ISSN: 2519 – 6138 (Print)
E-ISSN: 2663 – 8983(On Line)

TUJR
مجلة جامعة تكريت للحقوق
Tikrit University Journal for Rights

IRAQI Academic Scientific Journals
العراقية المجلات الاكاديمية العلمية

Tikrit University Journal for Rights
Journal Homepage : http://tujr.tu.edu.iq/index.php/t

كلية الحقوق
College of Rights

Addressing the illicit trade on the dark internet within the scope of public international law

Dr. Basheer Sabhan Ahmed
College of Rights, Tikrit University, Salahaddin, Iraq
Dr.bashersabhan@tu.edu.iq

Article info.

Article history:
- Received 25 Oct 2022
- Accepted 4 Jan 2023
- Available online 1 Mar 2023

Keywords:
- Dark internet.
- Illegal trade.
- International law.

Abstract: The international community needs to unite its efforts more to confront the dangers of the dark internet, which is a part of the internet that is not indexed by search engines, and therefore it is difficult to identify and track who uses it, which poses a great risk when used in illegal trade, and because it is a platform for everything that threatens the main foundations of the international community. In terms of security, peace and combating transnational crime, and despite the national efforts that have been made as well as international efforts, there remains the necessity for the United Nations to lead real efforts to unite countries in order to conclude an international agreement to address illegal trade on the dark internet, as it has previously addressed everything that threatens unity The international community and its security, Countries also need, at the national level, to renew judicial systems to facilitate the granting of licenses to search and track criminals. Law enforcement authorities also need to continuously develop their cadres to keep pace with every development that occurs in the world of technology.

© 2023 TUJR, College of Right, Tikrit University

التصدي للتجارة غير المشروعة على الانترنت المظلم في نطاق القانون الدولي العام

أ.م.د. بشير سبهان أحمد
كلية الحقوق، جامعة تكريت، صلاح الدين، العراق
Dr.bashersabhan@tu.edu.iq

معلومات البحث :

تواريخ البحث:
- الاستلام : ٢٥ / تشرين الاول / ٢٠٢٢
- القبول : ٤ / كانون الاول / ٢٠٢٣
- النشر المباشر : ١/ آذار /٢٠٢٣

الكلمات المفتاحية :
- الانترنيت المظلم.
- التجارة غير المشروعة.
- القانون الدولي.

الخلاصة: يحتاج المجتمع الدولي إلى توحيد جهوده اكثر لمواجهة مخاطر الانترنت المظلم وهو جزء من الإنترنت لا تتم فهرسته بواسطة محركات البحث، وبالتالي فانه يصعب تحديد وتعقب من يستخدمه، مما يشكل خطورة كبيرة عند استخدامه في التجارة غير المشروعة، ولأنه منصة لكل ما يهدد الأسس الرئيسية للمجتمع الدولي من امن وسلام ومكافحة الجريمة عبر الوطنية، وبالرغم من الجهود الوطنية التي بذلت وكذلك الجهود الدولية، تبقى هناك ضرورة بان تقود الأمم المتحدة جهود حقيقية لتوحيد الدول من اجل ابرام اتفاقية دولية للتصدي للتجارة غير المشروعة على الانترنت المظلم، كما تصدت من قبل لكل ما يهدد وحدة المجتمع الدولي وامنه، كما تحتاج الدول على المستوى الوطني إلى تجديد الأنظمة القضائية لتسهل منح رخص التفتيش والتعقب للمجرمين كما تحتاج سلطات انفاذ القانون إلى تطوير كوادرها بشكل مستمر لتساير كل تطور يحدث في عالم التكنلوجيا.

© ٢٠٢٣, كلية الحقوق، جامعة تكريت

المقدمة :

التطور امر حتمي في عالم التكنلوجيا وهناك دوما من يفتخر بان عالم اليوم يقاد من قبل الخبراء في عالم التقنية والمعلوماتية من مهندسين وخبراء وكل هذا مرتبط بما حققه العالم من ثورة تقنية من خلال ابتكار الانترنت وربط العالم افتراضيا إذ اصبح كقرية صغيرة، وهذا العالم الافتراضي اصبح ندا للعالم الحقيقي بما يحمله من مفاهيم تقليدية وقوانين وأنظمة، دائما كان هناك تساؤل حول مدى خضوع هذا العالم الافتراضي إلى نفس القوانين والمبادئ الحاكمة للعالم الحقيقي، ولعل هذا التطور لم يقف عند حد اكتشاف الانترنت وتوسيع نطاق انتشاره بل اصبح هناك تصنيف للأنترنت فاصبح لدينا الإنترنت المفتوح، الذي يمكن الوصول إليه مجانًا والبحث فيه، والذي يستخدم المستخدمون عادةً محركات البحث للعثور على مواقع الويب المفهرسة والمحتوى الذي يرغبون في زيارته واستهلاكه، اما النوع الثاني هو الانترنت العميق والذي يحتوي على جميع الأجزاء غير القابلة للبحث من الإنترنت إذ يقتصر ظهور محتوى الانترنت العميق والوصول إليه على المستخدمين الذين لديهم أذونات خاصة، والنوع الثالث هو الانترنت المظلم وهو الجزء غير المفهرس وغير القابل للبحث من الويب العميق الذي يتطلب حزم برامج

محددة للتنقل ولعل الهدف الرئيسي من الويب المظلم مع إخفاء هوية المستخدم والنشاط عبر الإنترنت وهنا تكمن خطورة هذا النوع من الانترنت إذ بدء عدد كبير من المجرمين وباعة المخدرات و الارهابيين باستخدام هذا النوع من الانترنت لتحقيق غاياتهم مما شكل إشكالية كبير لعدد من الدول إذ ان الغالبية العظمى من التجارة غير المشروعة التي تتم على هذا النوع من الانترنت تشمل أماكن ورقع جغرافية واسعة تمتد إلى عدد كبير من الدول وفي قارات مختلفة مما يشكل إشكالية كبير لأجهزة انفاذا القانون في الدول التي يتضرر مواطنوها او تتضرر مصالحها من تلك التجارة غير المشروعة وهنا تبرز إشكالية هذا البحث إذ تتصارع المفاهيم التقليدية حول سيادة الدول وعدم جواز انتهاك الحدود وعدم استخدام القوة الا لغرض الدفاع عن النفس والمطبقة في العالم الواقع، مع المفاهيم الجديدة المتعلقة بالأنترنت المظلم وصعوبة تعقب وتتبع مستخدميه وكأنه مضمار جديد لم تجربة المبادئ التقليدية للقانون الدولي العام.

سوف نتناول موضوع بحثنا (التصدي للتجارة غير المشروعة على الانترنت المظلم في نطاق القانون الدولي العام) من خلال الهيكلية التالية:

المبحث الأول: ماهية الانترنت المظلم.

المطلب الأول: التعريف بالأنترنت المظلم.

المطلب الثاني: أسواق التجارة غير المشروعة على الانترنت المظلم وطرق التصدي لها.

المبحث الثاني: الجهود الوطنية والدولية للتصدي للتجارة غير الشرعية على الانترنت المظلم.

المطلب الأول: الجهود الوطنية للتصدي للتجارة غير الشرعية على الانترنت المظلم.

المطلب الثاني: الجهود الدولية للتصدي للتجارة غير الشرعية على الانترنت المظلم.

