جامعة أكلي محند أولحاج- البويرة-

كلية الحقوق والعلوم السياسية

قسم القانون العام

الاتجـــــار بالأشـــــخاص عبر النـــــطاق الشبكي الخاص

مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية

تخصص القانون الجنائي والعلوم الحنائية

إعداد الطالبة:

حيدب سلوى

إشراف الأستاذ:

د. خليفي سمير

لجنة المناقشة

ربيع زهية	جامعة البويرة	رئيسا
خليفي سمير	جامعة البويرة	مشرفا ومقررا
عيساوي فاطمة	جامعة البويرة	مناقشا

تاريخ المناقشة 30 سبتمبر 2019

شكر و تقدير

الحمد لله رب العالمين و الصلاة و السلام على أشرف الأنبياء و المرسلين سيدنا محمَّد و على آله و صحبه و من تبعه بإحسان إلى يوم الدين ، و بعد ..

فإني أشكر الله تعالى على فضله حيث أتاح لي انجاز هذا هذا العمل بفضله ، فله الحمد أولاً و آخرًا.

ثم أشكر أولئك الأخيار الذين مدوا لي يدَ المساعدة ، خلال هذه الفترة ، و في مقدمتهم أستاذي المشرف على الرسالة

فضيلة الأستاذ الدكتور : خليفي سمير

الذي لم يدَّخر جهدا في مساعدتي ،فقد أعطاني أغلب وقته ،كما هي عادته مع كل طلبة العلم ، و كنت أجلس معه الساعات الطوال أقرأ عليه و لا يجد في ذلك حرجا ، و كان يحثني على البحث ، و يرغبني فيه ، و يقوي عزيمتي عليه فله من الله الأجر و مني كل التقدير حفظه الله و متعه بالصحة و العافية و نفع بعلومه .

الإهداء

بسم الله الرحمن الرحيم

بدأنا بأكثر من يد و قاسينا أكثر من هم و عانينا الكثير من الصعوبات و ها نحن اليوم و الحمد لله نطوي سهر الليالي و تعب الأيام و خلاصة مشوارنا بين دفتي هذا العمل المتواضع

إلى منارة العلم و الامام المصطفى إلى الأميّ الذي علم المتعلمين إلى سيد الخلق

إلى رسولنا الكريم سيدنا : محمد صلى الله عليه و سلم

إلى من كلله الله بالهيبة و الوقار .... إلى من علمني العطاء بدون انتظار ..... إلى من أحمل اسمه بكل افتخار يا من أفتقدك منذ الصغر .....يا من يرتعش قلبي لذكرك .....يا من أودعتني لله

– أبي رحمه الله –

إلى ملاكي في الحياة ...إلى معنى الحب و الحنان و....إلى بسمة الحياة و الوجود

إلى من كان دعاؤها سر نجاحي و حنانها بلسم جراحي إلى أغلى الحبايب

– أمي الحبيبة –

إلى من رافقتني منذ أن حملنا حقائب صغيرة و معك سرت الدرب خطوة بخطوة و ما تزال ترافقني حتى الآن ...

إلى شمعة تنير ظلمة حياتي

أختي : وسيلة ، إلهام

إلى رفيق دربي في هذه الحياة إلى من أرى التفاؤل بعينه و السعادة في ضحكته بنظرات الأمل

أخي : محمد

إلى التي في صلواتها دائما و بين كفيها تحمل لنا الكثير من الدعاء .....إلى ينبوع العطاء إلى اليد التي تمسح دمعي

إلى : جدتي حماك الله و أطال في عمرك

إلى أخوالي و أولادهم و خالاتي : لويزة و عيشة و ابنتها ايناس

إلى الاخوة و الأخوات ، إلى من تحلوا بالايخاء وتميزوا بالوفاء و العطاء إلى ينابيع الصدق الصافي

إلى من عرفت كيف أجدهم و علموني أن لا أضيعهم

أصدقائي : أمامة ، آسيا ، بسمة ، خولة ، عقيلة ، عيشة ، مريم .

إلى من علمونا حروفا من ذهب و كلمات من درر،إلى أساتذتي الكرام في جميع الأطوار وصولا للجامعة

إلى من جعلهم الله اخوتي بالله ..... و من أحببتهم بالله طلاب كلية الحقوق و العلوم السياسية

إلى من يسكنون في القلب و لم تذكرهم أقلامي... إلى من لم أعرفهم و لم يعرفوني .....

إلى من أتمنى أن أذكرهم ...إذا ذكروني

قائمة المختصرات

المختصرات بالغة العربية:

ق.ع.ج..... قانون العقوبات الجزائري.

ق.ص..... قانون الصحة.

ق.إ.ج.ج..... قانون الإجراءات الجزائية الجزائري.

م.ج..... المشرع الجزائري.

ج ر..... الجريدة الرسمية.

د ط ..... دون طبعة.

مج..... مجلد.

د ج..... الدينار الجزائري.

المختصرات بالغة الفرنسية:

Art…… Article.

Btc……. Bitcoine.

EUR…….. Euro.

Ibed……..même référence.

مقدمـــــــة

إن ظاهرة الاتجار بالأشخاص ليس بالأمر الجديد وإنما ظاهرة تمتد إلى عمق التاريخ، بحيث كانت عبارة عن نظام اجتماعي قائم في حضارات عريقة كالحضارة البابلية والمصرية، والحضارة اليونانية والرمانية، فقد كانت الحروب ومفاهيم القوة والغلبة سائدة آنذاك فالمنتصر من الحروب يقوم باستعباد المنهزم وإذلاله بجعله رقا يباع ويشترى، حاله كحال السلع، وهذا ما فعلته مصر القديمة حين تم بناء الأهرام من طرف العبيد تحت التعذيب، لهذا قال تعالى ممتنا عليهم بعد بسم الله الرحمن الرحيم:" وإذا نجيناكم من آل فرعون يسومونكم سوء العذاب يذبحون أبناءكم ويستحيون نساءكم وفي ذلكم بلاء من ربكم عظيم"[1].

وهناك من كان يتم الإحسان إلهم مثلما كان مع سيدنا يوسف عليه السلام عندما كان عبدا عند عزيز مصر، وهذا ما قال عنه الله تعالى في سورة يوسف. بعد بسم الله الرحمن الرحيم: "وقال الذي اشتراه من مصر لامرأته أكرمي مثواه عسى أن ينفعنا أو نتخذه ولدا وكذلك مكنا ليوسف في الأرض ولنعلمه من تأويل الأحاديث والله غالب على أمره ولكن أكثر الناس لا يعلمون"[2].

كانت تمارس هذه التجارة عبر سواق العبيد أو ما يعرف بسوق النخاسة، والتي يستغل فيها كلا الجنسين ومن مختلف الأعمار، حيث يتم أخذ العبيد قصرا أو تهديدا أو عن طريق الضغط من أجل بيعهم في الأسواق، إلا أنه و مع التطور التكنولوجي المعاصر تطورت هذه التجارة وأخذت شكلا أخر غير الشكل الذي تعرفه، كونها صارت تهدد المجتمع الدولي، بحيث خرجت هذه الجريمة من الدائرة التقليدية، وانتقلت إلى أعلا المستويات، من عالم المادي الممسوس إلى عالم

[1]– الآية 49 من سورة البقرة.

[2]– الأية 21 من سورة يوسف.

الافتراضي والشبكات الرقمية المشفرة التي تعطي إمكانية عالية للجناة للإفلات من العقاب.

وتعتبر جريمة الاتجار بالأشخاص ثالث أكبر تجارة غير مشروعة في العالم بعد التجارة في الأسلحة والمخدرات، خاصة إذا تعلق الأمر بشبكة الاتصال الدولية عامتا والإطار الشبكي الخاص خاصة. وهذا ما جعل من دول العالم تعطي لها أهمية كبير من خلال إجراء العديد من الاتفاقيات الدولية في إطار التعاون الدولي لوضع آليات وسبل من أجل مكافحة هذه الظاهرة من بينها اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة، والبروتوكول المتعلق بمنع الاتجار بالأشخاص لسنة 2000[1].

تعد التجارة بالأشخاص، عبر الموقع الشبكي الخاص من أخطر أنواع الممارسات الغير مشروعة، في مجال شبكة الاتصال الدولية، كون أن الولوج إلي هذه المنظومة المعلوماتية والتي تمثل 95%[2] منها" ديب ويب" أما 5% فتمثل "السيرفيس ويب"، ويظم "الديب ويب" 15% تمثل "الدارك ويب" التي تمارس فيه التجارة بالأشخاص[3].

واحتراما لمبدأ الشرعية الجنائية، وجب البحث في نصوص التشريع الجزائري من اجل تكيف هذا النوع من التجارة الرقمية من حيث مشروعيتها، كون أن موقع "الديب ويب" من المواقع

---

[1]- مرسوم رئاسي رقم 03-417، يتضمن التصديق بتحفظ على بروتوكول منع وقمع الاتجار بالأشخاص خاصة النساء والأطفال المكمل لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المعتمد من طرف الجمعية العامة لمنظمة الأمم المتحدة يوم 15نوفمبر 2000، (ج ر)، عدد 69، صادر بتاريخ 12نوفمبر 2003.

[2]– هاني سمير علي، مما لا تعرف على الانترنت الخفيdeep web ، تاريخ النشر: 03جولية 2015، تاريخ التصفح: 29ماي2019، الرابطة: http://www.arageek.com/tech/2015/what -you-do-not-know-about-.

[3]– محمد الغضبان، العالم الخفي، ما هو الديب ويب؟ وكيف تدخل إليه؟، دون تاريخ نشر، تاريخ التصفح 29ماي2019، الرابطة: http://www.netaawy.com/2016/what-is-the-deeb-web-and-how-to-accedd.

المشفرة التي يستحيل فيها مراقبة الاتصالات أو التعرف على هوية المستخدمين من خلال adresse IP.

واستنادا لما ذكر أعلاه يمكن طرح الإشكالية الآتية والمتمثلة في: كيف تتم عملية الاتجار بالأشخاص؟ وماهي الإجراءات المتخذة من أجل مكافحة هذه الظاهرة؟

للغرض البحث في الموضوع، من حيث تتبع معانيه التقنية والقانونية، وجب علينا الاعتماد على المنهج التحليلي الوصفي، أما بخصوص التجارة داخل "الدارك ويب" ودراسة النصوص التشريعية الجزائرية ذات الصلة، اتبعنا المنهج التحليلي النقدي.

ولعلى من بين أهمية الأسباب التي دفعتنا لدراسة هذا الموضوع، هو الطابع الحساس لهذه الجريمة والتي تتعلق بكيان الإنسان الذي له الحق في العيش عيشة كريمة.

أما أهداف الدراسة فقد تمحورت حول إعطاء مفهوم جديد لهذه الظاهرة، من خلال تعريفها مرورا إلى دراسة موقع الدرك ويب ومحاولة معرفة كيف تمارس هذه التجارة باعتبارها ظاهرة مستحدثة، ثم محاولة معرفة طرق مكافحتها من خلال الآليات الجديدة في عملية البحث والتحري الرقمي والمشاكل التي وجهتها هذه الآليات.

ولأجل إنجاز الدراسة قمنا بتقسيم هذا المبحث إلى فصلين، بحيث يتضمن الفصل الأول الإطار المفاهيمي العام للاتجار بالأشخاص عبر النطاق الشبكي الخاص، أما الفصل الثاني فقد خصص لدراسة المكافحة الجنائية للاتجار بالأشخاص عبر النطاق الشبكي الخاص.

الفصل الأول

الإطار المفاهيمي العام للاتجار بالأشخاص عبر النطاق الشبكي الخاص

يتواجد على إحدى مستويات "الديب ويب" أو ما يسمى بالانترنت المظلم العديد من الأنشطة الغير شرعية والإجرامية، والتي تمارس بأبشع الطرق والوسائل، من بين هذه الجرائم جريمة الاتجار بالأشخاص والتي تعتبر جريمة ضد الإنسانية قبل أن تكون جريمة ضد الأشخاص بحيث الهدف البارز منها ربح المال أو تحقيق أغراض شخصية. وإنما أصبحت ظاهرة متطورة تمارس عبر نطاق الشبكة الدولة بصفة عامة، والخاصة بشكل خاص، بحيث هذا الأخير يتميز بخصوصية خاصة وجد معقدة عن باقي الشبكات الدولية وهذا راجع للخوارزميات التي أنشا بموجبها.

وعليه قمنا بتقسيم الفصل الأول إلى مبحثين، بحيث نستعرض من خلال (المبحث الأول) مفهوم الاتجار بالأشخاص عبر النطاق الشبكي الخاص، أما (المبحث الثاني) فسنتطرق إلى المعاملات الخاصة بالاتجار بالأشخاص عبر نطاق الشبكي الخاص.

المبحث الأول

مفهوم الاتجار بالأشخاص عبر النطاق الشبكي الخاص

انطلاقا مما ذكرناه سابقا، يمكن القول أن ظاهرة الاتجار بالأشخاص من أخطر الجرائم التي تمس الكيان البشري خاصة حين أصبحت مرتبطة بالوسط الرقمي، الذي زادم من هذه الجريمة تعقيدا بسبب طبيعة الشبكة الخاصة المشفرة، لهذا وجب علينا البحث في هذا الموضوع من خلال تعريف النطاق الشبكي الخاص (المطلب الأول)، ومن بعدها التعرف على جريمة الاتجار بالأشخاص (المطلب الثاني).

المطلب الأول

تعريف النطاق الشبكي الخاص

يقول الكاتب عبد الرزاق طواهرية:" كل ما نتفحصه على مستوى شبكة الانترنت العادية، يعتبر جزءا صغيرا جدا من أصل وحش مرعب يدعى الانترنت العميق"[1].

وعليه حسب نطاق الدراسة، سنركز على النطاق الشبكي الخاص بدون النطاق الشبكي العام، والذي نوضحه من خلال: المقصود بالنطاق الشبكي الخاص(فرع الأول)، ثم الولوج إلى الشبكة الخاصة (فرع الثاني)، ويليه المتصفحات ومحركات البحث الخاصة (الفرع الثالث).

الفرع الأول

المقصود بالنطاق الشبكي الخاص

إن النطاق الشبكي الخاص بصفة أساسية متعلق بالويب العميق"deep "le web profond wep "، وويب داخل الويب العميق يعرف ب الويب المظلم " le web sombre dark wep"، بحيث لا يمكن لهذا النوع من الشبكة أن تظهر على مستوى الويب العادي[2].

1-عبد الرزاق طواهرية، شياطين بانكوك، جحيم الدارك ويب،الطبعة الثانية،المثقف للنشر والتوزيع، باتنة، الجزائر، 2017، ص24.

[1]- النطاق الشبكي العام: هو كل ما يمكن أن تصل إليه محركات البحث العادية والمعروفة ب "السيرفيس ويب" "le wep de surface- surface wep"، والتي هي عبارة عن مجموعة من المعلومات الرقمية الغير مشفرة والتي يمكن الولوج إليها بكل سهولة من خلال المتصفحات العادية، ومحركات البحث المعروفة، بحيث هذا النطاق يشكل 16%جزء من الشبكة الدولية.

وعليه سنقوم بالتطرق أولا إلى تعريف الويب العميق(أولا)، ثم الويب المظلم(ثانيا) بالإضافة إلى محتوى الدرك ويب(ثالثا).

أولا: الويب العميق (Deep Wep)

يمكن تعريف Deep Web ببساطة على أنه جزء من الإنترنت لا يتم فهرسته بواسطة محركات البحث. هذا يعني أنه لا يمكنك البحث عنها على محركات البحث مثل Google أو Yahoo، بل يجب عليك زيارة العنوان مباشرة. إذ انه ليس كل الويب العميق غير قانوني. فمعظم "ديب ويب" قانونية. يمكن الوصول إلى هذه المواقع باستخدام روابط خاصة على أي متصفح بحيث لا تحتاج إلى متصفح خاص. يستخدم "Deep Web" بشكل أساسي في الخدمات المصرفية وتحويل الأموال مثل الخدمات التي تتطلب الأمان والخصوصية.

وعليه يمكن القول أن "الديب ويب" يمثل الجزء الأكبر من شبكة الاتصال الدولية والتي تقدر بحوالي 95% من الحجم الكلي، أما 5% المتبقية فهي تمثل "السيرفيس ويب".

ثانيا: الويب المظلم (Deerk Wep)

يمثل 15% من الويب العميق "Deep wep". بحيث مواقع الويب المظلم Deerk wep غير متوفرة على محركات البحث تمامًا مثل شبكة الويب العميقة. والفرق هو أنه لا تحتاج إلى روابط خاصة للوصول إلى هذا النوع من المواقع، لكن في الواقع هناك بعض المتصفحات الخاصة المصممة لاستخدام هذه المواقع.

يتطلب الوصول إليها خاصة مثل برنامج الوكيل الخاص، والتوثيق للوصول مثل TOR (the onion router). تعتبر TOR واحدة من أفضل المتصفحات للوصول إلى شبكة الويب المظلمة. وفي حياتنا اليومية نستخدم العديد من المواقع التي يبدأ نطاقها بـ WWW لكن Dark Web له لنطاقات وروابط خاصة. تتم معظم الأعمال غير القانونية على هذه المواقع مثل شراء وبيع المخدرات وتسويق الأسلحة والبيت كوين الخ[1].

الفرع الثاني

محتوى الشبكة الخاصة

تحتوي المواقع الموجودة على هذه الشبكة مجموعة من أبشع أنواع الخدمات والسلع التي يمكن تداولها بين البشر، وهذه الشبكات تدار بواسطة أشخاص أو منظمات تعمل في الخفاء وتتخذ من هذه المواقع منافذ لعرض منتجاتها وخدماتها للمستخدمين، وهذه نبذة بسيطة عن الأشياء التي يتم عرضها في تلك المواقع. بحيث هناك مواقع تبيع جميع الأعضاء البشرية والتي تكون مسروقة أو تم الحصول عليها بشكل غير قانوني، بحيث أنه بعض الأعضاء قد يصل ثمنه 200,000.$ بالإضافة إلى بيع كافة أنواع المخدرات بأي كمية مطلوبة على Dark Web ، وهناك مواقع تعمل على استكشاف ثغرات أمنية في مواقع كبرى وبيع هذه الثغرات لأشخاص آخرين، كذلك تبيع الفيروسات والبرمجيات الخبيثة مثل فيروسات الفدية وغيرها من الفيروسات المدمرة. كما أنه هناك أسواق

[1]-Difference Between Dark Web, Deep Web And Surface Web، 20.18.2019 :تاريخ التصفح

متخصصة في بيع مختلف أنواع الأسلحة، وهذه الأسلحة تكون غير مسجلة، وتتولى هذه المواقع مهمة القيام بشحن الأسلحة إلى العنوان المطلوب إضافة إلى:

1-هناك مواقع تُقدم هويات شخصية مزيفة أو شهادات جامعية أو جواز سفر دولة معينة أو أي أوراق رسمية تريد استخراجها من أي جهة محلية أو دولية.

2-أيضًا هناك مواقع متخصصة في تعليم القرصنة والهاكينج حتى مرحلة متقدمة.

3-هناك مواقع تبيع عملة مزيفة مطابقة تقريبًا للعملة الأصلية فمثلًا 1000$ مزيفة يمكن أن يتم بيعها مقابل 300$ فقط، ويمكنها أن تتجاوز أدوات فحص الأموال.

4- من أبرز الأشياء المتاحة على الإنترنت المظلم هو استئجار القتلة، وغالبًا ما تستخدم في أعمال الاغتيال السياسي وتبدأ سعر العملية من 20000$ إلى أعلى.

5-كل الأشياء المسروقة مثل الحسابات الاجتماعية أو قواعد البيانات أو البطاقات الائتمانية أو الحسابات البنكية وغيرها يباع في الإنترنت المظلم.

الفرع الثالث

الولوج إلى الشبكة الخاصة

لقد قمنا من خلال الفروع السابقة بتحديد مفهوم الشبكة الخاصة، أما من خلال هذا الفرع سنقوم بدراسة المتصفحات الخاصة بهذه الشبكة(أولا)، ثم بعد ذلك محركات البحث(ثانيا).

أولا: المتصفحات الخاصة بالنطاق الشبكي الخاص

من المتعارف عنه في النطاق الشبكي العام المتصفحات الخاصة بيه هي المتصفحات العادية مثل" Google Crome، Mozilla "، لكن هذا الأمر يختلف في النطاق الشبكي الخاص، وهذا راجع إلى خصوصية النطاق في تشفير المعلومات وعدم الكشف على هوية المستخدم، حيث المتصفحات العادية لا تملك هذه الخاصية.

Tor.1: البصل راوتر هكذا يطلق عليه وذلك راجع لتشبيهه بحبة البصل التي تحتوي على العديد من الطبقات، إذ أنه لا توجد طريقة لإنشاء قائمة بأفضل متصفحات الويب المظلمة دون ذكر هذا المتصفح الذي فتح البوابات لتصفح الويب العميق[1].

TOR هو متصفح الويب العميق الأول والأكثر قوة والذي بدأ في تقديم أعلى درجات الأمان وعدم الكشف عن هويته قبل أي متصفحات ويب عميقة أخرى. بالرغم من تعرضه لمكتب التحقيقات الفيدرالي (FBI) للقرصنة في عام 2014، وبسبب هذا الاختراق جعل القائمين بالعمل عليه الاهتمام بجميع الثغرات وكذلك نقاط الضعف التي تؤدي إلى الاختراق في المقام الأول. ومع ذلك، يعتقد الناس أن متصفح TOR يتيح لك تصفح الويب المظلم بشكل مجهول. لكن هذا ليس صحيحًا. بل يقوم TOR ببساطة تصفح

[1]- DARK WEB LINKS DARK WEB SITES ، DEEP WEB LINKS 2018، تاريخ التصفح 2019/05/19 غبر الرابطة: https://www.torproject.org

2- أنظر كذلك: https://lists.torproject.org/pipermail/tor-dev/2017-March/012088.html

3- أنظر كذلك: Roger Dingledine. pre-alpha: run an onion proxy now، تاريخ الاطلاع: 5 ماي 2019 ، تاريخ النشر، 20 سبتمبر 2002.

الإنترنت الخاص بك من خلال عقد متعددة لجعل IP الخاص بك لا يمكن تتبعه بسهولة وأمان، ولكنه لا يخفيه. لإخفاء هويتك بالكامل، تحتاج إلى خدمة VPN إلى جانب متصفح TOR.

يمكن الوصول إلى متصفح TOR من أنظمة التشغيل الرئيسية مثل Mac OS و Windows و GNU / Linux.[1]

I2P.2 مشروع الانترنت الغير مرئي: على عكس متصفح TOR ، فإن I2P أو Invisible Internet Project هي حزمة مجمعة تقدم مجموعة واسعة من الخدمات المختلفة. يتيح لك برنامج I2P الوصول إلى الويب عبر تدفق بيانات ذو طبقات لحماية هويتك[2].

يتم تشفير الاتصال عبر I2P بشكل كامل مع كل من المفاتيح العامة والخاصة. يستخدم المستعرض بروتوكولات نقل بيانات TCP / UDP وIP لحماية نشاطك على الإنترنت ويستخدمها لتشفير جميع البيانات وحركة المرور عبر الإنترنت، بحيث يقوم I2P بإنشاء شبكة منفصلة للسماح للمستخدمين بالوصول إلى الإنترنت، كما يساعد I2P في التحكم في حركة مرور البيانات والبيانات على الإنترنت وتظل الطبقة الثانية من الإنترنت

[1]-- ibem https://www.torproject.org

– للمزيد راجع: Tor 0.3.3.2-alpha is released: bugfixes and DoS prevention، تاريخ الاطلاع: 01 مارس 2018 تاريخ النشر: 10 فبراير 2018.

[2] –-Francois Paget. Chercheur en cybercriminalité. Derknet et économie souterraine. Colloque économie de la cybersécurité Chaire Cybersécurité & Cyberdéfense. Université de Sorbon. Page 05-14 novembre 2016

مخفية وخصوصية. إضافة أنها تحمي شبكة التراكب المجهولة كل النشاط من أن يتم تعقبها بواسطة مراقبة شبكة السحب أو مراقبة مزود خدمة الإنترنت[1].

3. Whonix: هو متصفح ويب غامق مبني على برنامج TOR المجاني. يُعد عدم الكشف عن هويته وخصوصيته عاملين رئيسيين للوصول إلى محتوى الويب العميق. ويوفر تطبيق Whonix عبر شبكة ترحيل مفتوحة وموزعة تدعمهاTOR. بحيث يضمن TOR أن الاتصالات غير مضمونة وتزيل أي تسريبات لنظام أسماء النطاقات على الإطلاق. تجعل الاتصالات من خلال TOR من Whonix قوية إلى درجة أنه حتى البرامج الضارة التي لها امتيازات الجذر لا يمكنها تتبع عنوان IP الحقيقي للمستخدم.

أفضل جزء في Whonix هو أنه ليس فقط مستعرض ويب عميقًا، ولكن أيضًا نظام تشغيل كامل الوظائف حيث يمكنك إعداد وإدارة الخادم الخاص بك دون تتبع. يتم بالفعل تكوين العديد من التطبيقات الشائعة وتثبيتها للاستخدام الفوري.[2]

4. Subgraph OS: متصفح ويب عميق ومفتوح المصدر يستند إلى مشروع TOR. نظام Subgraph OS ليس مستعرضًا مستقلًا ولكنه نظام تشغيل كامل تمامًا مثل

---

[1]-- ملاحظة: I2P عبارة عن شبكة متنامية وأنها تنمو يومًا بعد يوم كلما توسعت الشبكة. لذا يعتبر أفضل رهان إذا كنت لا تريد اختيار TOR في الوقت الحالي.

-USP OF I2P: هو نظام تخزين الملفات اللامركزي وقاعدة بيانات الشبكة الموزعة. يستخدم تقنية "Darknet".

[2]-Whonix هو نظام التشغيل الوحيد المصمم للعمل على جهاز VM مقترن بـ TOR. واحدة من أفضل النقاط البارزة في Whonix هي ميزة "Data Stream Isolation". على الرغم من اقترانه بـ TOR، إلا أن فرص ارتباط الهوية قريبة من المستحيل لأن Whonix لا يستخدم نفس مرحلات الخروج ودارات TOR.

Whonix. الفكرة الرئيسية وراء Subgraph OS هي توفير بيئة مجانية وخاصة وآمنة للمستخدمين للوصول إلى شبكة الويب العالمية بأكملها[1].

5. الذيل نظام فقدان الذاكرة المتخفي لايف: مثل كل متصفحات الويب المظلمة الأخرى المذكورة أعلاه، تؤمن TAILS أيضًا اتصالاتها باستخدام شبكة TOR. TAILS، هو اختصار لنظام Amnesic Incognito Live System، وهو نظام تشغيل مباشر مصمم لضمان الخصوصية وإخفاء الهوية لمستخدميه. يمكنك الوصول إلى هذه الشبكة أو نظام التشغيل باستخدام عصا USB أو قرص DVD. يستخدم البرنامج أدوات التشفير المتقدمة للغاية لإضافة طبقة مشفرة لجميع الاتصالات. تضيف هذه الأدوات درعًا واقيًا لجميع الملفات ورسائل البريد الإلكتروني والرسائل الفورية التي ترسلها أو تستقبلها[2].

ثانيا: محركات البحث الخاصة بالنطاق الشبكي الخاص

إن البحث في الإنترنت العميق أو المظلم كما يدعوه البعض تجربة استثنائية خاصة لمن لم يعتاد عليها، فالأمر أشبه بالجبل الجليدي الذي لا يظهر منه سوي قمته بينما في القاع تكمن كل الأسرار، والمحركات العادية مثل Google لا يمكنها أن تقوم بالبحث داخل الانترنت المظلم، وهذا راجع لخصوصية الشبكة، لهذا قام خبراء البرمجة المختصين في النظام الشبكي بإنشاء مجموعة من محركات البحث والتي نظمن السرية وتشفير المعلومات .

