكِّنهم من العمل دون الكشف عن هويتهم، كما أن العملة المشفَّرة تسمح لهم بإجراء معاملات مالية ونقل العائدات الإجرامية دون الكشف عن هويتهم، أما السبب الثانى، فهو أن التكنولوجيا تيسر لهم تصيُّد الضحايا واستغلالهم، حيث يمكن استخدام مواقع الإعلانات المبوبة على الإنترنت وشبكات التواصل الاجتماعى كقنوات للاتِّجار بالبشر(٥٧)، وعلاوة على ذلك، فإن إساءة استخدام التكنولوجيا يمكن أن تيسر على المتَّجرين إبرام معاملات مع زبائنهم، ودخول أسواق جديدة، وتوسيع نطاق العمليات الإجرامية، ويمكن للمتَّجرين استخدام تطبيقات البث المباشر للوصول إلى سوق أوسع لزبائن ربما لم يسبق لهم قط أى اتصال فعلى بالضحية(٥٨).

فضلًا عن ذلك، فإن إساءة استخدام التكنولوجيات يمكن أن تساعد المتَّجرين على مراقبة الضحايا وإكراههم، ويمكن للمتجرين أن يستفيدوا من تطبيقات تتبع الحركة، وتحديد المكان لتيسير استغلال الضحايا، وحتى بعد أن يفلت الضحايا من قبضة المتَّجرين، يظل من الممكن تعقُّبهم حيث يكتشف الجناة أماكن وجود ضحاياهم باستخدام تطبيقات تتبع الحركة، وتحديد المكان الموجودة فى الهواتف النقالة للضحايا، وفى الوقت نفسه، تستخدم أجهزة إنفاذ القانون بالفعل تطبيقات تتبع الحركة، وتحديد المكان للكشف عن مكان وجود

المتَّجرين المشتبه فيهم أو غيرهم من الأفراد المشاركين فى شبكة الاتِّجار، 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[٥٩].

ووفقًا لليوروبول، أصبح بث اللقطات الحية للاعتداءات الجنسية عبر الغرف الحمراء خطراً حقيقيًا، ويتم بث تلك اللقطات من خلال تطبيقات وسائل التواصل الاجتماعى وتطبيقات الدردشة المرئية ومنصات الألعاب وغرف الدردشة على الإنترنت[٦٠]، ومن أهم المخاطر فى توزيع مواد الاستغلال الجنسى للأطفال عبر الإنترنت الزيادة المستمرة فى استخدام الشبكة الخفية، حيث أشارت مؤسسة رصد الإنترنت Watch Internet Foundation إلى أن المواقع الشبكية المقنَّعة، التى تستخدم طريقة "المسار الرقمى" لإخفاء صور الاعتداء الجنسى على الأطفال، لا تزال تمثل مشكلة كبيرة، وعلاوة على ذلك، لاحظت المؤسسة حدوث زيادة مطَّردة فى عدد عناوين المواقع الشبكية للاعتداء الجنسى على الأطفال فى السنوات الأخيرة: من ٠٩٢ ٦٨ عنوانًا فى عام ٢٠١٥ إلى ٠٤٧ ١٠٥ عنواناً فى عام ٢٠١٨[٦١].

وعلاوة على ذلك، فإن الأشخاص الذين يسعون إلى الاعتداء على الأطفال جنسيًّا باستخدام الإنترنت سوف يواصلون البحث عن سبل جديدة لتجنُّب الانكشاف كلما ازدادت مهارتهم التقنية، وفى الآونة الأخيرة، حدث تحول من استخدام المنتديات الكبيرة إلى تشكيل مجموعات صغيرة من المستعملين، وهو ما تيسِّره تطبيقات التراسل بالأجهزة المحمولة مع تشفير عمليات التراسل من بدايتها إلى نهايتها، وفى إطار مواجهة هذه الصور من الاعتداءات على شبكة الإنترنت، فقد أنشئت أيضًا قواعد بيانات خاصة لتحميل المواد التى تصور الاعتداءات الجنسية على الأطفال لاستخدامها كأدلة فى التحقيقات، مثل قاعدة البيانات الدولية للاستغلال الجنسى للأطفال التابعة للمنظمة الدولية للشرطة الجنائية، وفى

الولايـات المتحـدة الأمريكيـة، تـستخدم قاعـدة بيانـات المركـز الـوطنى للأطفـال المفقـودين والمستغَلِّين كمستودع مركزى لتخزين المواد المتعلقة بالاعتداءات الجنسية على الأطفال[٦٢].

وتشير بعض التقارير الصحفية إلى أن الانترنت المظلم قد أسهم فى إنقاذ طفل روسى عمره سبع سنوات من براثن أحد مشتهى الأطفال (البيدوفيليا)، والذى اختطفه واحتجزه فى مخبأ تحت الأرض لمدة ٥٢ يومًا فى روسيا، وكانت عملية تحرير الطفل قد تمت بتدخل من القوات الخاصة الروسية بالتعاون مع الإنتربول، حيث وردت المعلومات المتعلقة بالطفل عبر قنوات الإنتربول للشرطة الروسية، حيث إن وجود الطفل صار معروفًا من المنشورات فى الإنترنت المظلم[٦٣].

موقف التشريع المصرى:

تخضع عمليات الاتجار بالبشر عبر شبكة الإنترنت لأحكام القانون رقم (٦٤) لسنة ٢٠١٠، حيث عرفت المادة (٢) من القانون جريمة الاتجار بالبشر بأنها: "يعد مُرتكبًا لجريمة الاتجار بالبشر كل من يتعامل بأيّة صورة فى شخص طبيعىّ بما فى ذلك البيع أو العرض للبيع أو الشراء أو الوعد بهما أو الاستخدام أو النقل أو التسليم أو الإيواء أو الاستقبال أو التسلم سواء فى داخل البلاد أو عبر حدودها الوطنيّة إذا تم ذلك بواسطة استعمال القوة أو العنف أو التهديد بهما، أو بواسطة الاختطاف أو الاحتيال أو الخداع، أو استغلال السلطة، أو استغلال حالة الضعف أو الحاجة، أو الوعد بإعطاء أو تلقىّ مبالغ مالية أو مزايا مقابل الحصول على موافقة شخص على الاتجار بشخص آخر له سيطرة عليه– وذلك كله– إذا كان التعامل بقصد الاستغلال أيًّا كانت صوره بما فى ذلك الاستغلال فى أعمال الدعارة وسائر أشكال الاستغلال الجنسى، واستغلال الأطفال فى ذلك وفى المواد الإباحيّة أو السخرة أو الخدمة قسرًا، أو الاسترقاق أو الممارسات الشبيهة بالرق أو الاستعباد، أو التسول، أو استئصال الأعضاء أو الأنسجة البشريّة أو جزء منها"، وعاقبت المادة (٥) من القانون

كل من ارتكب جريمة الاتجار بالبشر بالسجن المشدد وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه أو بغرامة مساوية لقيمة ما عاد عليه من نفع أيهما أكبر.

عمليات تهريب المهاجرين:

هناك ارتباط وثيق بين شبكة الإنترنت المظلمة وعمليات تهريب المهاجرين؛ إذ ينتشر على الشبكة المظلمة العديد من المواقع التى تعرض للبيع جوازات السفر السليمة والمزورة، والتى يتم استخدامها فى العديد من عمليات تهريب المهاجرين، ومن جانب آخر، أصبحت تكنولوجيات المعلومات والاتصالات أداة مهمة يستخدمها المهاجرون ومن يوقعون بهم على حد سواء على نطاق واسع لنقل المعلومات عن الدروب والخدمات والأسعار(٦٤)، علاوَة على ذلك، زادت وسائط التواصل الاجتماعى من قدرة المهرِّبين على تغيير الدروب للإفلات من التدابير التى تتخذها أجهزة إنفاذ القانون فى بلدان العبور للتصدى لهم، مما زاد من فعالية عمليات التهريب وعرقلة التحقيق فى مثل هذه الجرائم وملاحقة مرتكبيها قضائيًّا، ويمكن أن تترتب على التطور السريع فى تكنولوجيا الأجهزة المحمولة آثار على العلاقة بين المهاجرين والمهرِّبين، ففي العديد من مجموعات الفيسبوك، يمكن للمهاجرين التحقق من موثوقية بعض المهرِّبين وتبادل المعلومات حول أفضل الأشخاص الذين يمكن أن يُتصل بهم، وقد وُصفت عمليات الاستيثاق تلك بأنها: "سلم الجدارة بالثقة"(٦٥).

كما أن المدفوعات للمهرِّبين كانت تتم من خلال نظم الدفع عبر الإنترنت، وقد تزيد العملات المشفَّرة من السهولة التى يتمكن بها المهرِّبون من تلقِّى الأموال وإخفائها ونقلها، ويمكن لهذه العملات أن تساعد على غسل الأموال وأن تعين المهرِّبين على تجنب التعرض للتحقيق أو التوقيف من خلال حجب هويتهم، والحد من الحاجة إلى حمل مبالغ نقدية كبيرة، وتضطلع التكنولوجيا كذلك بدور رئيسى فى إتاحة وثائق السفر أو الهوية المزورة التى تيسِّر تهريب المهاجرين، وتُستخدم أنواع مختلفة من المعدات لتزييف جوازات السفر أو تزويرها أو نسخها بطرق احتيالية، وفى بعض الحالات، تستخدم أدوات متقدمة تكنولوجيًّا لتنفيذ عمليات

تزييف عالية الجودة (إعداد جوازات سفر مطابقة تماماً للجوازات الصحيحة)[٦٦]، بيد أنه يمكن النظر إلى الابتكارات التكنولوجية من زوايا متعددة، وليس فقط من منظور الفوائد التى تعود بها على المهرِّبين، وتقلِّل الرقمنة أيضًا الفجوات فى المعلومات التى يمكن للمهرِّبين 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 فى أن عددًا متزايدًا من المهاجرين يتمتعون بالاكتفاء الذاتى طوال عملية الهجرة ويعتمدون بدرجة أقل على المهرِّبين، ويعطى هذا المهاجرين قدرًا أكبر من الاستقلالية ويقلِّل من تعرُّضهم للاستغلال[٦٧].