المبحث الأول

ماهية الانترنت المظلم

عالم الانترنت المظلم عالم لا يخضع لأي مراقبة وذلك لصعوبة الوصول إلى من يديرون المواقع عليه من قبل السلطات المختصة وبذلك يصبح من المستحيل تعقبهم ومحاسبتهم، عليه الانترنت المظلم عبارة عن سوق سوداء لكل ما هو غير مشروع ويعاقب علية القانون، فعلى مواقعه يمكن ان يجد أي شخص أيا كان عمرة وجنسه معلومات تتعلق عن كيفية صناعة المتفجرات والأسلحة كما انه يعتبر اسهل وسيله للحصول على الأسلحة وشرائها بدون أوراق ثبوتية، كما ينتشر على صفحات الانترنت المظلم أسماء القتلة الماجورين (أسماء مزيفة) لعقد صفقات من اجل تصفية الأشخاص مقابل مبالغ مالية، كما تباع على صفحاته بطاقات ائتمانية مسروقة وبرامج فيروسات خطيرة لاختراق اقوى أنظمة الحماية، كما

يمكن الحصول على أوراق ثبوتية رسمية مثل جوازات سفر وبأسماء جديدة وهي كلها مزورة ولا يمكن في الغالب التعرف عليها في المطارات والدوائر الرسمية، عليه يتبين مدى خطورة هذا النوع من الانترنت ومدى ضرورة إيجاد القيود القانونية الملاءمة للتصدي لما يدار عليه من تجارة غير مشروعة، في هذا المبحث سوف نتناول التعريف بالأنترنت المظلم وأسواق التجارة غير المشروعة على الانترنت المظلم وطرق التصدي لها وذلك في مطلبين، افردنا المطلب الأول منها لتعريف الانترنيت المظلم، بينما خصصنا المطلب الثاني للبحث في أسواق التجارة غير المشروعة على الانترنت المظلم وطرق التصدي لها.

المطلب الأول / التعريف بالأنترنت المظلم

أصل شبكة الويب المظلمة ليس شريرًا مثل أعماله الحالية، فقد تم إطلاقه من قبل مختبر الأبحاث البحرية الأمريكية في عام ٢٠٠٣ واستخدمته الوكالة لإنفاذ القانون والخدمات السرية ولمساعدة المعارضين السياسيين الذين يقاتلون من أجل حقوقهم في البلدان ذات الأنظمة القمعية، ولكن مع مرور الوقت، تم تجاوز الجانب الشرعي من الويب المظلم من قبل الأشخاص ذوي النوايا الخبيثة الذين استخدموا الموقع بشكل مجهول، فقد اصبحوا يقدمون خدمات الجريمة المنظمة، اليوم، تدعم شبكة الويب المظلمة المنعزلة وغير المكتشفة وغير المنظمة بشكل خفي شبكات الجريمة المنظمة التي تستفيد من حقيقة أن هذه المواقع لا يمكن مراقبتها بحذر من قبل السلطات، تعتبر التجارة غير المشروعة جزءًا من الأنشطة الإجرامية المختلفة التي يتم تقديمها في شبكة الإنترنت المظلمة، إذ تتوفر السلع المقلدة مثل الحقائب المصممة والعطور الفاخرة والأدوية الحقيقية المنقذة للحياة بسهولة، لكن شبكة الويب المظلمة تسهل أيضًا الجرائم البشعة مثل الاختطاف والقرصنة وحتى القتل[1]، ويعرف الويب المظلم بانه (جزء من الإنترنت لا تتم فهرسته بواسطة محركات البحث)، لا شك أن اغلب الناس قد سمعوا حديثًا عن "الشبكة المظلمة" باعتبارها بؤرة للنشاط الإجرامي وهي كذلك، فقد قام الباحثان دانيال مور وتوماس ريد من كينجز كوليدج في لندن بتصنيف محتويات ٢٧٢٣ موقع ويب مظلمة حية على مدى خمسة أسابيع في عام ٢٠١٥ ووجدوا أن ٥٧٪ يستضيفون مواد غير مشروعة، وأظهرت دراسة أجريت عام ٢٠١٩، بعنوان Into the Web of Profit ، أجراها الدكتور مايكل ماكجوير في جامعة ساري، أن الأمور أصبحت أسوأ، فقد ارتفع عدد قوائم الويب المظلمة التي يمكن أن تضر بالمؤسسات بنسبة ٢٠٪ منذ عام ٢٠١٦

---

(1)- Hernan Albamonte: Illicit Trade in the Dark Web, https://medium.com/@hernan.albamonte/illicit-trade-in-the-dark-web-a734ee605340 (17/8/2020).

ومن بين جميع القوائم (باستثناء تلك التي تبيع المخدرات)، يمكن أن تضر ٦٠٪ بالمؤسسات يمكنك شراء أرقام بطاقات الائتمان وجميع أنواع المخدرات والأسلحة والأموال المزيفة وبيانات اعتماد الاشتراك المسروقة وحسابات Netflix المخترقة والبرامج التي تساعدك على اقتحام أجهزة كمبيوتر الأشخاص الآخرين، قم بشراء بيانات اعتماد تسجيل الدخول إلى حساب بنك أوف أمريكا بقيمة ٥٠٠٠٠ دولار أمريكي مقابل ٥٠٠ دولار أمريكي، احصل على ٣٠٠٠ دولار من الأوراق النقدية المزيفة بقيمة ٢٠ دولارًا مقابل ٦٠٠ دولار، اشترِ سبع بطاقات خصم مسبقة الدفع، كل منها برصيد ٢٥٠٠ دولار، مقابل ٥٠٠ دولار (يشمل الشحن السريع) يصل حساب Netflix المميز "مدى الحياة" إلى ٦ دولارات، يمكنك استئجار متسللين لمهاجمة أجهزة الكمبيوتر نيابة عنك، يمكنك شراء أسماء المستخدمين وكلمات المرور ولكن ليس كل شيء غير قانوني، فالويب المظلم أيضًا له جانب شرعي على سبيل المثال، يمكنك الانضمام إلى نادي شطرنج أو BlackBook، وهي شبكة اجتماعية توصف باسم " Facebook of Tor"، كما ان التجارة على الويب المظلم ازدهرت بفضل عملة Bitcoin، إذ تجري جميع مواقع التجارة الإلكترونية المظلمة تقريبًا معاملات بعملة البيتكوين أو بعض الأشكال المختلفة لها، ولكن هذا لا يعني أنه من الآمن ممارسة الأعمال هناك، إذ يجب عدم الكشف عن هويته المتأصلة في مكان المحتالين واللصوص، لكن ماذا تتوقع عندما يكون هدفك هو شراء أسلحة أو مخدرات؟ تتمتع مواقع التجارة الإلكترونية المظلمة بنفس الميزات مثل أي عملية بيع بالتجزئة الالكترونية، بما في ذلك التقييمات / المراجعات وعربات التسوق والمنتديات، ولكن هناك اختلافات مهمة، واحدها هو مراقبة الجودة عندما يكون كل من المشترين والبائعين مجهولين، إذ يقدم معظم مزودي التجارة الإلكترونية نوعًا من خدمة الضمان التي تحافظ على أموال العملاء معلقة حتى يتم تسليم المنتج ومع ذلك، في حالة حدوث نزاع لا تتوقع الخدمة بابتسامة يعود الأمر إلى المشتري والبائع للتخلص منه، يتم تشفير كل اتصال، لذلك حتى أبسط المعاملات تتطلب مفتاح PGP حتى إتمام المعاملة لا يضمن وصول البضائع يحتاج الكثيرون إلى عبور الحدود الدولية، ويقوم مسؤولو الجمارك بقمع الطرود المشبوهة إذ يعج موقع الويب المظلم Deep.Dot.Web بقصص المشترين الذين تم القبض عليهم أو سجنهم لمحاولة الشراء[١].