[1] - https://subgraph.com/sgos تاريخ التصفح 19/05/2019

[2] - https://tails.boum.org تاريخ التصفح 19/05/2019

1. The Hidden Wiki: تعتبر مواقع wiki من أشهر المواقع التي اعتدنا رؤيتها في نتائج البحث، لكن الكثيرين لا يعلمون أنه يوجد موقع مخفي من wiki للوصول إلى الإنترنت المظلم. يمكن البحث عبر هذا المحرك على كثير من الأمور الغير موجودة في مواقع محركات البحث التقليدية، والتي تكون في بعض الأحيان غير قانونية. كما يوجد بعض الوثائق السرية المهربة والغير مصرح بها على هذا المحرك.

2..محرك بحث not evil: يعتبر محرك بحث not evil من المحركات الغير معروفة لدي الكثيرين لكن هذا لا يعني أنه أقل أهمية منهم، فهذا المحرك يسمح لك بالتصفح بمنتهي الحرية دون الحاجة لتسجيل معلوماتك، أو التعرض لأي محاولات إلهاء من أي نوع.

3. محرك بحث Tor Links : من أشهر واكبر المحركات ويضم الكثير من المواقع التي يمكنك المضاربة وشراء الأسهم من خلالها مثلTor Broker، أو التسوق وشراء أو بيع كل ما يخطر على بالك –حرفياً– من خلال Tor Shops. بحيث يتم التعامل في هذه المنتديات سواء عن طريق المضاربة، أو التسوق بعملة البيت كوين الشهيرة، يسمح هذا المحرك بشراء وبيع أي شئ بصورة سرية تماماً ودون الحاجة إلى الإعلان عن اسمك أو هويتك، حتى عند المضاربة وشراء أسهم فالمتصفح لا يطالبك ببياناتك الحقيقية.

4. محرك بحث Ahmia.fi: يعتبر هذا المحرك من أبسط محركات بحث الإنترنت العميق، فهو مثالي للمبتدئين في هذا العالم. يمتاز هذا المحرك بسهولة التصفح في مواقع deep

web مما يساعدك في الاعتياد على هذا العالم ويصبح من السهل عليك التعامل مع محركات البحث الأخرى الأكثر تعقيداً.

5. محرك بحث Torch : ينتمي إلى محركات البحث الشهيرة للانترنت العميق، ويعتبر هذا المحرك من المحركات الأكثر استخداما. كما أن هذا المحرك مثالي لتصفح كل شيء سواء التسوق لسلع فيزيائية أو غير مادية على الإطلاق، وتبادل العملات، وغيرها من الأنشطة التي يمكنك أن تجدها من مجرد ضغطة زر واحدة[1].

المطلب الثاني

التعريف التقليدي لاتجار بالأشخاص

تختلف جريمة الاتجار بالأشخاص في النطاق المادي الملموس عن النطاق الافتراضي، مما جعل منها جريمة رقمية حديثة تكتسب خصوصيات خاصة، لهذا وجب التطرق أولا إلى تعريف جريمة التجار بالأشخاص وفق المفهوم التقليدي (الفرع الأول)، ومن ثم معرفة أركان هذه الجريمة (الفرع الثاني)، ثم معرفة أشكال الاتجار عبر النطاق الشبكي الخاص (الفرع الثالث).

1-DEEPWEBADMIN،JANUARY 11//052019 -https://www.deepweb-sites.com/deep-web-search-engines.

الفرع الأول

المقصود التقليدي لجريمة الاتجار بالأشخاص

تعد جريمة الاتجار بالأشخاص من بين الجرائم التي تعرف خطورة، إذ أنها تهدد كيان الشخص وتهدم المجتمع، بحيث هي من الجرام أكثر انتشارا في العالم.

وعليه لتعريف هذه الجريمة وجب علينا التطرق لتعريف الفقهي (أولا)، ثم التعريف الدولي (ثانيا)، ومن ثم معرفة تعريف المشرع الجزائري (ثالثا).

أولا: التعريف الفقهي

عرف الفقه الاتجار بالأشخاص أنه :" كافة التصرفات المشروعة وغير المشروعة التي تحيل الإنسان إلى مجرد سلعة أو ضحية يتم التصرف فيها بواسطة وسطاء محترفين عبر الحدود الوطنية. بقصد استغلال في أعمال ذات أجر مند أو في أعمال جنسية أو ما شابه ذلك، سواء تم التصرف بإرادة الضحية أو قسرا عنه أو بأي صورة أخرى من صور العبودية "[1].

كما يعرف البعض الاتجار بالأشخاص أنه :" تجنيد أشخاص أو نقلهم بالقوة، أو الإرادة أو الخداع لغرض الاستغلال بشتى الصور، ومن ذلك الاستغلال الجنسي، العمل الجبري، الخدمة القسرية 'التسول'، الاسترقاق، تجارة الأعضاء البشرية وغير ذلك"[2].

[1] – سوزي علي ناشد، الاتجار في البشر بين الاقتصاد الخفي والاقتصاد الرسمي، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان،2008، ص15.

[2] – صفاء كزونة، جريمة الاتجار في البشر وفق الوثائق الدولية، مذكرة الماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2013-2014، ص11.

وعرفت كذلك: "إن الاتجار بالبشر جريمة تخزي الجميع، كل عام يتم الاتجار يالألاف الرجال والنساء والأطفال في بلدهم أو في الخارج، عن طريق الإكراه والقوة، يتم استغلالهم في عمالهم، أو لممارسة الجنس أو لأعضائهم"[1].

وعرفت أيضا:" كل تصرف بطريقة القوة الخشنة أو النعامة يقع على الإنسان".

ثانيا: التعريف القانوني

عرف برتوكول الأمم المتحدة في نص المادة03 فقرة أ :" تجنيد أشخاص أو نقلهم أو تنقيليهم أو استغلال حالة استضعاف أو بإعطاء أو تلقي مبالغ مالية أو مزايا لنيل موافقة شخص له سيطرة على شخص أخر لغرض الاستغلال، وشمل الاستغلال كحد ادني استغلال دعارة الغير أو سائل أشكال الاستغلال الجنسي أو السخرة أو الخدمة قسرا أو الاسترقاق أو الممارسات الشبيه بالرق والاستعباد أو نزع الأعضاء"[2].

ونصت الفقرة (ب) من نفس المادة" لا تكون موافقة ضحية الاتجار بالأشخاص على الاستغلال المقصود والمبين في الفقرة (أ)"[3].

وعرفت اتفاقية الدول العربية في المادة11 :"التجارة بالأشخاص هو ارتكاب أو المشاركة في أرتكب الأفعال التالية التي تقوم بها حماية إجرامية منظمة، أي تهديد بالقوة

[1] - office des nations unies contre la crime (DNNDC).

[2] - وثيقة أممية رقم:55/25 بروتوكول الأمم المتحدة الخاص بمنع وحضر وقمع الاتجار بالأشخاص. خاصة النساء و الأطفال، المكمل لاتفاقية الأمم المتحدة بمكافحة الجريمة المنظمة عبر الوطنية ، اعتمدته الجمعية العامة للأمم المتحدة في دورتها 55، المؤرخ في 15 تشرين الثاني نوفمبر 2000، تاريخ النفاذ، 25 كانون الأول ديسمبر 2003، صادقت عليه الجزائر بتحفظ في 09 مارس 2004.

[3] - المرجع نفسه.

أو استعمالها أو استغلال حالة الضعف وذلك من أجل استخدام أو نقل أو إيواء استقبال أشخاص لغرض استغلال، بشكل غير مشروع في ممارسة الدعارة (البغاء) أو وسائل أشكال الاستغلال الجنسي أو السخرية أو الخدمة قسرا، أو الاسترقاق أو الممارسات الشبيه بالرق والاستعباد. لا يعتد بالرضا الشخص ضحية الاتجار في كافة صور الاستغلال متى استخدمت فيها الوسائل المبينة في هذه الفقرة "[1].

كما نصت الفقرة الثانية من نفس المادة صور السلوك الإجرامي والمتمثلة استخدام الطفل أو نقله أو إغوائه... ولم تحدد الوسائل المستعملة في ذلك وتركت المجال مفتوحا بذكر عبارة – حتى– إذا لم ينطوي على استعمال أي من الوسائل المبينة في الفقرة (1)[2].

وفي رأينا أنه عدم الاعتداء برضا الضحايا من الأطفال وكذا عدم حصر الوسائل المستعملة من اجل استخدام ما هو إلا حماية لحقوق الطفل خصوصا أنهم الفئة أكثر عرضة للاتجار بهم في العالم.

ثالثا: موقف المشرع الجزائري

عرف المشرع الجزائري جريمة الاتجار بالأشخاص من خلال المادة 303مكرر4 من ق.ع.ج بأنه: " يعد الاتجار بالأشخاص تجنيد أو نقل أو تنقيل أو إيواء أو استقبال

[1] – وثيقة إقليمية رقم 36 المتضمنة اتفاقية الدول العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية لسنة 2012. الصادرة في 21 ديسمبر 2012، صادقت عليها الجزائر بموجب مرسوم رئاسي 25/14، المؤرخ في 08 سبتمبر 2014،ج ر ج ج، عدد50، الصادر في 20سبتمبر 2014.

[2] - أنظر المادة 11فقرة (2) من اتفاقية الدول العربية لمكافحة الجريمة المنظمة عبر الوطنية.

شخص أو أكثر بواسطة التهديد بالقوة أو باستعمالها أو غير ذلك من أشكال الإكراه... أو الممارسات الشبيهة بالرق أو الاستعباد أو نزع الأعضاء"[1].

وعليه من خلال التعريف الذي قدمه المشرع الجزائري في المادة 303مكرر4من ق،ع، فإن المشرع أعطى مفهوم بشأن هذه الجريمة على أنها" السيطرة الفعلية على الضحية وفق أشكال ووسائل محددة حصرا"[2]. لكن بالرغم من أتفاق المشرع الجزائري مع ما جاء في بروتوكول المكمل لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطن لسنة 2000، إلا أنه هناك اختلاف في صور الاستغلال، حيث أنها وردت في ق.ع.ج على سبيل الحصر وليس على سبيل المثال، وهذا لعدم ورود عبارة- يشمل الاستغلال كحد أدنى- المذكورة في البروتوكول أو أي عبارة أخرى بمفهوم الاستغلال على سبيل المثال، وهذا موقف منتقد لأنه يؤدي إلى تصنيف جريمة الاتجار بالأشخاص.

[1]- الأمر رقم 66-156، المؤرخ في 08جوان 1966م، يتضمن قانون العقوبات، (ح ر)،عدد 49، صادر بتاريخ 11جوان 1966، معدل ومتمم، سيما بأمر رقم 09-01، مؤرخ في 25فيفري2009، (ج ر)، عدد15، صادر بتاريخ 08 مارس 2009.

[2]-أنظر فؤاد جحيش، الاتجار الجنسي بالأطفال عبر النطاق الشبكي الخاص"بين خطورة الظاهرة الرقمية ومحدودية المكافحة الجنائية، دراسة تحليلية نقدية في ضل القانون الجزائري، مخبر الدولة والجرائم المنظم،كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، البويرة، الجزائر،2017 ، ص10.

الفرع الثاني

أركان الاتجار بالأشخاص

في هذا الفرع سنقوم- بدراسة- أركان جريمة الاتجار بالأشخاص من خلال تحديد الركن الشرعي (أولا)، ثم الركن المادي (ثانيا)، ويليه الركن المعنوي (ثالثا)

أولا: الركن الشرعي

نصت المادة 01 من ق.ع.ج" لا جريمة ولا عقوبة أو تدابير أمن بغير نص". وجريمة الاتجار بالأشخاص جرمها المشرع من خلال المادة 303 مكر 04 إلى غاية المادة 303 مكرر15.

ثانيا: الركن المادي:

إن الركن المادي بصفة عامة هو فعل خارجي له طبيعة ملموسة تدركه الحواس، ولا تقوم أي جريمة بدون توافر ركن مادي، وهو يتكون من ثلاثة عناصر هي:"السلوك الإجرامي والنتيجة و العلاقة السببية بين السلوك الإجرامي والنتيجة، كما يوجد أيضا الشروع بوصفه صورة لركن مادي لم تكتمل عناصره"[1].

1.السلوك الإجرامي: نصت المادة 303مكرر04 على أن السلوك ينقسم إلى: صور السلوك و وسائل إركاب الجريمة .

[1]-عبود السراج، شرح قانون العقوبات، القسم العام، نظرية الجريمة، مطبوعات جامعة دمشق، دمشق، سوريا، 2007، ص118.

أ: **صور السلوك:** من خلال نص المادة 303 مكرر04 " يعد الاتجار بالأشخاص، تجنيد أو نقل أو تنقيل أو إيواء أو استقبال شخص أو أكثر..."، لا يشترط في الجاني أن يأتي بالأفعال كلها، بل يكفي أن يأتي بفعل واحد فقط من هذه الأفعال المجرمة.

أ.**1.تجنيد الأشخاص:** يقصد بتجنيد الأشخاص، تطويع الأشخاص واستخدامهم كسلعة قابلة للتداول بالمخالفة للقوانين والأعراف الدولية بغرض الاستغلال وجني الأرباح أيا كانت الوسائل المستخدمة مشروعة أو غير مشروعة.

أ.**2.نقل الأشخاص:** يقصد بعبارة نقل الأشخاص في معرض تطبيق أحكام هذا القانون" نقل الأشخاص من مكان إلى مكان آخر داخل الحدود الوطنية أو عبرها"[1]. ويتحقق فعل النقل المكون الركن المادي لجريمة الاتجار بالأشخاص عندما يتم هذا الفعل بوسائل وأساليب غير مشروعة وخاصة عند نقل الأطفال عبر الحدود.

أ.**3. تنقيل الأشخاص:** وقد يستغرب البعض من إيراد تعبير التنقيل في نص المادة طالما أشارت إلى تعبير أو فعل النقل، فإذا كان تعبير التنقيل يوحي بنقل الأشخاص جبرا وأن فعل النقل يتم باستخدام القوة أو التهديد باستخدامها أو الإكراه... مما يعني أنه ليست هناك حاجة لإيراد التنقيل طالما هناك النقل الإجباري[2].

[1]–منجد منال، المواجهة الجنائية لجرائم الاتجار بالأشخاص في القانون السوري (دراسة تحليلية)، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 28، العدد الثاني، دمشق، سوريا، 2012، ص 46.

[2]– على مسعودان، تجريم الاتجار بالأشخاص في القانون الجزائري، مذكرة الماستر تخصص قانون جنائي، كلية الحقوق العلوم السياسية، جامعة محمد خيضر، بسكرة، ص45.

لكن التمييز بين النقل والتنقيل يكمن في أن الأول يعني تحويل الأشخاص من مكان إلى مكان آخر، بينما يعني الثاني انتقال تحويل الملكية إلى شخص آخر مثلما أسلفنا سابقا.

أ.**4.استقبال الأشخاص:** قد يفيد الاستقبال للوهلة الأولى معنى الإيواء، لكن التعمق أكثر في فحوى الاستقبال يبين أنه يختلف عن الإيواء لأن الأخير يفترض إبقاء المجني عليه في مكان معين سواء أكان منزلا أو حتى فندقا، أما الاستقبال فقد لا يفيد هذا المعنى، فقد يتحقق فعل الاستقبال دون اشتراط إبقاء المجني عليه في مكان معين[1].

ب.وسائل ارتكاب الجريمة: بعد أن عدد المشرع الجزائري أفعال الاتجار بالأشخاص، اشترط أن تتم هذه الأفعال بوسائل معينة بحيث لو تم الفعل بغيرها لأصبح الفعل غير مجرم، وهذه الوسائل ذكرها المشرع على سبيل حصر نذكر بعض منها:

ب.1.التهديد بالقوة كوسيلة لارتكاب جريمة الاتجار بالأشخاص: يعتبر التهديد إحدى الوسائل المستخدمة للضغط على إرادة المجني عليه لدفعه لاقتراف جريمة محددة، فمثلا نجد أن الشخص الخاضع للتهديد كان في إمكانه الامتناع عن إتيان السلوك الإجرامي الذي أمر به، إذا قبل أن يتحمل الضرر الجسيم على نفسه أو على نفس غيره ولكنه يرتكب الجريمة

[1]– أكرم عمر دهام، جريمة الاتجار بالبشر دراسة مقارنة، دون ط، دار الكتب القانونية، مصر، 2011، ص94.

مضطرا لأنه يفقد القدرة على الاختيار فيقدم على ارتكاب الجريمة تجنبا الوقوع الخطر الجسيم الذي يحيط به[1].

ب.2.استعمال القوة كوسيلة لإركاب الجريمة: ويتم ذلك من خلال الضرب أو إحداث جروح أو تقييد حركة المجني عليه يدويا أو باستخدام حبال أو قيود حديدية، ويستوجب أن تكون الوسيلة هي قوة الجاني اليدوية أو استخدامه آلات أو أجهزة تؤثر على إرادة المجني عليه[2].

ب.3.استعمال أي شكل من أشكال الإكراه: الإكراه هو أحد وسائل شل الإرادة للشخص، وقد يكون ذلك عن طريق الإكراه المادي أو الإكراه المعنوي[3].

2.النتيجة الإجرامية: من خلال نص المادة 303 مكرر 4 ق.ع.ج نستنتج أن النتيجة الجرمية لجريمة الاتجار بالأشخاص هي تحقيق الاتجار بالأشخاص في حد ذاته، فالجماعة الإجرامية المنظمة عند قيامها بتجنيد الأشخاص أو نقلهم أو تنقيلهم أو إيوائهم أو استقبالهم تسعى إلى تحقيق النتيجة الجرمية وهي الاتجار بالأشخاص، ونصت المادة 303 مكرر13:"يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بنفس العقوبة المقررة للجريمة التامة"، وبالتالي فلا حاجة لتحقيق النتيجة الجرمية حتى تقوم جريمة الاتجار بالأشخاص.

[1]– مبارك هشام عبد العزيز، ماهية الاتجار بالبشر بالتطبيق القانون البحريني رقم01 لسنة2008 بشأن مكافحة الاتجار بالأشخاص، مركز الإعلام الأمني البحريني،2009،ص 5-7.

[2]– على مسعودان، مرجع نفسه، ص47.

[3]– نبيل صقر، مرجع نفسه، ص77.

3.العلاقة السببية: يشترط لتحقيق الكيان المادي للجريمة، وجود رابطة سببي بين الفعل والنتيجة، أي أن يكون الفعل أو السلوك الإجرامي هو سبب وقوع النتيجة[1]. بمعنى آخر أن تجنيد الأشخاص أو تنقيلهم من طرف الجناة هو السبب في تحقيق الاتجار بالأشخاص.

ثالثا: الركن المعنوي

يضيف المشرع الجزائري لأي جريمة ركنا معنويا، حيث لا يكفي أن يرتكب الشخص الجريمة، بل يجب أن يكون هناك قصدا في ارتكابها، فالركن المكون من النشاط الذهني والنفسي هو المعبر الحقيقي من الشخصية الإجرامية[2]، ويتمثل الركن المعنوي في الجرائم العمدية إلى العلم بعناصرها واردة متجهة إلى تحقيقها، وباعتبار جريمة الاتجار بالأشخاص من الجرائم العمدية، فيتمثل قصدها الجنائي في قيام الجاني بتجنيد المجني عليه أو نقله أو استقباله أو إيوائه بمحض إرادته وهو عالم بذلك، مدرك بنشاطه، ولا يكفي توافر القصد الجرمي العام أي مجرد اتجاه إرادة الجاني إلى مباشرة أية صورة من صور السلوك الذي يقوم به الركن المادي مع علمه بذلك، وإنما يجب فضلا عن ذلك توافر قصد جرمي خاص يتمثل في أن يبتغي الجاني من وراء سلوكه الإجرامي تحقيق غرض نهائي غير مشروع يتمثل في استغلال المجني عليه[3].

[1]–عبود السراج،المرجع سابق، ص119.

[2]– على مسعودان، المرجع سابق، ص 53.

[3]– عبود السراج، المرجع نفسه، ص119.

وقد أوضحت المادة 303 مكرر 4 من قانون العقوبات الجزائري مدلول الاستغلال بنصها: "... ويشمل الاستغلال استغلال دعارة الغير أو سائر أشكال الاستغلال الجنسي او استغلال الغير في التسول أو السخرة أو الخدمة كرها أو الاسترقاق أو الممارسات الشبيهة بالرق أو الاستعباد أو نزع الأعضاء".

الفرع الثالث

صور الاتجار عبر النطاق الشبكي الخاص

من بين أهم أشكال الاتجار التي تحدث داخل الموقع الشبكي الخاص هي التجارة الجنسية بالنساء، من أجل استغلالهم في أعمال المشبوهة أو من أجل إرضاء غرائز المرضى النفسيين، أو من أجل بيع أعضائهم، وغيرها من الأعمال التي تمارس على مستوى هذا النطاق الشبكي[1].

أولا: الاتجار الجنسي بالأطفال عن طريق البيع المؤقت

يحتوي الويب الظلم، على العديد من المواقع ذات الصلة بإيجار الأطفال جنسيا سيما – الفتيات– لمدة معينة وبشروط وأثمان محددة من التاجر نفسه. الذي قد يكون فردا أو تنظيما، كما قد يكون عمله منظما و معتادا في شكل تجارة يحترفها، أو عملا عارضا

[1]– نجد أن الاتجار الشبكي بالأطفال حسب منظمة "Thom قد وصل إلى أرقام هائلة ومخيفة. حيث صدر عن المنظمة نفسها، أن 63% من الأطفال الناجين من الاتجار بالبشر تم تسويقهم على الانترنت في مرحلة ما أثناء اتصالهم بالشبكة، وأكثر من 60% من الأشخاص المتاجر بهم عموما، لا يزيد سنهم عن 24 سنة ويوجهون إلى الاستغلال الجنسي. كما أنه سنة 2016 احتوى أكثر من 57 موقع شبكي على صور اعتداء جنسي على الأطفال.

ياستهويه بشكل متقطع أو لمرة واحدة فقط. وفي هذا الإطار، نجد العديد من الفتيات المعروضات للإيجار الشهري أو النصف الشهري، من قبل موقع "Slave Girls"، الذي يعمل في إطار منظم. حيث يضع الموقع مجموعة من الأحكام – الشروط والمزايا– التي تقوم على أساسها عملية الإيجار الجنسي. والمحددة في مدة الاستفادة والثمن المطلوب وطريقة طلب الإيجار، وفوائد الطالب أو الزبون. فتتمثل مدة الاستفادة على سبيل الحصر في إما 15 يوما أو 30 يوما. كما يعد ثمن الإيجار ثابتا لا يقبل المساومة من جهة ولا يتغير من فتاة إلى أخرى من جهة أخرى. والمقدر ب 1590 دولار أمريكي بالنسبة للإيجار لمدة 15 يوم، و2980 دولار أمريكي للإيجار لمدة 30 يوم. وأما طلب الإيجار فيكون عبر البريد الرقمي للموقع نفسه، بعد اختيار الفتاة المطلوبة الحاملة للمواصفات المرغوب فيها، مع ضرورة أن يكون للزبون بريد رقمي يعمل مواصفات الويب المظلم.

وأما فوائد الزبون، فالموقع يعرضها صراحة في جملة واحدة مفادها : "أن الفتاة ستستوفي جميع رغبات الزبون الجنسية طلية مدة الإيجار"[1].

ثانيا: الاتجار الجنسي بالأطفال عن طريق البيع

نجد العديد من المواقع التي لها علاقة بالبيع، وذلك لأغراض نفسية عند الأشخاص الذين يعانون من أمراض نفسية.

[1]– فؤاد جحيش، مرجع نفسه، ص7.

وما يحدث داخل الويب المظلم من استغلال للأطفال لا يمكن تصوره، بحيث يعد البيع من أبشع الجرائم التي يتعرض لها الطفل من اغتصاب على المباشر، تقطيعه، صور إباحية، وغيرها من الأفعال التي يعجز التعبير عنها من بشاعتها، وهذا تلبيتا لرغبة الزبون.

وفي هذا الإطار، نجد العديد من مواقع الويب المظلم، التي تعرض بيع الأطفال بغرض الاستغلال الجنسي. سيما ما يوفره موقع "Baby Heart"، الذي يعرض أطفالا في سنجد مبكرة، قد لا تزيد حتى عن الخمس سنوات. ومن خلاله ينشر الزبائن ورقة شخصية عن ميولاتهم الجنسية، ومواصفات الطفل المراد الحصول عليه[1].

وفي السياق نفسه، يعمل الكثير من الأشخاص والتنظيمات على احتجاز الأطفال صغار السن أقل من 10 سنوات، بعد شرائهم من العصابات المتخصصة في ذلك أو خطفهم المباشر. وهذا بغرض ممارسة الجنس عليهم، وبيع الصور والفيديوهات ذات الصلة إلى أشخاص يدفعون المال. وأبرز موقع متصل بذلك نجد المسمى ب "الغرفة الحمراء"RED ROOM"، التي وصفها عبد الرزاق طواهرية في كتابه شياطين بانكوك[2]. الذي يقوم القائم عليه بتقديم عروض مباشرة وغير مباشرة لتعذيب الأطفال وحتى الرضع، وفي أشكال لا يمكن تصورها، سيما المباشرة الجنسية للرضيع حتى وفاته. ويمكن للراغب في الاستفادة من خدمات الموقع، إما أن يشترك في البث المباشر للاعتداء الجنسي

[1]– فؤاد جحيش، المرجع نفسه، ص8.

[2]– للمزيد أنظر عبد الرزاق طواهرية، شياطين بانكوك.

كعضو متفرج بقيمة 2 بيت كوين، أو كعضو قائد بقيمة1 بيت كوين، أو كعضو ممتاز بقيمة5 بيت كوين. أو قد يكتفي الزبون بتحميل الفيديوهات السابقة بثمن معين، مع استفادة الأعضاء المعتادين من خصومات معتبرة[1].

المبحث الثاني

المعاملات الخاصة بالاتجار بالأشخاص عبر النطاق الشبكي الخاص

تختلف المعاملات التجارية الرقمية التي تحدث على مستوي "السيرفيس ويب" والتي تكون مشروعة كأصل عام، لكن ما يحدث داخل الدرك ويب مختلف تماما، بحيث كل المعاملات الغير مشروعة تحدث داخل هذا النطاق الخاص، وهذا راجع لخصوصية الحفاظ على الهوية المشفرة، وعليه سنقوم بدراسة المعاملات التجارية وهذا ضمن (المطلب الأول)، ثم معرفة العملة المتداولة البيت كوين وهذا في (المطلب الثاني).

المطلب الأول

المـــــــعاملات التـــــجارية

أظهرت الدراسات على مستوى "ويكيبيديا" لسنة 2015، أن التجارة التي تحدث على مستوى "Deep wep" هي تجارة المخدرات بكل أنواعها المرتبة الأولى بنسبة 15,4%، تم تليها المحلات الرقمية التي تبيع عملة التجارة بنسبة 6,2%، وبنسب اقل نجد تجارة الأسلحة وتجارة القمار والأفلام الإباحية....الخ.

[1]– فؤاد جحيش، المرجع نفسه، ص8.

وفي دراسة الحال سنقوم بدراسة الاتجار بالمخدرات (الفرع الأول)، تم الاتجار بالأسلحة (الفرع الثاني)، ثم الاتجار بالأشخاص (فرع ثالث).

الفرع الأول

الاتـــــجار بالمـــخدرات

تتعدد المعاملات التجارية داخل "الديب ويب"، وهذا راجع إلى نوعية الزبون والطلب الذي يرغب به، وكما اشرنا سابقا تعد تجارة المخدرات من بين أكبر العروض، إلا انه هناك اختلاف مابين المخدرات المادية والمتعارف عنها في أرض الواقع والمخدرات الرقمية، لهذا سنقوم (أولا) بدراسة المخدرات المادية، ثم (ثانيا) المخدرات الرقمية.

