الجريمة السيبرانية في صورها المستحدثة

Cyber crime in its modern forms

ماينو جيلالي[1]

أستاذ التعليم العالي

كلية الحقوق والعلوم السياسية، مخبر القانون والتنمية، جامعة طاهري محمد، بشار

الجزائر

عروس كوثر

طالب دكتوراه

كلية الحقوق والعلوم السياسية، مخبر القانون والتنمية، جامعة طاهري محمد، بشار

الجزائر

تاريخ الإرسال: 31 / 05 / 2022-- تاريخ المراجعة:30 / 06 / 2022-- تاريخ القبول: 01 / 07 / 2022

الملخص:

ثمة تزايد مطَّرد في ربط المجتمعات بالإنترنت. ومع أنَّ الإنترنت تجعل حياتنا أسهل، فإنها قد تعرضنا لخطر الجريمة السيبرانية. إذ إنَّ مخاطر عالم الفضاء السيبراني الذي لا حدود له يمكن أن تتفاقم بتزايد انخراط أفراد وجماعات إجرامية منظمة يمكن أن تؤذينا. وتتجلَّى هذه المخاطر في أشكال مختلفة،

ومن الصور المعاصرة للإجرام السيبراني إستخدام تقنيات الذكاء الإصطناعي في ارتكاب الجرائم، وكذا جرائم العملات المشفرة ، والجرائم المرتبطة بأسواق الشبكة الخفية ، وغيرها من الجرائم السيبرانية المستحدثة والتي باتت تشكل تحديا كبيرا أمام المجتمع الدولي الذي يسعى لاتخاذ اجراءات لمكافحتها

الكلمات المفتاحية:

الجريمة السيبرانية، العملات المشفرة ، الذكاء الإصطناعي

[1] ماينو جيلالي

Abstract:
There is a steady increase in the connectivity of societies to the Internet. Although the Internet makes our lives easier, it may also expose us to the risk of cybercrime. The dangers of the borderless world of cyberspace can be exacerbated by the increasing involvement of individuals and organized criminal groups that can harm us. These risks manifest themselves in different forms.

Among the contemporary forms of cybercrime is the use of artificial intelligence techniques in committing crimes, as well as cryptocurrency crimes, crimes related to hidden network markets, and other emerging cyber crimes, which have become a major challenge to the international community, which seeks to take measures to combat it.

Keywords Cyber crime, cryptocurrency, artificial intelligence

مقدمة:

لا يكاد يخلوا الوقت الحاضر من بيت أو مؤسسة أو أفراد لا يستخدمون الإنترنت، والأجهزة الإلكترونية الذكية. ومع أنَّ الإنترنت تجعل حياتنا أسهل، فإنها قد تعرضنا لخطر الجريمة السيبرانية. إذ إنَّ مخاطر عالم الفضاء السيبراني الذي لا حدود له يمكن أن تتفاقم بتزايد انخراط أفراد وجماعات إجرامية منظمة يمكن أن تؤذينا.(الأمم المتحدة ، https://www.unodc.org/e4j/ar/index.html). فقد أصبحت الجرائم السيبرانية أكثر تعقداً، نظراً للتطور التكنولوجي مثل أنترنت الأشياء، والحوسبة السحابية والذكاء الاصطناعي وخدمات من قبيل برنامج حماية الخصوصية أونيون روتر والشبكة الخفية. كل هذه التكنولوجيا تعتبر سلاح ذو حدين: فهي تجلب مزايا للدول والحكومات ولكن تجلبها أيضا لمرتكبي جرائم معينة.(وفاء لطفي، 2022، ص152)

ففي ظل الحراك المعلوماتي والتطور التكنولوجي الهائل في مجال تقنية المعلومات والاتصال واقتصاد المعرفة، وفي ظل الانفتاح المعلوماتي والعولمة الرقمية، وبروز تقنيات الثورة الصناعية الخامسة والذكاء الاصطناعي في مختلف القطاعات، وفي ظل التحول الرقمي للدول وتضاعف الاعتماد على المنصات الرقمية ووسائلها الاتصالية، سواء

في التعليم، والعمل، والاستشارات الطبية، وعقد المؤتمرات، وغيرها من المجالات؛ نتيجة لما فرضته جائحة كورونا كوفيد 19 من عزلة وتباعد اجتماعي، الأمر الذي أسهم بالفعل في زيادة تفشي معدل الهجمات السيبرانية أو الهجمات على خدمات البنية التحتية الحيوية للدول في الفترات الأخيرة، وزيادة معدل انتشار الشائعات والمعلومات المفبركة (أميرة، 2021، ص 1767)