يمكن تقسيم الإنترنت من الناحية المفاهيمية إلى ثلاث طبقات: الطبقة الأولى هي الإنترنت المفتوح، الذي يمكن الوصول إليه مجانًا والبحث فيه، والذي نسميه "الويب الواضح"، يستخدم المستخدمون عادةً

(1) - Darren Guccione: What is the dark web? How to access it and what you'll find, https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html (19/8/2020).

محركات البحث (على سبيل المثال Google و Yahoo) للعثور على مواقع الويب المفهرسة والمحتوى الذي يرغبون في زيارته واستهلاكه، يتفاعل المستخدمون عادةً مع الويب الواضح عند تصفح الويب على أجهزة الكمبيوتر أو الأجهزة المحمولة، اما الطبقة الثانية هي "شبكة الويب العميقة"، والتي تحتوي على جميع الأجزاء غير القابلة للبحث من الإنترنت (على سبيل المثال غير المفهرسة بواسطة محركات البحث) والشبكات الداخلية المحلية (مثل شبكات الأعمال والمنزل المحلية) تستضيف الطبقة محتوى الويب الذي يتطلب غالبًا تسجيلات دخول العضوية، مثل الخدمات المصرفية عبر الإنترنت والسجلات الطبية وقواعد بيانات العضوية فقط (مثل قواعد البيانات الأكاديمية) والشبكات الداخلية للشركة، ويقتصر ظهور محتوى الويب العميق والوصول إليه على المستخدمين الذين لديهم أذونات وامتيازات خاصة، والطبقة الثالثة "الويب المظلم" هو الجزء غير المفهرس وغير القابل للبحث من الويب العميق الذي يتطلب حزم برامج محددة للتنقل، إذ تتيح حزم البرامج هذه (مثل Tor و I2P) الوصول إلى الويب المظلم مع إخفاء هوية المستخدم والنشاط عبر الإنترنت من تحليل المراقبة وحركة المرور، والوصول إلى الويب المظلم وتصفحه ليس غير قانوني لأن عدم الشرعية يركز أكثر على استخدامه[١].

ولا ينبغي هنا ان يتم ترك انطباعًا بأن كل شيء على الويب المظلم شائن أو غير قانوني، إذ بدأت شبكة Tor كقناة اتصالات مجهولة الهوية، ولا تزال تخدم غرضًا قيمًا في مساعدة الأشخاص على التواصل في بيئات معادية لحرية التعبير، إذا كنا نريد معرفة كل شيء عن حماية الخصوصية أو العملات المشفرة، فإن الويب المظلم لديه الكثير ليقدمه، فهناك مجموعة متنوعة من خدمات البريد الإلكتروني الخاصة والمشفرة، وإرشادات لتثبيت نظام تشغيل مجهول، وهناك أيضًا مواد لن تفاجأ بالعثور عليها على شبكة الإنترنت العامة، مثل روابط لإصدارات النصوص الكاملة للكتب التي يصعب العثور عليها، هناك العديد من مواقع المبلغين عن المخالفات، بما في ذلك نسخة الويب المظلمة من ويكيليكس Pirate Bay، موقع BitTorrent الذي أغلقه مسؤولو إنفاذ القانون مرارًا وتكرارًا، لا يزال على قيد الحياة وبصحة جيدة هناك، حتى Facebook لديه وجود مظلم على شبكة الإنترنت، هناك أيضًا الكثير من القيمة العملية لبعض المنظمات، إذ تراقب وكالات إنفاذ القانون على شبكة الإنترنت المظلمة بحثًا عن البيانات المسروقة من الانتهاكات الأمنية الأخيرة التي قد تؤدي إلى تعقب الجناة، تراقب العديد من المؤسسات الإعلامية الرئيسية مواقع المبلغين عن المخالفات بحثًا عن الأخبار[٢]، من كل ما تقدم يتبين ان الانترنت المظلم له

---

(1) - Giacomo Persi Paoli: The Trade in Small Arms and Light Weapons on the Dark Web, UNODA Occasional Papers, No. 32, October 2018, p.7-8.

(2)- Darren Guccione, op.cit.

جانبان، سلبي باعتباره اكبر منصة للتجارة غير المشروعة وايجابي إذ يوفر مساحة من الحرية لعدد من الناشطين إذ يتم مصادرة حرياتهم بشكل كبير كما انها توفر مصدرا للانتهاكات لبعض المنظمات ووكالات انفاذ القانون، الا ان الباحث يرى ان الجانب السلبي يطغى هنا فالمخاطر التي تتحقق من استخدامه اكبر مما يشكل مشكلة لأجهزة انفاذ القانون والدول ذاتها إذ يصعب تعقب مرتكبي الجريمة او الحواسيب التي تستضيف تلك المناطق مما يسبب اتساع نطاق الجرائم على بقع جغرافية واسعة يمكن ان تشمل دول عدة.

المطلب الثاني / أسواق التجارة غير المشروعة على الانترنت المظلم وطرق التصدي لها

قبل الحديث عن اهم الطرق المتبعة للتصدي للتجارة غير المشروعة على الانترنت المظلم سوف نتناول تحديد أهم الأسواق المستخدمة على اهم المواقع على الانترنت المظلم إذ يتم تمكين التداول غير القانوني على شبكة الإنترنت المظلمة من خلالها وذلك في الفرعين التاليين.

الفرع الأول / أنواع أسواق التجارة غير المشروعة على الانترنت المظلم

بشكل عام تنقسم أسواق التجارة غير المشروعة على الانترنت المظلم إلى نوعين رئيسيين هما:

اولاً/ أسواق العملات المشفرة:

يعود الاهتمام الأكبر بالعملات المشفرة إلى سببين، بادئ ذي بدء، يعود هذا إلى فكرة الحرية والاستقلال عن الأطراف الثالثة، مثل الدولة أو المؤسسات المالية، ثانياً، من وجهة نظر مكاسب الاستثمار المحتملة، القانونية وغير القانونية، من السمات الرئيسية للعملات المشفرة أنها تعمل كعملة افتراضية، يقوم حامل مثل هذه العملة المشفرة بتخزينها على جهاز الكمبيوتر الخاص به أو في تطبيق الهاتف الذكي فيما يسمى بالمحفظة التي لا يستطيع الوصول إليها إلا هو، إذا رغب في إجراء معاملة، فإنها تتم إلكترونيًا، مباشرة بينه وبين المقاول، لكل وحدة من وحدات العملات المشفرة رمز فريد يحتوي على معلومات تمنع نسخها أو إعادة إنفاقها، إن مفتاح مفهوم العملات المشفرة هو أيضًا حقيقة أنه لا يوجد منظم متداول، لذلك، لا يوجد، على سبيل المثال، البنك المركزي للعملات المشفرة، الذي قد يقرر، على سبيل المثال، زيادة المعروض من العملة المشفرة وبالتالي تقليل قيمتها، يقرر المنشئ للعملة مقدار ما يتم تداوله من عملة مشفرة في مرحلة إنشاء النظام، قيمته في أيدي السوق الحرة، يتم التداول في العملات المشفرة إلكترونيًا، دون مشاركة أي نظام مصرفي مباشرةً بين مستخدمي العملة المشفرة، أي في تقنية الند للند، هذا يعني أن المعاملة لا تخضع للإشراف بأي شكل من الأشكال، لذلك، لا يوجد كيان يقوم بإبلاغ السلطات الضريبية إذا أردنا بيع عدد كبير من العملات المشفرة، كما يحدث في حالة