أولا: المخدرات المادية

تشمل المخدرات كل أنواع النبتات المخدرة(الأفيون، الهروين، الكوكايين،المورفين، القنب الهندي)، والمستحضرات الطبية المصنعة(المستحضرات الطبية، المواد الطيارة)، والتي تكون مخدرة.بحيث هناك عدة تعاريف منها اللغوية، والعلمية، والقانونية.

1.التعريف القانوني للمخدرات: عرفه القانون أنه:"هي كل مادة يترتب على تأولها إنهاك جسم الإنسان، وتؤثر على عقله حتى تكاد تذهب به، وتكون عادة الإدمان التي تحرمه القوانين الوضعية"[1].

[1]– نبيل صقر، جرائم المخدرات في التشريع الجزائري، دار الهدى، الجزائر،2006، ص 15.

ذهب رأي الفقه بشأن تعريف وتحديد المخدرات إلى القول، أن المشرع لم يضع تعريفا شاملا للمواد المخدرة، ثم بين هذه المواد علي سبيل الحصر، والمتضمن، ق.ص وترقيتها رقم 05/85 بالإضافة إلى ما يستجد من مواد مخدرة"[1].

2.الركن الشرعي لجريمة المخدرات: جرم المشرع الجزائري السلوكيات المتعلقة بالمخدرات المادية التقليدية المرتكبة في الوسط المادي الملموس، دون تلك التي تساعد في ارتكابها عناصر الوسط الرقمي، حيث لم يذكر الوسيلة الرقمية كوسيلة حديثة لارتكاب هذه الجرائم، لا صراحة ولا ضمني. إلا أنه جاء م.ج سنة 2009، بنص خاص في القانون الخاص أخلط بموجبه كل المفاهيم المتصلة بمبدأ الشرعية الجنائية، حيث جعل من كل جريمة تقليدية ترتكب عبر عناصر الوسط الرقمي أو يكون مسهلا لها، وكأنه جاء ليقرر مبدأ شرعية عام يطبق على كل النصوص التقليدية، وبالتالي وفق هذا النص، نقول أن السلوكيات محل الدراسات تعد مجرمة ومعاقب عليها[2].

يرى الأستاذ جحيش فؤاد:" أن مبدأ الشرعية الجنائية يجب أن يكون خاص وليس عام، فإذا ما أراد المشرع أن يجرم سلوكيات متصلة بالوسط الرقمي، يجب عليه التدخل

[1]- نصر الدين مبروك، جريمة المخدرات في ضوء القوانين والاتفاقيات الدولية، دار هومة، الجزائر، 2007، ص20.

[2]- جحيش فؤاد، التجارة الرقمية عبر "الدارك ويب" قصور في التجريم وعجز في المتابعة " دراسة تحليلية نقدية في ظل القانون الجزائري"، مجلة صوت القانون السياسية، العدد02، 2017، ص77.

- راجع: المادة 17 من القانون رقم 04-18، مؤرخ في 25ديسمبر 2004، المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بها، عدد83، الصادر بتاريخ 26ديسمبر 2004.

-راجع: المادة 02/أ، من القانون 04-09، مؤرخ في 05أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها،(ج ر)، عدد47، صادر بتاريخ 06أوت 2009.

بالتعديل أو التتميم في القسم الخاص بالسلوكيات محل التعديل أو التتميم، وأبرز دليل عدم اكتفاء المشرع بالشرعية العامة الواردة بالمادة 02/أ بخصوص الجرائم الموصوفة بالأفعال الإرهابية، حيث تدخل سنة 2016، وتمم قانون العقوبات بالمادة 87مكرر 11 التي نص في أخرها على أنه، يعاقب المشرع على استخدام تكنولوجيات الإعلام الاتصال لارتكاب الأفعال المذكورة في المادة نفسها"[1].

ثانيا: المخدرات الرقمية.[2]

تختلف المخدرات الرقمية عن المخدرات المادية، كون أن هذه الأخيرة تكون بالطرق التقليدية (بيع_شراء)، لكن المخدرات الرقمية عبارة عن موجات صوتية وفيديوهات تؤثر على العقل البشري.

1.تعريف المخدرات الرقمية: هناك نوعين من المخدرات الرقمية، هناك النوع الأول والذي يعتبر جديد والمتمثل في المؤشرات الصوتية والتي تكون عن طريق الموسيقى، أما النوع الثاني والتي تكون تقليدية وتباع على مستوى "deep wep".

[1]– راجع المادة 02، من القانون رقم 16–02 ، مؤرخة في 19جوان 2016، يتمم الأمر رقم 66–156 المتضمن قانون العقوبات، (ج ر)، عدد 37، صادر بتاريخ 22جوان 2016.

[2]– في عام 1839 اكتشف العالم الفيزيائي Heinrich Wilhelm Dove أنه إذا سلطت ترددين مختلفين قليلاً عن بعضهما لكل اذن، فإن المستمع سيدرك صوت نبض سريع. سميت هذه الظاهرة بـ .binaural beats استخدمت هذه الآلية لأول مرة عام 1970 من أجل علاج بعض المرضى النفسيين لاسيما الاكتئاب الخفيف والقلق وذلك عند رفضهم العلاج الدوائي حيث كان يتم تعريض الدماغ إلى تذبذبات كهرومغناطيسية تؤدي لفرز مواد منشطة كالدوبامين و بيتا أندروفين بالتالي تسريع معدلات التعلم وتحسين دورة النوم وتخفيف الآلام وإعطاء احساس بالراحة والتحسن. واعتبر موقع Psychology Today أنه يمكن استخدام هذه التقنية لعلاج القلق

أ.**المخدرات الصوتية:** كل نوع من أنواع المخدرات، أي كل نوع من الأمواج الصوتية والترددات تقوم باستهداف نمط معين من النشاط الدماغي، ويتعلق الأمر بمدة التعرض و الظروف المواتية له وأحياناً يتم الاستعانة بالبصر لزيادة تحفيز الدماغ.

وعرفت أيضا:" هي ذبذبات تنساب إلى المخ عبر الأذن على شكل نغمات تؤثر على الذبذبات الطبيعية للمخ مدخلة المتلقي إلى عالم أخر من الاسترخاء والهدوء إلى حد يصل لتأثير المهدئات الكيميائية"[1].

أ.**1. كيفية عمل المخدرات الرقمية:** كما ذكرنا سابقا بان المخدرات الرقمية هي ملفات صوتية وأحياناً تترافق مع مواد بصرية وأشكال وألوان تتحرك وتتغير وفق معدل مدروس تمت هندستها لتخدع الدماغ عن طريق بث أمواج صوتية مختلفة التردد بشكل بسيط لكل أذن. ولأن هذه الأمواج الصوتية غير مألوفة يعمل الدماغ على توحيد الترددات من الأذنين للوصول إلى مستوى واحد بالتالي يصبح كهربائياً غير مستقر، وحسب نوع الاختلاف في كهربائية الدماغ يتم الوصول لإحساس معين يحاكي إحساس أحد أنواع المخدرات أو المشاعر التي تود الوصول إليها كالنشوة[2].

1-موقع wiki، المخدرات الرقمية، دار الشفاء للطب النفسي وعلاج الإدمان، تاريخ النشر 25فبراير2017،تاريخ الاطلاع 22ماي 2019، الرابطة: http://www.addiction-wiki.com 2019

[2]-محمد حبش، موقع tech-wd، ،المخدرات الرقمية، تاريخ النشر15 نوفمبر 2014، تاريخ الاطلاع 22ماي2019، رابطة النشر: www.tech-wd.com/wd/2014/11/15 أنظر كذلك، العربي الجديد – الرأي– BBC – CNN – الإمارات اليوم NOW – اللبنانية – الحياة.

تعمل المخدرات الرقمية على تزويد السماعات بأصوات تشبه الذبذبات والأصوات المشوشة، وتكون قوة الصوت أقل من 1000 إلى 1500 هيرتز كي تسمع منها الدقات[1]. الجانب المخدر من هذه النغمات فيكون عبر تزويد طرفي السماعة بدرجتين مختلفتين من الترددات الصوتية ويكون الفارق ضئيلاً يقدر من 30 هيرتز لذلك ينصح المروجين لها أن تكون السماعات ذات جودة عالية ومن نوع "ستاريو" كي تحقق أعلى درجات الدقة والتركيز، فالفارق بين طرفي السماعة هو الذي يحدد حجم الجرعة، فكلما زاد الفارق زادت الجرعة. ومن الجدير بالذكر أن هناك موقع "deep wep" متخصصة يقوم ببيع هذه النغمات، ولا توجد رقابة رسمية عليها في الوقت الحالي، حيث يتم ترويجها عبر مواقع التواصل الاجتماعي أيضاً مقابل القليل من الدولارات. أنظر الصورة.

ب- المخدرات التقليدية التي تباع على مستوى deep wep

تختلف أنواع المخدرات والعقاقير التي يتم الاتجار بها في "الديب ويب"، التبغ المهرّب والمحظور قانونياً، والقنّب والمنشّطات، والكوكايين وغيرها. وهناك أيضاً سوق"طريق الحرير" "The silk road"، وهي سوق سوداء اشتهرت بتجارة المخدرات لصاحبها روس أولبريخت Ross Ulbricht والذي خصص هذا الموقع لتجارة المخدرات بنسبة 70%،[2] أنظر الصورة.

[1]- محمد حبش، مرجع سابق.

[2]- في 27 يناير 2011 أنشأ روس أولبريخت موقع طريق الحرير والذي كان عبارة عن موقع تجارة إليكترونية ولكن ليس بالمعنى المألوف لمثل هذا النوع من المواقع ولكن كان موقع بروس يتاجر في أي شيء غير مشروع بداية من

تم غلق هذا الموقع بعد البحث والتحري من طرف مكتب التحقيقات الفدرالي الأمريكي سنة 2013. ووضعت عليها صورة المكتب بدل صورة الموقع، أنظر الصورة.

الفرع الثاني

الاتــجار بالأسلحـــة

من المتعارف عنه إن تجارة الأسلحة من التاجرات المشروعة ولكن في حدود التي يسمح بها القانون، إلا أنه ومع التطور التكنولوجي ظهر نوع جديد من الأسلحة والتي تسمى بالأسلحة الرقمية والتي تباع على مستوى "ألدارك ويب". وعليه سنقوم بمعرفة الأسلحة التقليدية والتي تباع في أسواق "ألدارك ويب" هذا (أولا)، ثم معرفة الأسلحة الرقمية(ثانيا).

أولا: الأسلحة التقليدية

المشرع الجزائري لم يعرف الأسلحة بشكل صريح وإنما أشار إليها ضمنيا من خلال مرسوم تنفيذي رقم98- 96[1] يحدد كيفية تطبيق الأمر رقم97-06 والمتعلق بالعتاد الحربي والأسلحة والذخيرة. بحيث المادة الأولى تضمنت:" يحظر عبر كامل التراب الوطني، مع مراعاة الأحكام المقررة في هذا الأمر، صناعة العتاد الحربي و الأسلحة

تجارة الأسلحة وجميع أنواع المخدرات والعقارات مرورًا بتجارة الجنس والأعضاء وتجارة الوثائق الشخصية المزورة أو رخص القيادة غير الحقيقة وبطاقات الائتمان والسلع المسروقة والبرمجيات القرصنة وغسيل الأموال وغيرها، كما بلغ عدد المنتجات المتاحة للشراء على الموقع تقريبا 10 ألاف سلعة حوالي 70% منها مخدرات.

[1]- 98-96 مؤرخ في9 ذي القعدة 1418 هـ الموافق18مارس1998.يحدد كفية تطبيق الأمر رقم 97-06المؤرخ في 12 رمضان 1417 الموافق 21 يناير 1997.

والذخيرة كما هي محددة و مصنفة في المواد 2 و 3 و 4 أدناه، كما يحظر استيراد ذلك و تصديره، والمتاجرة به واقتناؤه و حيازته، و حمله، و نقله"[1].

وعليه يمكن تعريف الأسلحة التقليدية بأنها:" كل أداة تستخدم من أجل الدفاع عن النفس أو العكس"[2]

1.تصنيف العتاد الحربي والأسلحة والذخيرة: إن تصنيف العتاد الحربي والأسلحة جاء من خلال المادة 3 من المرسوم 97-06 أما المادة 4 جاءت كاستثناء للعتاد الذي لا يصنف حربيا. أما المادة 3:" يعتبر عتادا حربيا و يصنف بهذا الشكل، كل الأسلحة و عناصر الأسلحة و الذخيرة و عناصر الذخيرة و كذا كل الوسائل المادية المعدة لذلك و/أو الموجهة للحرب البرية أو الجوية أو البحرية". و يعتبر عتادا حربيا كل سلاح يمكنه قذف الذخيرة المصنفة "عتادا حربيا"، و كذا كل الذخيرة التي يمكن قذفها بسلاح مصنف عتادا حربيا. كما يصنف العتاد الحربي في الأصناف 1،2،3. أما المادة 4:" تصنف الأسلحة و عناصرها والذخيرة وعناصرها التي لا تعتبر عتادا حربيا في الأصناف 4،5،6،7،8.

2.مشروعية التجارة بالأسلحة: إن تجارة السلاح لا يكون إلا برخصة وهذا ما أقرته جل التشريعات والمعاهدات الدولية، من بينها معاهدة الأمم المتحدة لتجارة الأسلحة لسنة 2013، كما أن المشرع الجزائري من خلال الأمر 97-06 جرم فعل تجارة الأسلة التي

[1]- بختيل عبد الرحمن، التنظيم الدولي للأسلحة الخفيفة، مذكرة من أجل الحصول على شهادة الماجستير في الحقوق، فرع القانون الدولي والعلاقات الدولية، كلية الحقوق بن عكنون، جامعة الجزائر1، الجزائر، ص 26.

[2]- مرجع نفسه، ص 24.

تكون بدون رخصة من خلال المادة 26:" يعاقب بالسجن المؤبد كل من صنع العتاد الحربي المشار إليه في الأصناف1،2،3. أو استورده أو صدره أو تاجر به بدون رخصة من السلطة المؤهلة قانونا".

من خلال نص المادة المبينة أعلاه فإن المشرع الجزائر عاقبة على فعل التجارة للأصناف 1،2،3 بالنسبة للأشخاص(شخص طبيعي أو معنوي) الذين لا يملكون رخصة من السلطة المؤهلة قانونا، والملاحظ أن المشرع الجزائري من خلال الباب الثاني الفصل الأول والفصل الثاني تحدث عن التجارة التقليدية في بيع السلاح.

ثانيا: الأسلحة الرقمية

إن الأسلحة الرقمية نوع جديد من الأسلحة الفتاكة والتي يصعب التحكم فيها والتجارة بها لا تحتاج إلى نقل أو تفكيك مثل الأسلحة التقليدية إلى أنه سوف نتطرق إلى معرفة المتاجرة بالأسلحة التقليدية عبر النطاق الشبكي الخاص، ثم التطرق كذلك إلى الأسلحة الرقمية والمتمثلة في الجريمة السبيرينة[1].

1.جرائم الاتجار بالأسلحة عبر deep wep: يأتي السلاح بأنواعه المختلفة في المرتبة الثانية على مواقع الإنترنت المظلم ويتم تصنيفه داخل قوائم متعددة بداية من المسدسات الصغيرة إلى الكلاشنكوف والبنادق الآلية ولقنابل الصغيرة وأجهزة المفرقعات الذكية، وليس هذا فقط بل يوجد صفحات لبيع الذخيرة بأنواعها وأشكالها، ووفقا لتقرير نشر مؤخرا على موقع

[1]– الأسلحة التقليدية، معاهدة تجارة الأسلحة/https://www.un.org/disarmament/ar

techinsider البريطاني فالإنترنت المظلم يساعد في ترويج السلاح بين المواطنين خاصة في الدول التي تفرض قواعد صارمة على بيع وامتلاك سلاح مثل فرنسا وغيرها، لذلك أصبح المواطنون يلجئون لتلك الموقع التي تضم عشرات الآلاف من الصفحات الخاصة بالسلاح، وكل ما على المستخدم فعله الدخول والبحث والدفع عن طريق زر الشراء، وتم توريط أكثر من موقع على شبكة الإنترنت المظلم في الهجمات الإرهابية التي تحدث حيث يقوم المتطرفون بالحصول على السلاح من خلال المواقع سرا دون أن يعرف أحد هويته مطلقا، وخلال هجمات باريس أغلق عدد من المواقع على رأسها Nucleus القسم الخاص بالسلاح خوفا من التتبع، وأشهر الأسلحة التي يتم بيعها عبر مواقع الإنترنت المظلم[1] هو السلاح المفضل لي داعش مثل "كلاشنكوف "AK-47s وهو متاح على الموقع السري المشفر على شبكة الإنترنت المظلم بسعر 1500 يورو، والسلاح لا يباع بكميات كبيرة على مواقع الإنترنت المظلم بل يكون قطعا على عكس المخدرات وهذا بسبب صعوبة التوصيل والنقل.

بالنظر إلى هذه الجرائم وهذه المنظومة المعلوماتية المشفرة والتي تمارس من خلالها الأعمال الغير مشروعة والنظر إلى نص المادة 2/أ من القانون 09-04 والتي تنص على:"جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون

[1]- إسراء حسني، الإنترنت المظلم".. السوق الأول لتجارة المخدرات والسلاح سرا على الإنترنت.. اقتحام عقول الشباب وتوصيل الممنوعات لباب المنزل.. ولا عزاء للحكومات، تاريخ النشر:21 جانفي2016، الرابطة:
2549805.https://www.youm7.com/story/2016/1/21/-

العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"[1].

فإن هذا النص يعتبر الأصل العام في التجريم، لكن احتراما لمبدأ الشرعية الجنائية الخاص يقيد العام وكما ذكرنا سابقا في الجريمة الموصوفة بأنها عمل إرهابي وضع لها قانون خاص، وعليه وجب على المشرع الجزائري وضع قانون يعدل أو يتمم 97-06[2] المتعلق بالعتاد الحربي والأسلحة والذخيرة، أو يعدل القانون 09-04[3].

2.الجريمة السيبرية: هي جريمة رقمية لا تحتاج إلى أسلحة تقليدية، وإنما تقوم على برمجيات خاصة يصعب العمل عليها ومن بينها[4]:

أ.مواقع القرصنة: توجد مواقع مخصصة للهكرز والقرصنة الاحترافية، في هذه المواقع يتم الاختراق مقابل مبالغ مالية معينة من المال. تباع أيضا برامج ودورات الاختراق النادرة والتي لا يعرف احد شيئاً عنها. تعتبر هذه المواقع من المواقع الخطرة لأن أصحابها

[1]– إيهاب شوقي، الحرب السيبرية... حرب المستقبل المفزعة، تاريخ النشر 19 فبراير 2015، تاريخ الإطلاع 05 جوان 2019، رابطة النشر: https://www.hespress.com

[2]- راجع الأمر 97-06، سالف الذكر.

[3]- راجع الأمر 09-04، سالف الذكر.

[4]– الحسين أخدوش، الأسلحة الرقمية من خيال العلم إلى واقع الحرب السيبرية، مقال منشور بتاريخ: 25مارس2019، تاريخ الإطلاع 01 جوان 2019، رابطة المقال: https://www.hespress.com/writers/426460.html

والعاملين فيها هم من عمالقة الاختراق ولا يعتبر التعامل معهم أمر سهل إذ قد يتم اختراقك بمجرد دخولك احد مواقعهم أو تحميل شيء من محتوى مواقعهم[1].

ب:الحوسبة الساحبة computing cloud: تتم عن طريق وضع برامج المؤذية malware في ضيافة الشركات ذات السمعة النظيفة، لا يعاني الهاكرز من أي اعتراض لتداولاتهم من جانب الأنظمة الأمنية، أشارت دراسات حديثة أن 16% من البرمجيات المؤذية في العالم وقنوات توزع الهجمات الالكترونية بدأت من سحابة أمازون[2].

الفرع الثالث

الاتـــجار بالأشخـــاص

إن جريمة الاتجار بالأشخاص من الجرائم التي تشهد رواجا كبيرا على موقع "الدارك ويب" خاصة الأطفال وهذا ما تم دراسته في المطلب الثاني من هذا الفصل، أما ألان سندرس كيف تمارس هذه التجارة.

أولا: تجارة البشر

تتعدد أشكال وأنواع الاتجار بالبشر، والنوع الذي يعود إلى قديم الأزل هو بيع أفراد للخدمة، وبعد تطور البشرية جرمت القوانين الدولية الاتجار بالبشر تحت أي بند، ولذلك لجأ نخاسي العصر الجديد إلى الشبكة المظلمة لبيع النساء والأطفال.

[1] – شروق صباري، من تجارة الأطفال إلى أكل لحوم البشر.. الإنترنت الخفي.. جنة الجريمة، تاريخ النشر 2017/08/09، الرابطة: -https://www.mobtada.com/details/637219

[2] – الحسين أخدوش، مرجع نفسه.

وهناك نوع آخر من الاتجار بالبشر، وهو تجارة الأعضاء البشرية التي تكون مسروقة أو تم الحصول عليها بطرق غير شرعية[1].

ثانيا: بث الأفلام الجنسية للأطفال

يعانى عدد كبير من الناس أمراضًا واضطرابات وهوسًا جنسيًا تجعلهم يبحثون عن المتعة بطرق غير مشروعة وغير طبيعية، مثل مشاهدة الجنس مع الأطفال، بل ممارسته، وهو أمر غير متاح بسهولة، نظرًا لملاحقة مقدمها قانونيًا من الحكومات ومن الجمعيات المهتمة بشئون الأطفال، بالإضافة إلى تقديم الأفلام الجنسية التي تعتمد على الإيذاء البدني والتعذيب.

ثالثا: الغرفة الحمراء

وهى غرف دردشة بالفيديو يتم فيها عرض أعمال تعذيب وذبح أشخاص حقيقيين أمام الكاميرا ليشاهدها أصحاب الميول من المنزل مقابل الدفع «البيت كوين»، ويشكك عدد من الناس في وجود الغرف الحمراء من عدمه في الواقع، حيث إن معظم الشهود على وجودها ليس لديهم أدلة أو صور منها إنما مجرد روايات يحكونها من ذاكرتهم ويرددها الآخرون[2].

[1]– مقال منشور عبر الرابطة: https://www.hopeeg.com/digital-drugs/

[2]– عبد الرزاق طواهرية، مرجع سابق، ص 28.

رابعا: التجارب على البشر

هناك عدد من المواقع الغامضة تديرها مجموعة تخطف البشر، وتدعى أنها تقدم فيديوهات لتجارب حقيقية تجرى على البشر للتسلية فقط، وتشمل تلك التجارب التجويع والتعرض للإشعاع وحقن المواد الكيميائية في الجسم، ضمن أشياء أخرى كثيرة.

خامسا: ألعاب الموت

هناك بعض الألعاب المظلمة الخطيرة التي تجدها على" الديب ويب"، مثل «تحدى انتحار الحيتان الزرقاء» التي ظهرت على الشبكة العميقة ثم انتشرت مؤخرًا على الشبكة السطحية، وارتبطت ارتباطًا وثيقًا بحوالي 130 حالة وفاة للمراهقين في جميع أنحاء. وحول إمكانية حجب الشبكة العميقة عن الجمهور، قال الدكتور توفيق إسماعيل، الخبير التكنولوجي، إن السيطرة على الشبكة العميقة ممكنًا، لكنه لا يصل إلى نسبة 100%، وذلك يتم من خلال استخدام الحائط الناري " fire Wall". وأضاف «إسماعيل» أن شركات الإنترنت تستطيع جعل السواد الأعظم من المستخدمين غير قادرين على الولوج إلى الشبكة العميقة، ولكن لا يمكن التعميم والقول إنه سيتم منع جميع المستخدمين لان أي فرد يستطيع أن يستخدم الـ proxy الذي يتيح للمستخدم الدخول إلى شبكة الإنترنت من IP خارج الدولة، وحجب البروكسى ليس مستحيلًا، ولكنه يحتاج حائطًا ناريًا أكثر تطورًا، وهو غير متاح في كثير من الأماكن لارتفاع تكاليف تلك النسخ[1].

[1]–**محمد نور**،"deep wep" الوجه القبيح لـ"الإنترنت، تاريخ النشر 07جوان2018، رابطة https://www.albawabhnews.com/3179834

المطلب الثاني

العملة المتداولة (البت كوين)

من أجل القيام بالإعمال التجارية داخل "الدارك ويب" يجب أن تتوفر نوع من العملة التي تتناسب مع الطابع المشفر لهذه المنظومة.

قام اخصاء البرمجيات بإنشاء عملة افتراضية تسمي"البيت كوين" والتي لها خاصية عدم إمكانية تتبع هذه العملة، وعلي هذا سنقوم بتعريف "البت كوين" (الفرع الأول)، ثم معرفة سعر صرف "البت كوين" أمام العملة الجزائرية (الفرع الثاني)، ثم بعد ذلك موقف المشرع الجزائري من عملة "البيت تكوين" (فرع ثالث).

الفرع الأول

تــعريف البيت كويـــن.[1]

يعرف القانون النقدي والمالي العملات المشفرة بأنها "أي أداة تحتوي على الشكل العددي لوحدات القيمة غير النقدية التي يمكن الاحتفاظ بها أو نقلها في غرض الحصول على سلعة أو خدمة ولكن لا يمثل مطالبة على المصدر.

[1]– أنشئت في عام 2009 من قبل مجموعة من علماء الكمبيوتر باستخدام الاسم المستعار "ساتوشي ناكاموتو" ، أصبح البيتكوين تدريجيا ظاهرة نقدية دولية حقيقية. خصوصية هذا النوع من العملات هو أن سعره مستقل عن أي بنك مركزي، إنه عالمي، خالي من الإطار القانوني ولا يعتمد على أي بلد بخلاف العملات النقدية الأخرى. يتم التحقق من جميع المعاملات من قبل "العقد" للشبكة، أي أجهزة الكمبيوتر لمستخدمي cryptocurrency. بفضل هذا النظام، الذي يعتمد على تقنية "blockchain" المزعومة، يتم تأمين مدفوعات البيتكوين.

2– Art L. 561-2 du Code monétaire et financier

أولا: المقصود بالبيت كوين.

للبتكوين دلالتين الأولى دلالة مالية والثانية دلالة تقنية.

1.من الناحية المالية: تعتبر"البيت كوين" عملة معماة حيث يتم الاحتفاظ بالأرصدة باستخدام المفاتيح عامة وخاصة وهي سلاسل طويلة من الأرقام والحروف المرتبطة بخوارزمية التشفير الرياضية التي تستخدم لإنشائها، والمفتاح العام (مماثل لرقم الحساب البنكي) وهو العنوان الذي ينشر على مستوى العالم حيث يمكن للآخرين إرسال عملات "البيت كوين" الخاصة بهم إليه، أما المفتاح الخاص (يشبه رقم التعريف الشخصي لأجهزة الصراف الآلي) فإنه تم صنعه لكي يكون سري، ويستخدم فقط للتحكم في إرسال عملة "البيت كوين".

وتجدر الإشارة أنه لا يوجد وجود فيزيائي "للبيت كوين"، حيث يتم حفظ الرصيد في دفتر الأستاذ العام وذلك جنبا إلى جنب مع جميع معاملات" البيت كوين"، ويتم التحقق منها من خلال كميات ضخمة من قوة الحوسبة، وعلاوة على أن "البيت كوين" لا يتم إصداره أو دعمه من قبل أي بنوك أو حكومات ولا أيضا الأشخاص الذين يقدرون قيمة "البيت كوين" كسلعة، وعلى الرغم من أنها ليست عملة قانونية إلا أن"البيت كوين" انتشرت بشكل واسع، وكذلك أدت إلى إطلاق العملات الافتراضية الأخرى التي يشار إليها مجتمعة باسم "ألتك وينز".