وتتجلَّى هذه المخاطر في أشكال مختلفة من الإجرام المعتمد على الفضاء السيبراني والذي لن يكون ممكناً بدون الإنترنت والتكنولوجيات الرقمية، فهو يتخذ من التكنولوجيا هدفاً وأداة للإجرام. وعلى سبيل المثال يتم باستحداث فيروسات حاسوبية وتعميمها ونشرها، فضلا عن عمليات السرقة الممنهجة للبيانات الشخصية، والدخول غير المشروع وغير المرخص به لمختلف الفضاءات السيبرانية، وشَنّ هجمات على مرافق تكنولوجيا المعلومات الوطنية الحساسة واستخدام تقنيات الذكاء الإصطناعي ، وكذا الإنترنت المظلم والأسواق المشفرة للقيام بأعمال إجرامية باتت تهدد الأمن القومي العالمي، مثل الاحتيال الإلكتروني والتجارة الإلكترونية في سلع غير مشروعة، مثل المخدِّرات أو الأسلحة النارية، واستغلال الأطفال والتعدي عليهم جنسيًّا من خلال الإنترنت.

هذه الصور من الجرائم السيبرانية المستحدثة وغيرها باتت تنتشر بسرعة كبيرة جدا، دفعت المجتمع الدولي إلى دق ناقوس الخطر من أجل التصدي لها ومحاربتها في ظل الإتجاه العالمي إلى الإعتماد بشكل كبير على أدوات الفضاء السيبراني. وما يزيد من خطورة هذه الجرائم السيبرانية أن لها صلة بخصوصيات الناس. إذ إنَّ وجود الشخص على الإنترنت ونشاطه يفضي بالضرورة إلى الكشف عن بياناته الخصوصية، وهو ما يسهِّل تعرُّضه لأخطار مختلفة في الفضاء السيبراني تزداد معه أهمية أمان التواصل عبر الإنترنت .

إن الحديث عن الجرائم السيبرانية لا يمكن حصره في دراسة موجزة لشساعة محاوره، وتشعبها على جميع الأصعدة، ما دفعنا إلى التركيز على إبراز بعض الصور المستحدثة منها ، والتي باتت مصدر قلق كبير على المستوى

العالمي، ويتم التطرق إليها في مختلف المحافل الدولية ذات الصلة، وعلى سبيل المثال قامت الأمم المتحدة بدراسة موضوع الجريمة السيبرانية في صورها المستحدثة ضمن مؤتمرات الأمم المتحدة لمنع الجريمة والعدالة الجنائية وخاصة المؤتمر الثالث عشر المنعقد بالدوحة، فضلا عن تشكيل فريق عالمي للتحضير لإبرام اتفاقية دولية في هذا المجال.

نعالج موضوع الدراسة من خلال الخطة التالية:

المطلب الأول: مفهوم الجريمة السيبرانية

المطلب الثاني: الأنماط المستحدثة للجريمة السيبرانية

المطلب الأول: مفهوم الجريمة السيبرانية

رغم الإنتشار الواسع والرهيب للجرائم السيبرانية ، والذي ارتبط أساسا بالإستخدام المتزايد للإنترنت وأدوات الإتصال الحديثة، إلا أن مسألة تحديد وإعطاء تعريف موحد ودقيق لهذه الجريمة كانت محل خلاف بين فقهاء القانون للإرتباط والتداخل بين هذه التقنية وغيرها من مجالات العلوم الأخر، كما أن هذه الجريمة تحمل الكثير من الميزات والخصائص المتفردة التي جعلتها مميزة عن غيرها من الجرائم، سواء بالنسبة للجريمة في حد ذاتها أو بالنسبة لمرتكبيها، وهم ما سنوضحه من خلال النقاط التالية.