المعاملات المصرفية بمبلغ يتجاوز ما يعادل ١٥٠٠٠ يورو، لا أحد يستطيع أيضًا حظر حساب ما بالنظر إلى ما سبق، اتضح أن مهمة العملة المشفرة تتلخص حقًا في كلمة واحدة، وهي "الحرية"[١]، وتداول العملات المشفرة هو عملية المضاربة على تحركات أسعار العملات المشفرة عبر حساب تداول العقود مقابل الفروقات، أو شراء وبيع العملات الأساسية عبر البورصة، وتداول العقود مقابل الفروقات عبارة عن مشتقات تمكنك من المضاربة على تحركات أسعار العملات المشفرة دون امتلاك العملات الأساسية، يمكنك الشراء إذا كنت تعتقد أن قيمة العملة المشفرة سترتفع، أو الشراء القصير ("البيع")، كلاهما من المنتجات ذات الرافعة المالية، مما يعني أنك تحتاج فقط إلى إيداع وديعة صغيرة – المعروفة باسم الهامش – للحصول على تعرض كامل للسوق الأساسي، لا يزال يتم احتساب ربحك أو خسارتك وفقًا للحجم الكامل لصفقتك، لذا ستزيد الرافعة المالية من الأرباح والخسائر، كما ان شراء شخص ما وبيعه العملات المشفرة عبر البورصة فأنه يشتري ويبيع العملات نفسها، ستحتاج إلى إنشاء حساب صرف، وطرح القيمة الكاملة للأصل لفتح مركز، وتخزين الرموز المميزة للعملات المشفرة في محفظتك الخاصة حتى تكون جاهزًا للبيع[٢]، وتبدو أسواق العملات المشفرة مشابهة للأسواق القانونية عبر الإنترنت مثل eBay أو Amazon إذ يجب على العملاء عادةً إعداد حسابات لعرض السوق والوصول إلى الصفحة الرئيسية بمجرد تسجيل الدخول، تحتوي الأسواق على مجموعة من الفئات المحددة مسبقًا والتي يمكن للبائعين، المعروفين باسم "البائعين"، تصنيف قوائمهم للسماح للعملاء بتحديد نوع المنتج أو الخدمة التي يبحثون عنها[٣].

ثانياً/ أسواق البائعين الفرديين:

متاجر البائعين، بشكل عام، واجهة مرئية أبسط بكثير، كما هو الحال مع العديد من المتاجر القانونية عبر الإنترنت التي أنشأها الأفراد أو الشركات لبيع منتجاتهم وخدماتهم، نظرًا لأن متاجر البائعين تستضيف بائعين فرديين متخصصين في منتجات معينة، فإن هذه الأسواق بها قوائم أقل مقارنة بأسواق العملات المشفرة بينما يتم تصنيف بعض قوائم محلات البائعين وبالمثل، كما هو الحال في أسواق

---

(1)- Ireneusz Miciuła: The Condition of the Cryptocurrency Market and Exchanges in Poland, 2019, p.97, https://www.researchgate.net/publication/335559967_The_Condition_of_the_Cryptocurrency_Market_and_Exchanges_in_Poland (20/8/2020).

(2)- What is cryptocurrency trading and how does it work? : https://www.ig.com/en/cryptocurrency-trading/what-is-cryptocurrency-trading-how-does-it-work (20/8/2020).

3 - Giacomo Persi Paoli, op.cit, p.9-11.

العملات الرقمية، فإن متاجر البائعين الأخرى تسرد جميعها منتجاتهم على صفحاتهم الرئيسية، محلات البائعين محدودة الوظائف مقارنة بأسواق العملات المشفرة، المناسبة لأسواقهم هيكل الأعمال في البيع مباشرة للعملاء، ولكن الروابط سوف عادة ما تكون متاحة للعملاء للتسجيل وتسجيل الدخول، من أجل معلومات الاتصال بالبائع وأحيانًا للأسئلة الشائعة[١]، وأسواق البائعين هذه تجمع معاً بائعين متعدّدين، والذين تم تسميتهم باللغة الإنجليزية بمصطلح " vendors " بإدارة مديري السوق مقابل عمولة على المبيعات مؤدية إلى مقارنات مع أسواق شرعية مشابهة على الإنترنت الواضح على غرار سوقي إي باي (eBay) وأمازون (Amazon) وتقدم الأسواق المشفرة خدمات أطراف ثالثة توفر درجة من حماية الدفع للزبائن وهو ما يسمى بالضمان (إذ لا يتم الإفراج عن المبالغ للبائعين إلا بعد أن يكون الزبائن قد استلموا مشترايتهم ورضوا عنها) والفصل في نزاعات الأطراف الثالثة وتستخدم الأسواق المشفرة العملات المشفرة للدفع وتتيح للزبائن تقديم التغذيات الراجعة المرتبطة بمشترياتهم، مع تجميع النقاط وعرضها من قِبل السوق لتوجيه الزبائن في اختيار البائعين الموثوقين والمنتجات ذات التصنيف العالي وتميل الأسواق المُشفّرة إلى التخصّص في المقام الأول بالمخدرات غير الشرعية، ولكنّها تقدّم أيضاً قوائم مرتبطة بنشاطات غشّ اخرى، بما فيها بطاقات الائتمان المسروقة ومعلومات الهوية، وتُعتبر أنواع أخرى من المنتجات، والأسلحة النارية أحد الأمثلة عنها، متوفرة للبيع بشكلٍ أقل شيوعاً[٢].

الفرع الثاني / طرق التصدي لأسواق التجارة غير المشروعة على الانترنت المظلم

هناك سؤال مهم يجب الإجابة عليه، قبل الخوض في مسألة الجهود الوطني والدولية في التصدي للتجارة غير المشروعة على الانترنت المظلم، وهو، كيف يمكن لإنفاذ القانون معالجة النشاط الإجرامي المتزايد على شبكة الويب المظلمة؟ حدد بحث سابق أجرته مؤسسة RAND أربع استراتيجيات رئيسية تدخل يمكن استخدامها من أجل معالجة التجارة غير المشروعة من خلال الإنترنت المظلم، في حين أنه تم تحليل هذه الاستراتيجيات فيما يتعلق بتجارة المخدرات، يمكن تكييف مبادئها العامة والتحديات ذات الصلة بها ونقلها إلى سياق الاتجار غير المشروعة بشكل عام، وهذه الاستراتيجيات هي:

١- تقنيات التحقيق التقليدية: تقنيات مُستَخدَمة من أجل استهداف مراحل سلسلة الإمداد إذ يلتقي العالمان على الإنترنت غير الحقيقي "الافتراضي" والحقيقي "غير الافتراضي" (مثال شحن وتسليم المنتجات) تشمل الأمثلة المراقبة واستخدام المُخبِرين والبضائع المشحونة المُراقبَة، الا ان ابرز

([1])- Giacomo Persi Paoli, op.cit, p.11.

([٢])- جياكومو بيرسي باولي واخرون: خلف الستار التجارة غير المشروعة بالأسلحة النارية والمتفجرات والذخيرة على الانترنت المظلم، مؤسسة Rand، كالفورنيا، ٢٠١٧، ص١٠-١١.

العوائق التي تواجه هذه الاستراتيجية هي التكاليف العالية والمنافع المحدودة بشكل محتمل بالنظر إلى تنوع المشترين المحتملين وعددهم المرتفع.