وتختلف كيفية استخدام المهاجرين لوسائل التواصل الاجتماعى باختلاف جنسيتهم وانتمائهم العرقى وموطنهم الأصلى وخلفيتهم التعليمية، وكذلك بمدى قدرتهم على الوصول إلى الإنترنت واستعمالها [٦٨]، 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[٦٩].

ومن منظور إنفاذ القانون، هناك اهتمام متزايد بإيجاد سبل لاستغلال التكنولوجيا لتعطيل شبكات تهريب المهاجرين، كما أن الأدلة المتحصَّل عليها من وسائط التواصل الاجتماعى، أو من خلال استخدام التكنولوجيا قد تدعم شهادات المهاجرين المهرَّبين فى الإجراءات الجنائية ذات الصلة، ويساعد الاستخدام المناسب للتكنولوجيا الحكومات والقطاع الخاص والمنظمات غير الحكومية على منع تهريب المهاجرين والتخفيف من حدته، كلٌّ فى 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.

موقف التشريع المصرى:

عرفت المادة الأولى من قانون مكافحة الهجرة غير الشرعية وتهريب المهاجرين رقم (٨٢) لسنة ٢٠١٦ جريمة تهريب المهاجرين بأنها: "تدبير انتقال شخص أو أشخاص بطريقة غير مشروعة من دولة إلى أخرى من أجل الحصول بصورة مباشرة أو غير مباشرة على منفعة مادية أو معنوية أو لأى غرض آخر"، وقد عاقبت المادة (٦) من القانون كل من ارتكب جريمة تهريب المهاجرين أو الشروع فيها أو توسط فى ذلك، بالسجن وبغرامة لا تقل عن خمسين ألف جنيه ولا تزيد على مائتى ألف جنيه أو بغرامة مساوية لقيمة ما عاد عليه من نفع أيهما أكبر.

عمليات الاتجار بالأسلحة النارية:

تشير التقديرات الدولية إلى أن شبكة الإنترنت الخفية يمكن أن تتحول إلى ساحة مفضلة لأعضاء الجماعات الإجرامية المنظمة والأفراد الذين يريدون شراء أسلحة نارية دون الكشف عن هويتهم أو لأغراض غير مشروعة[٧٠]، وفى ضوء دراسة أعدها مكتب الأمم المتحدة لشئون نزع السلاح على أساس مشروع بحثى أكبر أجرته مؤسسة Europe RAND فى عام ٢٠١٧[٧١]، وقدمها إلى اللجنة الأولى للجمعية العامة للأمم المتحدة فى عام ٢٠١٨، لوحظ أن هناك حاجة ماسة إلى تعاون دولى جديد لمكافحة مبيعات الأسلحة غير المشروعة التى أصبحت ممكنة من خلال حجب الهوية فى الشبكة الخفية[٧٢]، ويبدو أنَّ حجم مبيعات الأسلحة عبر الشبكة الخفية أقل من حجم مبيعات غيرها من البضائع غير المشروعة[٧٣]، وتبين دراسة حديثة تركز فقط على قوائم السلع المتصلة بالأسلحة المعروضة على الشبكة الخفية أن قوائم الأسلحة النارية هى الأكثر شيوعًا، حيث تشكل نسبة (٤٢٪) من جميع القوائم على الشبكة الخفية، تليها المنتجات الرقمية المتصلة بالأسلحة بنسبة (٢٧٪)، ومنتجات أخرى مثل الذخيرة بنسبة (٢٢٪)[٧٤].

ولا غنى عن السعى 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 الوطنى، ينبغى لواضعى السياسات الحرص على تزويد أجهزة إنفاذ القانون بما يكفى من الموظفين والمعدات والتدريب للتصدى للتحديات ذات الصلة، وقد توفر الأطر القانونية الدولية القائمة، ولا سيما اتفاقية الجريمة المنظمة وبروتوكولها الخاص بالأسلحة النارية، أساسًا لاعتماد نُهُج شاملة للتصدى لهذه الظاهرة، ويلزم إجراء تحليل متعمق لما إذا كانت تسرى عليها لوائح السمسرة القائمة، المنصوص عليها فى بروتوكول الأسلحة النارية (المادة ١٥)، ومعاهدة تجارة الأسلحة (المادة ١٠)[٧٥].

موقف التشريع المصرى:

تخضع عمليات بالاتجار بالأسلحة عبر شبكة الإنترنت للقانون رقم (٣٩٤) لسنة ١٩٥٤ بشأن الأسلحة والذخائر وتعديلاته، حيث نصت المادة (٢٨) من قانون الأسلحة والذخائر على أنه: "ويعاقب بالسجن وبغرامة لا تقل عن خمسمائة جنيه ولا تجاوز ألف جنيه، كل من اتجر أو استورد أو صنع أو أصلح بغير ترخيص سلاحًا ناريًا من الأسلحة المنصوص عليها فى الجدول رقم(٢). وتكون العقوبة السجن المشدد، إذا كان السلاح مما نص عليه فى البند (أ) من القسم الأول من الجدول رقم (٣) وتكون العقوبة السجن المؤبد إذا كان السلاح مما نص عليه فى البند (ب) من القسم الأول أو فى القسم الثانى من الجدول رقم(٣)[٧٦].

عمليات التصيد الاحتيالى: تتم عمليات التصيد الاحتيالى من خلال عدة طرق، من أشهرها برامج الفدية، وهى برامج خبيثة يتم إرسالها للأفراد عبر البريد الإلكترونى، تعمل على تشفير البيانات والملفات الموجودة على أجهزة الحاسب الآلى، ويطلب الجناة مبالغ مالية يتم دفعها عن طريق العملة المشفرة البتكوين لإرسال ملف فك التشفير، وهو ما أكدت عليه وأعلنته الشركة الروسية للأمن الإلكترونى Kaspersky من أن الشبكات السوداء قد أفرزت نوعًا جديدًا من البرامج الخبيثة يطلق على Ware Ransom، أصبح يعتمد على برنامج TOR حتى يتمكن المهاجمون من إخفاء هويتهم، وهذا النوع من البرامج الخبيثة يتم من خلاله السيطرة على الحاسب الآلى وإغلاق نظام التشغيل الخاص به، وإجبار المستخدم على دفع

فدية حتى يعود جهازه للعمل من جديد، ولقد زادت خطورة هذه البرامج إلى الحد الذى باتت فيه تهدد الأجهزة الحكومية ذاتها؛ إذ أصيب جهاز الشرطة فى ولاية ماساتشوستس الأمريكية عام ٢٠١٣ بأحد هذه البرامج، والذى أطلق عليه Cryptolocker واضطروا إلى دفع ١٣٣٨ دولارًا كفدية حتى يتخلصوا من هذا البرنامج(٧٧).

المطلب الثالث

الجهود الدولية والوطنية لمواجهة الأنشطة الإجرامية المنظمة عبر شبكة الإنترنت المظلمة.

أولًا: التحديات الأمنية التى تواجه أجهزة إنفاذ القانون فى تعقب الأنشطة الإجرامية على شبكة الإنترنت المظلمة:

هناك بعض التحديات التى تعترض التحرى عن أنشطة الشبكة الخفية، منها:

١- عدم فهرسة المعلومات الموجودة بها، مما يجعل من محاولة تحديد موقع تلك المعلومات باستخدام محركات البحث أو الكلمات الرئيسية أمراً غير يسير للمحققين.

٢- استخدام المجرمين منصات لامركزية، لاستضافة خوادمهم الشبكية، مما يتيح انتشار خدمات قد يكون من الصعب اكتشافها (٧٨).

ثانياً: الحلول التقنية للتعامل الأمني مع الأنشطة غير المشروعة على شبكة الإنترنت المظلمة:

هناك فرص متاحة أمام أجهزة إنفاذ القانون لرصد أسواق الشبكة الخفية وإجراء تحريات بالاتصال الحاسوبى المباشر(٧٩)، وللمساعدة التقنية أهميتها فى هذا الشأن، ولذا يعمل مكتب الأمم المتحدة المعنى بالمخدرات والجريمة والمنظمة الدولية للشرطة الجنائية (الإنتربول) بجد على توفير أنشطة للتدريب تركز على أساليب التحرى المتعلقة بالشبكة الخفية، وهناك طائفة من الأدوات، التى يمكن أن تتيح فى هذا السياق حلولًا فعالة، نذكر منها:

١- الزواحف الشبكية التى يمكن استخدامها لفهرسة البيانات على الإنترنت بشكل متكرر.
٢- أدوات التنقيب عن البيانات للبحث فى مجموعات البيانات الضخمة.
٣- الأدوات التحليلية للعملات المشفَّرة لتعقُّب مسار المدفوعات.
٤- برمجيات سلاسل كتل البيانات المشفَّرة المستخدمة لتعقُّب الأدلة[٨٠].

ثالثاً: دور المنظمة الدولية للشرطة الجنائية (الانتربول):

فى إطار حرص الإنتربول [٨١] على مواجهة صور الإجرام المنظم، عبر شبكة الإنترنت المظلمة، فقد اضطلع باتخاذ الخطوات التالية[٨٢]:

١- استحداث أداة لتحليل سجل المعاملات الإلكترونية Blockchain أُطلق عليها اسم GraphSense، تتيح تعقب الصفقات بالعملات المشفرة، وبفضل هذه الأداة يمكن للمحققين البحث عن عناوين العملات المشفرة ورموزها ومعاملاتها من أجل تحديد المجموعات المرتبطة بعنوان ما وبالتالى تقفّى أثر الأموال، لدعم تحقيقاتهم.