2.الناحية التقنية: من الناحية التقنية، فإن كل قطعة "بيت كوين" نقدية هي: عبارة عن شفرة تم توليدها وفق خوارزمية التشفير الشهيرة، والقوية SHA-256 بصيغة ست عشرية، ويتم تخزين قطع "بيت كوين" الخاصة بالمستخدم في ملف خاص يُدعى بالمحفظة "Wallet"، يحتفظ هذا الملف كذلك بكل عنوان قام المستخدم بإرسال مبالغ إليه أو استقبالها منه، يوجد لكل مستخدم عنوان "البيت كوين"، يمكن تشبيهه بعنوان البريد الإلكتروني لكنه ليس كذلك، بل هو عبارة عن شفرة معينة تميز كل مستخدم، لكنها لا يمكن أن تشير إلى هويته الحقيقية، تقوم "البيت كوين" على تقنيات مفتوحة المصدر بشكل كامل، وبالتالي لا يوجد ما هو مخفي أو مجهول في أسلوب عملها[1].

ثانيا: خصائص البيت كوين.[2]

من مميزات عملة "البيت كوين" هي سهولة الدفع من خلالها والسماح لعملة "البت كوين" لمستخدميها أن يتحكموا في أموالهم بحرية كاملة، فيمكن إرسال واستقبال الأموال دون أي قيود لذلك أصبحت عملة "البت كوين" طريقة سهلة للتسوق في الكثير من المتاجر الإلكترونية التي تقبل الدفع الإلكتروني، وأيضا تستخدم في بعض الشركات التي تدعم تلك العملة، من أمثلة هذه الشركات شركة مايكروسوفت التي كانت تدعم تلك العملة في عام 2014، ولكنها ألغت التعامل "بالبت كوين" في عام 2016 دون ذكر السبب.

[1] – العملات الإلكترونية ماهي؟وكيف يتم شرائها أو تداولها؟، تاريخ النشر 06جوان2018، الرابطة: www.arincen.com.

[2] –https://www.islamicbitcoin.com/مميزات-عملة-البيتكوين.

1.السرعة والرسوم المنخفضة: عندما تتم عملية شراء بين شخص وتاجر تكون الحاجة إلى وسيط لنقل الأموال، وهذا الوسيط يقوم بخصم نسبة من المال, مع وجود عملة "البت كوين" تتم هذه العملية بدون وسيط وتسمى (P2P).

2.سرية البيت كوين: تتمتع عملة "البت كوين" بقدر عالي من السرية حيث أن لا يمكن تتبعها أبدا وذلك ما أدى ألي اعتماد عملة "البيت كوين" من مستخدمي الانترنت المجهول (Deep Web) في المتاجر التي تبيع المنتجات المحظورة.

3.انتشار البت كوين حول العالم: لا ترتبط عملة "البت كوين" بموقع جغرافي فيمكن اعتبارها عملة محليه لكل الدول، ومع ذلك تأخر كثيرا انتشارها في الدول العربية حتى عام 2016 تغير الآمر وأصبح الكثير من الدول العربية تستحوذ بعض التعاملات المالية عبر الانترنت.

4. بيت كوين عملة لا مركزية: بيت كوين لا تتبع أي دولة ولا بنك ولا أي هيئة تنظيمية، فهي عملة مشفرة لا يمكن تتبعها بسهولة لأنها لا تملك أرقام متسلسلة، ويتم بيعها وشراءها مباشرة بين البائع والمشترى بدون وجود أي وسيط.

5.بيت كوين عملة معماة: تعتمد عملة "البيت كوين" تماما على التشفير من جميع الجوانب، وهى العملة الأولى في العالم الرقمي التي تعتمد التشفير وهي أيضا مفتوحة المصدر فيمكن التعديل عليها وإدخال أكواد جديدة يمكن من خلالها صنع عملات أخرى.

ثالثا: مخاطر التعامل بالبيت كوين

رغم النجاح الذي عرفته هذه العملة، فإن بعض التقارير الصادرة مؤخرا حذرت من مخاطر استخدامها، بسبب ما تعرضت له من تقلبات كبيرة في قيمتها في فترة قصيرة حيث يصعب مراقبتها ومتابعتها، وتأمين أجهزة المتعاملين بها، وعدم قدرة أية جهة التحكم والسيطرة على سوقها.

وحذر تقرير لبنك التسويات الدولي "بي.آي.إس" في سويسرا من أن العملات الرقمية خطرة وضارة وعديمة القيمة، وخصص التقرير السنوي للبنك المعروف بأنه البنك المركزي العالمي للبنوك المركزية الوطنية، فصلا كاملا عن العملات الرقمية وخطورتها على النظام المالي العالمي، وعلى ثروات الأفراد، وأوضح أن العملات الرقمية تصبح بلا قيمة من خلال عمليات الغش أو القرصنة، وغالبا ما يتم التداول فيها عبر صناديق وهمية تودي بثروة المواطنين بعيدا عن قواعد التعامل الرسمية.

وبالنظر إلى مميزاتها مقابل كم المخاطر الناتجة عنها، فإنه يبقى من المستبعد تهديد العملات الرقمية لنظيرتها الرسمية كالدولار أو اليورو في الوقت الحالي، غير أن هذا لا يمنع ضرورة السعي لوضع تشريعات وقوانين لتنظيم عملها وحماية حقوق المتعاملين بها[1].

[1] – أحمد بوخريص، العملة الافتراضية خصائصها ومخاطر التعامل بها،المركز الديمقراطي العربي، تاريخ النشر 20ديسمبر 2018، الرابطة: https://democraticac.de/?p=58064

الفرع الثاني

سعر صرف "البت كوين" أمام العملة الجزائرية

تعتبر "البيت كوين" واحدة من العملات الرقمية الأولى التي تستخدم تقنية الند للند لتسهيل المدفوعات الفورية، ويعرف الأفراد المستقلين والشركات التي تملك القدرة على القوة الحاسوبية الحاكمة ويشاركون في شبكة "البيت كوين بـ "المنقبين"، ويتم تحفيزهم من خلال المكافآت (بإطلاق بيت كوين جديد) ورسوم الصفقات المدفوعة في "البيت كوين"، ويمكن اعتبار هؤلاء المنقبين بمثابة السلطة اللامركزية التي تفرض مصداقية شبكة "البيت كوين"، ولقد تم إطلاق "البيت كوين" الجديد للمنقبين بأسعار ثابتة لكن انخفضت النسبة بشكل دوري، بحيث يبلغ إجمالي عرض "البيت كوين" إلى ما يقرب من 21 مليون.

يعتبر تعدين "البيت كوين" عملية يقوم من خلالها إطلاق "البيت كوين" ليدخل في عملية التداول، وبشكل أساسي، ينطوي على حل لغز صعب حسابيا لاكتشاف كتلة جديدة والتي يتم إضافتها إلى سلسلة الكتل، واستقبال جائزة في شكل عدد قليل من "البيت كوين"، وكانت مكافأة الكتل 50 "بيت كوين" جديد في عام 2009 ، والتي تقل كل أربع سنوات، وكلما تم إنشاء "بيت كوين" أكثر وأكثر، كلما كانت عملية التعدين أصعب، حيث تبدأ صعوبة التعدين عند 1.0 مع ظهور "البيت كوين" لأول مرة عام 2009، وفي نهاية العام كانت فقط 1.18، وبحلول عام 2017، تخطت صعوبة التعدين 4.24 مليار،

وذات يوم، كانت أجهزة الكمبيوتر العادية تفي لإجراء عملية التعدين، ولكن الآن، للتغلب على مستوى الصعوبة، يجب على المنقبين استخدام أجهزة أسرع مثل تطبيقات الدوائر المتكاملة المحددة (ASIC)، ووحدات معالجة أكثر تقدما مثل وحدات معالجة الرسومات (GPUs).[1]

أولا: البيت كوين أمام عملة الدولار الأمريكي

1.دراسة تحليلية لسعر البيت كوين ل 24ماي 2019

أزواج العملاتBTC/USD

- **تحليل المنحنى:**

هبطت أسواق بالتكوين خلال معظم جلسة يوم الخميس لكنها وجدت المشترين في الأسفل لتشكل مطرقة جميلة المظهر. يعمل هذا على تعزيز الفكرة التي لدي في هذا السوق والتي تشير إلى وجود الكثير من المشترين الذين يتطلعون إلى الاستفادة من

[1] -https://trading-secrets.guru/البيتكوين-مصطلحات-bitcoin

القيمة. بالنظر إلى هذا الرسم البياني، من الواضح أن هناك الكثير من المقاومة عند المستوى 8250$، ولكن من الواضح أيضًا أن المشترين مستعدون للتدخل والتقاط البتكوين في كل مرة تنخفض فيها.

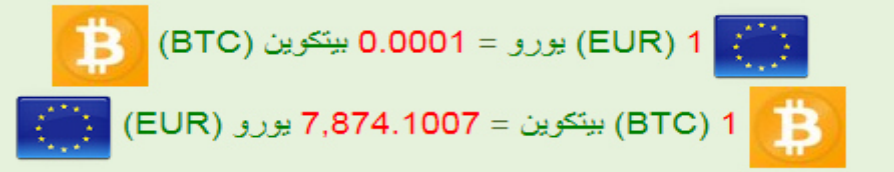
هذا أمر منطقي بطبيعة الحال بالنظر إلى أن السوق قد اخترق حاجز مقاومة رئيسي على شكل المستوى 6000$ في السابق، ثم أنطلق مباشرة. يعني هذا بالطبع أنه قد تمت السيطرة على حاجز مقاومة رئيسي، ومن المحتمل أن يؤدي اختراق هذه المنطقة إلى جلب المزيد من الأموال إلى هذا السوق، وأعتقد أن هذه مسألة وقت فقط قبل أن نستمر في الارتفاع. على المدى القصير، من المحتمل جدًا أن نحتاج إلى إيجاد زخم كافٍ للتحرك أخيرًا في الاتجاه الصعودي، وفي النهاية أعتقد أن التهدئة قليلاً في هذه المنطقة أمر منطقي. حقيقة قيامنا بتشكيل هذه الشمعة تخبرني أن هناك اهتمامًا كبيرًا بالشراء أكثر من الاهتمام بالبيع، لذلك فهي علامة جيدة جدًا.

المستوى 7000 دولار تحته دعم كبير، لذلك إذا ما هبطنا إلى ما دون ذلك المستوى، فعندئذ أعتقد أننا قد نشعر بالراحة نحو المستوى 6000 دولار وهو بصراحة أكثر جاذبية. طالما بقينا فوق المستوى 6000 دولار. إذا تمكنا من الخروج فوق المستوى 8250$،

فمن المحتمل جدًا أن نذهب إلى المستوى 10 آلاف دولار. هذا بالطبع سيكون مجال الاهتمام الشديد.[1]

ثانيا: البيت كوين أمام عملة أورو

أ- محول وحاسبة أسعار العملات



- جدول أسعار اليورو للبيت كوين خلال 7 أيام سابقة

التاريخ	سعر الصرف
2019/05/26	1 بيتكوين = 7,813.168 يور
2019/05/25	1بيتكوين= 7,192.001يورو
2019/05/42	1بيتكوين = 7,192.001 يورو
2019/05/23	1بيتكوين = 7,041.974 يورو
2019/05/22	1بيتكوين = 6,846.604 يورو
2019/05/21	1بيتكوين = 7,135.659 يورو
2019/05/20	1 بيتكوين = 7,173.083 يورو

من خلال الجدول يتضح أنا سعر الصرف "للبيت كوين" خير مستقر خلال هذا الأسبوع.

ثالثا: البيت كوين أمام الدينار الجزائري[2]

1- محول وحاسبة أسعار العملات

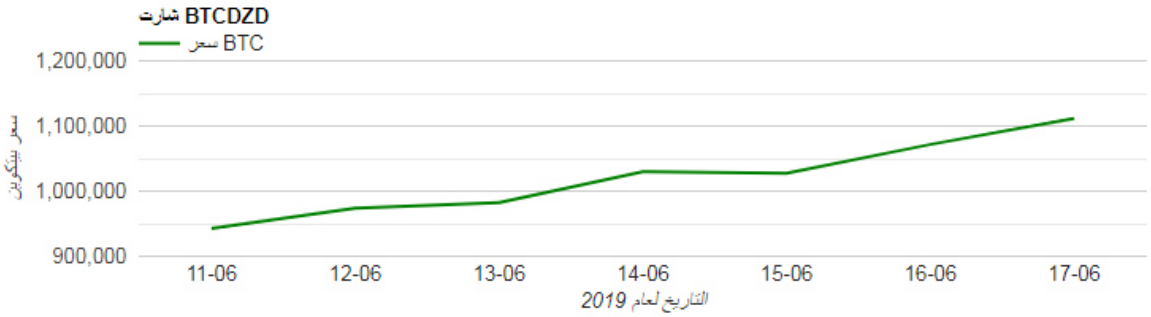
[1] https://arab.dailyforex.com/forex-technical-analysis/2019/05/تحليل-أسعار-البيت كوين-اليوم-24-مايو-2019/116612

[2]- https://www.currencyc.com/ar/dzd-btc.html

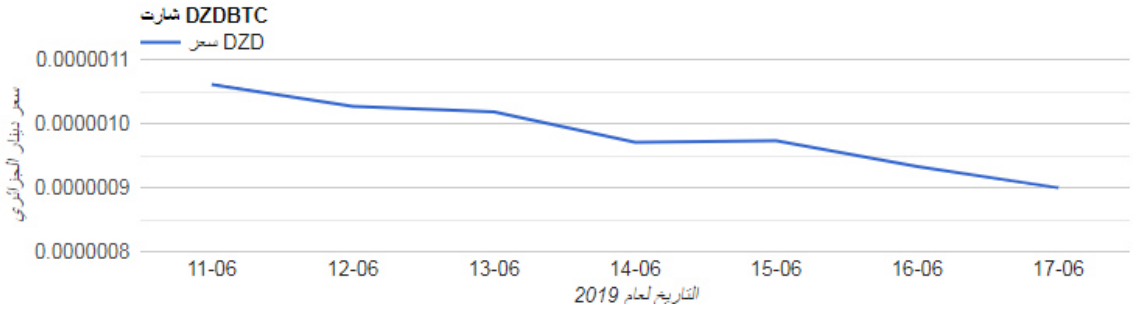
2- جدول أسعار البيت كوين للدينار الجزائري خلال 7 أيام سابقة

التاريخ	سعر الصرف
2019-06-17	1 بيت كوين = 1,111,466.141 دينار الجزائري
2019-06-16	1بيت كوين = 1,071,636.878 دينار الجزائري
2019-06-15	1 بيتك وين = 1,027,615.496 دينار الجزائر
2019-06-14	1بيتكوين = 1,029,901.835 دينار الجزائري
2019-06-13	1بيتك وين = 982,207.779 دينار الجزائري
2019-06-12	1بيتكوين = 973,942.213 دينار الجزائري
2019-06-11	1 بيتك وين = 942,572.752 دينار الجزائري

3- الرسم البياني الشارة للبيتك وين مقابل دينار الجزائري خلال الأيام الستة الماضية



4- الرسم البياني الشاة للدينار الجزائري مقابل بيتك وين خلال الأيام الستة الماضية



من خلال الجدول والمنحنين البياني فان سعر البيت كوين مرتفع أمام الدينار الجزائري والعكس صحيح.

الفرع الثالث

المبادرات القانونية والتنظيمية الرئيسة التي تعالج التحديات المتصلة بالعملات الافتراضية

نظرا لعدم وجود بنوك مركزية أو مؤسسة حكومية تصدر هذه النقود الافتراضية والتي يتم تداولها إلكترونيا، بحيث تشرف عليها وتنظم التعامل بها وهذا لاتسامها بالصفة الدولية، فهي ليست منظمة ولا تخضع لأي تشريع، وليس لها أي ايطار أو حماية قانونية بل مجرد قيمة مالية إلكترونية، وعليه وجب معرفة مدى التعامل الدولي بهذه العملة الافتراضية (أولا)، ثم التطورات التنظيمية الدولية (ثانيا)، ويليه التنظيم المبكر والمشاكل القانونية (ثالثا).

أولا: التعامل الدولي بالعملة الافتراضية

يكون ذلك من خلال قانون الدولة الموحدة والمتمثل في قانون تنظيم العملة الافتراضية، بحيث أنه في فيفري 2016 نشر المؤتمر الوطني للمفوضين المعني بقوانين الدولة الموحدة (NCCUSL) مشروع مناقشة لقانون تنظيم عمل العملات الافتراضية (قانون العمال التجارية)، كما هو الحال مع مشاريع أخرى مماثلة، قانون الأعمال (VC) يهدف إلى توفير قانون موحد للدولة بحكم تشغيل أي نشاط تجاري، أينما كان موجودا، يشارك في "عمل العملة الافتراضية". ويعرف مصطلح عمل العملة الافتراضية على نطاق واسع ليشمل تقديم خدمات تحويل العملات وتخزنها افتراضيا، وتقديم تحويل العملة الافتراضية،

أو تخديم الخدمات والمنتجات الأخرى التي تساعد سكان دولة أو ولاية قضائية لاكتساب أو تحويل العملة الافتراضية[1].

ثانيا: التطورات التنظيمية الدولية

خارج الولايات المتحدة، تظهر قوانين ولوائح وسياسات العملة الافتراضية على المستوى العالم، وسنعرض عدد من الدول القضائية التي لها تأثير كبير على صناعة الخدمات المالية العالمية وكذا موقف المشرع الجزائري منها. (1) الاتحاد الأوربي، (2) المملكة المتحدة"UK"، (3) لجنة بازل للمراقبة المصرفية، (4) موقف المشرع الجزائري من العملة الافتراضية.

1. الاتحاد الأوربي: سلطة البنك الأوربي: بعد الأزمة المالية العالمية لعام 2008، أنشأ الإتحاد الأوربي (السلطة المصرفية الأوربية)، الغرض من **"EBA"**، هو:"المساهمة في إنشاء دليل القواعد الأوربية الموحدة في القطاع المصرفي الذي يهف إلى توفير مجموعة واحدة من القواعد الاحترازية المنسقة للمؤسسات المالية في جميع أنحاء الإتحاد الأوربي".

[1] -national conférence of commissioners on Uniform state laws. « Uniform régulation of Virtual-currency businesses act », annual conférence one-hundred-and-twenty-six th year, San Diego, Californie,14-20 July, 2017.

وعلاوة على ذلك، فإن "EBA" مكلفة بتعزيز التقارب من الممارسات الرقابية وتقييم المخاطر ومواطن الضعف في القطاع المصرفي في الاتحاد الأوربي، وهو أول منظمة تنظيمية للخدمات المالية فوق الوطنية في العالم.[1]

في ديسمبر 2013، أصدرت "EBA" تحذير المستهلكين من العملة الافتراضية، وكان السبب المؤكد للنشر هو إصدار تحذير لتسليط الضوء على المخاطر المحتملة، المرتبطة بيع العملات الافتراضية "البيت كوين" أو الاحتفاظ بها أو تداولها.

2.المملكة المتحدة: أعلنت حكومة المملكة المتحدة سنة 2014 على برنامج يبحث في فوائد والمخاطر الخاصة المرتبطة بالعملات الافتراضية والتكنولوجيا الأساسية، مع التركيز بشكل خاص على مسألة التنظيم، وفي سنة 2014 نشرت الحكومة أسئلة تتعلق بالعملة الافتراضية وتلقت 120 ردا من الأفراد الذين يستخدمون العملات الافتراضية، مطوري العملات الافتراضية، وأصحاب الأعمال التجارية ذات الصلة بالعملة الافتراضية والبنوك وشركات الدفع[2].

4.**موقف المشرع الجزائري من العملة الافتراضية:** مع توسع انتشار العالمي، يزداد اهتمام الجزائريين بتداول العملات الرقمية "البيت كوين" ما دفع الحكومة إلى تحديد موقفها

[1] -Gabriel gimigiliano, bitcoin and mobile payments : Constructing a European Union Framework, Plagrave-Macmillan, london,2016,p94.
[2] -HM Treasury, Digital Currencies-Call for information. Banking and Credit Team, Horse Guards Road, London , 2014,pp1-12.

النهائي من هكذا تداولات على سلعة افتراضية أو مشفرة ليس لها تغطية نقدية[1]، حيث المادة 117 من قانون المالية لسنة 2018 "يمنع شراء العملة الافتراضية وبيعها واستعمالها وحيازتها. العملة الافتراضية هي تلك التي يستعملها مستخدمو الانترنت عبر شبكة الانترنت، وهي تتميز بغياب الدعامة المادية كالقطع والأوراق النقدية وعمليات الدفع بالصك أو البطاقة البنكية، يعاقب على كل مخالفة لهذا الحكم، طبقا للقوانين والتنظيمات المعمول بها[2].

ودافعت الحكومة الجزائرية عن موقفها بالقول في المادة ذاتها إن "الجزائر تسعى إلى إقامة نظام مراقبة أكثر صرامة لتتبع التعاملات الالكترونية التي يمكن أن تستعمل في تجارة المخدرات والتهرب الضريبي أو تبيض الأموال، بفضل السرية المضمونة لمستخدمي العملات المشفرة.

ثالثا: التنظيم المبكر والمشاكل القانونية

بسبب سهولة واضحة في تسهيل غسل الأموال وشراء المواد غير قانونية، فإن bitcoin تتعرض بشكل متزايد لتدقيق من جانب الوكالات التنظيمية لمختلف حكومات الولايات المتحدة والحكومات الفدرالية.

[1]- قانون رقم 17-11، المؤرخ في 27 ديسمبر 2017، المتعلق بقانون المالية لسنة 2018، الجريدة الرسمية رقم 76، الصادر بتاريخ 28ديسمبر 2017، ص54.

[2]-www.akhbarelyoum.dz 01 :30 à 17 jun2019.

1.طريق الحرير: إن طريق الحرير يمثل تحديا أساسيا لنظام الحضر العالمي. يتم تشكيل هذا التحدي من خلال الصعوبات التكنولوجية، فتعقيدات طريق الحرير قد تعاملت مع وكالات تنفيذ القانون والهيئات التشريعية التي تبحث تنظيم وتوسيع هذا النظام الحظر العالمي، فجهود تنفيذ القانون في هذا المجال هو إشكال محكوم عليها بالفشل.

إن طريق الحرير هو واحد فقط من هذه المواقع التي تستخدم لإدامة النشاط غير المشروع، ويعرف هذا الجزء من الانترنت عادة باسم الويب المظلم، وهي عبارة نشير إلى محتوى لا يمكن الوصول إليه أو فهرسته من قبل محركات البحث مثلGoogle [1] .

Mt.Gox Asset.2: ضبطت السلطات الأمريكية أصول Mt.Gox سنة 2013، وهي واحد من أكبر التبادلات بواسطة bitcoin في العالم، حيث Gox يشترك في أعمال نقل الأموال دون ترخيص مناسب. وعلى وجه الخصوص، وفي أواخر فيفري 2014، أغلقت Gox موقعها على شبكة الانترنت ثم فدمت للإفلاس في 28 فيفري 2014، بعد أن خسرت ما يقرب من 750.000 من عملاء bitcoin بعد خرق أمني[2].

3. مستقبل العملات الافتراضية: بعد تطورات السوق لافتراضية، مطورا bitcoin متفائلون للإعمال التجارية، وهكذا أطلقت GitHup فكرة أخذت من bitcoin، وفقا للعملية المشفرة،

[1]- Reza Raccsi, The Silk Road, bitcoin, and the Global prohibition Regime on the international Trade in licit Drugs : Can This Strom Be Weathered ?, Glendon Journal of International Studies, 2015, p03.

[2] - Matthew Kien-Meng Ly, Coining Bitcoin's legal bits : Examining the regulatory frameworl for bitcoin and Virtual currencies, Harvard Journal of Lwa & technology, vol27, N^0 02 Spring 2011.

فالمطورين هم أول من يعتمدوا التكنولوجيا الجديدة الجديدة، ويعملون مع الأجهزة الحديثة ومعظمهم لديهم حساب على GitHub .

- فمن المتوقع أن تنمو القطع النقدية الافتراضية التي من شانها دعم الشركات الكبيرة، وبالتالي قامت كل من:

American Express، بإلجاد عملة حقيقية، Amex، مما يمكن العملاء من استهلاك أكثر مما يمكن تحمله.

- Amazon، واحدة من أكبر المخازن على الانترنت شهرة في العالم، أطلقت العملة الافتراضية الخاصة بها، Coins Monday ، يمكن استخدامها من قيل المستخدمين لمخازن أمازون، لشراء التطبيقات والألعاب.
- Facebbok لديه شيء مثل القطع النقدية الرقمية، أو[1] Facebbok Credit

[1] - Sova, A Methedintu & al, Virtual Currency »bitcoin » -Challenges and Controverdied, Annal of the constantin Brancusi University of Targu Jiu, Economy Series, N^{0}03, 2016.

الفصـــــــل الثانـــــي

المكافحة الجنائية للاتجار بالأشخاص عبر النطاق الشبكي الخاص

إن كانت الثورة المعلوماتية قد أثرت على نوعية الجرائم التي صاحبتها ظهور أنماط مستحدثة من الجرائم عرفت بالجرائم المعلوماتية، فإنها في المقابل أثرت على وسائل إثبات هذه الجرائم، إذ أصبحت الطرق التقليدية التي جاءت بها نصوص قانون الإجراءات الجزائية غير كافية لاستخلاص الدليل بخصوص هذا النوع الإجرامي المستجد الذي يحتاج إلى طرق وتقنية جديد تتناسب مع طبيعته، ويمكنها فك رموز وترجمة نبضاته وذبذباته إلى كلمات وبيانات محسوسة ومقروءة تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية.

واعتبارا للطبيعة الخاصة للجرائم الالكترونية في عناصرها ووسائل وتقنيات ارتكبها، جعل من المشرع يعيد النظر في كثير من المسائل الإجرائية خاصة فيما تعلق بمسألة التحقيق والإثبات، لأن الوسائل التقليدية لم تعد تستطيع القيام بهذا الأمر.

وانطلاقا من هذا قمنا بتخصيص الفصل من اجل دراسة المتابعة الجزائية للجرائم التي ترتكب عبر النطاق الشبكي الخاص ضمن (المبحث الأول)، ثم دراسة صعوبة المكافحة الجنائية الإجرائية لجرائم الشبكة الخاصة وهذا من خلال (المبحث الثاني).

المبحث الأول

المتابعة الجزائية للجرائم التي ترتكب عبر النطاق الشبكي الخاص

من المتعارف عنه في القانون الجنائي تجريم السلوكيات بعد أن يتم حصر هذه السلوكيات لتكون محل تجريم يعاقب عليها القانون، وهذا ما قام بيه المشرع الجزائري بشأن جريمة الاتجار بالأشخاص، من خلال النصوص الجانية الموضوعية النافذة في حق مرتكبي الأفعال التي نص عليها في قانون العقوبات في الباب الخامس مكرر01 من المواد 303مكرر04إلى المواد 303مكرر15، وعلى أساس هذا سيتم تخصيص (المطلب الأول) لدراسة الخصوصية الجنائية كجريمة تقليدية ترتكب في وسط رقمي خاص، ثم بعد ذلك إجراءات المتابعة الجزائية للاتجار بالأشخاص عبر النطاق الشبكي الخاص وهذا ضمن (المطلب الثاني).