٢- الكشف والاعتراض البريديان: وهي أساليب لتتبع وتعقب الطرود ورصد التقدم ومسح الطرود المشتبه بها، وأبرز العوائق التي تواجهها هي العبء على النظام البريدي والجمركي نظرا للعدد الكبير للطرود اليومية التي يجب التعامل معها.

٣- الكشف والرصد على الانترنت: الجمع بين مصادر البيانات وأدوات وتقنيات مختلفة باستخدام تحليلات البيانات الضخمة والتعلّم الآلي للربط بين مختلف مصادر البيانات والكشف في نهاية المطاف عن هوية الجهات الفاعلة الخاصة بالأسواق المُشفّرة؛ رصد مستمر لأسواق الإنترنت المُظلم؛ رصد وتتبّع صفقات البتكوين (Bitcoin) خلال تحليل سلسلة الكُتل، ولعل من أبرز المعوقات في هذا الشأن هو التشفير لأنه حتى لو تم القبض على خادم يستضيف سوقا مشفرة يبقى تحديد المستخدمين او المواقع صعبا.

٤- التعطيل على الانترنت: من خلال التسلل إلى السوق المشفرة من اجل اجراء عمليات تقوض الثقة بشأن عدم الكشف عن الهوية والموثوقية، ولعل من أبرز المعوقات لهذه الطريقة هي هجرة البائعين والمشترين إلى أسواق مشفرة أخرى، او من خلال انشاء أسواق مشفرة جديدة[١].

من كل ما تقدم يتضح للباحث ان العدد والتنوع في الأسواق على الويب المظلم بدأت بالازدياد والتنوع، كما ان الاليات المقترحة للتصدي للتجارة غير المشروعة على هذه النوع من الانترنت لم تثبت نجاعتها إذا ما بقت على مستوى دولة واحدة او مجموعة محدودة من الدول مما يؤكد الحاجة إلى تعاون دولي أكبر في هذا الشأن.

المبحث الثاني

الجهود الوطنية والدولية للتصدي للتجارة غير الشرعية على الانترنت المظلم

لقد بذلت العديد من الجهود على المستوى الوطني والدولي للتصدي للتجارة غير المشروعة على ما يعرف بأسواق الانترنت المظلم وهذه الجهود تتفاوت في قوتها ومدى تحقيقها لغاياتها وهو ما سنتناوله في المطلبين التاليين.

---

[١])- جياكومو بيرسي باولي واخرون، مصدر سابق، ص٧١-٧٢.

المطلب الأول / الجهود الوطنية للتصدي للتجارة غير الشرعية على الانترنت المظلم

إحدى الممارسات التي استخدمتها وكالات إنفاذ القانون حول العالم (على المستوى الوطني)، بشكل شائع هي التحقيق السري على الويب، وقد تضمنت مثل هذه التحقيقات استخدام وكيل إنفاذ "غرف الدردشة الخاصة بالتحقيق" أو " شبكات نظير إلى نظير" الأخرى من أجل "الظهور كمجرمين"، أو مشاركين في أنشطة غير مشروعة، وقد أسفرت طريقة الإنفاذ هذه عن نتائج مهمة، على سبيل المثال، نجح مكتب التحقيقات الفيدرالي في إلقاء القبض على روس أولبريخت، مبتكر سوق "طريق الحرير" على الانترنت المظلم في عام ٢٠١٣، وقد وصف مكتب التحقيقات الفيدرالي طريق الحرير بأنه "السوق الإجرامي الأكثر تطورًا واتساعًا على الإنترنت اليوم" وبحسب ما ورد، تم الكشف عن تورط أولبريخت في طريق الحرير من قبل عميل سري حدد موقع سلسلة من المنشورات على شبكة الويب المظلمة والمنتديات، وبعد مراقبة الحسابات المشتبه في ارتباطها بطريق الحرير، وجد الوكيل منشورًا قدم فيه أولبريخت حساب Gmail الخاص به، والذي تمكن من خلاله مكتب التحقيقات الفيدرالي من تحديد مكانه، بينما شهدت العمليات السرية نجاحًا تاريخيًا، إلا أنها بدأت تفقد شعبيتها نظرًا لوجود الكثير من التواجد السري للشرطة على الإنترنت مما يتسبب في زيادة الشك لدى مجرمي الإنترنت، في حين أن التحقيقات السرية هي أداة مفيدة للغاية لإنفاذ القانون على شبكة الويب المظلمة، فإن الوعي بين المجرمين فيما يتعلق بهذه التحقيقات يمنع هذه التحقيقات من أن تصبح حلاً دائمًا للمشكلة، طريقة أخرى لفرض القانون على شبكة الويب المظلمة هي استخدام "مصائد الجذب"، وهذه المصائد عبارة عن مواقع ويب "يُزعم أنها" مرتبطة بنشاط غير مشروع "ولكنها في الواقع أنشأتها الشرطة وهي مصممة لالتقاط عنوان IP" لمستخدمي الويب، وقد استخدم مكتب التحقيقات الفيدرالي هذا التكتيك عندما أنشأت الوكالة موقعًا يسمى "Playpen" لجذب مجرمي الإنترنت، ونتج عن ذلك رد فعل عنيف إذ أن الموقع "تضمن روابط لأكثر من ٢٣٠٠٠ صورة ومقاطع فيديو جنسية صريحة للأطفال ... بما في ذلك أكثر من ٩٠٠٠ ملف يمكن للمستخدمين تنزيلها مباشرة من مكتب التحقيقات الفيدرالي" ردًا على استخدام مكتب التحقيقات الفيدرالي لهذه الملفات، صرحت وزارة العدل أن "الأطفال الذين يظهرون في مثل هذه الصور يتعرضون للأذى في كل مرة يتم مشاهدتهم فيها، وبمجرد أن تغادر تلك الصور سيطرة الحكومة، لا يملك العملاء أي وسيلة لمنع نسخها وإعادة نسخها إلى أجزاء أخرى من الإنترنت"، تمسك مكتب التحقيقات الفيدرالي باستخدامه للملفات، إذ ادعى أحد المسؤولين أنه "لا توجد طريقة أخرى يمكننا من خلالها تحديد أكبر عدد ممكن من اللاعبين" على شبكة الويب المظلمة بصرف النظر عن المعضلات الأخلاقية التي