٢- استحداث أداة تحليل تدعى Darkwe Monitor، تتمثل وظيفتها فى جمع البيانات عن الأنشطة الإجرامية على الشبكة الخفية واستخدامها لتوفير مواد استخباراتية يمكن الاستناد إليها لاتخاذ ما يلزم من إجراءات لدعم التحقيقات التى تجريها أجهزة الشرطة على الصعيد الدولى، وستساعد هذه البيانات والتحليل اللاحق لها على تحديد اتجاهات جديدة ودعم البحوث وإسداء المشورة بشأن أنشطة الوقاية، وتشمل قائمة البيانات (عناوين العملات المشفرة؛ مفاتيح برمجية التشفير Pretty Good Privacy"PGP "؛ عناوين بروتوكول الإنترنتIP؛ أسماء المستخدمين والأسماء المستعارة؛ عناوين البريد الإلكترونى؛ نطاقات الأسواق الإلكترونية على الشبكة الخفية؛ المنتديات على الشبكة الخفية؛ سجل البيانات التى جُمعت من الشبكة الخفية منذ عام ٢٠١٥).

٣- تصنيف الشبكة الخفية والعملات المشفرة: تقوم فرقة عمل الإنتربول المعنية بالشبكة الخفية والعملات المشفرة حاليًا بإعداد تصنيف عالمى للعملات المشفرة يحدد فئات

البيانات التى ينبغى تجميعها ذات الصلة بالصفقات المشبوهة، وقد تشمل هذه مثلًا عمليات تبادل العملات التى أجريت أو نوع الجريمة المرتبطة بها الصفقة، وستُضاف هذه الفئات رقميًا إلى كل عملة مشفرة مثلما تضاف إلى صورة رقمية البيانات المتعلقة بمكان وتاريخ أخذها ونوع المعدات المستخدمة، وهذا التصنيف الذى يمكن الاطلاع عليه على الإنترنت يتمحور حول ثلاث فئات من المعلومات (الكيانات، أى الأشخاص والمنظمات والكيانات الرقمية؛ الخدمات، أى أسواق الشبكة الخفية، وعمليات تبادل العملات المشفرة، والجهات التى تسهّل تبادل الرسائل، وسائر مزودى الخدمات المرتبطين بالصفقة؛ أنواع الجرائم، أى الجرائم التى ترتبط بها الصفقة كبيع المخدرات أو الأسلحة غير المشروع على الإنترنت)، وسيُوَفَّر التصنيف النهائى على الصعيد العالمى كدليل معيارى يمكن لأجهزة إنفاذ القانون والقطاع الخاص والأوساط الأكاديمية استخدامه لإضافة الفئات إلى العملات المشفرة.

٤- دعم التحقيقات على الإنترنت لمكافحة الإرهاب Cap act: فى إطار مشروعCap act ، الذى يديره مركز الإنتربول للابتكار، يجرى إعداد دليل لمساعدة أجهزة إنفاذ القانون فى جنوب شرق آسيا على التصدى لإساءة استخدام الشبكة الخفية والعملات المشفرة من قبل الإرهابيين، وسيوفر الدليل المعنون (دليل الممارسين فى بلدان رابطة أمم جنوب شرق آسيا لمكافحة الإرهاب المرتبط باستخدام الشبكة الخفية والعملات المشفرة) للمستخدمين فى أجهزة إنفاذ القانون مبادئ توجيهية شاملة تتعلق بالتحقيق فى الأنشطة الإرهابية على الشبكة الخفية، بما فى ذلك الأنشطة التى تنطوى على استخدام العملات المشفرة، وسيُحدد أيضا مختلف الأدوات والنهج والإجراءات لتحليل بيانات الاستخبارات المتصلة بالإرهاب على الإنترنت.

٥- تنظيم دورات تدريب ومبادرات لبناء القدرات على الصعيد الدولى من قبيل منصة تدريب على الإنترنت تقوم على محاكاة الأسواق والمنتديات الإلكترونية على الشبكة الخفية؛

التدريب على التحقيق فى منظومات المعاملات بالعملات المشفرة، التى تعزز حجب الهوية، لمواجهة الصعوبات التى يمكن أن تعترض المحققين، أثناء جمع الأدلة ذات الصلة بمثل هذه الجرائم.

رابعاً: الجهات الدولية المعنية بمواجهة الأنشطة الإجرامية على شبكة الإنترنت المظلم: ومن أبرزها:

- فرقة عمل معنية بالشبكة الخفية والعملات المشفرة بالإنتربول: جمع الإنتربول ووزارة العدل فى ولاية بافاريا الألمانية الفريق العامل المعنى بالشبكة الخفية والعملات المشفرة، الذى يتألف من خبراء عالميين، لمشاطرة الأساليب والأدوات التى تساعد على كشف المجرمين الذى يستغلون الطابع السرى الذى تتيحه العملات المشفرة والشبكة الخفية؛ وتبادل الاطلاع على أفضل الممارسات فى مجال التحقيقات على الإنترنت؛ ووضع معايير فى مجال التحقيق وحلول فى مجال الأدلة الجنائية وتوفيرهما لأجهزة إنفاذ القانون، ولمواجهة أشد الصعوبات التى كشفها الفريق العامل، تم إنشاء فرقة عمل معنية بالشبكة الخفية والعملات المشفرة ستركز على (استحداث قاعدة بيانات دولية لمحفظات العملات المشفرة المرتبطة بالجريمة؛ وضع قاعدة بيانات تضم علامات الترميز (tag packs) التى تخصص للعملات المشفرة، والتى يمكن تحليلها للمساعدة فى التحقيقات؛ توحيد اللغة المستخدمة لتصنيف البيانات المجمّعة من الشبكة الخفية، أو التى جرى تعقّبها فيها؛ التشجيع على إنشاء شبكة من المبتكرين ومطورى البرمجيات ينتمون إلى أجهزة إنفاذ القانون لقيادة الجهود التى تُبذل فى هذا المجال).
- فريق الويب المظلم التابع لليوروبول: يمثل هذا الفريق إحدى مبادرات منظمة اليوروبول فى إنشاء نهج منسق لإنفاذ القانون لمعالجة الجريمة على شبكة الإنترنت المظلمة، كما يشمل وكالات إنفاذ القانون من جميع أنحاء الاتحاد الأوروبى وخارجه

وشركاء ومنظمات أخرى ذات صلة، مثل Euro just، وقد كانت العلة من فريق الويب المظلم المتخصص هى العمل مع شركاء الاتحاد الأوروبى وجهات تطبيق القانون فى جميع أنحاء العالم لتقليل حجم هذا الاقتصاد السرى غير القانونى، وتقديم نهجٍ كاملٍ ومنسقٍ، من خلال مشاركة المعلومات؛ تقديم الدعم العملى والخبرة فى مجالات الجريمة المختلفة؛ تطوير الأدوات والتكتيكات والتقنيات لإجراء تحقيقات الويب المظلم؛ تحديد التهديدات والأهداف، ويهدف الفريق أيضًا إلى تعزيز الإجراءات الفنية والاستقصائية المشتركة، وتنظيم مبادرات التدريب وبناء القدرات، جنبًا إلى جنب مع حملات الوقاية والتوعية – إستراتيجية ٣٦٠ درجة ضد الإجرام على شبكة الإنترنت المظلمة.

- المركز الأوروبى للجرائم الإلكترونية (EC3) التابع لليوروبول وفريق العمل المشترك لمكافحة الجرائم الإلكترونية (J-CAT) فى اليوروبول: وهو فريق تشغيلى دائم يتألف من ضباط اتصال إلكترونى من دول مختلفة يعملون فى تحقيقات الجرائم الإلكترونية رفيعة المستوى.

خامساً: أبرز الجهود الأمنية الدولية لمواجهة الأنشطة الإجرامية المرتكبة على شبكة الإنترنت المظلمة:

على الرغم من صعوبة تعقب الأنشطة الإجرامية المرتكبة على شبكة الإنترنت المظلمة، فإن الجهود الدولية تتكاتف مع بعضها للتصدى لهذه الأنشطة الخطيرة، ومن أبرز النجاحات التى حققتها الأجهزة الأمنية الدولية ما يلى:

- غلق موقع سوق الحرير: والذى كان يُعد من أكبر المواقع الإلكترونية للاتجار فى المخدرات وعمليات غسل الأموال على شبكة الإنترنت المظلمة، حيث تمت عملية الغلق فى عام ٢٠١٣، بمعرفة السلطات الأمريكية (مكتب التحقيقات الفيدرالى "FBI" وإدارة مكافحة المخدرات) لموقع سوق طريق الحرير، وأُعتقل مالكها "روس أولبريخت"،

لاستخدامه فى ترويج السلع والخدمات غير القانونية كالمخدرات وغسل الأموال، حيث أشارت الإحصائيات إلي قيام عشرات الآلاف من المستخدمين بشراء وبيع سلع وخدمات غير قانونية بقيمة أكثر من ٢٠٠ مليون دولار فى سوق طريق الحرير، وقد قدرت الأرباح المتحصلة عن أنشطة الموقع غير المشروعة آخر سنتين قبل غلقه بمبلغ ١,٢مليار دولار، ومنذ ذلك الحين أغلقت وكالات إنفاذ القانون الأمريكية والأوروبية أسواق حلفاء طريق الحرير، بما فى ذلك "خليج ألفا" و"سوق هانزا"، وكان مكتب التحقيقات الفيدرالى الأمريكى قد أعلن أن هذا الموقع قد حقق منذ إنشائه عمولات مالية تقدر بحوالى ٨٠ مليار دولار، وأن السلطات الأمريكية قد تمكنت بعد إغلاقه من التوصل إلى العديد من تجار المخدرات من مستخدمى هذا الموقع من العديد من البلدان، من بينها الولايات المتحدة الأمريكية، وبريطانيا، وأستراليا، والسويد، وعلى الرغم من هذا النجاح للسلطات الأمريكية فى غلق هذا الموقع، فقد أعاد أحد معاونى صاحب الموقع الأصلى إطلاق موقع (طريق الحرير ٢) بعد شهر واحد من إغلاق الموقع السابق، بحيث تضمن الموقع الجديد بعد إطلاقه أكثر من ٥٠٠ قائمة من المخدرات، إلى أن تمكنت السلطات الأمريكية من إغلاقه من جديد.