المطلب الأول

الخصوصية الجنائية كجريمة تقليدية ترتكب في وسط رقمي خاص

احتراما لمبدأ الشرعية الجنائية، والتي نصت عليها المادة 01 من قانون العقوبات الجزائري "لا جريمة ولا عقوبة إلا بنص أو تدابير أمن ..."[1]، وكذلك نص المادة 04" لا جريمة ولا عقوبة أو تدابير أمن إلا بغير قانون"، وعليه لا يعتبر الفعل أو ترك الفعل جريمة إلا إذا نص المشرع عليها بنص صريح، إذ أنه هناك تكامل بين قاعدة التجريم

[1]– قانون رقم 66–156، سالف الذكر.

والعقوبة، لا كن نحن في هذا العمل نقوم بدراسة الجريمة كظاهرة رقمية ترتكب في وسط رقمي خاص يتميز بالخصوصية والتشفير وصعوبة الكشف عنه، لهذا وجب عليا دراسة مدى تطابق أشكال الاتجار في الشبكة الخاصة، مع النصوص التجريم للمتاجرة التقليدية، ومنه قيام المشروعية الجناية من عدمها، وهذا ما سيتم التطرق إليه أولا من خلال المشروعية الجنائية الركن المادي (أولا)، ثم المشروعية الركن المعنوي (ثانيا).

الفرع الأول

خصوصية الركن المادي للجريمة

يقوم الركن المادي في جريمة الاتجار بالأشخاص عل سلوكيات ووسائل حددها الشرع الجزائري على سبيل الحصر، بحيث عدم توفر هذه السلوكيات والوسائل نكون خارج جريمة الاتجار بالأشخاص وتصبح جريمة أخرى، وعليه سنقوم بدراسة مدى تطابق السلوكيات ووسائل الركن المادي للجريمة، ثم القيام بإسقاطها على الشبكة الرقمية.

أولا: مدى تطابق السلوكيات ووسائل الركن المادي

حدد المشرع الجزائري السلوكيات محل التجريم في جريمة الاتجار بالأشخاص من خلال المادة 303مكرر04 ب: (تجنيد الأشخاص، التجنيد القسري، التجنيد الخداع الكلي، التجنيد الخداع الجزئي، نقل الأشخاص، تنقيل الأشخاص، إيواء الأشخاص، استقبال الأشخاص)، أما الوسائل فقد حصرها ب:(التهديد بالقوة، استعمال القوة، استعمال أي شكل من أشكال الإكراه، الاختطاف، الاحتيال، الخداع، اسائة استعمال السلطة، استغلال

حالة الاستضعاف، إعطاء أو تلقي مبالغ مالية أو مزايا بقصد الاستغلال). أما المتاجرة بالأشخاص عبر النطاق الشبكي الخاص فنه لا يخرج عن دائرة السلوكيات الشبكية.

فالمجرم الشبكي، قبل ظهور الشخص محل التجارة في الشبكة الخاصة، يجب أن يكون قد احتجزه فعليا، الأمر الذي عرفه المشرع الجزائري صراحة بالإيواء ، الذي يتحقق بعد مراحل يشارك فيها أشخاص آخرون أو يقوم بها الجاني بنفسه.[1]

فالمجرم ألمعلوماتي[2] يتطابق مع المجرم العادي بحيث بإمكانه استخدام احدي السلوكيين المذكورين في جريمة الاتجار بالأشخاص وهب (الاحتيال الشبكي و الخداع الشبكي)، فهذه الجريمة يمكن تطبيقها الكترونيا عن طريق الشبكة الرقمية وخاصة الخاصة منها إذ يكون الاحتيال في الشبكة الخاصة (الدارك ويب) باستخدام أحد الوسائل الالكترونية.

وعليه يمكن القول أن الجاني يعتمد على عدة وسائل من اجل تحقيق السلوكيات المذكور، بحيث يكون الاحتلال عن طريق الإيواء الممهد للاستغلال من خلال الاحتيال على الأشخاص بتوفير عمل أو غير ذلك من الأمور التي تستدرج المجني عليه أو يكون

[1]– جحيش فؤاد، الاتجار الجنسي بالأطفال عبر النطاق الشبكي الخاص، المرجع السابق، ص 11.

[2]– المجرم ألمعلوماتي: هو كل شخص سواء طفل، رجل ، أنثى، يأتي أفعالا إرادية تشكل سلوكا ايجابيا أو سلوكا سلبيا باستخدام تقنية المعلوماتية لإحداث نموذج إجرامي بالاعتداء على حق أو مصلحة للمزيد راجع: محمد على سالم، حسن علي سالم، الجريمة المعلوماتية، مجلة جامعة بابل للعلوم الإنسانية، مـج14، عدد 03، 2007، ص88.

بالقوة كالخطف، كما يمكن أن يحدث الإيواء بطريقة رضائية مثل المواقع التي عرض فيديوهات مخلة بالحياء لنساء تمارس دعارة.

ثانيا: من حيث إنجاز السلوكيات والوسائل عبر النطاق الشبكي الخاص

يتم إنجاز هذه السلوكيات عن طريق وسائل الويب المظلم والذي هو محل الدراسة، بحيث أن المشرع الجزائري عندما تطرقه للاحتيال في قانون العقوبات 2009، لم يكن يقصد الويب المظلم الذي انتشر بصورة سريعة نظرا للتشفير وصعوبة التتبع، إلا انه حين اصدر قانون 04-09 سالف الذكر وتحديدا المادة 02الفقرة أ بحيث جرم المشرع الجزائري الجرائم التقليدية المرتكبة عبر او يسهل ارتكابها بواسطة الإعلام والاتصال، وهذا يعني الشبكة بكل مكونتها.

وعليه الوسائل الالكترونية المستعملة والتي تتطابق مع الوسائل التقليدية من حيث تحقق النتيجة والمستعملة في deerk net هي:

1.السوق السوداء: بحيث يم استدراج الضحية وبيعها داخل السوق السوداء، مع الإشارة أن الحديث هنا عن الضحية الرقمية التي تستخدم العديد من المواقع كال face book، وغيرها من المواقع والتي يمكن التواصل مع الضحية الرقمية ومثال ذلك (المواقع التي تنشر عن إجراءات عمل التوظيف فتستدرج الضحية ويتم الإيقاع به من طرف المافيا وهذا ما يعرف بموقع القاتلين المأجورين)، بحيث ذكر الأستاذ عبد الرزاق طواهرية في

كتابه شياطين بانكوك– استطعت أخيرا أن أجد الرابط الصحيح للموقع الالكتروني الخاص بالقتلة المأجورين[1].

2.موقع الشبكة الروبوتية: هذه الخدمات عادة ما تكون مأجورة وتستخدم لغايات ومن بينها الترصد بالأشخاص من اجل المتاجرة بهم، بحيث يتم إرسال البريد الاحتيالي (Spam mail)حتى هجمات رفض الخدمة (Denial of Service Attacks) التي تعتمد على طلب الوصول إلى موقع أو مخدم ما لعدد كبير من المرات بحيث يتم إرهاق موارد المخدم التي تحاول إرسال ملفات الموقع لعدد كبير من العناوين في وقت واحد، وغالباً ما يؤدي الأمر إلى إغراقها بهذه الطلبات المزيفة بحيث لا يستطيع المستخدمون العاديون الوصول إلى المحتوى.[2]

3.مواقع الاختراق المأجورين: لمخترقون (Hackers) ينقسمون إلى مجموعات عديدة تبعاً لغاياتهم، فمنهم من يحاول تحقيق الكسب المادي بنشر البرمجيات الخبيثة أو اختراق حسابات بنكية ومعلومات بطاقات الائتمان، أو باستخدام برمجيات الرهينة (Ransom-ware) أو يقومون بالاختراق لأسباب عقائدية أو انتقامية حتى، لكن بعضهم ببساطة يعملون كمرتزقة مأجورين يقومون بأعمالهم حسب الطلب ليلبوا رغبات الزبائن، ومع أن العديد من المجموعات تقوم بهذه الأعمال، فكثيراً ما ينتهي الأمر باستغلال المخترقين

[1]– عبد الرزاق طواهرية، المرجع السابق، ص27.

[2]– الشبكات الروبوتية أو Botnets هي عبار عن مخدمات صغيرة نسبياً لكن مزودة ببرمجيات خاصة تسمح لها بالتصرف بشكل مماثل لبعضها البعض ببرمجة بسيطة فقط.

لجهل الزبائن ويتحول الأمر إلى مجرد عملية احتيال لا يمكن تتبع من قام بها بدلاً من تنفيذ العمل[1].

4.مواقع الخداع الاحتيال: نظراً لسمعة الشبكة المظلمة بكونها مملوءة بالجريمة ويمكن شراء أي شيء منها، فهناك العديد من المواقع التي تستغل هذه السمعة لصنع واجهات متاجر وهمية تسمح للمستخدمين بطلب العديد من المنتجات والخدمات، لكنها لا تقوم بإيصالها أو توفيرها بل تأخذ الأجر فقط، ومع كون التعاملات بالعملات الرقمية غير قابلة للتراجع عنها، فالمستخدمون سيجدون أنفسهم في دائرة الاحتيال بدون أن يستطيعوا التصرف حيال الأمر[2].

الفرع الثاني

خصوصية الركن المعنوي للجريمة

ذكرنا في الدراسة السابقة أن الركن المعنوي في جريمة الاتجار بالأشخاص له خصوصياته، وهذا راجع لطبيعة الجريمة التي يكون الهدف منها الاستغلال لإغراض

[1]– على وديع حسين، ماهي الشبكة المظلمة "dark web" وبماذا تختلف عن الشبكية العميقة" deep web"؟، تاريخ النشر 18أكتوبر2017، تاريخ التصفح 22جوان 2019، الرابطة: https://dkhlak.com/dark-web-and-deep-web

[2]– " شبكة ماريانا" واحدة من أكبر الأساطير المتعلقة بالشبكة المظلمة هي أسطورة "شبكة ماريانا" (التي تستمد اسمها من خندق عميق في المحيط الأطلسي يحمل نفس الاسم) التي تتفق مختلف إصدارات الأسطورة على أنها جزء حصري جداً من الإنترنت غير متاح للعامة ويتضمن أهم الأسرار البشرية وغير البشرية حتى ومن هنا تتفرع الأساطير وتختلف تبعاً للمصابين بجنون الارتياب ومخترعي نظريات المؤامرة، فالبعض يقول أنها مقر ذكاء صنعي يتحكم بكامل الإنترنت دون معرفة أحد، فيما يقول آخرون أنها مكان خاص للمتنورين (Illuminati) يمارسون منه هيمنتهم العالمية. للمزيد راجع: https://dkhlak.com/dark-web-and-deep-web

محددة. لهذا وجب علينا النظر من حيث تطابق هذه الاستغلال مع شكل الاتجار عبر النطاق الشبكي الخاص هذا (أولا)، ثم من حيث هدف الاستغلال عبر النطاق الشبكي الخاص (ثانيا).

أولا: من حيث تطابق الاستغلال مع أشكال الاتجار عبر النطاق الشبكي الخاص

إذا نظرنا إلى القصد الجنائي في جريمة الاتجار بالأشخاص فإنه تنحصر في القصد العام والذي يكون في جميع الجرائم، أما القصد الخاص فينحصر في صور الاستغلال كمفهوم عام[1] وهذا ما نصت عليه المادة 303مكرر04 من قانون العقوبات الجزائري بحيث ينحصر صور الاستغلال في: (الاستغلال لأجل دعارة الغير، سائر أشكال الاستغلال الجنسي، استغلال الغير في التسول، استغلال الغير عن طريق السخرة، الخدمة كرها، الاسترقاق، الممارسات الشبيه بالرق، الاستعباد، نزع الأعضاء البشرية).

وهذا ما نجده ينطبق مع البعض من أشكال الاتجار عبر المنظومة الشبكية الخاصة، بحيث الجاني الجنائي الرقمي شكل التجارة يكون لمدة زمنية مقابل ثمن معين أو يكون عن طريق البيع، إذ أنه التجارة من أجل أغرض جنسية تكمن في تقديم خدمة مؤقت من طرف الشخص محل الخدمة سواء قاصر أو بالغ، مرآة أو طفل أو رجل وهذا من أجل إرضاء الزبون جنسيا وفق المدة المتفق عليها. وهذا يدخل في ايطار استغلال

[1]– مبارك هشام عبد العزيز، الاتجار بالبشر بين الواقع والقانون، مركز الإعلام الأمني، المنامة، البحرين، 2010، ص 03.

الغير من اجل ممارسة الدعارة وكذا الاسترقاق، إضافة إلى بيع الأشخاص كسلعة، ليع الفيديوهات التي تحتوي على صور جنسية وهذا ما يتطابق مع الاستغلال الجنسي[1].

ثانيا: من حيث هدف الاستغلال عبر النطاق الشبكي الخاص

أن المشرع الجزائري من خلال نص المادة 303 مكرر04 من ق. ع. ج، لم يكن يقصد أشكال الاستغلال التي تحدث عبر الويب المظلم، وإنما جاءت هده المادة في ايطار الجرائم التقليدية التي ترتكب بوسائل تقليدية ، والذي تم توضحه سابقا في الفصل الأول ، وهدا الأمر يقابله جنائيا نص المادة 02 ف أ من القانون 09_04[2]. بحيث هذه المادة تحدثت عن الجرائم التقليدية التي ترتكب بواسطة منظومة معلوماتية، وبإسقاطها على ظاهرة الاتجار عبر النطاق الشبكي الخاص. والمتمثل في بيع الفيديوهات وكل الأشكال المذكورة فإن الويب المظلم يصبح الطريق الأسهل للقيام بهذه الجريمة.

الفرع الثالث

العجز التشريعي في مواجهة جرائم derk web

ذكرنا سابقا أنه لا يمكن تجريم فعل إلا بوجود نص تشريعي يجرمه، وهدا الأصل العام احتراما لمبدأ الشرعية الجنائية، لهذا وجب علينا أن نتحدث أولا عن مبدأ الشرعية الجنائية

[1]– مطر محمد يحي وجمع من المختصين، الجهود الدولية في مكافحة الاتجار بالبشر، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2010، ص07.

[2]– أنظر: المادة 1/02–أ، قانون رقم 09–04.

ثم بعد ذلك التطرق إلى مدى تطبيق هذا المبدأ على جريمة الاتجار بالأشخاص عبر النطاق الشبكي الخاص باعتباره وسط رقمي.

أولا: أحكام عامة لمبدأ الشرعية الجنائية

يعتبر مبدأ شرعية الجرائم من المبادئ الأساسية التي تقوم عليها التشريعات العقابية الحديثة فما هو تعرفه.

1.تعريف مبدأ الشرعية الجنائية: عرفه الأستاذ نجيب حسني وفتوح عبد الله بأنه "حصر عدم المشروعية الجنائية في نصوص القانون الجنائي التي تحدد الجرائم والعقوبات" ويعني هذا المبدأ أنه لا جريمة ولا عقوبة إلا بنص قانوني، أي مصدر الصفة غير المشروعة للفعل هو نص القانون، إذ يقال لهذا النص " نص التجريم"، والذي هو في نظر القانون الجزائي يشمل قانون العقوبات والقوانين المكملة له والقوانين الجزائية الخاصة[1].

وعليه كل نص يحتوي على الشروط التي يتطلبها في الفعل كي يخضع لهذا النص ويستمد منه الصفة غير المشروعة، كما يحدد العقوبة المقررة لهذا الفعل، بحيث القاضي لا يستطيع أن يعتبر فعلاً معنياً جريمة إلا إذا وجد نصاً يجرم هذا الفعل، فإذا لم يجد مثل هذا النص فلا سبيل إلى اعتبار الفعل جريمة ولو اقتنع بأنه مناقض للعدالة أو الأخلاق أو الدين، يكمن أساس هذا المبدأ في حماية الفرد و ضمان حقوقه و حريته.

[1]– عمار خوري، شرح قانون العقوبات –القسم العام– كلية الحقوق، جامعة الجزائر، 2007.ص18.

إلا أنه يوجد اتجاه فقهي يعارض فكرة الركن الشرعي، على أساس أن النص الموجد للجريمة لا يمكن أن يكون أحد أركانها، ويرون كذلك أن النص لتجريمي، هو وعاء نموذج الجريمة، بالإضافة إلى إمكانية ارتكاب السلوك المجرم بالنص، لكن لا تقوم الجريمة مثل حالة أسباب الإباحة[1].

2.نتائج مبدأ الشرعية الجنائية: يمكن أن نستخلص نتائج الشرعية الجنائية في بعض النقاط التالية:

أ. **قاعدة عدم رجعية النص الجنائي:** لمعاقبة شخص لابد أن تكون الجريمة قد حددت أركانها بموجب قانون مطبق وقت ارتكابها ، ولا يجوز معاقبة شخص على فعل كان مباحًا وقت ارتكابه ثم صدر قانون يجرمه. بالإضافة إلى القانون الأصلح للمتهم كاستثناء[2].

ب.حظر القياس في المسائل الجزائية: عرف الأستاذ ناصر حمودي القياس "إلحاق واقعة بواقعة غير منصوص علي حكمها بواقعة أخرى منصوص على حكمها لاشتراك

[1]– عبد الله أوهايبية، شرح قانون العقوبات الجزائري، المؤسسة الوطنية للفنون المطبعية، الجزائر، 2011 ،ص86–77.

[2]– ناصر حمودي، (القانون الجنائي العام): الأحكام العامة لقانون العقوبات والنظرية العامة للجريمة)، محاضرات موجهة لطلبة السنة الثانية حقوق، معهد الحقوق، المركز الجامعي العقيد آكلي محند أولحاج– البويرة،2012–2013، ص88–87.

الواقعتين في علة الحكم"، غلا أنه في المجال الجنائي القياس غير جائز بناءا على مبدأ لا جريمة ولا عقوبة إلا بنص.[1]

ج. **حضر التفسير الواسع للنصوص الجنائية:** وهذا من خلال الإلزام بالتفسير الضيق للنص الجنائي، بحيث يجب البحث عن إرادة المشرع الحرفية، الحقيقية، وقت وضع النص[2].

د.**إنفراد المشرع بالتجريم والعقاب:** بمعنى، للمشرع الحق الأصيل في التجريم والعقاب، ولا يمكن للسلطة التنفيذية أو القضائية أن تجرم وتعاقب.

هـ.**أحكام خاصة بتطبيق النص الجنائي من حيث المكان:** يطبق النص الجنائي على كل شخص ارتكب الجريمة في إقليم الدولة المعنية، وفق مبدأ الإقليمية، ويكفي أن يرتكب السلوك أو تتحقق النتيجة في الإقليم، كما يمكن تطبيق النص وفق حالات أخرى[3].

ثانيا: مبدأ الشرعية الجنائية وجرائم الشبكة الخاصة

إن الجرائم التقليدية التي تحدث داخل الوسط الرقمي، تندرج ضمن جرائم الوسط الرقمي والمتمثل في الاعتداء على المنظومة المعلوماتية[4]، إلا أنه حدث اختلاف بين الفقهاء

---

[1]– ناصر حمودي، مرجع سابق، ص 86.

[2]– فؤاد جحيش، جرائم الوسط الرقمي، تجريم حديث بأبعاد تقليدية، دراسة تحليلية، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية تخصص جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، البويرة، الجزائر، 2015، ص24.

[3]– المرجع نفسه، ص25.

[4]– مصطلح الاعتداء على المنظومة المعلوماتية في جريمة الاتجار بالأشخاص يعنى: استغلال المنظومة المعلوماتية من أجل إركاب هذه الجريمة، والتي تمنح للجاني ألمعلوماتي الأمن في عدم كشف الهوية من خلال التشفير لهذه الشبكة والتي لم يتطرق إليها المشرع الجزائري حين وضع قانون 09_04، وبالتالي نحن لا نتحدث عن الجانب المتعلق بالاعتداء على المنظومة، والذي حدده بالدخول والبقاء في نص المادة 394مكرر إلى غاية 394 مكرر07.

حول هذه الجرائم التقليدية، حيث اعتبروها جرائم منفصلة عن جرائم المعلوماتية تحكمها النصوص التقليدية.مما أوقع بالفقهاء في إشكاليات أبرها:

1.إشكالية ارتكاب الجريمة التقليدية في الوسط الرقمي: قد ترتكب جرائم تقليدية في الوسط الرقمي مثل جريمة الاتجار بالأشخاص.إلا أنه مع القصور التشريعي في هذا الجانب، اختلف الفقه الجنائي حول إمكانية تطبيق النص التقليدي من عدمه على النحو التالي:

أ-**يرى جانب من الفقه:** أنها جرائم تقليدية ترتكب بواسطة وسائل حديثة، لكنه رأي منتقد الخروج عن مبدأ التفسير الضيق للنص الجنائي، فوقت وضع النص لم تكن توجد عناصر الوسط الرقمي[1].

ب- **كما يرى جانب آخر من الفقه:** أن هذا النوع من السلوكيات يشكل جرائم حديثة تتطلب نصوص حديثة، لكنه رأي منتقد كذلك، لكونها تتصف بنفس سلوكيات الجريمة التقليدية وتختلف عنها في الوسط فقط، فإفراد لها نصوص جديدة سوف يقودنا إلى التكرار[2].

ج-**أما الرأي الثالث وهو الأرجح:** فيتمثل في تطوير النصوص التقليدية الموجودة بإضافة فقرات أو مصطلحات حديثة تتناسب مع الجريمة محل الدراسة، بالإضافة إلى الاعتماد على تقنيين وفنيين عند وضع المصطلحات وشرحها[3].

---

[1]- يوسف صغير، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013، ص60.

[2]- مرجع نفسه، ص61.

[3]-فؤاد جحيش، جرائم الوسط الرقمي، تجريم حديث بأبعاد تقليدية، دراسة تحليلية ، المرجع السابق، ص26.

2.إشكالية تحديد مكان ارتكاب جرائم الوسط الرقمي: في حال ارتكاب الجريمة عن طريق شبكة الاتصال الدولية، قد يكون السلوك الإجرامي في دولة ويمر عبر عدة دول ثم تتحقق النتيجة في دولة أخرى، الرأي الراجح بهذا الخصوص، البحث في مكان ارتكاب الفعل ومكان تحقق النتيجة فقط، انطلاقا من الأحكام التقليدية للجريمة[1].

3.إشكالية عدم مواكبة التشريع لسرعة التطور الرقمي: تتطور سلوكيات جرائم الوسط الرقمي بصورة ديناميكية، فكل مرة تظهر أساليب جديدة كظاهرة تمس بالحقوق والحريات وما إلى ذلك، مما يوجب على المشرع التدخل لتجريمها[2].

ثالثا: مدى تطابق مبدأ الشرعية الجنائية من حيث النطاق على جرائم derk web

يطبق النص الجنائي على كل شخص ارتكب الجريمة في إقليم الدولة المعنية؛ وفق مبدأ الإقليمية، وهذا ما نصت عليه المادة 03 من قانون العقوبات[3].

وباعتبار جريمة الاتجار بالأشخاص جريمة تقليدية ترتكب بواسطة موقع رقمي وهو derk web، فإن ارتكاب الجريمة عن طريق شبكة الاتصال الدولية يتم من خلال السلوك الرقمي الذي يستخدمه المجرم الرقمي والذي تم توضحه سابقا في طريقة عمل متصفح Tor الذي يكون أكثر أمان من خلال إخفاء موقع الاتصال، أي صعوبة تحديد

[1]–فؤاد جحيش، جرائم الوسط الرقمي، تجريم حديث بأبعاد تقليدية، دراسة تحليلية، المرجع السابق، ص26.

[2]–عادل يوسف عبد النبي الشكري، "الجريمة المعلوماتية وأزمة الشرعية الجزائية"، مجلة مركز دراسات الكوفة، مج01، عدد07، 2008، ص117.

[3]– المادة 03 من قانون العقوبات نصت على: " يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية. كما يطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائية طبقا لأحكام قانون الإجراءات الجزائية".

مكان الجاني وكذلك تحقيق النتيجة في بلد أخر وهذا راجع لاستخدام الشبكية الدولية. والتي تجعل من الجريمة عالمية تخضع لمبدأ العالمية.

وعليه وفقا لهذا المبدأ وطبيعة الشبكة الخاصة يصعب علينا تحديد ما إذا كان المشرع الجزائري مختص أم لا لصعوبة تحديد هوية الأشخاص القائمين بهذه الممارسات.

المطلب الثاني

إجراءات المتابعة الحديثة للاتجار بالأشخاص عبر النطاق الشبكي الخاص

ذكرنا سابقا أن الطبيعة المعقدة للمنظومة المعلوماتية والسلوكيات التي تحدث داخل هذه المنظومة، والتي وجب أن تكون مجرمة من طرف المشرع الجزائري، جعل السلطات المختصة تقوم بإجراءات متابعة تتطابق مع خصوصيات هذا النطاق. والمتمثلة في جمع الأدلة الجناية الرقمية، زيادة على ذلك تعدد صور وأشكال الجريمة المعلوماتية[1]، وعليه للحصول على هذا النوع من الأدلة الجنائية يجب إتباع طرق ووسائل معقدة، والمتمثلة في الوسائل المادية(فرع الأول)، ثم الوسائل الإجرائية (فرع الثاني).

[1]– محمد الناصر محمد فرغلى ومحمد عبد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية(دراسة تطبيقية مقارنة)، جامعة نايف العربية للعلوم الأمنية، السعودية، 2007، ص34

الفرع الأول:

الوسائل المادية الحديثة في جمع الأدلة الجنائية الرقمية

عملت الجهات القضائية المختصة بإجراءات تحري وتحقيق رقمية حديثة، كونها الأنسب في متابعة جرائم الوسط الرقمي، خاصة الاعتماد على البروتوكول TCP-TP، لكن مع ظهور الدارك ويب، صعب من الأمر مما جعل من السلطات تعود إلى الوسائل المادية التقليدية[1].

أولا: استخدام بروتوكول IP/TCP لمواجهة جرائم "الدارك ويب"

من خلال هذا الجزء سنقوم بتعريف بروتوكول IP/TCP كوسيلة حديثة رقمية تستخدم في عملية الكشف على الجرائم الرقمية، ثم بعد ذلك سنتحدث عن عجز هذا البروتوكول في مواجهة جرائم "الدارك ويب".

1.تعريف بروتوكول IP/TCP: يعتبر بروتوكول IP-TCP من أكثر البروتوكولات المستخدمة في شبكة الانترنت لأنه جزء أساسي منه، والمسؤول عن تراسم جزم البيانات عبره وتوجيهها إلى أهدافها[2].

[1] – **الوسائل المادية:**" تلك الأدوات الفنية التي غالبا تستخدم في بيئة نظم المعلومات، والتي يمكن باستخدامها يتم تنفيذ إجراءات وأساليب التحقيق المختلفة، والتي تثبت وقوع الجريمة وتحدد شخصية مرتكبها للمزيد راجع: سليمان مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات، (رسالة الماجستير)، أكاديمية نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2003، ص98.

[2] – المرجع نفسه، ص98

زيادة على ذلك يعمل عنون IP بشكل متزامن مع بروتوكول أخر وهو بروتوكول التحكم بالنقل TCP، والذي تكمن وظيفته في تقسيم المعلومات إلى حزم معلومات، ويقوم برتوكول IP بعنونة كل حزمة مع إضافة معلومات أخرى إليه[1]، ومنه فيتم استخدام عنوان IPمن خلال البحث عن رقم الجهاز وتحديد موقعه الجغرافي، بالإضافة إلى إمكانية مراقبة المستخدم من طرف مزود خدمة الانترنت وتقديم المعلومات التي تفيد في التحقيق، بناءا على أن لكل جهاز حاسب ألي يتصل بالانترنت عنون IP خاص به[2].

2.عجز بروتوكول IP/TCP: إن الطبيعة الرقمية "للدارك ويب" جعلت منه موقع مشفر لا يمكن التعدي عليه بسهولة، وهذا من خلال برنامج TOR الذي يضمن عدم كشف هوية المستخدم أو حتى تحديد مكان المتصل لأن طريقة عمله تضمن تغير مكان المتصل كل ثانيتين، وهذا ما صعب الأمر على رجال البحث والتحري الرقمي .