يطرحها تطبيق القانون المشاركة في نشاط غير قانوني "للقبض" على مجرمي الإنترنت، هناك مخاوف أخرى بخصوص طريقة الإنفاذ لهذا الشاغل الأساسي هو أن الكثيرين "يرون مصائد الشراك كشكل من أشكال الإيقاع وانتهاك الحريات المدنية"، في حين أن مفهوم ردع المجرمين عن العمل على الويب بسبب احتمال وجود مصائد مخترقة هو أمر جذاب، فهناك العديد من التعقيدات الأخلاقية التي تصاحب استخدام مثل هذه التكتيكات، علاوة على ذلك، لا يوجد قدر كبير من البيانات التي تشير إلى أن مصائد مواضع الجذب هي الطريقة الأكثر فعالية لمراقبة النشاط غير القانوني على الويب المظلم يشير هذا إلى جانب المخاوف الأخلاقية المحيطة بالمصائد إلا أنه قد تكون هناك حلول أكثر ملاءمة متاحة في غضون السنوات الأخيرة، بدأ تطبيق القانون في جميع أنحاء العالم في الاعتماد على استخدام القرصنة لملاحقة المجرمين المجهولين على الإنترنت، أدى ظهور شبكة الويب المظلمة إلى توفير الحماية لمجرمي الإنترنت من إذ أنه "يحجب البصمات الرقمية التي تُترك لأطراف ثالثة، مما يجعل أساليب المراقبة الحالية عفا عليها الزمن"، كما انه هناك "تقنيات القرصنة" التي تنشر برامج المراقبة عبر الإنترنت للوصول المباشر إلى أجهزة المجرمين والتحكم فيها وتمارس هذه البرامج الضارة سيطرة مطلقة على أجهزة الكمبيوتر الأجنبية ويمكنها حتى إجبار الكمبيوتر المستهدف على تحميل الملفات سرًا إلى خادم يتحكم فيه تطبيق القانون أو قيادة أجهزة الكمبيوتر التي ترتبط بالهدف عن طريق، على سبيل المثال، الوصول إلى موقع ويب يستضيفه، في حين أن أسلوب تعقب مجرمي الويب المظلم يتميز بإمكانات هائلة، إلا أن هناك مجموعة من المخاوف المتعلقة باستخدامها، إذ تسمح القاعدة الفيدرالية للإجراءات الجنائية للقاضي بإصدار أوامر تفتيش لموقع الجهاز إذا "تم إخفاء الموقع من خلال الوسائل التكنولوجية" والمشكلة المحتملة في هذا هو أنه يمكن أن يؤدي إلى "أكبر توسع في الإنفاذ خارج الحدود الإقليمية للاختصاص القضائي في سجل مكتب التحقيقات الفيدرالي باعتبار انه يقع حوالي ٨٠٪ من أجهزة الكمبيوتر على الويب المظلم خارج الولايات المتحدة، ونظرًا لطبيعة متصفحات الويب المظلم وهذا يعني أن أي هدف معين لإنفاذ القانون من المرجح أن يكون موجودًا في الخارج، ويستمر تطوير هذا الحل الموجه نحو التكنولوجيا لمشكلة الجريمة في شبكة الويب المظلمة[١].

وبالرغم من أن ممثلي وكالات إنفاذ القانون دائما ما يشيرون إلى عدد من العمليات الناجحة التي تشمل المجموعة الكاملة لاستراتيجيات مثل عملية أونيموس (Operation Onymous)، الا انهم سلطوا

---

(1) - Clayton Davis: Addressing the Challenges of Enforcing the Law on the Dark Web, THE UNIVERSITY OF UTAH, December 11, 2017, https://law.utah.edu/addressing-the-challenges-of-enforcing-the-law-on-the-dark-web/#_ftnref19 (21/8/2020).

الضوء أيضا على أنه من أجل تحقيق جهود مستدامة ونتائج تدوم طويلا، يعتبر التزام سياسي قوي، بما فيه اعتراف واضح بالتهديد، خطوة ضرورية فعلى سبيل المثال، التزمت المملكة المتحدة بمراجعة أمن الدفاع الاستراتيجي للعام ٢٠١٦ التابعة الاستراتيجية الأمن الوطني لمعالجة الاستخدام الإجرامي للإنترنت المظلم من خلال تأسيس "وحدة استخباراتية للإنترنت المظلم" (Dark Web intelligence Unit) جديدة، والهدف من تأسيس الوحدة هو تمكين تحيل مصدر بيانات متعددة، والتنسيق مع وكالات متعددة والعمل مع القضايا على مقياس واسع، إن هذا النوع من الالتزام ضروري لحشد الموارد اللازمة والتأكد من أن وكالات إنفاذ القانون تحصل على "الغطاء الكامل" لإجراء عملياتها[١]، من كل ما تقدم يتضح للباحث ان الأنظمة الأمنية الوطنية تسعى باستمرار إلى تطوير اساليبها وامكانياتها للتصدي لمكائد المجرمين على الانترنت المظلم، وهذا بالتأكيد يحتاج إلى موازنات مالية مستقلة وكبيرة في نفس الوقت، كما انها تحتاج إلى دعم من السلطة القضائية من إذ سرعة منح رخص التفتيش للمواقع المحتملة لتواجد المجرمين.

المطلب الثاني / الجهود الدولية للتصدي للتجارة غير الشرعية على الانترنت المظلم

بالرغم من أهمية توحيد الجهود الدولية للتصدي للأنترنت المظلم، الا ان الجانب المتجاوز للحدود الإقليمية لعمليات القرصنة لإنفاذ القانون تعرض لانتقادات عامة حادة من قبل مجموعة واسعة من المعلقين والأكاديميين ومنظمات الحريات المدنية وشركات التكنولوجيا، إذ حذرت شركة Google العملاقة للتكنولوجيا من أن استخدام تقنيات التحقيق في الشبكة في ملاحقة أهداف على الويب المظلم من شأنه أن يقوض سيادة الدول من خلال "السماح للحكومة بإجراء عمليات بحث خارج الولايات المتحدة"، وحذرت شركة Google وشركات أخرى من أن تخفيف القيود الإقليمية على سلطة البحث والاستيلاء الحكومية تثير عددًا من المخاوف الدستورية والقانونية والجيوسياسية الضخمة والمعقدة للغاية، بينما أشارت اللجنة الاستشارية لقواعد الإجراءات الجنائية في الولايات المتحدة إلى هذا القلق، مشيرة إلى الفجوة التنظيمية المحتملة فيما يتعلق بعمليات التفتيش عبر الحدود، فقد تركت صراحة مثل هذه "القضايا التي قد يكون لها انعكاسات على السياسة الخارجية" يتم التعامل معها من خلال "التنسيق بين السلطة التنفيذية" ما إذا كان يُسمح بإنفاذ القانون بإطلاق عمليات التسلل الإلكتروني عبر الحدود هو الأحدث في سلسلة من الأسئلة التي تختبر حدود أنشطة التحقيق الأحادية في عالم متصل بالشبكات العالمية، ويكمن جوهر التحقيق في البديهية الراسخة في القانون الدولي والتي تنص على أنه لا يجوز لدولة ما أن تمارس

)[١]– جياكومو بيرسي باولي واخرون، مصدر سابق، ص٧٣.