- غلق موقع السوق السوداء[٨٣]: ومن أحدث العمليات الأمنية التى تمت خلال الآونة الأخيرة هى غلق موقع السوق السوداء Dark Market، والذى كان يعد أكبر سوق غير قانونى فى العالم على شبكة الإنترنت المظلمة، وقد تم غلقه وإيقاف نشاطه الإجرامى فى عملية دولية شارك فيها عدة دول، هى: ألمانيا وأستراليا والدنمارك ومولدوفا وأوكرانيا والمملكة المتحدة (الوكالة الوطنية لمكافحة الجريمة) والولايات المتحدة الأمريكية "مكتب التحقيقات الفيدرالية FBI ومصلحة الضرائب DEA بدعم من منظمة الشرطة الأوروبية اليوروبول، حيث تمت عملية غلق الموقع وإزالته بتحليل تشغيلى متخصص وتنسيق الجهود المشتركة عبر الوطنية بين البلدان المعنية، وكانت

ألمانيا قد أخذت بزمام المبادرة فى هذه العملية الدولية، حيث ألقت إدارة التحقيقات الجنائية المركزية فى مدينة أولدنبورغ الألمانية القبض على مواطن أسترالى يُشتبه فى أنه المشغل لموقع السوق السوداء بالقرب من الحدود الألمانية الدنماركية خلال عطلة نهاية الأسبوع، حيث سمح التحقيق، الذى قادته وحدة الجرائم الإلكترونية فى مكتب المدعي العام فى كوبلنز، للضباط بتحديد موقع السوق وإغلاقه وإغلاق الخوادم والاستيلاء على البنية التحتية الجنائية – أكثر من ٢٠ خادمًا فى مولدوفا وأوكرانيا بدعم من مكتب شرطة التحقيقات الجنائية الفيدرالى الألمانى (BKA)، حيث منحت البيانات المخزنة المحققين خيوطًا جديدة لمزيد من التحقيق مع الوسطاء والبائعين والمشترين، وقد عملت منظمة اليوروبول على تسهيل عملية تبادل المعلومات على الصعيد الدولى، وتوفير الدعم التشغيلى المتخصص، وتوفير تحليلات متقدمة ساعدت السلطات الألمانية فى تحديد وتعقب المسئول المزعوم، ودعم ألمانيا فى تنسيق الجهود التعاونية عبر الحدود التى تشارك فيها شركاء دوليون، بمشاركة فاعلة من فريق الويب المظلم التابع لليوروبول، وتظهر الأرقام والإحصائيات الخاصة بموقع السوق السوداء Dark Market مدى خطورة أنشطته الإجرامية، حيث كان يستخدمه ما يقرب من نصف مليون (٥٠٠٠٠٠) مستخدم؛ ويتعامل فيه أكثر من (٢٤٠٠) بائع؛ وتتم من خلاله أكثر من (٣٢٠٠٠٠) معاملة؛ وكان يتم من خلاله نقل أكثر من (٤٦٥٠) bitcoin و (١٢٨٠٠)monero بالمعدل الحالى، وهذا يتوافق مع مبلغ يزيد على ١٤٠ مليون يورو، حيث كان الباعة يتاجرون فى السوق المشار إليه بشكل أساسى بجميع أنواع الأدوية، ويبيعون الأموال المزيفة، وتفاصيل بطاقات الائتمان المسروقة أو المزيفة، وبطاقات SIM المجهولة والبرامج الضارة.

- ضبط مديرى إحدى المنصات الإلكترونية لنشر صور الاعتداء الجنسى على شبكة الإنترنت المظلمة[٨٤]: نجحت منظمة الشرطة الأوروبية "اليوروبول" بالتعاون مع كل

من الشرطة الألمانية والأمريكية فى ضبط أربعة ألمان أداروا منصة لنشر صور الاعتداء الجنسى على الأطفال على شبكة الإنترنت المظلم يزورها قرابة نصف مليون مستخدم، والمعروفة باسم Boys town فى عملية أمنية متعددة الوكالات بتعاون أمنى دولى فعال، بمشاركة كل من الشرطة الجنائية الفيدرالية الألمانية والشرطة الهولندية والشرطة السويدية والمركز الأسترالى لمكافحة استغلال الأطفال والشرطة الفيدرالية الأسترالية وخدمة شرطة كوينزلاند ومكتب التحقيقات الفيدرالى الأمريكى وإدارة الهجرة والجمارك الأمريكية وشرطة الخيالة الكندية الملكية، وقد بدأت هذه العملية الأمنية الدولية بتحقيق من مكتب الشرطة الجنائية الفيدرالية الألمانى حول واحدة من أكثر منصات الاعتداء الجنسى على الأطفال انتشارًا فى أوروبا على شبكة الإنترنت المظلمة، حيث تمت الاعتقالات للمشتبه بهم فى كل من ألمانيا (٣) وباراغواى (١)، وكان للمعتقلين أدوار مختلفة فيما يتعلق بالموقع الذى تم الاستيلاء عليه، حيث تمت إزالة منصة الويب المظلمة، من قبل فرقة عمل دولية أنشأتها الشرطة الجنائية الفيدرالية الألمانية، والتى تضمنت اليوروبول ووكالات إنفاذ القانون من هولندا والسويد وأستراليا وكندا والولايات المتحدة، وقد ركز هذا الموقع على الاعتداء الجنسى على الأطفال، وكان لديه ٤٠٠٠٠٠ مستخدم مسجل عند إزالته، كما تم فى نفس المناسبة الاستيلاء على عدة مواقع دردشة أخرى على الشبكة المظلمة يستخدمها الأطفال الذين يرتكبون جرائم جنسية، وتُظهر مجتمعات المجرمين الأطفال عبر الإنترنت على الويب المظلم (وفق ما يراه اليوروبول) مرونة كبيرة فى الاستجابة لإجراءات إنفاذ القانون التى تستهدفهم، تتضمن ردود أفعالهم إحياء المجتمعات القديمة، وإنشاء مجتمعات جديدة، وبذل جهود قوية لتنظيمها وإدارتها، حيث تم استخدام الصور وبيانات الفيديو التى تم الاستيلاء عليها خلال هذا التحقيق لفرق عمل تحديد هوية الضحايا التى يتم تنظيمها بشكل منتظم فى اليوروبول، ومن المتوقع حدوث المزيد من الاعتقالات

وعمليات الإنقاذ على مستوى العالم حيث تقوم الشرطة فى جميع أنحاء العالم بفحص حزم المعلومات الاستخبارية التى جمعتها اليوروبول.

- ضبط أحد المشتبه بهم لتوظيفه قاتل محترف عبر شبكة الإنترنت المظلمة[٨٥]: دعمت منظمة الشرطة الأوروبية "اليوروبول" شرطة البريد والاتصالات الإيطالية (Polizia Postale e delle Comunicazioni) فى اعتقال مواطن إيطالى يُشتبه فى قيامه بتوظيف قاتل محترف على شبكة الإنترنت المظلمة، القاتل، الذى تم توظيفه من خلال موقع اغتيال على الإنترنت مستضاف على شبكة TOR، تم دفع ما قيمته حوالى ١٠٠٠٠ يورو من عملات البيتكوين لقتل صديقة المشتبه به السابقة، وقد أجرى اليوروبول تحليل تشفير عاجل ومعقد لتمكين تتبع وتحديد المزود الذى اشترى المشتبه به العملات المشفرة منه، ثم تواصلت الشرطة الإيطالية مع مزود خدمة التشفير الإيطالى الذى تم تحديده، والذى أكد المعلومات التى تم الكشف عنها أثناء التحقيق وزود السلطات بمزيد من التفاصيل حول المشتبه به، حيث أدى التحقيق فى الوقت المناسب إلى منع وقوع أى ضرر ضد الضحية المحتملة.
- ضبط أحد مشتهى الأطفال عن طريق شبكة الإنترنت المظلم: تشير بعض التقارير الصحفية إلى أن الإنترنت المظلم قد أسهم فى إنقاذ طفل روسى عمره سبع سنوات من براثن أحد مشتهى الأطفال (البيدوفيليا)، والذى اختطفه واحتجزه فى مخبأ تحت الأرض لمدة ٥٢ يومًا فى روسيا، وكانت عملية تحرير الطفل قد تمت بتدخل من القوات الخاصة الروسية بالتعاون مع الإنتربول، حيث وردت المعلومات المتعلقة بالطفل عبر قنوات الإنتربول للشرطة الروسية، حيث إن وجود الطفل صار معروفًا من المنشورات فى الإنترنت المظلم.
- مداهمة أحد مراكز استضافة مواقع الديب ويب فى مخبأ سابق للناتو بألمانيا[٨٦]: تمكنت السلطات الألمانية من مداهمة أحد أكبر أوكار ومراكز استضافة مواقع