وعليه بسبب هذا التشفير الذي يمنح الأمن للمستخدمين جعل من هذا الموقع وكر للمجرمين الذين يرتكبون العديد من الجرائم دون رقابة قانونية، وبطبيعة الحال المحقق الجنائي في مجال الرقمنة يصعب عليه كشف هوية المجرمين أو المشتبهين فيهم ومكان اتصالهم بالشبكة الخاصة، إذ لا يمكن بناءا على هذا إجراء عملية التفتيش والحجز، ولا مراقبة تحرك هؤلاء المجرمين الرقمين.

---

[1] - ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكومبيوتر و الانترنت، دار الكتاب القانونية، مصر، 2006، ص101.

[2] -Debra littlejohn Shinder, seene of the cyber crime (computer forensie Hanadbook), publishing by Syngress(Inc), United states of America,2002,p240.

ثانيا: استخدام برنامج الكوكيز Cookies

عند زيارة مستخدم الانترنت أي موقع من مواقع الويب، تفتح هذه الأخيرة ملفا صغيرا على القرص الصلب يسمى كوكي Cookie بهدف جمع بعض المعلومات عنه[1] وتحسين عملية تصفح الموقع[2]، ومنه فهو يسجل العديد من المعلومات التي يمكن أن تساعد في التحقيق من بينها تاريخ زيارة الموقع الالكتروني، أو تاريخ إجراء التعديلات عليه أو الانتهاء منها، وزيادة على ذلك الاحتفاظ بكلمات السر الخاص بالمستخدم عند زيارة الموقع[3].

ثالثا: استخدام معلومات البروكسي Proxy

في بادئ الأمر تم تطوير تقنية البروكسي Proxy لاستخدامها كحواجز نارية Firewalls لشبكة الإنترنت[4]. بحيث يشتغل هذا النظام كوسيط بين شبكة الانترنت ومستخدميها يضمن توفير خدمات الذاكرة الجاهزة، ويقوم هذا النظام على تلقي مزود البروكسي طلبا من المستخدم للبحث عن صفحة ما ضمن الذاكرة الجاهزة، فيتحقق نظام البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، ويقوم بإرسالها إلى المستخدم دون

[1]– ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص69

[2] - Steve Bunting and william wei, **Encase computer forensie,** Wiley Publishing (inc), United States of America, 2006, p 371.

[3]- Ibem, p 371.

[4]– الحاجز الناري: عبارة عن نظام أمني يفرض توليد جميع الرزم المرسلة أو الواردة من خلال جهاز وحيد، وتمريرها من خلال الحاجز الناري، ومنه فإن الدور الأساسي الذي تقوم به هو قيامها بدور الوسيط بين مستخدم شبكة الإنترنت وبين مواقعها، وذلك بطلب المعلومات من تلك المواقع وتقديمها للمستخدم للمزيد راجع: سليمان مهجع العنزي، مرجع سابق، ص 99.

الحاجة إلى إرسال الطلب إلى الشبكة العالمية مرة أخرى، أما إذا لم يتم تنزيلها من قبل، فيقوم بتحويل الطلب إلى الشبكة العالمية مستعينا في ذلك بأحد عناوينIP. ومن بين أهم ما تتميز به مزودات البروكسي Proxy هو إمكانيتها في تسريع الوصول إلى شبكة الإنترنت، بالإضافة إلى احتوائها على تدابير أمنية للتحكم بعملية الاتصال بالإنترنت، ومثال ذلك التعرف على الأشخاص المسموح لهم بالاتصال بالشبكة، وتحديد الخدمات التي يمكن استخدامها، أو حتى تحديد الأيام والأوقات المسموح بها بزيارة شبكة الإنترنت، وعليه فكل هذه العمليات والمعلومات التي يحتويها البروكسي Proxy، يتم حفظها في قاعدة بياناته، مما يجعل دورها قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة[1].

بالرغم من المميزات التي تتمتع بها مزودات البروكسي Proxy إلا أنها تحتوي على عدة مساوئ قد تشكل عائقا في التحقيق، من بينها منع الوصول إلى صفحات المواقع إلكترونية وهذا ما ينطبق على الشبكة الخاصة "دارك ويب"، أو الحصول على صفحات قديمة أو ناقصة أحيانا.

[1]– سليمان بن مهجع العنزي، المرجع السابق، ص 99.

رابعا: برامج التتبع وكشف الاختراق[1]

تقوم هذه البرامج بالتعرف على محاولات الاختراق ومن قام بها وإشعار الجهة المتضررة بعملية الاختراق، ومن الأمثلة على تلك البرامج، برنامج Hack Tracer v 1.2 وهو مصمم للعمل في الأجهزة المكتبية Web و ساكتا في خلفية سطح المكتب، و عندما يرصد أي محاولة للقرصنة أو اختراق جهاز الحاسب الآلي يسارع بإغلاق منافذ الدخول أمام المخترق. ثم يبدأ في عملية مطاردة تستهدف اقتفاء اثر مرتكب عملية الاختراق حتى يصل إلى الجهاز الذي حدثت العملية من خلاله، وقد تمت إجراء تجربة عملية على البرنامج محليا، وتم التأكد من أنه برنامج فعال، وذكر صاحب التجربة، أنه خلال اختبار البرنامج تعرض جهازه، لأكثر من (17) محاولة اختراق في فترة قصيرة، وبعد اقتفاء الأثر قاد البرنامج صاحب التجربة إلى أفراد من مدن[2].

خامسا:أدوات الضبط

تحتاج جهات جمع الاستدلالات إلى ضبط الجريمة، وإثبات وقوعها، والمحافظة على الأدلة، حتى نسبتها إلى الجاني، لتقديمها إلى هيئة التحقيق والادعاء العام، لكسب اعترافه والذين بدورهم يقدمون تلك الأدلة محفوظة إلى القضاء للمحاكمة. ولذا يوجد أدوات تقوم بضبط الجريمة كغالبية برامج الحماية، وأدوات المراجعة Auditing، وأدوات مراقبة

[1]– محمد بن ناصر السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب و الانترنت" دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية"، رسالة لنيل درجة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص 84.

[2]– سليمان مهجع العنزي، المرجع السابق، ص 100.

المستخدمين للشبكة، وأدوات التصنت على الشبكة والتقارير التي تنتجها نظم أمن البيانات، ومراجعة قاعدة البيانات، وبرامج النسخ الاحتياطي والتسجيل وأدوات الضبط الأخرى مثل Content Management[1] , MNM4 Windows , IDS.

سادسا: الأدوات المساعدة بالتحقيق

يتطلب على المحقق اختيار ما يناسبه من الأدوات التي تساعده في التحقيق، بما قد يواجهه من أن الجاني قد قام بتشفير البرامج، أو غير كلمات المرور، أو أخفى تلك المعلومات أو غيرها، أو أتلف أدوات الحفظ الخارجية، أو دمر المعلومات بأدوات الجريمة مثل الفيروسات و غيرها ولذا يحتاج إلى أدوات مساعدة كأدوات استرجاع المعلومات من الأقراص التالفة مثل View Disk وبرامج كسر كلمة المرور، وبرامج الضغط وفك الضغط Pkzip، برامج البحث عن الملفات العادية والمخفية مثل Xtreepro Gold، برامج تشغيل الحاسب مثل Bootable Diskette، وبرامج نسخ البيانات مثلLap Link، كما يتطلب استخدام برامج منع الكتابة على القرص الصلب بعد ارتكاب الجريمة وذلك لحماية مسرح الجريمة[2].

[1]–المرجع نفسه، ص 101.

[2]– سليمان مهجع العنزي، المرجع السابق، ص101–102.

الفرع الثاني

الوسائل الإجرائية الحديثة في جمع الأدلة الجنائية الرقمية

بعد التسليم بعجز الإجراءات الجزائية النافذة في الجزائر وغيرها من الدول، عن مكافحة جريمة الاتجار بالأشخاص عير النطاق الشبكي الخاص، وجب الرجوع إلى الإجراءات بديلة تساعد في ردع هذه الجريمة، وهذا ما تطرقت إليه الجهات المختصة في البحث والتحري الرقمي، وفي الأخير انحصر الأمر في الاعتماد على التسرب كبرنامج لمكافحة هذه الظاهرة وكذا برنامج الربط بين البرامج.

أولا: التسرب

إن التسرب عملية معقدة جدا تتطلب أحيانا من العون أو ضابط الشرطة القضائية المساهمة المباشرة في نشاط الخلية الإجرامية التي تم التسرب إليها وارتكاب أفعال محظورة قصد تحقيق الهدف النهائي من العملية، بل أحيانا يكون القيام بتلك الأفعال ضرورة لقبوله في الخلية. لذلك اعتبار لهذه الضرورة تفطن المشرع الجزائري وجرد الضابط أو العون المتسرب من المسؤولية الجنائية عن كافة الأفعال غير المشروعة التي قد يقدم على ارتكابها أثناء عملية التسرب[1].

[1]– جمال براهيمي، التحقيق الحنائي في الجرائم الإلكترونية،أطروحة لنيل شهادة الدكتوراه في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2018، ص84.

1.شروط التسرب: من اجل أن تتم عملية التسرب وإنجاح العملية وتسهيل متابعة الجريمة المعلوماتية والمجرمين ومهام المتسرب[1]، فقد أحاط المشروع جملة من الشروط يعين مراعاتها عندما تقتضي التحريات كون هذا الإجراء من أخطر الإجراءات انتهاكا لحرمة الحياة الخاصة للمشتبه فيه، وتتمثل هذه الشروط في شروط شكلية وأخرى موضوعية.

أ. الشروط الشكلية:

– أن يكون الإذن مكتوبا وألا وقع تحت طائلة البطلان[2].

– ذكر اسم الضابط الذي تتم عملية التسرب تحت مسؤوليته او عون الشرطة القضائية باعتباره مساعدا له[3].

– المدة المطلوبة لعملية التسرب 4 أشهر محددة قانونا قابلة للتجديد ويمكن توقيفها حتى انتهاء المدة المحددة لها[4].

ب.الشروط الموضوعية:

– تسبيب الإذن بالتسرب خاصة إذا أثبت أن الاعتداء على الوسائط الفعلية العادية غير كاف للتوصل إلى الحقيقة ومن ثمة لابد من وكيل الجمهورية أو قاضي التحقيق إن يقدم تبريرا أو الأساس الذي تم الاعتماد عليه من اجل السماح بالقيام بعملية التسرب.

---

[1]– محمد حزيط. مذكرات في قانون الإجراءات الجزائية الجزائري، الطبعة02، دار هومة، الجزائر، 2010، ص 65.

[2]– أنظر المادة65 مكرر 15 من القانون 06_22 مؤرخ في 10ديسمبر2006، يعدل ويتمم الأمر رقم 66–155، يتضمن قانون الإجراءات الجزائية، جريدة رسمية، العدد84، صادر بتاريخ 24ديمبر2006.

[3]– أنظر المادة 65 مكرر 16 من تعديل 2006 ل ق.إ.ج.ج.

[4]–أنظر المادة 65مكرر15 فقرة 03 تعديل 2006 ل ق.إ.ج.ج.

– إن نوع الجريمة هي من الجرائم الماسة بأنظمة المعالجة الآلية لمعطياته[1].

2.الاعتماد على التسرب كوسيلة لمواجهة جرائم الدارك ويب: من بين الوسائل الإجرائية الممكن إتباعها للإيقاع بجناة الويب المظلم عموما، إجراء التسرب[2]. حيث يقوم ضابط شرطة القضائية المختصين، بالولوج إلى مواقع الويب المظلم المتصلة بالاتجار الجنسي للأطفال – كالغرفة الحمراء مثلا–، على أنه زبون جنسي، ويشتري من الجاني الجنس المصور في العديد من المرات، على أن يوهمه بعد فترة أنه يرغب في أن يصبح مساعدا له، ومع الوقت يكسب ثقته، إلى أن يكشف له عن هويته الحقيقية وهو ما يعد مستبعدا نظرا لفطنة الجناة[3].

[1]– أنظر المادة65 مكرر 05 تعديل ف.إ.ج.ج2006.

[2]– تعرف المادة (65 مكرر12) من القانون الإجراءات الجزائية الجزائري التسرب على انه قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم انه فاعل معهم أو شريك أو خاف.

– هو التعريف الذي تبناه المشرع الفرنسي في المادة 706–81 من قانون الإجراءات الجزائية التي تنص:

<<...un officier ou un agent de police judicaire spécialement habilité, et agissant sous la responsabilité d'un officier de police judicaire charger de cordonner l'opération peut...surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes, comme un de leurs co-auteurs, complices ou receleurs >> voir la loi N 2001-1062, de 15 novembre 2001 portant code de procédures pénales, JORF 16 nov 2001

[3]– فؤاد جحيش، الاتجار الجنسي بالأطفال عبر النطاق الشبكي الخاص، مرجع نفسه، ص 14.

ثانيا: الاعتماد على برامج الربط لمكافحة جرائم النطاق الشبكي الخاص

أطلقت وكالة "داربا"- الذراع البحثية لوزارة الدفاع الأمريكية – سنة 2014، ما يسمى ببرنامج "memex"، الذي يقوم آليا بالبحث في الويب المظلم عن الممارسات التي تحوي اتجار بالبشر عموما، ويربط الشبكات يبعضها البعض ويتتبعها بهدف إلقاء القبض على الجاني المتنقل. وكأقل تقدير، يقوم بمسح الإعلانات ذات الصلة بالاتجار الجنسي بالأشخاص بعد أن يميزها آليا عن بائعات الهوى، وهو ما حصل فعلا بمسح في مرحلة سابقة لأكثر من 100 إعلان جنسي[1].

ثالثا: مراقبة الاتصالات الالكترونية

تعتبر المراقبة من أهم مصادر التحري التي غالبا ما يستعان بها في البحث والتقصي عن الجرائم سواء تلك التقليدية أو المستحدثة كجرائم الانترنت وهي ما يعرف بمراقبة الالكترونية[2].

وقد نص عليها المشرع الجزائري في قانون الإجراءات الجزائية الجزائري في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور[3].

---

[1]- المرجع نفسه، ص14.

[2]- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات،دار الفكر الجامعي، الإسكندرية، 2013، ص197.

[3]-اختلفت المشرع الجزائري في إعطاء المصلح واحد للمراقبة الالكترونية فأحيانا يقر بمصطلح العرفية الالكترونية كما قررها في الفنون 04 / 09 وأحيانا أخر بمصطلح أساليب التحري الخاصة إلا أنها نفس الإجراءات تختلف فقط في التسمية والقانون الذي قررها- د. نظر المادة 34 من دستور 1996

من خلال هذا يتضح أن أساليب التحري الخاصة هي إجراءات خطيرة تمس بحرمة الحياة الخاصة للأشخاص المكفولة دستوريا.

ومن أجل ذلك قرر المشرع في قانون الإجراءات الجزائية خلال تعديل 2006 الذي طرأ عليه وفق القانون 22 / 06 الذي حصر وجوبيه اللجوء إلى مثل هذا الإجراء على الجرائم السنة الخطيرة ومن بينها الجريمة المعلوماتية الذي أعطاها اسم "جريمة المساس بأنظمة المعالجة الآلية للمعطيات" وتتمثل هذه الأساليب في

- اعتراض المراسلات.
- التقاط الصورة
- تسجيل الأصوات.

1.اعتراض المراسلات[1]: هي جميع الخطابات والرسائل والطرود والبرقيات، والمشرع الجزائري[2] في المادة 65 مكرر05 من ق.إ.ج.ج، حصر مفهوم المراسلات في تلك التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية فقط.

ويكون بذلك قد استبعد المراسلات المكتوبة العادية والخطابات الخطية التي تتم عن طريق البريد العادي أو الالكتروني.

[1]- أنظر المادة 39 دستور 1996.

[2]- يقصد بالمراسلات الالكترونية: هي الخدمة التي تسمح بانتقال الرسائل المرسلة عبر نظام الرسائل الالكترونية عن طريق شبكة الكترونية.

2. تسجيل الأصوات: يقصد به مراقبة الأحاديث وتسجيلها وكل الاتصالات التي تتم عن طريق سلكي أو لا سلكي، أي أن عمليات المراقبة تشمل كل أدوات الاتصال سواء سلكية أو لا سلكية، وتتمثل في وضع تقنية دون موافقة المعنيين من اجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص[1].

3.التقاط الصور: هي تلك العملية التقنية التي يتم بواسطتها التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

أما فيما تعلق بالوسائل الحديثة التي يستخدمها المشرع الجزائري لمكافحة الإجرام الخطيرة هي في حقيقة الأمر استثنائية عن الأصل العام الذي يمنع التقاط الصور باعتباره تدخل في الحياة الخاصة وهذا مانص عليه المشرع في المادة 39 من الدستور" لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون"[2].

[1]– المادة 65 مكرر05 و مكرر10 ق.إ.ج.ج تعديل 2006.

[2]– احمد غاي، ضمانات المشتبه فيه أثناء التحريات الأولية، طبعة 2005، دار الهومة، الجزائر، 2005، ص 231.

المبحث الثاني

صعوبة المكافحة الجنائية الإجرائية لجرائم الشبكة الخاصة

بحسب الدراسة المنجزة في هذا الموضوع،اتضح أن الممارسات التي تتم على مستوى "الدارك ويب" هي أعمال تجارية غير شرعية، مجرمة في جل التشريعات العالمية. إذ أنه بمجرد الولوج إلى هذا الوسط الرقمي وارتكاب السلوكيات محل التجريم التقليدي أصبحنا حينها أمام جرائم الوسط الرقمي. وهذا بعد تدخل المشرع الجزائري إلى تجريمها عملا بمبدأ الشرعية الجنائية، إلا أن هذه النصوص و الإجراءات تعاني من قصور نظرا لطبية الرقمية المشفرة، انطلاقا مما سبق سنقوم بدراسة صعوبة الاستدلال في الجريمة الرقمية ضمن (المطلب الأول)، ثم أزمة قوانين مكافحة جرائم الوسط الرقمي(المطلب الثاني)

المطلب الأول

صعوبة الاستدلال في الجريمة الرقمية

تحدثا سابقا أن الجريمة الالكترونية بصفة عامة جريمة جد معقدة لطبيعة الرقمية الافتراضية الغير محسوسة. وهذا ما يصعب من عملية اكتشاف الجرائم التي تحدث بواسطة هذه الشبكة.

وعلى أساسي هذا قمنا بتقسيم هذا المطلب إلى ثلاثة فروع، بحيث خصصنا (الفرع الأول) لدراسة صعوبة اكتشاف الجريمة، أما (الفرع الثاني) صعوبة كشف هوية الجناة، و (الفرع الثالث) نقص الخبرة في مجال الاستدلال.

الفرع الأول

صعوبة اكتشاف الجريمة

انطلاقا مما قمنا بتوضيحه أعلاه، فإن بعد حدوث الجريمة واكتشافها يصبح أمام رجال ضباط الشرطة القضائية تحديات من أجل المواجهة الفعالة، ويرجع سببها إلى عدة اعتبارات.

أولا: غياب الأثر المادي للجريمة وسهولة محو الدليل :

توصف الجريمة الالكترونية بالهادئة، لان ارتكابها لا يحتاج إلى استعمال العنف أو القوة ولا إلى سفك الدماء أو وقوع جثث، وهذا ما تم التطرق إليه في جريمة الاتجار بالأشخاص عبر النطاق الشبكي الخاص، بحيث يقوم المجرم الرقمي باستدراج الضحايا من خلال جملة من الوسائل من بينها الاحتيال[1].

وعليه فالجريمة الالكترونية من الجرائم المستحدثة التي لا ترك شهودا يمكن الاستدلال بأقوالهم ولا بصمات يمكن تحليلها، إنما تقع في بيئة الكترونية افتراضية عن طريق استدراج الضحايا من خلال معلومات مغلطة مما يجعل من الجريمة غير مرئية[2].

[1]– حسين بن سعدي الغافري،"التحقيق و جمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، ص19. مقال متوفر في الموقع التالي: www.eastlaws.com

[2]– عمر حسين عباس، أدلة الإثبات الجنائي والجرائم الالكترونية" بحث مقدم إلى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكية في الوطن العربي، المنظم من طرف دولة مصر بمقر جامعة الدول العربية خلال الفترة الممتدة من 16-17أفريل2008، ص08.

ولعلى ما يزيد اكتشاف الجريمة الالكترونية والياتها أكثر صعوبة هو الوسيلة المستعملة في ارتكابها، والتي تشم في معظم الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد[1]، وهذا ما ينطبق على جرائم "derk web" باعتباره شبكة رقمية مشفرة يصعب فك وفتح شفرتها. هذا الأمر الذي يؤدي إلى تجريد الكيانات الإجرامية من الآثار والمعالم المادية التي يمكن الاستدلال من خلالها على وقوع الجريمة وإسنادها إلى شخص معين وهذا راجع إلى عدم كشف هوية المجرم الالكتروني الذي يمتلك قدرات فنية عالية والمعرفة الواسعة، والتي تسمح له بالتحكم في فريسته بثقة كبيرة من خلال اختيار الفترة والطريقة المناسبتين لارتكابها تجعل المجني عليه لا يشعر بها ولا يدري حتى بوقوعها رغم حدوثها على مرأى أعينه. وهذه القدرات الفنية العالية جدا كثيرا ما يكتسبها المجرمين من خلال مختلف المواقع الالكترونية ومنتديات القراصنة التي تضمن لهم الاتصال باستمرار فيما بينهم.

وتعتبر سهولة إخفاء الدليل الذي تخلقه الجريمة الالكترونية و سرعة محوه من الأسباب الجوهرية التي تقف دون اكتشاف الجريمة الالكترونية إثباتها[2]، إذ يستعمل المجرم الالكتروني عدة أساليب وتقنيات تسمح له بإخفاء كل آثار الجريمة والتستر عنها بسهولة كبيرة من أهمها، أسلوب التغليط والتضليل الذي يتم إما عن طريق التلاعب بقواعد

[1]– عمر حسين عباس، مرجع سابق، ص 08.

[2]– حسين بن سعدى الغافري، مرجع سابق، ص 09.

البيانات والبرامج أو إدخال بيانات مختلقة مزيفة أو محرفة في نظام معلومات الحاسب، أو تغيير مسار البيانات الصحيحة المدخلة دون أن يحس المجني عليه بذلك. أو نتيجة تردد عدد كبير من الأشخاص على المكان أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط بين زمن ارتكابها وبين حدوث النتيجة الإجرامية (كما هو الحال بالنسبة لمقاهي الانترنت) مما يفسح المجال لحدوث تغيرات أو عبث في الآثار المادية للجريمة أو زوال بعضها، وهو ما يلقي ظلالا من الغموض على الدليل[1].

بالإضافة إلى ذلك، فإن الدليل في الجريمة الالكترونية يتمثل عادة في بيانات أو معطيات الالكترونية على شكل كتابة أو تسجيلات صوتية أو صورية أو فيلمية، تخزن بذاكرة الحاسب بلغة رقمية في صورة برامج أو أنظمة تشغيل تتجسد في وحدات حسابية لا يمكن لأي شخص قراءتها و فهمها إلا باستعادتها في شاشة الحاسب، لذا يسهل محوها والتخلص منها بسرعة فائقة بمجرد الضغط على زر واحد في لوحة المفاتيح. ومن أمثلة ذلك، قيام أحد مهربي الأسلحة بالنمسا بإدخال تعديلات على الأوامر العادية لنظام تشغيل حاسب صغير يستخدمه في تخزين عناوين عملاته و المتعاملين معه، على نحو يجعل أية محاولة دخول إلى هذا الحاسب أو نسخ و طبع هذه العناوين قد تؤدي إلى المحو الفوري لكل البيانات[2].

[1]– حسين بن سعدي الغافري،المرجع السابق، ص19.

[2]– سليمان أحمد فضل، المواجهة التشريعية و الامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة للنشر والتوزيع، القاهرة،2000 ص 345-346.

ثانيا: العزوف عن التبليغ بوقوع الجريمة الإلكترونية

من بين الأسباب الرئيسة التي تحول دون اكتشاف الجريمة الالكترونية، تكتم المجني عليه عنها و عم تبليغ السلطات المختصة عن وقوعها بعد اكتشافها. إذ أثبتت التجارب أن معظم الجهات المجني عليها، لاسيما المؤسسات التجارية والمالية الخاصة أو العمومية تمتع عن الكشف حتى بين موظفيها عما تعرضت لها من اعتداءات إلكترونية، وتكتفي فقط باتخاذ إجراءات إدارية وأمنية داخلية دون أن تبلغ السلطات المختصة عنها. ويجد هنا الموقف مبرره في أمرين، الأمر الأول يتمثل في حرص هذه المؤسسات على عدم المساس بسمعتها وفقدان زبائنها والمتعاملين معها الثقة في كفاءتها وقدرتها على حماية مصالحهم[1]. والأمر الثاني هو تشكيكها في قدرة و كفاءة سلطات الأمن على التصدي لهذا النمط الإجرامي الجديد، وتخوفها من أن تؤدي أعمال البحث والتحري إلى حجز حواسبها أو تعطيل شبكتها و نشاطها لفترة طويلة، ما قد يتسبب في زيادة خسائرها بالمقارنة مع الخسائر التي سببتها الجريمة أصلا[2].

إثباتا لهذا الواقع، كشفت إحدى الدراسات الإحصائية التي أجراها المعهد الوطني للقضاء التابع لوزارة العدل الأمريكية مؤخرا بأنه أكثر من 70% من الجرائم الالكترونية

[1]– هشام محمد فريد رستم،"الجرائم المعلوماتية–أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي" بحوث مؤتمر القانون والكومبيوتر و الانترنت، جامعة الإمارات المتحدة، كلية الشريعة والقانون، المجلد02، ط3، من 1–3 ماي2000، ص435–436.

[2] - VERGUCHT Pascal, la répression des délits informatique dans une perspective internationale, thèse pour l'obtention du doctorat en droit, soutenue a la faculté de droit de l'université de Montpellier 1, Paris, 1996, p 323-326.

التي يتم اكتشافها لا تبلغ عنها إلى سلطات الأمن. وهي النتيجة نفسها التي أكدتها الدراسة المنجزة من طرف معهد أمن الحاسوب بمشاركة مكتب التحقيق الفيدرالي في الولايات المتحدة الأمريكية[1].

ومن أجل التقليل من ظاهرة التكتم عن الجرائم الالكترونية، عمدت بعض الدول إلى فرض التزاما على عاتق جهات المجني عليها بالإبلاغ عن هذه الجرائم بمجرد عمهم بوقوعها، و جعلت أي تقصير أو إخلال بهذا الالتزام يعرض صاحبه إلى عقوبات جزئية[2].

إلا أن هذا الحل تعرض لانتقادات شديدة من طرف الفقه والقضاء الدوليين، مفادها أنه من غير المقبول أبدا تحويل المجني عليه إلى مجرم يتم معاقبته بمجرد عدم تبليغه عن الجريمة التي وقع ضحية فيها، في حين يبقي المجرم الحقيقي دون عقاب[3].

[1]– حسين بن سعدي الغافري، المرجع السابق، ص19–20.

[2]– جمال براهيمي، المرجع السابق، ص200.

[3]– هشام جمال رستم، المرجع السابق، 438.

الفرع الثاني

صعوبة كشف هوية الجناة

إن اكتشاف هوية الجناة الرقمين من ابرز العراقيل في عملية التحقيق الالكتروني، ويعود ذلك (أولا) تعذر تحديد عنوان المجرم الالكتروني، وكذا فرض الجناة لتدابير أمنية(ثانيا).

أولا: تعذر تحديد عنوان المجرم الالكتروني[1]

من بين المسائلة الشائكة التي تعرقل عملية التحقيق في الجرائم الالكترونية صعوبة تحديد مكان تواجد جهاز الحاسب الآلي مصدر النشاط الإجرامي، والذي يسمح من خلاله الكشف عن المجرم.