بشكل منفرد وظائف إنفاذ القانون الخاصة بها في أراضي دولة أخرى، وهو ما لم يتم تناوله بشكل كاف من قبل المحاكم أو البحوث الدراسية في سياق الفضاء الإلكتروني في حين أن هناك ثروة من البحوث الدراسية حول العلاقة بين الإنترنت وسيادة الدولة، إلا أن تركيزها كان بشكل شبه حصري على جواز قوانين دولة ما التي تنظم سلوك الإنترنت الذي يحدث في دولة أخرى (ممارسة "الولاية القضائية الإلزامية")، بدلاً من جواز تنفيذ دولة الامتثال لتلك القوانين في أراضي دولة أخرى (ممارسة "سلطة إنفاذ")، وربما يقدم المحامي الأمريكي جاك جولدسميث التركيز الأكثر استدامة على مسألة سلطة إنفاذ القانون عبر الحدود وهو يجادل بأنه " بينما قد تنظم عدة دول من الناحية النظرية نفس المعاملة عبر الإنترنت، فإن النظام ككل مستقر جزئيًا لأن كل دولة يمكنها فقط فرض اللوائح داخل أراضيها، وهكذا، في حين أن الدول قد تجرم السلوك الذي يحدث بالكامل خارج حدودها، فإن النظام ككل مستقر ان الدول لا تمارس مباشرة وظائف إنفاذ القانون في بلدان أخرى دون الحصول على الموافقة أولاً "[١]، وأحد المنتديات البارزة التي تُناقش فيها هذه القضايا هو فريق الخبراء الحكوميين التابع للأمم المتحدة (UN) الذي يتعامل مع القضايا الإلكترونية في سياق الأمن الدولي، فريق الخبراء الحكوميين هو هيئة أنشأها الأمين العام للأمم المتحدة بتفويض من الجمعية العامة للأمم المتحدة لدراسة، من بين أمور أخرى، كيفية تطبيق القانون الدولي على الأنشطة السيبرانية للدول، بهدف تعزيز التفاهمات المشتركة، ففي عام ٢٠١٣، أقرت الدول الخمس عشرة التابعة لفريق الخبراء الحكوميين بقابلية تطبيق القانون الدولي الحالي على الأنشطة الإلكترونية للدول، ففي العام ٢٠١٦ فقط ، توسع فريق الأمم المتحدة اللاحق بشأن نفس الموضوع ليشمل ٢٠ دولة، مبنيًا على تقرير ٢٠١٣ واتخذ خطوة إضافية من خلال الاعتراف بإمكانية تطبيق الحق المتأصل في الدفاع عن النفس في الفضاء الإلكتروني على النحو المعترف به في المادة ٥١ من ميثاق الأمم المتحدة، إذ أقر تقرير فريق الخبراء الحكوميين لعام ٢٠١٥ أيضًا بقابلية تطبيق المبادئ الأساسية للإنسانية في النزاع المسلح والضرورة والتناسب والتمييز على سير الأعمال العدائية في خلال النزاع في الفضاء الإلكتروني، من خلال البيانات الثنائية والمتعددة الأطراف الأخيرة، بما في ذلك البيانات الصادرة عن قادة مجموعة الدول العشرين (G20) في عام ٢٠١٥، يتبين إجماعًا ناشئًا على أن القانون الدولي الحالي ينطبق على الأنشطة السيبرانية للدول[٢]، وفي سياق مماثل، ركزت البحوث الدراسية التي تستجوب الجوانب الخارجية لمراقبة إنفاذ القانون على الإنترنت على النطاق المتجاوز

(1)- Ahmed Ghappour: Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web, volume 69, Stanford. L. Rev, 2017, p.1082-1083.

(2)- Brian J. Egan: International Law and Stability in Cyberspace, volume 35, issue 1, Berkeley J. Int'l Law, 2017, p.170-171.

للحدود الإقليمية لحقوق التعديل الرابع للدستور الامريكي إنه يفتقر إلى معالجة شاملة للاحتكاكات القضائية بين الدول التي تنتج والآثار التي قد تترتب على مثل هذا السلوك على مفاهيمنا للسيادة والعلاقات الخارجية وإدارة الإنترنت، على الطرف الآخر، أصبح تهديد العمليات السيبرانية الضارة عبر الحدود حاضرًا دائمًا ويثير تساؤلات حول قدرة الدول على حماية مصالحها السيادية في البنية التحتية الإلكترونية الإقليمية، هناك إجماع علمي على أنه من الناحية النظرية، يمكن وصف العملية الإلكترونية عبر الحدود بأنها "فعل غير مشروع دوليًا" (السماح لدولة ما بالرد بإجراءات مضادة بموجب القانون الدولي العرفي)، و "استخدام القوة" المحظور (بخلاف الإذن باستخدام القوة في الدفاع عن النفس)، أو "الهجوم المسلح" (يمنح الدول المتضررة الحق في استخدام القوة المحظورة في الدفاع عن النفس)، اعتمادًا على النطاق وشدة الضرر الناجم عن العملية تستخدم الدول أيضًا قوانينها المحلية الخاصة بجرائم الكمبيوتر لتجريم العمليات الإلكترونية عبر الحدود من قبل كل من الجهات الحكومية وغير الحكومية التي لها آثار في أراضيها، ومن المؤكد أن تقنيات القرصنة الحالية لمكتب التحقيقات الفيدرالي، والتي تم تنفيذها بشكل صحيح، لا ترقى إلى مستوى "الهجوم المسلح" الإلكتروني، والذي من شأنه أن يسمح للدولة بالرد بقوة بموجب المادة ٥١ من ميثاق الأمم المتحدة، حظر العمليات السيبرانية عبر الحدود من منظور القانون الدولي، لكن نطاق الضرر الذي قد تسببه عملية إلكترونية عبر الحدود يختلف، كما هو الحال مع تفسير المعايير الدولية القائمة، وفي الواقع، على وجه التحديد، عندما تنتهك عملية إلكترونية غير رضائية سيادة دولة أخرى، في نهاية المطاف سيتم حلها من خلال الممارسة والرأي القانونيين في الدول، على هذا النحو، فإن الولايات المتحدة ترى ان لديها مصلحة في قيادة الجهود لتوضيح المعايير الدولية الحالية عند تطبيقها على القرصنة الحكومية وتطوير المعايير من خلال الإجراءات الدبلوماسية، وتسلط هذه الظروف الضوء على فشل القواعد الحالية في تنظيم استخدام تقنيات التحقيق في الشبكة، إذ يتمتع مسؤولو إنفاذ القانون بسلطة تقديرية بشأن الجرائم التي تؤدي إلى استخدام تقنيات القرصنة، ومجموعة التقنيات التي يمكن استخدامها بمجرد أن يأذن أمر التفتيش بالبحث، والقدرة على استهداف أجهزة الكمبيوتر غير المشتبه فيها[1]. ويبدو مما سبق ان الاتجار غير المشروع بالأسلحة والمخدرات وغيرها بتمكين من الإنترنت المظلم، هي اكثر دوليا منه داخليا، يجعل ذلك التعاون الدولي الفعال أساسية للاستجابة إلى هذا النوع من النشاط الإجرامي، ومع ذلك، وعلى الرغم من أن ممثلي عدد من وكالات إنفاذ القانون قد أشاروا إلى مستوى جيد من التعاون في بعض العوائق العملية بسبب الولايات القضائية

(1)- Ahmed Ghappour, op.cit, p.1083-1085.

المختلفة أو بسبب التشريعات الوطنية التي قد تختلف فيما يتعلق بما يمكن بيعه بشكل شرعي مثال: القطع، المكونات، الذخيرة، الأسلحة بالطلقات الفارغ، بالإضافة إلى ذلك، يعتبر التعاون بين وكالات إنفاذ القانون ومزودي خدمة البريد / البريد السريع العامة أو الخاصة أساسيا للتأكد من ان الاليات موجودة للتدخل بسرعة ما أن يتم تحديد طرد مشتبه به او مرسله أو مستلمة، وتعني الطبيعة الدولية للتجارة غير المشروعة على الانترنت المظلم أن على وكالات إنفاذ القانون أن تأخذ بعين الاعتبار وتمتثل للتشريعات ذات الصلة (بما فيها، إن كان ذلك ضرورياً، في بلدٍ ثالثٍ في حال دعت الحاجة إلى مساعدة قانونية دولية) التي تحكم حقوق الخصوصية وحماية البيانات والمعلومات وقيود قانونية أخرى ذات صلة برصد السلوك على الإنترنت أو إجراء عمليات على الإنترنت، بالإضافة إلى مسح الطرود أو إجراء المراقبة التقليدية[١].