الـ"Darkweb" فـى العـالم، والـذى كـان فـى مخبـأ قـديم تـابع لحلـف شـمال الأطلـسى (الناتو) فى قرية "ترابن تراراباخ" على ضفاف نهر "موسيل" بألمانيا، وتعود وقائع هذه المداهمة إلى اشتباه الشرطة الألمانية فى مجموعة من الأشخاص الذين كانوا يترددون على المخبأ، وبعد المراقبة والتحريات تم التأكد من أنه أحد أوكار مواقع الـ Dark web ، الذى تتم فيه أنشطة غير قانونية، فتم اقتحام المكان بقوة أمنية مكونة من ٦٠٠ شرطى، وكان المبنى المشار إليه على مساحة ٥٠٠٠ متر مربع ومغلق بأبواب مصفحة، ويمتد بعمق خمسة أدوار تحت الأرض، ويقع على أرض مساحتها ٣,٢ فدان مؤمنة بسياج شائك وكاميرات مراقبة، وقد صرح يوهانس كونز "رئيس الشرطة الإقليمية" بأن: "المهمة لم تكن مجرد اقتحام للأسوار الحديدية، وإنما من اللازم كذلك اختراق الحماية الرقمية لمركز البيانات Data center الموجود بالمخبأ"، كما أضاف كونز إلى ذلك أن عملية اختراق الـ servers للوصول للبيانات الموجودة بداخلها كانت صعبة جدًا لكنهم نجحوا فيها بعد ساعات من الاقتحام، وقد قامت الشرطة الألمانية بمصادرة أكثر من ٢٠٠ سيرفر servers مع ملفات مهمة فيها معلومات عن أماكن وجهات حكومية وخاصة حول العالم ومبالغ مالية كبيرة، كما تمكنت الشرطة الألمانية من القبض على ١٣ شخص تتراوح أعمارهم ما بين ٢٠ و٥٩ سنة منهم من كان موجودًا وقت المداهمة، ومن منهم من ثبت تورطه فى هذه الأنشطة غير المشروعة.

- تفكيك شبكة لاستغلال الأطفال عبر الدارك ويب: أسفرت جهود الإنتربول عن تفكيك شبكة دولية لاستغلال الأطفال جنسيًا بتاريخ ٢٠١٩/٥/٢٣م، كانت تتواصل عبر شبكة الدارك ويب، فى عملية أسفرت عن توقيف ٩ أشخاص فى ثلاث دول، وكان الإنتربول قد أطلق هذه العملية فى ٢٠١٧ إثر اكتشاف مواد تظهر استغلالًا جنسيًا لأطفال على موقع عبر شبكة الدارك ويب، يضم نحو ٦٣ ألف عضو، وقد سمحت هذه العملية بإنقاذ ٥٠ طفلًا، حيث حلل محققون من عدة دول إثر طلب "الإنتربول"

المواد المنشورة، وتمكنوا من تحديد عناوين إلكترونية (أى بي) فى تايلاند وأستراليا والولايات المتحدة، بينما عطلت هيئة مكافحة الجرائم الإلكترونية فى بلغاريا الموقع الذى كان ينشر مواد جديدة بصورة أسبوعية على مدى سنوات عدة، ومن بين المشتبه بهم التسعة الذين أوقفوا، تم التعرف على المشغل الرئيسى للموقع، وهو رجل مقيم فى تايلاند اتهم بارتكاب انتهاكات جنسية فى حق الأطفال الأحد عشر، ومن بينهم أحد أقاربه، وكذلك أوقف أحد المشغلين الآخرين لهذا الموقع فى أستراليا وعثر بحوزته على آلاف الوثائق التى تظهر انتهاكات جنسية بحق أطفال تم تصويرهم فى تايلاند وأستراليا، وأوضحت هذه الصور أنه المسئول الرئيسى عن الانتهاكات فى حق أطفال لم يتعد عمر أحدهم ١٥ شهرًا، فيما حكم على أحد الرجلين بالسجن ١٤٦ عامًا والثانى ٤٠ عامًا فى بلديهما.

سادساً: الجهود الوطنية:

تتجه الآن العديد من دول العالم للتصدى إلى المواقع الموجودة على الشبكة السوداء ومحاولة الكشف عن مستخدميها، حيث قامت بعض الدول بتطوير برامج خبيثة، تتم من خلالها مهاجمة أجهزة الحاسب الآلى لعدد كبير من الأفراد للتوصل إلى مستخدمى برنامج TORوالكشف عن هويتهم، وهو الأسلوب نفسه الذى اتبعته أيرلندا فى ٢٠١٣ للقبض على إريك أوين ماركيز Eric Marques Eoin، الذى كان يدير شبكة سوداء كبيرة تدعى hosting Freedom.

كما أعلنت روسيا عن جائزة تقدر بنحو أربعة ملايين روبل لمن يستطيع اختراق مواقع الشبكة السوداء، ولكن وكما أظهرت حالة SilkRoad، ليس من السهل محاربة هذا النوع من الشبكات، والتصدى لانتشار استخدامها، والحد من الأنشطة الإجرامية التى تمارس من خلالها.

وعلى الرغم من هذه الجهود لمجابهة صور الإجرام عبر الشبكة المظلمة، فإن هناك بعض الأصوات التى تؤيد استخدام الشبكات المظلمة وبرنامج TOR والبرامج المثيلة له، نظرًا لاستخدامهم كأدوات للتعبير عن الرأى وحماية خصوصية المواطنين فى مواجهة الرقابة الحكومية، علاوة على التوقعات المستقبلية لاستخدام الشبكات السوداء والمواقع والتطبيقات المنبثقة عنها فى إحداث تغييرات جذرية فى النظام العالمى وفواعله، وبصفة خاصة العملات الافتراضية، والتى يتصاعد استخدامها فى المجتمعات الافتراضية، حيث من المتوقع أن يواجه النظام الاقتصادي العالمى إشكالية تآكل الثقة فى التعاملات المالية، مما قد يتسبب فى أزمات اقتصادية على المستوى العالمى، فى مقابل تزايد نفوذ أصحاب ومديري هذه الشبكات الافتراضية، وتراكم ثرواتهم بطريقة غير مشروعة، كما أن هذه الشبكات من الممكن أن تحتكر خدمات الاتصالات فى الفضاء الإلكترونى بشكل يؤثر مستقبلًا على سيادة الدول، ويفقدها السيطرة على التفاعلات عبر المجال الافتراضى(٨٧).

الخاتمة

استعرض الباحث خلال السطور السابقة موضوع المواجهة الجنائية للأنشطة الإجرامية المنظمة على شبكة الإنترنت المظلمة، مع الإشارة إلى نصوص التشريع المصرى لمواجهة هذه الصور، وقد تناول البحث التعريف بشبكة الإنترنت المظلمة، وخصائصها ومخاطر استخدامها، وصور الإجرام المنظم المنتشرة بها؛ كعمليات الاتجار بكل من المخدرات والأسلحة النارية والبشر وغسل الأموال وتمويل الإرهاب، واستغلال التنظيمات الإجرامية المنظمة لهذه الشبكة المظلمة فى تحقيق أرباح طائلة، ثم تناول البحث جهود منظمة الإنتربول فى مواجهة هذه الجرائم وبعض الجهود الوطنية على الصعيد الدولى، وقد انتهى البحث إلى مجموعة من النتائج والتوصيات على النحو التالى:

أولاً: **النتائج**:

١- انتقال جزء من أنشطة الجماعات الإجرامية المنظمة إلى الواقع الافتراضى، مستغلين الشبكة المظلمة كسوق سوداء وبيئة خصبة لمباشرة أنشطتهم الإجرامية، وتشير التقديرات إلى تحقيق هذه الجماعات المنظمة لأرباح ضخمة من هذه الأنشطة غير المشروعة، معتمدين فى ذلك على العملات الافتراضية المشفرة.

٢- استغلال المجرمين المعلوماتيين ما تتسم به الشبكة المظلمة من سرية واستخدام تقنيات التشفير المعقدة التى تصعب عملية متابعتهم وتعقبهم، لمباشرة أنشطتهم الإجرامية، بعيدًا عن نظر سلطات العدالة الجنائية، بما يشكل عائقًا فى ملاحقة هذه العناصر الإجرامية، وصعوبة إثبات الجرائم المرتكبة.

٣- تبذل الدول والمنظمات الدولية ذات الصلة بمكافحة أنشطة الإجرام المنظم جهودها المضنية لمواجهة الأنشطة الإجرامية المنظمة التى ترتكب على الشبكة المظلمة، على الرغم من صعوبة تتبع هذه الأنشطة الإجرامية بسبب استخدام تقنيات التشفير.

ثانياً: **التوصيات**:

١- ضرورة تضافر الجهود الدولية وتعزيز التعاون الدولى الأمنى والقضائى، لتحقيق المواجهة الفعالة لمواجهة أنشطة الإجرام المنظم عبر الشبكة المظلمة.

٢- النظر نحو استحداث وحدات أمنية متخصصة لمكافحة جرائم الشبكة المظلمة والعملات المشفرة، وتعزيز دور منظمة الإنتربول فى التنسيق بين هذه الوحدات، لتحقيق المواجهة الفعالة فى مكافحتها.

٣- العمل على دعم أجهزة إنفاذ القانون بالمساعدات التقنية والتدريب المتقدم اللازم لإجراء أعمال التحرى المتعلقة بالشبكة الخفية وكيفية ضبط الجرائم المرتكبة عبر الشبكة المظلمة.

٤- مواصلة العمل على تطوير الحلول التقنية المساعدة لرصد وكشف الجرائم المرتكبة على الشبكة المظلمة كأدوات التنقيب على المعلومات والزواحف الشبكية لفهرسة البيانات على الشبكة المظلمة والأدوات التحليلية لتعقب مسارات العملات الافتراضية المشفرة، وبرمجيات سلاسل الكتل للتحفظ على الأدلة الرقمية.