لذلك تستعين سلطات التحقيق عادة لتحديد مكان الحاسب الآلي أو الجهاز مصدر الفعل الإجرامي بنظام فحص الكتروني يسمي يعلم البصمات المعاصر، الذي يتم من خلاله نبع الحركة العكسية لمسار الانترنت، أو الحركة التراسلية للنشاط الممارس عبر الانترنت[2] إلى غاية الوصول إلى عنوان رقي للجهاز (padresse internet protocole IP).

[1]– طرح بشدة في مؤتمر الدولي لجرائم الحاسوب المنعقد في أوسلو في الفترة الممتدة بين 29 و 31 ماي 2000، مشكل عدم إمكانية البنية التحتية للانترنت من التوصل إلى تحديد هوية مرتكب الجريمة أو المصدر الحقيقي لها، رغم توفر إمكانية التعرف على مكان ورقم الحاسوب أو الجهاز المرتبط بالانترنت والمستعمل كوسيلة لارتكاب الجريمة عن طريق عنوان(IP) . ولكن مقابل ذلك، اعتبر بعض المشاركين في المؤتمر مسألة عدم الكشف عن شخصية و هوية الفاعل الذي يتستر وراءها مرسل الرسالة غير المشروعة هي أمر نسبي، إذ لا يوجد تجهل بالمعني الكلي لشبكة المعلومات، حيث يترك الفاعل في كل الأحوال آثار أثناء تنقله في شبكة المعلومات تسمح للمحقق الوصول إليه، بالتالي فان هذا الأمر يتوقف بالدرجة الأولى على فطنة رجال الضبطية القضائية من خلال الإسناد إلى فكرة الدلائل الكافية وما ينبثق منها من الشبهات، كما لو كان الحاسب الذي تم بواسطته ارتكاب الجريمة هر حاسب شخصي، ففي هذه الحالة يمكن للمحقق استجواب صاحب هذا الحاسب المشتبه فيها عما إذ سمح لشخص آخر استعمال جهازه، تاريخ و مدة استعماله، ثم يقارن كل هذه المعلومات مع معلومات الجريمة، كما يتوقف الأمر كذلك على مدى فعالية ونجاعة أساليب تتبع الآثار عبر الانترنت (la Traçabilité) وتحديد هوية المستخدمين حتى يتسنى تحتية هوية الشخص المسئول جنائيا. للمزيد اطلع على: **أرجومة موسى مسعود**، "الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية غبر الوطنية"، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلومات والقانون، المنظم من طرف أكاديمية الدراسات العليا طرابلس الفترة الممتدة من 28–29أكتوبر 2009.

[2]– عبد الحميد عبد المطلب، استخدام برتوكول (TCP/IP) في البحث وتحقيق الجرائم على الكمبيوتر، ص05، بحث منشور على الموقع:.www.arablaw.info.com

وهذا العنوان هو عبارة عن بروتوكول لعنونة البيانات و المواقع في شبكة الانترنت، الانترنت، والذي يتم التعرف بقضاء على الجهاز الموصول بشبكة الانترنت من خلال عناوين حدية، مع العلم أن لكل جهاز الكتروني عنوانه الوحيد و الخاص به يسمي (IP)، وكل عنوان (IP) مكون من جزئيين، الجزء الأول يشمل أرقام الشبكة والثاني يشمل أرقام مقدم الخدمة. وإذا كانت الاستعانة بالمعلومات والعناوين والمصادر التي يحتويها نظام (IP/TCP) يساعد حقيقة على الكشف عن مصير الجهاز المستخدم في ارتكاب جريمة الكترونية ما و موقعه، وبالتالي الكشف عن المجرم التي يفترض أن يكون صاحب هذا الجهاز، إلا أن هذه النتيجة ليست دائما صحيحة و موثقة، لأن ما يتم التوصل إليه من خلال التقنية السابقة هو عنوان رقمي للحاسب فقط (adresse IP)، وهذا لا يكفي وحده لإسناد الفعل الإجرامي إلى صاحب الحاسب المذكور[1] . إذ من المحتمل جدا أن لا يكون هذا الأخير هو مرتكب الجريمة.

---

[1]– راسل تاينر،أهمية التعاون الدولي في منع جرائم الانترنت بحث مقدم إلى الندوة الإقليمية جول: الجرائم المتصلة بالكومبيوتر، الجارية المملكة المغاربية في الفترة 19–20جوان2007، ص113–114.

2– أكدت المحكمة الفرنسية هذه الاحتمالات في قضية شهيرة تدعي فوريسيوا (Faurission)، حين نشرت رسالة الكترونية عنصرية ضد الصهيونية تحمل اسم الفرنسي(Robert Faurission)، ولما اكتشفت على الموقع (Aaargh) الذي تم إيوائه في الولايات المتحدة الأمريكية حركت دعوى قضائية ضد هذا الشخص، إلا أن المحكمة لم تستطيع إقامة الدليل على أن المتهم هو الناشر الحقيقي للرسالة المجرمة. وبالتالي قضت بأن وجود اسم المتهم في ذيل الرسالة لا يثبت بأنه مصدرها الحقيقي ولا يكفي أن يكون دليل إدانة، لأن هذا الاسم يمكن لأي شخص أن يكتبه إمعانا في التمويه، الأمر الذي يقتضى إلزام متعهد الوصول بتحديد شخصية المشترك و عدم توصيل الأسماء المجهولة. للمزيد راجع:

T.G.I.novembre.1998.disponible a l’adresse suivant
http://www.legalis.jnet.decision/ilcite-devert/correct-paris-1998-htm.

ثانيا: فرض الجناة لتدابير الأمن

يتميز المجرم الالكتروني عن المجرم العادي بالذكاء و المعرفة الفنية الواسعة ، وهذه الخصلة تمكنه من التخطيط جيدا لجريمته قبل أن يقدم على ارتكابها، وإحاطتها بأساليب أمنية وتدابير الحماية الفنية التي تحول دون كشف أمره وتعيق مهمة أجهزة الاستدلال والتحقيق في الوصول إلى الدليل، فالمجرم الالكتروني غالبا ما يضرب سياجا أمنيا على أفعاله غير المشروعة قبل ارتكابها، وذلك باستخدام كلمات المرور السرية وترميز البيانات المخزنة إلكترونية والمنقولة عبر شبكات الاتصال، وتشفيرها بشكل يستحيل على سلطات البحث والتحري تعقب آثار الجريمة واستخلاص الدليل حولها دون الحصول على هذه الرموز والشفرات [1].

قد يلجا المتهم إلى تشفير[2] البيانات المخزنة داخل حاسوبه للحيلولة دون وصول المحقق إلى الأدلة التي تدينه، وهنا أيضا يجد المحقق نفسه أمام خيارين لحل مشكلة التشفير وهما، إما أن يحصل على مفاتيح الشفرات من المتهم مشغل الحاسوب، وإما أن يحاول فك الشفرات بنفسه. إلا أن في الخيار الثاني يجب أن يكون المحقق متمكن يعلم

[1]– جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجية الحديثة، دار النهضة العربية، القاهرة، 2002، ص 115.

[2]– راسل تاينر،أهمية التعاون الدولي في منع جرائم الانترنت بحث مقدم إلى الندوة الإقليمية جول: الجرائم المتصلة بالكومبيوتر، الجارية المملكة المغاربية في الفترة 19–20جوان2007، ص115.

[3]– ويقصد بتشفير البيانات استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها البيانات أو المعلومات المراد تمريرها أو إرسالها غير قابلة للفهم من قبل الغير، أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومات المخزنة في الحاسوب بدونها، مع العلم أن عملية التشفير تتم وفق معادلات رياضية معقدة تسمى الخوارزميات.

تحليل الشفرات أو ما يعرف بعلم استرجاع النص الواضح بعبارة معينة بدون معرفة المفاتيح، ويرتكز هذا العلم على الرياضيات التطبيقية وفروعها المختلفة مثل نظرية الاحتمالية و نظرية الإعداد والإحصاء والجبر، وهو الأمر المفقود لدى المحقق، ومن ضمن الأساليب الأمنية والتدابير الحماية الفنية المهمة التي يستعين بها المجرم الالكتروني لإعاقة مهمة أجهزة الاستدلال والتحقيق في الوصول إلى الدليل[1].

الفرع الثالث

نقص الخبرة في مجال الاستدلال

إذا كانت السلطات القائمة بالتحقيق من رجال الضبطية و قضاة تلعب دورا كبيرا في التحري عن الجرائم و البحث عن مرتكبيها في إطار الجرائم التقليدية، فإن دورها في مكافحة الجرائم الالكترونية محدود ولا يرقى إلى الدرجة نفسها، وذلك راجع إلى عدة أسباب بعضها مرتبط بشخصية المحقق، والبعض الأخر يتعلق بنقص مهاراتهم الفنية في استخدام الوسائل الالكترونية الحديثة والانترنت، وقلة خبرتهم في تقنيات البحث والتحقيق بخصوص الجرائم المتصلة بهذه الوسائل، الناتج عن عدم إلمامهم بأساليب ارتكاب الجرائم الالكترونية وعدم معرفتهم باللغة العلمية الرقمية.

[1]– محمد حسام لطفي،"الجرائم التي تقع على الحاسبات أو بواسطتها" بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 1993، ص496.

على غرار تلك، فان الطبيعة الخاصة للبيئة الالكترونية والخصوصية اللامادية لدليل الالكتروني الرقمي الذي يتطلبه إثبات الجريمة الالكترونية ينعكس سلبا على عمل الجهات المكلفة بالبحث والتحري، إذ يتطلب الكشف عن هذه الجرائم اكتساب جهات التحقق مهارة خاصة على نحو يساعدهم على مواجهة التقنيات المعلوماتية العالية[1]، فنقص الخبرة لدي هؤلاء قد يقضي إلى تدمير الدليل وإتلافه، على اعتبار أن جهلهم بأساليب ارتكاب الجرائم المعلوماتية بجعلهم في كثير من الأحيان يقعون في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية أو تدميرها[2]، وقد ترتكب جرائم إلكترونية على مرأى ومسمع من سلطات الضبط، بل قد يقدمون على تقديم يد العون لمرتكبي هذه الجرائم عن جهالة دون أن يشعروا بذلك. من هنا يرى المتخصصون في مكافحة الجرائم الالكترونية أن الأنظمة المعلوماتية و ما يقع عليها من جرائم تعد تحديا حقيقيا لأجهزة العدالة الجنائية، ذلك لأن رجل الأمن غير المتخصص والذي انحصرت معلوماته وخبراته في الجرائم التقليدية من قل وضرب وسرقة لن يكون قادرا على التعامل مع الجريمة الالكترونية الحديثة التي ترتكب بواسطة تقنيات عالية[3].

[1]– محمد الأمين البشيري،" التحقيق في جرائم الحاسب الألى" بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، ط الثالثة، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة من 1 إلى 3 ماي2004، ص1070.

[2]– جميل عبد الباقي الصغير، مرجع السابق، ص 115.

[3]– حسين بن سعيد بن سيف الغافري، مرجع السابق، ص410.

رغم هذه الجهود المبذولة إلا أن أجهزة القضاة لازالت عاجزة على مواجهة هذا نوع من الأنظمة التكنولوجية المتطورة خاصة"الدارك وايب"، ويرجع هذا العجز لعدم تفرغ القضاة لهذا النوع من الجرائم الالكترونية، مما جعل من هذا الأمر ضرورة إنشاء وحدات خاصة في التحقيق في هذا النوع من الجرائم. وقد يكون لحداثة هذا النوع من الجرائم وقلة المستكشف عنها عامل أخر لعدم اكتساب تلك الأجهزة خبرة التعامل معها، إضافة إلى الكم الهائل من المعلومات الموجودة على شبكة الانترنت، مما يستلزم الإلمام بالموضوع ومعرفة معلومات الشبكة من خلال البحث فيها وكذلك تدريب المحققين عنها.

المطلب الثاني

صعوبة قوانين مكافحة الجرائم المتعلقة بالشبكة الخاصة

نظرا لحداثة جرائم الشبكة الرقمية وسرعة تطورها خاصة التي هي محل دراستنا، وكذا النصوص التقليدية التي أصبحت عاجزة على مواجهة هذا النوع من الجرائم الرقمية المتطور، خاصة أن النصوص التقليدية جاءت وفق مفاهيم تقليدية لا تتفق مع الطابع الرقمي، انطلاقا من هذا قمنا بتقسيم هذا المطلب إلى ثلاثة فروع،(الفرع الأول) عدم كفاية النصوص العقابية التقليدية، (الفرع الثاني) قصور إجراءات التحقيق مع جرائم الشبكة الخاصة.

الفرع الأول

قصور النصوص العقابية التقليدية

بالرغم من التطور التكنولوجي في مجال المعلوماتية، إلا أنه أفرز العديد من الجرائم المستحدثة ذات الطبيعة الخاصة"دارك ويب"، مما جعل مكافحتها صعب وهذا يتعلق بالنصوص العقابية المألوفة التي وضعت لكي تطبق على الجرائم التقليدية،إذ ترتب عليه الكثير من المشكلات بالنسبة لملاحقة هذه الجرائم الالكترونية ذات الطابع المعنوي و التي قد تتعدد أماكن ارتكابها داخل الدولة الواحدة، أو يمتد نطاقها ليشمل الكثير من الدول عبر شبكة الانترنت، فيتعذر تبعا لذلك اتخاذ إجراءات جمع الدليل بالنسبة لها، أوقد تلحق عدم المشروعية بهذه الإجراءات.

إن عدم تطور القوانين بنفس السرعة والوتيرة التي تتطور بها وسائل الإعلام والتكنولوجيا و مهارات الذهن البشري في تسخير مبتكرات التكنولوجية، جعل القوانين التقليدية تقف عاجزة عن مواجهة العديد من الجرائم الجديد التي ارتبطت بظهور و انتشار الوسائل والأجهزة الالكترونية، خاصة إذا علمنا أن القوانين الوضعية السائدة في أغلب دول العالم يحكمها مبدأ الشرعية الجزائية الذي ينص"**على أنه لا جريمة و لا عقوبة إلا بالنص**"، وأن نطاق التجريم بالقياس في ظل هذا المبدأ يكون ضيقا جدا[1].

[1]– سرحان حسن المعيني، التحقيق في جرائم تقنية المعلومات، مجلة الفكر الشرطي، مجلد 20، عدد 79، صادر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، أكتوبر 2011،ص21.

فثمة أفعالا جديدة كثيرة خاصة في الدول المتخلفة، مرتبطة باستعمال الحاسب الآلي غير مجرمة بمنظور القوانين العقابية التقليدية، ولا تمتد إليها لمكافحتها رغم تهديدها للمصالح العامة و تشكل خطورة بالغة على النظام العام، ومن الأمثلة على هذه الأفعال الاعتداء على حرمة الحياة الخاصة المعلوماتية، هذا النوع من الاعتداء لا يعاقب عليه قانون العقوبات إلا إذا كان مرتبطا بمكان خاص، أما التسلل والنفاذ إلى أسرار الفرد وخصوصياته الشخصية أو المهنية من خلال الوصول إلى المعلومات المخزنة لديه في أنظمته المعلوماتية داخل الحاسب، فان هذا التصرف لا يخضع للتجريم وفقا للقواعد العامة[1].

كما أن الدخول في نظام حاسب مملوك للغير وسرقة المعلومات منه، لا يعد جريمة بمفهوم القوانين التقليدية لان السرقة حسب هذه الأخيرة لا ترد إلا على المال المنقول، وهذه الصفة لم تثبت بعد للمعلومات كونها تعتبر سوى أفكار معنوية بحتة، زيادة على ذلك فان فعل السرقة أو الاختلاس بالمفهوم الكلاسيكي يعني تجريد الغير من ماله في حين أن اختلاس المعلومات يتمثل في أخذ نسخة منها مع الإبقاء بأصلها عند صاحبها، لذا فإنها لا يحميها التجريم المقرر في جرائم الأموال[2].

2- غنام محمد غمام،"عدم ملائمة القواعد التقليدية في القانون العقوبات لمكافحة جرائم الكمبيوتر"، بحث مقدم إلى مؤتمر القانون و الكمبيوتر والانترنت، كلية الشريعة والقانون،جامعة الإمارات العربية المتحدة، الفترة الممتدة من 01 إلى 03 ماي 2003، ص 625.

[2]- غنام محمد غمام، المرجع السابق، ص 646.

في مثل هذه الحالات، تثور العديد من الصعوبات أمام تطبيق نصوص التجريم التقليدية، مردها أن هذه النصوص وضعت أساسا لحماية الأشياء المادية في مواجهة صور الاعتداء المألوفة والتقليدية مما يتعذر معه أو يستحيل أن يقع تحت طائلة العقاب الاعتناء على عناصر ومكونات الأنظمة المعلوماتية المتمثلة في صور غير مادية، فضلا عن أن تطبيق مثل هذه النصوص قد يتعارض أحيانا مع طبيعة الوسائل المستخدمة لتنفيذ الجرائم التي يكون محلها البيانات أو المعلومات بشتى أنواعها المرئية أو المصورة أو المكتوبة[1].

ونظرا للعجز الكبير الذي أثبتته القوانين العقابية التقليدية في مواجهة الجرائم الالكترونية، حاولت بعض الدول خاصة المتقدمة منها في استدرك الوضع بسن تشريعات جديدة تتجاوب مع الطبيعة الخاصة لهذه الجرائم الحديثة، فمنها التي اختارت تعديل قوانينها العقابية وإضافة نصوص جديدة إليها تتجاوب مع الظاهرة الإجرامية الحديثة لسد الفراغ التشريعي القائم في هذا المجال[2]، ومنها التي فضلت استحداث نصوص جديدة خاصة بهذا النوع المستجد من الإجرام، غير أن الملاحظ في هذه القوانين، أنها لا تشمل كافة الأفعال غير المشروعة الناتجة من استعمال التكنولوجيا الحديثة، بسبب عدم تطورها بالوتيرة نفسها التي تتطور بها الجرائم الالكترونية، كما أن معظم دول العالم خاصة

[1]– جمال براهيمي، مرجع السابق، ص 222.

[2]– مرجع نفسه، ص 223.

المتخلفة منها لم تسن بعد قوانين تجرم مثل هذه الأفعال غير المشروعة، واكتفت فقط بتطبيق القواعد القانونية القائمة رغم ثبوت قصورها، ولعل السبب في ذلك هو افتقارها إلى الخبرة والتخصص والمعرفة الكافية للبيئة الالكترونية العالية التقنية والمعقدة[1].

الفرع الثاني

قصور إجراءات التحقيق مع جرائم الشبكة الخاصة

لم يتوقف الأمر عند قصور النصوص العقابية في مواجهة الجرائم الالكترونية، بل تعد إلى القوانين الإجرائية، وهذا راجع(أولا) صعوبة إخضاع المكونات المنطقية للحاسوب الألى للتفتيش والضبط،(ثانيا) صعوبة معاينة الجرائم الإلكترونية.

أولا: صعوبة إخضاع المكونات المنطقية للحاسوب الألى للتفتيش والضبط

إذا كان الهدف الأساسي من التفتيش كوسيلة إجرائية هو الحصول على دليل مادي يثبت الجريمة وينسبها إلى مرتكبيها، فإنه بذلك يتنافى مع الطبيعة غير المادية للمكونات المنطقية للحاسب الآلي، كونها مجرد برامج و بيانات الكترونية ليس لها أي مظهر محسوس في العالم الخارجي[2]. ويرجع هذا التناقض أساسا إلى غياب مفهوم واضح ومتفق عليه المصطلح (**شيء**) الذي يفترض أن يكون محلا للتفتيش والضبط، فإذا كان التفتيش كما هو متعارف عليه ينصب على شيء مادي فقد أثير تساؤل حول مدى انطباق لفظ

[1]– جمال براهيمي، المرجع السابق، ص223.

[2]– نبيلة هبة هروال، مرجع سابق، ص 225.

(الشيء) على الكيانات المعنوية أو الوسط الافتراضي للحاسوب؟ وهي المسألة التي انقسم رأي الفقه الجنائي فيها إلى ثلاثة اتجاهاه مختلفة[1].

فذهب الاتجاه الأول(اليوناني، كندا) إلى جواز تفتيش وضبط المكونات المعنوية للحاسوب بمختلف إشكالها، وحجته في ذلك هي أن القوانين الإجرائية عندما تنص على جواز تفتيش وضبط أي شيء يتعلق بالجريمة أو يساعد على كشف حقيقة وقوعها، فان ذلك يجب أن يفسر بالمعني الواسع ليشمل كل من المكونات المادية والمعنوية للحاسوب معا[2].

وبالمقابل ذهب اتجاه فقهي آخر وهو الغالب(الألماني، أمريكا الجنوبية)، إلى عدم إمكانية إخضاع المكونات المعنوية للحاسوب من برامج و بيانات العملية التفتيش و الضبط، لأن الغرض الأساسي من التفتيش هر ضبط الأدلة المادية، ولما كانت هذه المكونات الالكترونية المنطقية تفتقر إلى مظهر مادي ملموس كالأشياء المادية فلا يمكن تفتيشها ولا ضبطها، إلا إذا تم تعديل غاية التفتيش تلك بجعلها تشمل ضبط الأدلة المادية وغير المادية على حد سواء[3].

[1]– نبيلة هبة هروال، مرجع السابق، ص225.

[2]– خالد ممدوح إبراهيم، مرجع السابق، ص197.

[3]– هلال عبد الله احمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 2006، ص 89.

وعكس ما ذهب إليه الاتجاهين الفقهين الأول و الثاني، يري اتجاه فقهي ثالث بأنه لا يجب الخلط عند تحديد مدلول (الشيء بالنسبة لمكونات الحاسب بين الحق الذهني للشخص على البرامج والبيانات والكيانات المنطقية الأخرى، وبين طبيعة هذه البرامج والكيانات، إنما ينبغي الرجوع في ذلك إلى تحتية مدلول كلمة(المادة) في العلوم الطبيعية لما كانت المادة تعرف بأنها " كل ما يشغل حيزا ماديا في فراغ معين ، وكان الحيز مما يجوز قياسه و التحكم فيه، فان البرامج و الكيانات المنطقية باعتبارها تشغل حيزا مادها في ذاكرة الحاسب الآلي ويمكن قياس حيزها بوحدات قياس خاصة هي، البايت (bite) والكيلوبايت (kilobit) والميجابايت (Mégabit) والجيجابايت (Gigabit)، وتأخذ شكل نبضات الكترونية، تتوفر على خصائص المادة و تتشابه مع التيار الكهربائي الذي اعتبره الفقه والقضاء من قبيل الأشياء المادية[1].

صحيح هناك بعض الدول التي تدخلت مؤخرا لحل هذا المشكل(قانون 09-04)، عن طريق إحداث تعديلات في تشريعاتها الإجرائية التقليدية بما يضمن سريان إجراء التفتيش والضبط على المكونات المادية والمنطقية للحاسوب على حد سواء، إلا أن هذا المشكل مازال قائما في معظم دول العالم خاصة المتخلفة منها، بسبب احتفاظها بالقوانين الإجرائية التقليدية لمواجهة الجرائم الالكترونية رغم عدم ملائمتها مع طبيعة هذه الأخيرة.

[1]– رشاد خالد عمر،المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، دراسة تحليلية مقارنة، المكتب الجامعي الحديث، القاهرة،2013،ص147.

وهذا الأمر من شأنه أن يشكل عقبة كبيرة أمام هيئات التحقيق بحيث يجدون أنفسهم في موقف حرج مبقيين بين جواز وعدم جواز إستاد التفتيش و الضبط ليضم المكونات المعنوية، مما قد يدفعهم في نهاية المطاف إلى وقف التحقق ومن ثمة إفلات المجرم الإلكتروني.

ثانيا: صعوبة معاينة الجرائم الالكترونية

لا تتمتع المعاينة في مجال كشف غموض و ملابسات جرائم الالكترونية وإثباتها بالدرجة نفسها من الأهمية التي تتمتع بها في مجال الجرائم التقليدية، وذلك راجع إلى عدة أسباب أولها أن هذه الأخيرة لها مسرح تجري عليها الوقائع و الأحداث، وتخلف أثارا مادية تقوم عليها الأدلة كالبصمات أو قطرات دم[1].

هذا المسرح يعطي المجال أمام سلطات التحقيق والاستدلال الجنائي في كشف الجريمة عن طريق المعاينة الميدانية و التحفظ عن الآثار المادية التي خلفتها هذه الجريمة، في حين أن فكرة معاينة مسرح الجريمة الالكترونية يتضاءل دوره في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة، لأن معظم الجرائم التي تقع على نظم المعلومات وشبكات الانترنت قلما تخلف ورائها آثارا مادية[2]

كما أنه من الممكن أن يتردد عددا كبيرا من الأشخاص على مكان أو مسرح الجريمة خلال الفترة الزمنية الممتدة من لحظة وقوع الجريمة حتى اكتشافها والتي تكون عادة

[1]– هشام محمد فريد رستم، مرجع السابق، ص59.

[2]– مرجع نفسه، ص60.

طويلة نسبيا[1]، مما يفسح المجال لحدوث تغيير أو تلف أو عبث بالآثار المادية أو زوال بعضها، وهو ما يلقي ظلالا من الشك على الدليل المتحصل من المعاينة، ناهيك عن إمكانية تلاعب الجاني في البيانات أو المعطيات محل المعاينة عن بعد أو محوها عقب الولوج إليها عبر الانترنت بواسطة جهاز أخرى مرتبط بها[2]

أضف إلى ذلك، فان عدم دراية وتحكم المحقق بالجوانب الفنية والتقنية للاستخدام شبكة الانترنت، ونقص كفائتهم العلمية في مجال الحاسبات واسترجاع المعلومات، وأساليب التعامل مع نوعية الآثار والأدلة التي يمكن أن يحويها مسرح الجرائم الالكترونية، قد يؤثر سلبا على المعاينة في هذه الجرائم، الأمر الذي يعطي الفرصة للمحكمة بالتشكيك في صحة ومشروعية الدليل الموجه ضد المتهم، وبالتالي استبعاده.

[1]– صغير يوسف، مرجع سابق، ص 131.

[2]–جمال الإبراهيمي، المرجع السابق، ص229.

الخـــــــاتمة

من خلال الدراسة المنجزة، يتضح لنا أن جريمة الاتجار بالأشخاص لم تعد تلك الجريمة التقليدية، بل أصبحت جريمة بشعة خالية من الإنسانية لا يتقبلها عقل أو قلب بشري طبيعي، وهذا راجع لارتباطها بالشبكة الدولية الخاصة "الويب المظلم".

إضافة إلى ذلك، شهدت الجريمة ارتفاع متزايد مع التطور التكنولوجي لهذه الشبكة، والذي يرجعه الخبراء التقنين إلى سرية الموقع وتشفره، مما جعل من أمر المكافحة الجنائية له صعب.

HAوقد تضمنت هذه الدراسة، إيضاحا لرؤية إجرائية و موضوعية تتناول مسألة الإجراءات المتخذة في هذه الجريمة باعتبارها جريمة تقليدية ترتكب في وسط رقمي، وكذا مسألة العجز الإجرائي والتشريعي في مواجهة هذه الجريمة.

من جانب الإجراءات الموضوعية، فإن المشرع الجزائري جرم فعل المتاجرة بالأشخاص في قانون العقوبات، كما انه جرم هذه الأفعال التقليدية التي ترتكب بواسطة منظومة معلوماتية، وهو لا يعاب على هذا. لان الجاني في كلتا الحالتين لا يمكنه الهروب من مسؤوليته الجنائية. لكن ما يعاب عليه، هو عدم تجريمه لتجارة التي تستخدم داخل هذا النطاق، باعتبار أن التجارة الرقمية مسموحة، كون أن هذه الأخيرة "الدارك ويب" من المواقع المشفرة ولا يمكن معرفة ما يحدث داخله من معاملات تجارية، إذ انه لو كانت النشطات القائمة بداخلة مشروعة لما شفرت.