من كل ما تقدم يتبين للباحث ان الجهود الدولية التي يتم بذلها في سبيل التصدي للتجارة غير المشروعة على الانترنت المظلم هي جهود جيدة لكن تحتاج إلى مزيد من التنسيق نظرا إلى ان الغالبية العظمى من ما يدار على الانترنت المظلم من تجارة غير مشروعة هو ذو مستوى دولي وهذا يوجب بان لا يكون الدور الرئيسي في التصدي لها من قبل دولة واحدة معينة مثل "الولايات المتحدة الامريكية" بالرغم من التقدم التقني الذي تتمتع به الا ان ذلك يهدد بشكل او باخر سيادة الدول، هذا وان كان الدور الذي قامت به منظمة الأمم المتحدة من خلال انشاء " فريق الخبراء الحكوميين " هو دور محمود وقد أسس لأمر مهم وهو فرض سيطرة القانون الدولي العام على الفضاء السيبراني وهذا أمر مهم، الا انه مازال امام منظمة الأمم المتحدة دور رئيسي وهو ان تؤسس لاتفاقية دولية تنظم التجارة غير المشروعة في ظل الانترنت المظلم نظرا لصعوبة تتبع خيوط الجرائم التي ترتكب فيه وتعدد وتنوع أطرافها وصعوبة تعقبها.

---

(١)- جياكومو بيرسي باولي واخرون، مصدر سابق، ص٧٣.

الخاتمة :

وفي ختام بحثنا هذا فقد توصلنا إلى مجموعة من الاستنتاجات والتوصيات وهي كالتالي:

أولا- الاستنتاجات:

١- يعرف الانترنت المظلم بانه جزء من الإنترنت لا تتم فهرسته بواسطة محركات البحث، وبالتالي فانه يصعب تحديد وتعقب من يستخدمه، مما يشكل خطورة كبيرة عند استخدامه في التجارة غير المشروعة.

٢- هناك نوعان رئيسيان من الأسواق تستخدم لأغراض التجارة المشروعة وغير المشروعة على الانترنت المظلم وهما، أسواق العملة المشفرة إذ يتم تداول العملات الاكترونية وانشاءها وتحديد أسعارها، والنوع الثاني أسواق البائعين الفرديين وهذه الأسواق بها قوائم أقل مقارنة بأسواق العملات المشفرة بينما يتم تصنيف بعض قوائم محلات البائعين وبالمثل، كما هو الحال في أسواق العملات الرقمية، فإن متاجر البائعين الأخرى تسرد جميعها منتجاتهم على صفحاتهم الرئيسية، محلات البائعين محدودة الوظائف مقارنة بأسواق العملات المشفرة، المناسبة لأسواقهم هيكل الأعمال في البيع مباشرة للعملاء.

٣- لقد تم تحديد عدة طرق للتصدي للأسواق التي تتم عليها التجارة غير الشرعية في الانترنت المظلم، من أهمها تقنيات التحقيق التقليدية، والكشف والاعتراض البريديان، والكشف والرصد على الانترنت، والتعطيل على الانترنت.

٤- هناك جهود وطنية بذلت وتبذل على مستوى العالم للتصدي للتجارة غير الشرعية على الانترنت المظلم الا أن هذه الجهود تحتاج دوما إلى تحديث اساليبها.

٥- بالرغم من أهمية توحيد الجهود الدولية للتصدي للأنترنت المظلم، الا ان الجانب المتجاوز للحدود الإقليمية لعمليات القرصنة لإنفاذ القانون تعرض لانتقادات عامة الا ان هذه الانتقادات لم تقلل من قيمة تلك الجهود.

ثانيا- المقترحات:

١- يحتاج المجتمع الدولي إلى توحيد جهوده اكثر لمواجهة مخاطر الانترنت المظلم كونه منصة لكل ما يهدد الأسس الرئيسية للمجتمع الدولي من امن وسلام ومكافحة الجريمة عبر الوطنية لذلك ينبغي ان تقود الأمم المتحدة جهود حقيقية لتوحيد الدول من اجل ابرام اتفاقية دولية للتصدي

للتجارة غير المشروعة على الانترنت المظلم كما تصدت من قبل لكل ما يهدد وحدة المجتمع الدولي وامنه.

٢- على المستوى الوطني نحتاج إلى تجديد الأنظمة القضائية لتسهل منح رخص التفتيش والتعقب للمجرمين كما تحتاج سلطات انفاذ القانون إلى تطوير كوادرها بشكل مستمر لتساير كل تطور يحدث في عالم التكنلوجيا.

المصادر :

أولا/ المصادر باللغة العربية:

١- جياكومو بيرسي باولي واخرون: خلف الستار التجارة غير المشروعة بالأسلحة النارية والمتفجرات والذخيرة على الانترنت المظلم، مؤسسة Rand، كالفورنيا، ٢٠١٧.

ثانيا/ المصادر باللغة الانجليزية:

1- Ahmed Ghappour: Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web, volume 69, Stanford. L. Rev, 2017.
2- Brian J. Egan: International Law and Stability in Cyberspace, volume 35, issue1, Berkeley J. Int'l Law, 2017.
3- Clayton Davis: Addressing the Challenges of Enforcing the Law on the Dark Web, The University Of Utah, December 11, 2017, https://law.utah.edu/addressing-the-challenges-of-enforcing-the-law-on-the-dark-web/#_ftnref19 (21/8/2020).
4- Darren Guccione: What is the dark web? How to access it and what you'll find, https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html (19/8/2020).
5- Giacomo Persi Paoli: The Trade in Small Arms and Light Weapons on the Dark Web, UNODA Occasional Papers, No. 32, October 2018.
6- Hernan Albamonte: Illicit Trade in the Dark Web, https://medium.com/@hernan.albamonte/illicit-trade-in-the-dark-web-a734ee605340 (17/8/2020).
7- Ireneusz Miciuła: The Condition of the Cryptocurrency Market and Exchanges in Poland, 2019, https://www.researchgate.net/publication/335559967_The_Condition_of_the_Cryptocurrency_Market_and_Exchanges_in_Poland (20/8/2020).
8- What is cryptocurrency trading and how does it work? : https://www.ig.com/en/cryptocurrency-trading/what-is-cryptocurrency-trading-how-does-it-work (20/8/2020).

Sources :

First: Sources in Arabic:

1- Giacomo Percy Paoli et al.: Behind the Curtain: The Illicit Trade in Firearms, Explosives, and Ammunition on the Dark Web, Rand Corporation, California, 2017.

Second: English sources:

1- Ahmed Ghappour: Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web, volume 69, Stanford. L. Rev, 2017.

2- Brian J. Egan: International Law and Stability in Cyberspace, volume 35, issue1, Berkeley J. Int'l Law, 2017.

3- Clayton Davis: Addressing the Challenges of Enforcing the Law on the Dark Web, The University of Utah, December 11, 2017, https://law.utah.edu/addressing-the-challenges-of-enforcing-the-law -on-the-dark-web/#_ftnref19 (8/21/2020).

4- Darren Guccione: What is the dark web? How to access it and what you'll find, https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find .html (8/19/2020).

5- Giacomo Persi Paoli: The Trade in Small Arms and Light Weapons on the Dark Web, UNODA Occasional Papers, No. 32, October 2018.

6- Hernan Albamonte: Illicit Trade in the Dark Web, https://medium.com/@hernan.albamonte/illicit-trade-in-the-dark-web-a734ee605340 (8/17/2020).

7- Ireneusz Miciuła: The Condition of the Cryptocurrency Market and Exchanges in Poland, 2019, https://www.researchgate.net/publication/335559967_The_Condition_of_the_Cryptocurrency_Market_and_Exchanges_in_Poland (20/8/2020).

8- What is cryptocurrency trading and how does it work?: https://www.ig.com/en/cryptocurrency-trading/what-is-cryptocurrency-trading-how-does-it-work (8/20/2020).