المراجع

١- راجع: ذوقان عبيدات وآخرون: مناهج وأساليب البحث العلمى، دار صنعاء للنشر، عمان، الأردن،١٩٩٦م، ص٢٢٠.

٢- نوران شفيق، تهديدات الشبكة السوداء للأمن الافتراضي للدول، مرجع سابق، ص٥٢.

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

٤- نوران شفيق، تهديدات الشبكة السوداء للأمن الافتراضى للدول، مرجع سابق، ص٥٣.

٥- ظهر برنامج تور لأول مرة فى سبتمبر ٢٠٠٢، والذى من خلاله يمكن تشفير مكان وعنوان بروتوكول الإنترنت للمستخدمين الذين يقومون بتحميل البرنامج، فهذا البرنامج يعمل على إرسال إشاراتٍ رقميةٍ مشفرة عبر شبكةٍ من التحويلات المنتشرة فى كل أنحاء العالم، فى محاولةٍ لإخفاء محتوى هذه الإشارات، وهوية مرسلها والمكان الذى أرسلت منه.

٦- انظر: الموقع الإلكترونى لمركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء المصرى على الرابط، تاريخ الاطلاع، ٢٠٢١/٢/٩م:

https://www.idsc.gov.eg/IDSC/Infomedia/List.aspx?id=1

٧- ومن أخطر هذه البرمجيات التى تتواجد بكثرة: Vawtrack، وهى برمجياتٌ تم تصميمها بهدف الوصول للمعلومات المالية لمستخدم الحاسوب المخترق، وSkynet، ويستخدم لسرقة عملات البيتكوين الإلكترونية والاشتراك فى هجمات (DDoS) على مواقعَ أخرى باستخدام جهاز الكمبيوتر المخترق، وNionspy ويمكن لهذه البرمجية الخبيثة تسجيل النقرات على لوحة المفاتيح، بالإضافة إلى سرقة المستندات من أقراص تخزين الحاسوب المصاب، وتسجيل الصوت والفيديو عبر أجهزة الإدخال الموجودة ضمن الحاسوب المُخترق.

٨- تتسم الجريمة المنظمة ببعض السمات المُميزة عن غيرها من الجرائم التقليدية، من أبرزها:

أ- الطابع الهيكلى المُتدرج: حيث تقوم جماعات الجريمة المنظمة على أساس التدرج الرئاسى للسلطة والمسئولية، والعمل يسير وفق نظام المستويات والتسلسل الرئاسى والالتزام به، حيث إن الهيكل التنظيمى للجماعة محكم، ويتميز بالثبات والاستمرارية، ويشترك أعضاء الجماعة فى ارتكاب

الجرائم بناء على توزيع الأدوار والمهام وأسلوب ارتكاب الجرائم وتوقيتها وفقًا لما تحدده قيادات الجماعة الإجرامية.

ب- استخدام العنف وإفساد الموظفين العموميين: حيث يعد استخدام العنف أو التهديد به أحد مظاهر التنظيم الإجرامى، وأحد الأساليب الهامة لضمان عدم قيام السلطات الرسمية باتخاذ إجراءاتها الضبطية، كما أن الضحايا أو أعضاء التنظيم لن يقوموا بالإبلاغ عن الجرائم ومرتكبيها، وأن المنافسين الجدد لن يتخطوا إلى داخل مناطق تخصصهم أو نفوذهم، وعلى صعيد آخر، تعمل عصابات الجريمة المنظمة على إفساد الموظفين العموميين وتجنيدهم بكافة السبل ومنها تقديم الرشاوى لهم بهدف تسهيل وإزالة كافة العقبات التى تواجه عملياتهم الإجرامية.

ج- استهدافها للربح: حيث يعد تحقيق الأرباح هو الهدف من عمليات وأنشطة عصابات الجريمة المنظمة، وهو يعد كذلك إحدى السمات الرئيسية لأنشطتها، حيث تهدف تلك الأنشطة للحصول على المال بأى وسيلة وهذه الخاصية هى التى تميزها عن المنظمات الإرهابية، والنشاط الأساسى للجريمة المنظمة يكون على مستوى عال من الكفاءة والفاعلية حتى يجلب أرباحًا خيالية، مع أقل قدر من الخطورة والتضحيات، وهو مؤسس بالدرجة الأولى على استغلال نقاط الضعف فى النفس البشرية كالمخدرات والقمار والدعارة والإفساد، وتمثل الجريمة المنظمة نشاطًا اقتصاديًا غير مشروع يحقق أرباحًا خيالية، لأنها تقوم بالإمداد بسلع وخدمات تشبع رغبات بعض الناس بالرغم من مخالفتها للقيم السائدة فى المجتمع مثل الجنس والمخدرات والقمار، وهى تسعى إلى إحكام السيطرة الكلية أو الجزئية على تلك الأنشطة التى تمارسها ولا تسمح لغيرها بأية منافسة.

د- الاستمرارية: ويقصد بهذه الخاصية امتداد حياة المنظمة حتى مع انتهاء حياة أو عضوية أى فرد فيها، فقد يخرج من عضوية الجماعة قيادات أو أعضاء لأسباب مختلفة، بينما تستمر المنظمة فى نشاطها عاملة من أجل تحقيق أهدافها غير المشروعة.

هـ- السرية: حيث يخضع جميع أعضاء التنظيم الإجرامى إلى نظام سرى يحكم كل ما يتصل بعضوية الأفراد المنتمين للجماعة وتأمينهم، ونشاطهم والقواعد الحاكمة والمنظمة لعملها، وطريقة وأسلوب العمل، والخروج على هذه القواعد يرتب عواقب وخيمة وعقوبات متنوعة كالطرد من الجماعة أو القتل إذا لزم الأمر.

ز- الطابع عبر الوطنى: فكثيرًا ما تكون الأنشطة الإجرامية الخاصة بالإجرام المنظم عابرة للحدود، لذا فإنه من الصعب على الجهات الأمنية لإحدى الدول التى اقترفت فيها القيام بإجراءات التحرى والتحقيق فى تلك الجرائم لأن المعلومات المتوفرة قد تكون قاصرة ما لم تكملها معلومات من الدول الأخرى التى وقعت بها أجزاء من النشاط أو نتيجة من نتائجه. انظر: د.عبد الرحمن خلف، كيفية إعداد رجل الشرطة لمواجهة الجريمة المنظمة، مجلة مركز بحوث الشرطة، العدد (٣٦)، يوليو ٢٠٠٩، أكاديمية الشرطة، القاهرة، ص ص١٣٠، ١٣١؛ د. محمد إبراهيم زيد، الجوانب العلمية والقانونية للجريمة المنظمة، مجلة الفكر الشرطى، شرطة الشارقة، الإمارات، أبريل ١٩٩٨، ص ص١٤٤-١٤٧؛ د. شريف سيد كامل، الجريمة المنظمة فى القانون المقارن، دار النهضة العربية، ط٢، ٢٠٠٨، ص ص٨٥-١٢٢؛ د. طارق سرور، الجماعة الإجرامية المنظمة، دار النهضة العربية، ٢٠٠٠، ص٦٤؛ د. عبد الرحمن خلف وآخرون، التعاون الدولى لمواجهة الجريمة المنظمة عبر الوطنية، دراسة مركز بحوث الشرطة، أكاديمية الشرطة، القاهرة، الإصدار (٨)، يناير ٢٠٠٦، ص ص٦٥ -٧٣؛ د. حسنين توفيق إبراهيم، الأمن فى عالم متغير، مجلة الفكر الشرطى، المجلد السادس، العدد الثالث، ديسمبر ١٩٩٧، ص٣٥٧؛ د. محمد عبد المعبود مرسى، احتراف الجريمة، المجلة العربية للدراسات الأمنية والتدريب، العدد (١٩)، محرم ١٤١٦هـ، ص١٤١ وما بعدها.

9- BAE Systems Detica and London Metropolitan University, 2012. Organised Crime in the Digital Age.

10- Moore, T., Clayton, R., Anderson, R., 2009. The economics of online crime. Journal of Economic perspectives, 32(3):3-4.

11- BAE Systems Detica and London Metropolitan University, 2012. Organised Crime in the Digital Age.

12- Norton Cybercrime Report. 2011. Available at:
http://us.norton.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USAHuman%20Impact-A4_Aug4-2.pdf

13- Lu, C.C., Jen, W.Y., Chang, W. and Chou, S., 2006. Cybercrime & Cybercriminals. Journal of Computers, 1(6):11-18.

14- See http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom

15- Fortinet 2013 Cybercrime Report; Panda Security, 2010. The Cybercrime Black Market: Uncovered; and Group IB, 2011. State and Trends of the Russian Digital Crime Market.

16- Moore, T., Clayton, R., Anderson, R., 2009. The economics of online crime. Journal of Economic perspectives, 32 (3): 3-4.

١٧- انظر: دراسة شاملة عن الجريمة السيبرانية، إصدارات مكتب الأمم المتحدة المعنى بالمخدرات والجريمة، الأمم المتحدة، نيويورك، ٢٠١٣، ص٦٩.

18- BAE Systems Detica and London Metropolitan University, 2012. Organised Crime in the Digital Age, op. cit.