والمشرع الجزائري من خلال القانون 09-04، جرم فعل الدخول/أو البقاء في منظومة المعلوماتية، وهذا حماية للمنظومة، لكنه لم يجرم فعل الدخول/أو البقاء في الشبكات المشرفة.

وعليه من هذا الجانب التجاري الرقمي المشفر، وجب على المشرع الجزائري التدخل في إطار التعديل لقانون 09-04، بتجريم فعل الدخول أو البقاء في الشبكات المشفرة.

إضافة أنه يعاب على حصر صورة الاستغلال باعتبارها لا تتناسب مع القصد الجنائي الخاص، كونها لا تتناسب مع طبيعة الشبكة الرقمية.

من الجانب الإجرائي، فإن اعتماد المشرع الجزائري على جملة من الإجراءات الحديثة التي تدخل ضمن مكافحة جرائم المعلوماتية، فيمكن القول أنها نافعة بشكل يتناسب إلى حد بعيد مع الجرائم التي تحدث في "السر فيس ويب"، وهي غير مجدية مع الجرائم التي تحدث في "الديب ويب"، وهذا راجع لتشفير وسرية الموقع، خاصة لما عجز البرتوكولTCP في تحديد هوية الجناة، وكذا مراقبة الاتصالات الرقمية بشكل مباشر، والذي يعتمد علية المحققون في مجال البحث والتحري الرقمي، إضافة إلى أن الجاني من خلال هذه الشبكة لا يترك أي أثر رقمي له صله بالجريمة، مما يجعل من أمر المعاينة والتفتيش والحجز وغيرها من الإجراءات غير مجدية. مما يستلزم الرجوع إلى التسرب الإلكتروني، مع توفير الأمن وسلامة المتسرب.

ومنه في ايطار مكافحة جريمة الاتجار بالأشخاص عبر النطاق الشبكي الخاص، فإن البحث في آليات الدمج بين المكافحة التقنية والمكافحة الجنائية، من خلال إنشاء مخابر مختصة لهذه الظاهرة الرقمية، وكذا فرق علمية تهتم بالجانب التقني الحديث، تسعى إلا الولوج لهذه الشبكة من أجل كشف أسرارها، وكذا وضع البرامج القوية لمكافحتها(مكافحة الفيديوهات التي تدعو للممارسات التي كانت محل الدراسة).

قائـمة المـــصادر

و المـــــراجع

المصـــــــــــــــــــادر

- **القرءان الكريم.**

المراجـــــــــــــــــــع

أولا: المراجع بالغة العربية

1. الكـــــــتب:

أ- الكتب العامة:

- احمد غاي، ضمانات المشتبه فيه أثناء التحريات الأولية، طبعة 2005، دار الهومة، الجزائر، 2005، ص 231.
- عبد الله أوهايبية، شرح قانون العقوبات الجزائري، المؤسسة الوطنية للفنون المطبعية، الجزائر، 2011.
- عبد الرزاق طواهرية، شياطين بانكوك، جحيم ألدارك ويب،الطبعة الثانية،المثقف للنشر والتوزيع، باتنة، الجزائر، 2017.
- عبود السراج، شرح قانون العقوبات، القسم العام، نظرية الجريمة، مطبوعات جامعة دمشق، دمشق، سوريا، 2007.
- – محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، الطبعة02، دار هومة، الجزائر، 2010.

ب- الكتب المتخصصة:

- أكرم عمر دهام، جريمة الاتجار بالبشر دراسة مقارنة، دون ط، دار الكتب القانونية، مصر، 2011.
- سليمان أحمد فضل، المواجهة التشريعية و الأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة للنشر والتوزيع، القاهرة،2000.
- سوزي عدلي ناشد، الاتجار في البشر بين الاقتصاد الخفي والاقتصاد الرسمي، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان،2008.

- مبارك هشام عبد العزيز، الاتجار بالبشر بين الواقع والقانون، مركز الإعلام الأمني، المنامة، البحرين، 2010.
- مطر محمد يحي وجمع من المختصين، الجهود الدولية في مكافحة الاتجار بالبشر، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2010.
- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكومبيوتر و الانترنت، دار الكتاب القانونية، مصر، 2006.
- نبيل صقر، جرائم المخدرات في التشريع الجزائري، دار الهدى، الجزائر،2006.
- نصر الدين مبروك، جريمة المخدرات في ضوء القوانين والاتفاقيات الدولية، دار هومة، الجزائر، 2007.
- هلال عبد الله احمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 2006.
- مبارك هشام عبد العزيز، ماهية الاتجار بالبشر بالتطبيق القانون البحريني رقم01 لسنة2008 بشأن مكافحة الاتجار بالأشخاص، مركز الإعلام الأمني البحريني،2009.
- عايد شيحان العيسى، فاعلية التكامل الأمني والعدلي في مكافحة جرائم الاحتيال، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2006.

2- المقالات العلمية:

- إيهاب شوقي، الحرب السيبرية... حرب المستقبل المفزعة، تاريخ النشر 19 فبراير2015، تاريخ الإطلاع 05 جوان 2019، رابطة النشر: https://www.hespress.com
- جحيش فؤاد، التجارة الرقمية عبر "الدارك ويب" قصور في التجريم وعجز في المتابعة " دراسة تحليلية نقدية في ظل القانون الجزائري"،مجلة صوت القانون السياسية، العدد02، 2017.
- حسين بن سعدي الغافري،"التحقيق و جمع الأدلة في الجرائم المتعلقة بشبكة الانترنت. مقال متوفر في الموقع التالي: www.eastlaws.com

– سرحان حسن المعيني، التحقيق في جرائم تقنية المعلومات، مجلة الفكر الشرطي، مجلد 20، عدد 79، صادر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، أكتوبر 2011.

– عبيد عبد الله عبد، جريمة الاختطاف بين الشريعة والقانون، مجلة جامعة كركوك للدراسات الإنسانية، المجلد السابع، العدد الأول، السنة السابعة، كركوك، العراق، 2012.

– عادل يوسف عبد النبي الشكري، "الجريمة المعلوماتية وأزمة الشرعية الجزائية"، مجلة مركز دراسات الكوفة، مج01، عدد07، 2008.

– محمد خلف بن سلامة، جريمة الاتجار بالبشر في الشريعة الإسلامية والقوانين الوضعية، مجلة الفقه والقانون، عدد 38، 2015.

– محمد على سالم، حسن علي سالم، الجريمة المعلوماتية، مجلة جامعة بابل للعلوم الإنسانية، مـج14، عدد 03، 2007.

– منجد منال، المواجهة الجنائية لجرائم الاتجار بالأشخاص في القانون السوري (دراسة تحليلية)، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 28، العدد الثاني، دمشق، سوريا، 2012.

– الحسين أخدوش، الأسلحة الرقمية من خيال العلم إلى واقع الحرب السيبيرية، مقال منشور بتاريخ: 25مارس2019، تاريخ الإطلاع 01 جوان 2019، رابطة المقال: https://www.hespress.com/writers/426460.html

3–الرسائل و المذكرات:

أ.الرسائل:

– بختيل عبد الرحمن، التنظيم الدولي للأسلحة الخفيفة، مذكرة من أجل الحصول على شهادة الماجستير في الحقوق، فرع القانون الدولي والعلاقات الدولية، كلية الحقوق بن عكنون، جامعة الجزائر 1، الجزائر.

– سليمان مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات، (رسالة الماجستير)، أكاديمية نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، 2003.

– محمد بن ناصر السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب و الانترنت" دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية"، رسالة لنيل درجة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

– يوسف صغير، الجريمة المرتكبة عبر الانترنت، رسالة لنيل شهادة الماجستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2013.

ب. المذكرات:

– فؤاد جحيش، جرائم الوسط الرقمي، تجريم حديث بأبعاد تقليدية، دراسة تحليلية، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية تخصص جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، البويرة، الجزائر، 2015.

– جمال براهيمي، التحقيق الحنائي في الجرائم الإلكترونية،أطروحة لنيل شهادة الدكتوراه في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2018.

– صفاء كزونة، جريمة الاتجار في البشر وفق الوثائق الدولية، مذكرة الماستر تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2013–2014.

– على مسعودان، تجريم الاتجار بالأشخاص في القانون الجزائري، مذكرة الماستر تخصص قانون جنائي، كلية الحقوق العلوم السياسية، جامعة محمد خيضر، بسكرة، 2013–2014.

4– أعمال الندوات و المؤتمرات:

– أرجومة موسى مسعود،"الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية غبر الوطنية"، بحث مقدم إلى المؤتمر ألمغاربي الأول حول المعلومات والقانون، المنظم من طرف أكاديمية الدراسات العليا طرابلس الفترة الممتدة من 28–29أكتوبر 2009.

– جحيش فؤاد، مداخلة للمشاركة في المؤتمر الدولي الثاني حول جريمة الاتجار بالبشر. الشكل الجديدة والتحديات الراهنة، جامعة أكلي محند أولحاج، البويرة، الجزائر،2017.

- الاتجار الجنسي بالأطفال عبر النطاق الشبكي الخاص"بين خطورة الظاهرة الرقمية ومحدودية المكافحة الجنائية، دراسة تحليلية نقدية في ضل القانون الجزائري، مخبر الدولة والجرائم المنظم، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، البويرة، الجزائر،2017

- راسل تاينر،أهمية التعاون الدولي في منع جرائم الانترنت بحث مقدم إلى الندوة الإقليمية جول: الجرائم المتصلة بالكومبيوتر، الجارية المملكة المغاربية في الفترة 19-20جوان2007.

- عمر حسين عباس، أدلة الإثبات الجنائي والجرائم الالكترونية" بحث مقدم إلى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكية في الوطن العربي، المنظم من طرف دولة مصر بمقر جامعة الدول العربية خلال الفترة الممتدة من 16-17أفريل2008، ص08.

- غنام محمد غمام،"عدم ملائمة القواعد التقليدية في القانون العقوبات لمكافحة جرائم الكمبيوتر"، بحث مقدم إلى مؤتمر القانون و الكمبيوتر والانترنت، كلية الشريعة والقانون،جامعة الإمارات العربية المتحدة، الفترة الممتدة من 01 إلى 03 ماي 2003.

- محمد الأمين البشيري،" التحقيق في جرائم الحاسب الألى" بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، ط الثالثة، كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة من 1 إلى 3 ماي2004.

- محمد حسام لطفي،"الجرائم التي تقع على الحاسبات أو بواسطتها" بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 1993.

- هشام محمد فريد رستم،"الجرائم المعلوماتية-أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي" بحوث مؤتمر القانون والكومبيوتر و الانترنت، جامعة الإمارات المتحدة، كلية الشريعة والقانون، المجلد02، ط3، من 1-3 ماي2000.

5- المحاضرات والبحوث:

- عمار خوري،شرح قانون العقوبات –القسم العام- كلية الحقوق، جامعة الجزائر، 2007.

- محمد الناصر محمد فرغلى ومحمد عبد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية(دراسة تطبيقية مقارنة)، جامعة نايف العربية للعلوم الأمنية، السعودية، 2007.

- ناصر حمودي، (القانون الجنائي العام): الأحكام العامة لقانون العقوبات والنظرية العامة للجريمة)، محاضرات موجهة لطلبة السنة الثانية حقوق، معهد الحقوق، المركز الجامعي العقيد آكلي محند أولحاج- البويرة،2012-2013.
- رشاد خالد عمر،المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، دراسة تحليلية مقارنة، المكتب الجامعي الحديث، القاهرة،2013.

6- النصوص التشريعية والقوانين:

أ. النصوص التشريعية الجزائرية:

أ-1) الدستور:

- مرسوم رئاسي رقم 96-438، المؤرخ في 07 ديسمبر 1996، يتعلق بإصدارنص تعديل الدستور الجزائري،(ج ر)، عدد 76، صادر بتاريخ 08 ديسمبر 1996، معدل ومتمم.

أ-2) النصوص القانونية:

- الأمر رقم 66-156، مؤرخ في 08جوان 1966، يتضمن قانون الإجراءات الجزائية،(ج ر) عدد49، صادر بتاريخ 11 جوان 1966، معدل ومتمم.
- الأمر رقم 66-156، المؤرخ في 08جوان 1966م، يتضمن قانون العقوبات، (ح ر)،عدد 49، صادر بتاريخ 11جوان 1966، معدل ومتمم، سيما بأمر رقم 09-01، مؤرخ في 25فيفري2009، (ج ر)، عدد15، صادر بتاريخ 08 مارس 2009.
- مرسوم رئاسي رقم 03-417، يتضمن التصديق بتحفظ على بروتوكول منع وقمع الاتجار بالأشخاص خاصة النساء والأطفال المكمل لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المعتمد من طرف الجمعية العامة لمنظمة الأمم المتحدة يوم 15نوفمبر 2000، (ج ر)، عدد 69، صادر بتاريخ 12نوفمبر 2003.
- القانون رقم 04-18، مؤرخ في 25ديسمبر 2004، المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بها، عدد83، الصادر بتاريخ 26ديسمبر 2004.

- القانون 04-09، مؤرخ في05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها،(ج ر)، عدد47، صادر بتاريخ 06أوت 2009.
- القانون رقم 16-02 ، مؤرخة في 19جوان 2016، يتمم الأمر رقم 66-156 المتضمن قانون العقوبات، (ج ر)، عدد 37، صادر بتاريخ 22جوان 2016.
- قانون رقم 17-11، المؤرخ في 27 ديسمبر 2017، المتعلق بقانون المالية لسنة 2018، الجريدة الرسمية رقم 76، الصادر بتاريخ 28ديسمبر 2017.
- القانون 06_22 مؤرخ في 10ديسمبر2006، يعدل ويتمم الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، جريدة رسمية، العدد84، صادر بتاريخ 24ديمبر2006.

7- الوثائق القانونية:

- وثيقة أممية رقم: 55/25، بروتوكول الأمم المتحدة الخاص بمنع وحضر وقمع الاتجار بالأشخاص. خاصة النساء و الأطفال، المكمل لاتفاقية الأمم المتحدة بمكافحة الجريمة المنظمة عبر الوطنية ، اعتمدته الجمعية العامة للأمم المتحدة في دورتها 55، المؤرخ في 15 تشرين الثاني نوفمبر 2000، تاريخ النفاذ، 25 كانون الأول ديسمبر 2003، صادقت عليه الجزائر بتحفظ في 09 مارس 2004.
- وثيقة إقليمية رقم 36 المتضمنة اتفاقية الدول العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية لسنة 2012. الصادرة في 21 ديسمبر 2012، صادقت عليها الجزائر بموجب مرسوم رئاسي 25/14، المؤرخ في 08 سبتمبر 2014،ج ر ج ج، عدد50، الصادر في 20سبتمبر 2014.

8- مواقع شبكة الاتصال الدولية:

- أحمد بوخريص، العملة الافتراضية خصائصها ومخاطر التعامل بها،المركز الديمقراطي العربي، تاريخ النشر 20ديسمبر 2018، الرابطة: https://democraticac.de/?p=58064
- اسراء حسني، الإنترنت المظلم".. السوق الأول لتجارة المخدرات والسلاح سرا على الإنترنت.. اقتحام عقول الشباب وتوصيل الممنوعات لباب المنزل.. ولا عزاء للحكومات، تاريخ النشر:21 جانفي2016، الرابطة: https://www.youm7.com/story/2016/1/21/

- شروق صباري، من تجارة الأطفال إلى أكل لحوم البشر الإنترنت الخفي، تاريخ النشر 2017/08/09، الرابطة:https://www.mobtada.com/details/637219

- محمد حبش، موقع tech-wd، ،المخدرات الرقمية، تاريخ النشر 15 نوفمبر 2014، تاريخ الاطلاع 22ماي2019، رابطة النشر: www.tech-wd.com/wd/2014/11/15 أنظر كذلك، العربي الجديد– الرأي – BBC – CNN – الإمارات اليوم NOW اللبنانية – الحياة.

– عبد الحميد عبد المطلب، استخدام برتوكول (TCP/IP) في البحث وتحقيق الجرائم على الكمبيوتر، ص05، بحث منشور على الموقع: www.arablaw.info.com

ش– محمد الغضبان، العالم الخفي، ما هو الديب ويب؟ وكيف تدخل إليه؟، دون تاريخ نشر، تاريخ التصفح 29ماي2019، الرابطة:
http://www.netaawy.com/2016/what-is-the-deeb-web-and-how-to-accedd.

– محمد نور،"deep wep" الوجه القبيح لـ"الإنترنت، تاريخ النشر 07جوان2018، رابطة https://www.albawabhnews.com/3179834

- موقع wiki، المخدرات الرقمية، دار الشفاء للطب النفسي وعلاج الإدمان،تاريخ النشر 25فبراير 2017،تاريخ الاطلاع 22ماي2019، الرابطة:
http://www.addiction-wiki.com 2019

- هاني سمير علي، مما لا تعرف على الانترنت الخفيdeep web ، تاريخ النشر: 03جولية 2015، تاريخ التصفح: 29ماي2019، الرابطة:
http://www.arageek.com/tech/2015/what -you-do-not-know-about-.

- العملات الإلكترونية ماهي؟وكيف يتم شرائها أو تداولها؟، تاريخ النشر 06جوان2018، الرابطة:https:// www.arincen.com

- مميزات-عملة-البيتكوين https://www.islamicbitcoin.com/

- تحليل أسعار البيت كوين https://arab.dailyforex.com/forex-technical-analysis/2019/05/

– https://www.trendlords.com/2019/02/difference-between-dark-web-deep-web.html

– DARK WEB LINKS | DARK WEB SITES | DEEP WEB LINKS 2018

‹Difference Between Dark Web, Deep Web And Surface Web –

https://www.torproject.or ، February 18, 2019

https://lists.torproject.org/pipermail/tor-dev/2017 March/012088.html - -

.DEEP WEB LINKS 2018 DARK WEB SITES DARK WEB LINKS –

https://www.torproject.org

https://dkhlak.com/dark-web-and-deep-web -

https://www.currencyc.com/ar/dzd-btc.html / -

DEEPWEBADMIN/JANUARY11,2019://www.deepweb sites.com/deep - web-search-engines

pre-alpha: run an onion proxy now. Roger Dingledine -

Tor 0.3.3.2-alpha is released: bugfixes and DoS prevention -

office des nations unies contre la crime (DNNDC) -

ثانيا: المراجع بالغة الفرنسية:

1. OUVRAGES :

a- Francois Paget. Chercheur en cybercriminalité. Derknet et économie souterraine. Colloque économie de la cybersécurité Chaire Cybersécurité & Cyberdéfense. Université de Sorbon. Page 5.14 novembre 2016.

b- Debra littlejohn Shinder, **seene of the cyber crime (computer forensie Hanadbook),** publishing by Syngress(Inc), United states of America,2002.

c- Gabriel gimigiliano, bitcoin and mobile payments : Constructing a European Union Framework, Plagrave-Macmillan, london,2016..

d- Matthew Kien-Meng Ly, Coining Bitcoin's legal bits : Examining the regulatory frameworl for bitcoin and Virtual currencies, Harvard Journal of Lwa & technology, vol27, N^0 02 Spring 2011.

e- Steve Bunting and william wei, **Encase computer forensie,** Wiley Publishing (inc), United States of America, 2006.

2. TEXTES JURIDIQUES ET CONVENTION INTERNATIONALES/

a- textes juridique:

a-1) loi N 2001-1062, de 15 novembre 2001 portant code de procédures pénales, JORF 16 nov 2001.

b- convention internationales :

3. RAPPORT ET RECHARECHES/

a- HM Treasury, Digital Currencies-Call for information. Banking and Credit Team, Horse Guards Road, London , 2014.
www.akhbarelyoum.dz 01:30 à 17 jun2019.

b- national conférence of commissioners on Uniform state laws. « Uniform régulation of Virtual-currency businesses act », annual conférence one-hundred-and-twenty-six th year, San Diego, Californie,14-20 July, 2017.

c- Sova, A Methedintu & al, Virtual Currency »bitcoin » -Challenges and Controverdied, Annal of the constantin Brancusi University of Targu Jiu, Economy Series, $N^0$03, 2016.

d- T.G.I.novembre.1998.disponible a l'adresse suivant :
http://www.legalis.jnet.decision/ilcite-devert/correct-paris-1998-htm.

e- VERGUCHT Pascal, la répression des délits informatique dans une perspective internationale, thèse pour l'obtention du doctorat en droit, soutenue a la faculté de droit de l'université de Montpellier 1, Paris, 1996, p 323-326.

f- Reza Raccsi, The Silk Road, bitcoin, and the Global prohibition Regime on the international Trade in licit Drugs : Can This Strom Be Weathered ?, Glendon Journal of International Studies, 2015.

الفـــــــــــــــهرس

الفهرس **الصفحة**

مقدمة.....2-5

الفصل الأول: الايطار ألمفاهيمي العام للاتجار بالأشخاص عبر النطاق الشبكي الخاص.....**03-60**

المبحث الأول: مفهوم الاتجار بالأشخاص عبر النطاق الشبكي الخاص.....**03**

المطلب الأول: تعريف النطاق الشبكي الخاص.....03

الفرع الأول: المقصود بالنطاق الشبكي الخاص.....03

أولا: الويب العميق (Deep Wep).....04

ثانيا:الويب المظلم (Deerk Wep).....05

الفرع الثاني: محتوى الشبكة الخاصة.....05

الفرع الثالث: الولوج إلى الشبكة الخاصة.....07

أولا: المتصفحات الخاصة بالنطاق الشبكي الخاص.....07

ثانيا: محركات البحث الخاصة بالنطاق الشبكي الخاص.....13

المطلب الثاني: التعريف التقليدي الاتجار بالأشخاص عبر النطاق الشبكي الخاص.....16

الفرع الأول:المقصود التقليدي لجريمة الاتجار بالأشخاص.....16

أولا: التعريف الفقهي.....17

ثانيا: التعريف القانوني.....18

ثالثا: المشرع الجزائري.....19

الفرع الثاني: أركان الاتجار بالأشخاص.....20

أولا: الركن الشرعي.....21

ثانيا: الركن المادي.....21

ثالثا: الركن المعنوي.....25

الفرع الثالث: صور الاتجار عبر النطاق الشبكي الخاص.....26

أولا: الاتجار الجنسي بالأطفال عن طريق البيع المؤقت.....26

ثانيا: الاتجار الجنسي بالأطفال عن طريق البيع.....27

المبحث الثاني: المعاملات الخاصة بالاتجار بالأشخاص عبر النطاق الشبكي الخاص.....29

المطلب الأول: المعاملات التجارية.....29

الفرع الأول: الاتجار بالمخدرات.....29

أولا: المخدرات المادية.....30

ثانيا: المخدرات الرقمية.....32

الفرع الثاني: الاتجار بالأسلحة.....36

أولا: الأسلحة التقليدية.....36

ثانيا: الأسلحة الرقمية.....38

الفرع الثالث: الاتجار بالأشخاص.....41

أولا: تجارة البشر.....41

ثانيا: بث الأفلام الجنسية للأطفال.....42

ثالثا: الغرفة الحمراء.....42

رابعا: التجارب على البشر.....43

خامسا: ألعاب الموت.....43

المطلب الثاني: العملة المتداولة (البت كوين).....44

الفرع الأول: تعريف البيت كوين.....45

أولا: المقصود بالبت كوين.....45

ثانيا: خصائص البيت كوين.....47

ثالثا: مخاطر التعامل بالبيت كوين.....49

الفرع الثاني: سعر صرف البيت كوين أمام الجزائرية.....50

أولا: البيت كوين أمام عملة الدولار الأمريكي.....52

ثانيا: البيت كوين أمام عملة أورو.....53

ثالثا: البيت كوين أمام الدينار الجزائري.....54

الفرع الثالث: المبادرات القانونية والتنظيمية الرئيسة التي تعالج التحديات المتصلة بالعملات الافتراضية.....56

أولا: التعامل الدولي بالعملة الافتراضية.....56

ثانيا: التطورات التنظيمية.....57

ثالثا: التنظيم المبكر والمشاكل القانونية.....59

الفصل الثاني: المكافحة الجنائية للاتجار بالأشخاص عبر النطاق الشبكي الخاص.....62

المبحث الأول: المتابعة الجزائية للجرائم التي ترتكب عبر النطاق الشبكي الخاص.....63

المطلب الأول: الخصوصية الجنائية كجريمة تقليدية ترتكب في وسط رقمي خاص.....63

الفرع الأول: خصوصية الركن المادي للجريمة.....64

أولا: مدى تطابق السلوكيات ووسائل الركن المادي.....64

ثانيا: من حيث إنجاز السلوكيات والوسائل عبر النطاق الشبكي الخاص.....66

الفرع الثاني: خصوصية الركن المعنوي للجريمة.....69

أولا: من حيث تطابق الاستغلال مع أشكال الاتجار عبر النطاق الشبكي الخاص.....69

ثانيا: من حيث هدف الاستغلال عبر النطاق الشبكي الخص.....70

الفرع الثالث: العجز التشريعي في مواجهة جرائم derk web.....71

أولا: أحكام عامة لمبدأ الشرعية الجنائية.....71

ثانيا: مبدأ الشرعية الجنائية وجرائم الشبكة الخاصة.....73

ثالثا: مدى تطابق مبدأ الشرعية الجنائية من حيث النطاق على جرائم derk web.....75

المطلب الثاني: إجراءات المتابعة الحديثة للاتجار بالأشخاص عبر النطاق الشبكي الخاص.....76

الفرع الأول: الوسائل المادية الحديثة في جمع الأدلة الجنائية الرقمية.....77

أولا: استخدام بروتوكول IP/TCP لمواجهة جرائم "الدارك ويب".....77

ثانيا: استخدام برنامج الكوكيز Cookies.....79

ثالثا: استخدام معلومات البروكسي Proxy.....79

رابعا: برامج التتبع وكشف الإختراق.....81

خامسا: أدوات الضبط.....81

سادسا: الأدوات المساعدة بالتحقيق.....82

الفرع الثاني: الوسائل الإجرائية الحديثة في جمع الأدلة الجنائية الرقمية.....83

أولا: التسرب.....83

ثانيا: الاعتماد على برامج الربط لمكافحة جرائم النطاق الشبكي الخاص.....85

ثالثا: مراقبة الاتصالات الالكترونية.....86

المبحث الثاني: صعوبة المكافحة الجنائية الإجرائية لجرائم الشبكة الخاصة.....89

المطلب الأول: صعوبة الاستدلال في الجريمة الرقمية.....89

الفرع الأول: صعوبة اكتشاف الجريمة.....90

أولا: غياب الأثر المادي للجريمة وسهولة محو الدليل.....90

ثانيا: العزوف عن التبليغ بوقوع الجريمة الإلكترونية.....93

الفرع الثاني: صعوبة كشف هوية الجناة.....94

أولا: تعذر تحديد المجرم الالكتروني.....95

ثانيا: فرض الجناة تدابير الأمن.....97

الفرع الثالث: نقص الخبرة في مجال الاستدلال.....98

المطلب الثاني: صعوبة قوانين مكافحة الجرائم المتعلقة بالشبكة الخاصة.....100

الفرع الأول: قصور النصوص العقابية التقليدية.....101

الفرع الثاني: قصور إجراءات التحقيق مع جرائم الشبكة الخاصة.....104

أولا: صعوبة إخضاع المكونات المنطقية للحاسوب الألى للتفتيش والضبط.....104

ثانيا: صعوبة معاينة الجرائم الالكترونية.....107

خاتمة.....110-111

قائمة المصادر والمراجع.....113-122

الفهرس.....124-129