١٩- فعلى سبيل المثال، جهاز خادم مع برمجة خبيثة مخزنة عليه يشغل مجموعات أو مكونات شبكة روبوت يكلف فى أى مكان مبلغًا قدره ما بين ٨٠ إلى ٢٠٠ دولارًا أمريكيًا فى الشهر، ومجموعة إدارة روبوت واحد، تعرف باسم مجموعة Eleonore Exploit Pack، تساوى فى قيمة التجزئة مبلغ ألف دولار، أما استئجار شبكة روبوت ما بين ١٠ إلى ٢٠ جهاز حاسب آلى تدار باستخدام هذه المجموعة، فتبلغ تكلفته فى المتوسط ٤٠ دولارًا فى اليوم، أما عدة "زيوس" V1,3 فتبلغ تكلفتها من ثلاثة إلى أربعة آلاف دولار، وتعد هذه التكاليف منخفضة نسبيًا بالمقارنة مع المكاسب المالية المحتملة التى قد تصل من عشرات الآلاف إلى عشرات الملايين من الدولارات. انظر: دراسة شاملة عن الجريمة السيبرانية، إصدارات مكتب الأمم المتحدة المعنى بالمخدرات والجريمة، الأمم المتحدة، نيويورك، ٢٠١٣، ص٦٩، وكذا انظر:

ESET Latin America's Lab, 2010. ESET, Trends for 2011: Botnets and Dynamic Malware. Available at: http://go.eset.com/us/resources/white-papers/Trends-for-2011.pdf

تجدر الإشارة إلى أن البرمجية الخبيثة "زيوس" يرجع ظهورها إلى استخدام أحد مهندسى البرامج فى أوروبا الشرقية هذه البرمجية التى بمجرد أن يفتح المجنى عليه رسالة بريد إلكترونى، يتم اختراق حاسبه، والوصول إلى أرقام حسابات البنك الخاصة به، وإن كانت الرسالة تبدو غير ضارة. انظر: دراسة مكتب الأمم المتحدة المعنى بالمخدرات والجريمة عن الجريمة السيبرانية، مرجع سابق، ص٧٠.

20- 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.

21- Spapens, T., 2010. Macro Networks, Collectives, and Business Processes: An Integrated Approach to Organized Crime. European Journal of Crime, Criminal Law and Criminal Justice, 18:285-215.

22- BAE Systems Detica and London Metropolitan University, 2012. Organised Crime in the Digital Age, op. cit.

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

24- 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.

٢٥- انظر: التقرير المنشور حول فعاليات حلقة العمل بعنوان: "الاتجاهات الراهنة للجريمة، والتطورات الأخيرة والحلول المستجدة، لا سيما التكنولوجيات الجديدة بوصفها وسائل لارتكاب الجريمة وأدوات لمكافحته"، مرجع سابق، ص٦.

٢٦- يرجع ظهور العملات الرقمية المشفرة إلى عام ١٩٧٧ فى الولايات المتحدة الأمريكية، حيث اخترع الثلاثى (ليونارد أدليمان وآدى شامير ورونالد ريفست) فى معهد ماساتشوستس للتقنية، خوارزمية RSA، والتى شكلت النواة الأولى لتشفير هذه العملات وتأمين معاملاتها، وبعدها بسنوات فى عام ١٩٩٣ اخترع عالم الرياضيات ديفيد تشوم e-cash، ما يقال بأنها أول عملة رقمية، بعدها عمل على جمع الأموال لتمويل فكرته ونجح فى إنشاء شركة Digi-Cash التى تدير هذه العملة الرقمية المركزية، بينما فى عام ٢٠٠٨ أعلن ساتوشي ناكاموتو عن إتاحة عملة "البتكوين" للجمهور كأول عملة رقمية مشفرة، ومنذ ذلك الحين أثارت البتكوين أنظار البنوك والمؤسسات المالية وأخذت فى الانتشار فى عدد من الدول، ودخلت فى قطاعات كثيرة، منها: الطب والعقود الذكية والتجارة والتدريس وغيرها، وفى عام ٢٠٠٩، تمكن ساتوشى من تعدين ٥٠ وحدة منها، وبعدها بأيام تمت أول صفقة للعملة بين ناكاموتو وهال فينى، ليصل سعر البتكوين عام ٢٠١١ إلى ١ دولار، وقد أخذت قيمة البتكوين فى الارتفاع مقابل العملات الرئيسية الأخرى مثل: الدولار واليورو.

٢٧- أشارت بعض الدراسات إلى توقع بعض التداعيات الاقتصادية السلبية لانتشار استخدام العملات المشفرة، من أبرزها: المساهمة فى زيادة معدلات التضخم العالمي، وإضعاف فاعلية أدوات السياسة النقدية والتأثير على قدرة البنك المركزى فى اتخاذ السياسات المالية الملائمة، والتأثير على حجم الإيرادات الضريبية، وزيادة فرص التهرب الضريبى والجمركى وتعميق ظاهرة الاقتصاد الخفى، والتأثير على استقرار نظم المدفوعات وأسعار الصرف والأسواق المالية. د. خالد محمد نور الطباخ، تداول

العملات الافتراضية فى تمويل الإرهاب وغسل الأموال، القاهرة، دار النهضة العربية، ط١، ٢٠٢٠، ص٧٧ وما بعدها.

28- European Central Bank (1998), " Report on electronicmoney", Frankfurt, Germany, August, p. 7.

٢٩- عبد الله بن سليمان بن عبد العزيز، بحث بعنوان النقود الافتراضية (مفهومها وأنواعها وآثارها الاقتصادية) المجلة العربية للاقتصاد والعلوم الإدارية، العدد (١) يناير ٢٠١٧م، ص٢١.

٣٠- د. أحمد الضبع، إشكالية مواجهة الإرهاب بين النظرية والتطبيق، مرجع سابق، ص١٠٧، هامش رقم ١.

٣١- د. خالد محمد نور الطباخ، تداول العملات الافتراضية، مرجع سابق، ص٦٠.

٣٢- د. أشرف توفيق شمس الدين، مخاطر العملات الافتراضية فى نظر السياسة الجنائية، وثائق المؤتمر الدولى الخامس عشر لكلية الشريعة والدراسات الإسلامية بجامعة الشارقة، تحت عنوان: "العملات الافتراضية فى الميزان"، يومى ١٦و٢٠١٩/٤/١٧، ص٦٧٢-٦٨٠.

٣٣- لم يكن المجرمون بمعزل عن استخدام العملات المشفرة فى ارتكاب أنشطتهم الإجرامية، حيث تم ضبط أحد السماسرة فى سبتمبر ٢٠١٩، لقيامه بممارسة نشاط الوساطة فى هذه العملات من خلال تحويل أرصدة إلكترونية مُعرفة بالدولار الأمريكى إلى نقد بالجنيه المصرى بسعر صرف مخالف للأسعار المتداولة فى السوق المصرفى، بالمخالفة لقانون البنك المركزى المصرى رقم ٨٨ لسنة ٢٠٠٣ وتعديلاته، وفى قضية أخرى فى مايو ٢٠١٧ سبق ضبط أحد الأشخاص لقيامه بالنصب على المواطنين مستخدمًا أحد مواقع التسويق الشبكى، وتعامله بالبيع والشراء لعملة "وان كوين" المشفرة وتحويل قيمتها إلى رصيد نقدى لعملائه، مستخدمًا فى هذا النشاط اسم أحد البنوك العاملة بالبلاد، بإدعاء أن جميع تلك المعاملات تتم تحت إشراف البنك المشار إليه.

٣٤- د. أشرف توفيق شمس الدين، المرجع السابق، ص٦٥٥؛ توفيق محمد صلاح الدين الشربجى، العلاقة بين العملات الافتراضية وجرائم غسل الأموال وتمويل الإرهاب، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، ٢٠١٩، ص١٩ وما بعدها. ومن الفقه المقارن، انظر:

J. (Everette) and others: Risks and vulnerabilities of virtual currency, cryptocurrency as a payment method, Public-Privat Analytic Exchange Program 2017, p.18.

٣٥- محمد على محمود كرباس، جرائم غسل الأموال فى ضوء الفقه والقضاء- دراسة مقارنة، رسالة ماجستير، جامعة أم درمان الإسلامية، السودان، ٢٠١٨، ص٥٢.

٣٦- د. أحمد الضبع، إشكالية مواجهة الإرهاب بين النظرية والتطبيق، موسوعة الثقافة القانونية، الهيئة المصرية العامة للكتاب، ٢٠١٩، ط١، ص١٠٧، هامش رقم ١ وص١١٦، ومن الفقه المقارن، انظر:

Goldman, Z. K., Maruyama, E., Rosenberg, E., Saravalle, E., & Solomon-Strauss, J., Terrorist use of virtual currencies, Containing the Potential Threat, Washington DC: Center for a New American Security, May, 3.(2017), p. 27.

٣٧- انظر: د. أشرف توفيق شمس الدين، المرجع السابق، ص ص٦٥٣-٦٨٨؛ د. خالد محمد نور الطباخ، تداول العملات الافتراضية، مرجع سابق، ص٤٩ وما بعدها.

٣٨- د. محمد عبد اللطيف فرج، أطر التعاون الدولى لمواجهة غسل أموال المخدرات، مجلة كلية الدراسات العليا، عدد (١١)، يوليو ٢٠٠٤، أكاديمية الشرطة، القاهرة، ص٥٢٠.

٣٩- انظر: دليل استخدام شبكة الإنترنت فى أغراض إرهابية، وثائق مكتب الأمم المتحدة المعنى بالمخدرات والجريمة، نيويورك،٢٠١٣، ص٧.

٤٠- د. أحمد فتحى سرور، الوسيط فى قانون العقوبات- القسم الخاص، ج١، القاهرة، دار النهضة العربية، ٢٠١٩، ص١٦١.

٤١- المرجع السابق، ص ص١٦٢، ١٦٣.

٤٢- المرجع السابق، ص١٦٢.

٤٣- المرجع السابق، ص١٦٤.

٤٤- الموضع السابق.

٤٥- المرجع السابق، ص١٦٥.

٤٦- انظر: تقرير المخدرات العالمى ٢٠١٩، لمحة عامة عن الطلب على المخدرات وعرضها على الصعيد العالمى، منشورات الأمم المتحدة، الكتيب الثانى، ص٤.

47-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.

48- 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; 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.

49- 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.

50- Nathaniel Popper, "Opioid dealers embrace the dark web to send deadly drugs by mail", New York Times, 10 June 2017.

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

٥٢- نوران شفيق، تهديدات الشبكة السوداء للأمن الافتراضى للدول، مرجع سابق، ص٥٥.

٥٣- شملت المادة (٣٣) من قانون مكافحة المُخدرات المعاقبة على أفعال جلب وتصدير المواد المخدرة، وإنتاج وتصنيع الجواهر المخدرة، وزراعة النباتات المخدرة، بالإضافة إلى تأليف أو إدارة عصابة للاتجار بالمُخدرات. انظر: د. فوزية عبد الستار، شرح قانون مكافحة المُخدرات، القاهرة، دار النهضة العربية، ١٩٩٦، ص٤١ وما بعدها؛ ولذات المؤلفة: المواجهة التشريعية لظاهرة انتشار المُخدرات فى المجتمع المصرى، الندوة العلمية التى نظمها مركز بحوث ودراسات مكافحة الجريمة ومعاملة المجرمين بكلية الحقوق، جامعة القاهرة، فبراير ١٩٩٣، ص٩٤ وما بعدها.

٥٤- انظر: المذكرة الإيضاحية لمشروع تعديل القانون رقم (١٨٢) لسنة١٩٦٠ فى شأن مكافحة المُخدرات وتنظيم استعمالها والاتجار فيها.

٥٥- د. فوزية عبد الستار، شرح قانون مكافحة المُخدرات، مرجع سابق، ص٤٢، ٤٣.

٥٦- على الرغم من أن جرائم الاعتداء على الأطفال واستغلالهم جنسيا موجودة من قبل ظهور الإنترنت، فإن البعد الإلكترونى لهذه الجرائم قد مكَّن الجناة من التفاعل فيما بينهم والحصول على مواد الاستغلال الجنسى 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 مرتكبى الجرائم ذات الصلة، وأصبح التقدم فى التكنولوجيا محوريًّا فى الاستغلال الجنسي التجارى للأطفال، ويمكن للسياح الذين يمارسون الجنس مع الأطفال الاستفادة من تطبيقات الحوسبة الحسابية لتخزين الصور أو مقاطع الفيديو، ومن ثمَّ تجنب المخاطرة بالنقل الفعلى لمواد تصور اعتداءات جنسية على الأطفال، وعلاوة

على ذلك، تربط تكنولوجيا الهاتف المحمول بين منظِّمى عمليات استغلال الأطفال والاعتداء عليهم جنسيًّا والضحايا والمستهلكين، ومن ثم، تقل حاجة المنتجين والموزعين إلى الحضور شخصيًّا أثناء المعاملات، مما يؤدى بدوره إلى تحسين فرصهم فى تحاشي كشف أمرهم.

57- 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.

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

٥٩- جدير بالذكر أن استخدام التكنولوجيا فى جهود مكافحة الاتِّجار أمر يتطلب التعاون على نطاق قطاعات مختلفة، وقد أقامت دوائر صناعة تكنولوجيات المعلومات والاتصالات والمنظمات الدولية شراكة لاستكشاف كيفية تسخير التكنولوجيات لأغراض منع الاتِّجار بالأشخاص والمساعدة على إعادة تأهيل الضحايا، ويقدم ائتلاف التكنولوجيا ضد الاتجار Tech Against Trafficking، الذى يضم شركات تكنولوجيا بارزة ومؤسسات أكاديمية والمنظمة الدولية للهجرة، قائمة بحلول تكنولوجية لمكافحة الاتِّجار بالبشر، والعمل على بناء قدرات جميع الجهات الفاعلة المعنية مقوم محورى للتغلب على تحديات استخدام التكنولوجيا فى الاتِّجار بالأشخاص، ومن ثم يجب إجراء دراسات دقيقة من أجل تطوير التكنولوجيا التى يستخدمها الممارسون من أجل مكافحة الاتِّجار بالأشخاص وتعهد هذه التكنولوجيا ورصدها وتقييمها، على أن يُراعى فى تطوير تلك الأدوات، التى يمكن أن يستعين بها الأشخاص المعرضون لخطر الاتجار بهم فى حماية أنفسهم، التحسب للاختلافات القائمة بينهم واستيعاب تلك الاختلافات، انظر:

Felicity Gerry, Julia Muraszkiewicz and Niovi 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; Business for Social Responsibility, "List of technology tools and initiatives identified by tech against trafficking", 15 January 2019; Inter-Agency Coordination Group against Trafficking in Persons, "Human trafficking and technology", p.4; 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.

60- Europol, Internet Organised Crime Threat Assessment (IOCTA) 2018, p. 35.

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

62- Victoria Brains, “Online child sexual exploitation: towards an optimal international response”, SSRN, Electronic Journal, 29 August 2018.

٦٣- انظر: مقال بعنوان: "اختفى ٥٢ يومًا..الإنترنت المظلم ينقذ طفلًا مخطوفًا فى مخبأ"، منشور على موقع جريدة أخبار اليوم، بتاريخ ٢٠٢٠/١١/٢٥، على الرابط https://akhbarelyom.com/news/newdetails/3174288/1، تاريخ الاطلاع ٢٠٢١/١/٣.

64- Europol and INTERPOL, “Migrant smuggling networks: executive summary” (May 2016), p. 8.

65- 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.

66- 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.

67- trafficking in persons and smuggling of migrants – Technology in smuggling of migrants, www.unodc.org/e4j/

68- European Commission, “The use of social media in the fight against migrant smuggling”, European Migration Network (EMN) Inform (September 2016).

69- 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.

70- RAND Europe, “International arms trade on the dark web” (2019), Findings section, para. 8.

71- 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).

72- 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.

73- Damien Rhumorbarbe and others, “Characterising the online weapons trafficking on cryptomarkets”, Forensic Science International, vol. 283, December 2018, pp. 16–20.

74- RAND Europe, “International arms trade on the dark web” (2019), Findings section, para.4.

75- 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.

٧٦- د. محمد الجمال، القوانين الجنائية المكملة لقانون العقوبات، مطبعة كلية الشرطة، ٢٠٠٨، ص ص٤٤-٦٥.

٧٧- نوران شفيق، تهديدات الشبكة السوداء للأمن الافتراضى للدول، مرجع سابق، ص٥٤.

78-International Criminal Police Organization (INTERPOL) “Innovation report: anonymous networks and darknet” (September 2018), pp. 12–13.

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

80- 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); INTERPOL, "Innovation report", p.14.

٨١- تم إنشاء المنظمة الدولية للشرطة الجنائية International Criminal Police Organization والتى تعرف اختصارًا بمنظمة الإنتربول (INTERPOL) عام١٩٢٣، وتضم المنظمة حاليًا (١٩٤) دولة، منها مصر، ويقع مقر الأمانة العامة للإنتربول فى مدينة ليون بفرنسا، وتستهدف المنظمة الدولية للشرطة الجنائية منع الجريمة عبر تسهيل التعاون الدولي بين أجهزة الشرطة فى الدول الأعضاء من خلال تمكين أجهزة الشرطة فى دول العالم من تبادل المعلومات عن الجرائم ومرتكبيها، وتقديم الدعم الفنى والميدانى للدول الأعضاء لمواجهة التحديات الإجرامية المتنامية التى يشهدها القرن الحادي والعشرون.

٨٢- انظر موقع المنظمة الدولية للشرطة الجنائية على شبكة الإنترنت على الرابط: https://www.interpol.int/ar/٢/٤/٥، تاريخ الإطلاع ٥/١٢/٢٠٢٠م.

٨٣- انظر: موقع الشرطة الأوروبية "اليوروبول" على الرابط، تاريخ الاطلاع، ١٢/١/٢٠٢١م:
https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down

٨٤- انظر: موقع الشرطة الأوروبية "اليوروبول" على الرابط، تاريخ الاطلاع، ٣/٥/٢٠٢١م:
https://www.europol.europa.eu/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuse-platform-some-half-million-users?fbclid=IwAR1TM767B9R-4A-lvR_RQUV38HbggsTH2q1PZ6WLyvLMJKVz5Gg0Xb3Hjwg

٨٥- انظر: موقع الشرطة الأوروبية "اليوروبول" على الرابط، تاريخ الاطلاع، ٧/٤/٢٠٢١م:
https://www.europol.europa.eu/newsroom/news/dark-web-hitman-identified-through-crypto-analysis

٨٦- انظر: موقع الإذاعة الألمانية "DW" على الرابط، تاريخ الاطلاع، ١٢/٣/٢٠٢١م:
https://www.dw.com/en/darknet-cybercrime-servers-hosted-in-former-nato-bunker-in-germany/a-50618469?fbclid=IwAR3WTYRhw5r5Nl-OeHNS4Gp-q8cXA7gKqoX3fZvvRNJB1f4ebW5A8DtEEdI

٨٧- نوران شفيق، تهديدات الشبكة السوداء للأمن الافتراضى للدول، مرجع سابق، ص٥٥.

Combating Organized Crime via Dark Web
Analytical Study of Egyptian Legislation

Ramy Metwally El-Kady

Criminal and terrorist organizations seek to benefit from the advantages of using the dark web, especially its confidential nature and the difficulty of tracking its users, to achieve their direct criminal activities without any oversight or legal accountability. There are sites on this network sell forged and stolen documents, credit card data and personal accounts, in the way that this network has become a black market for all illegal activities. It is a hotbed for criminals, hackers, hired killers, counterfeiters and human traffickers activities, etc. The persent research aims to shed light on illegal criminal activities across the dark web, and to discuss ways to combat them in light of the relevant technical and legal challenges. The role of national legislation in limiting these activities; the role of the international police in tracking them; and the best way to deal with them are also discussed.