أولا: تعريف الجريمة السيبرانية

إن مصطلح الجريمة السيبرانية هو إحدى المصطلحات الحديثة والمستخدمة عن جرائم الإنترنت الذي تعددت مصطلحاته، وذلك لنشأة وتطور ظاهرة الإجرام المرتبط والمتصل بتقنية المعلومات (الصحفي، 2021، ص5) . وقد صيغ مصطلح الجريمة السيبرانية لأول مرة من قبل ويليام جيبسون Wiliam Gibson في عام 1982، ومنذ ذلك الحين اتسعت الحدود التي تحدد الجريمة السيبرانية، وخلال نشأتها فضل الأجيال الأولى من العلماء والمنظمات مصطلح جرائم الكمبيوتر بالمعنى الأضيق للجريمة السيبرانية على مصطلح الجريمة السيبرانية، بالمعنى الأوسع للكلمة (الطريف، 2021، ص 1841)

ومع تطوُّر المصطلحات المستخدَمة، جرى بذل جهود أكاديمية لتعريف تعبير" الجريمة السيبرانية ولا بدَّ لأيّ نهج عصري في هذا الشأن أن يُسلِّم بأنَّ تعبير" الجريمة السيبرانية "ليس مصطلحًا قانونيا قائمًا بذاته، بل هو تعبير جامع

يشمل مجموعة أفعال مرتكبة ضد بيانات أو نظم حاسوبية أو باستخدامها ،وثمة نهوج أخرى تركِّز على الجرائم المرتكبة بحقِّ المعلومات الحاسوبية أو على استخدام موارد المعلومات لأغراض غير مشروعة(الأمم المتحدة، 2015، ص8)

ويمكن القول أيضا أن الجريمة السيبرانية هي فعل أو امتناع عمدي ينشأ عن الإستخدام غير المشروع لتقنية المعلومات، يهدف إلى الاعتداء على الأموال المادّية أو المعنوية أو الاعتداء على خصوصية الأفراد، أو هي عمل أو امتناع يأتيه الإنسان إضرارا بمكوّنات الحاسب وشبكات الاتّصال الخاصّة به، و من جهة أخرى هي الجريمة التي يكون النّظام المعلوماتي فيها وسيلة لارتكاب جريمة تقليدية، إمّا ضدّ الأموال كالتّحويل الإلكتروني غير المشروع للأموال، أو ضدّ الأشخاص كجريمة السّب أو القذف عبر الإنترنت.(إدريس نبيل، 2017، ص30)

فالجريمة السيبرانية هي فعل ينتهك القانون، والذي يُرتكب باستخدام تكنولوجيا المعلومات والاتصالات لاستهداف الشبكات والأنظمة والبيانات والمواقع الإلكترونية و/أو التكنولوجيا أو تسهيل ارتكاب جريمة.(الأمم المتحدة، 2022، https://www.unodc.org)

وتتفاقم الجريمة السيبرية بوتيرة سريعة للغاية مع ظهور اتجاهات جديدة باستمرار. ويصبح مرتكبو الجرائم السيبرية أكثر مرونة، فيستغلون أدوات التكنولوجيا الحديثة بسرعة فائقة، ويخططون لاعتداءاتهم بدقة باستخدام أساليب جديدة، ويتعاونون فيما بينهم بطرائق لم نعهدها من قبل. وتنشط الشبكات الإجرامية المتشعبة في أرجاء العالم وتنسق اعتداءاتها المعقدة خلال دقائق. (الإنتربول،https://www.interpol.int/ar).

ثانيا: خصائص الجريمة السيبرانية

الجريمة السيبرانية هي امتداد طبيعي لنمو أجهزة الكمبيوتر، مثل الحوسبة نمت الجريمة السيبرانية بشكل هائل على مدى العقدين الماضيين، تطورت الجريمة السيبرانية من قضية ثانوية إلى ظاهرة عالمية، مما يؤثر عمى أعداد غير مسبوقة من الناس وتسبب الملايين من حالات الإيذاء في كل عام ومن آثار هذه الجرائم، تتراوح حجم الخسارة المالية بالمليارات وخسارة الكثير من الوقت في سرقة الهوية والاحتيال، وتتسبب في الاضطراب العاطفي المرتبط بالقلق، والإكتئاب، أو حتى الأفكار الانتحارية مثل التحرش عبر الإنترنت / العنف الإلكتروني والتعرض لوسائل الإعلام المتطرفة (شحاته،2019 , ص 13)

تمتاز الجريمة السيبرانية بطائفة من الخصائص التي جعلتها متفردة في صورتها عن باقي الجرائم الأخرى بالنظر إلى مجموعة من المعطيات الخاصة بها بالدرجة الأولى، سواءا من حيث أداة ارتكابها أو مرتكبها أو حتى كيفية إثباتها ومعاينتها.

1- إن طبيعة الجرائم السيبرانية وتميزها عن الجرائم التقليدية يرجع إلى الوسط الذي ترتكب فيه الجريمة وهي الأداة أو الوسيلة التي استخدمها الجاني في ارتكاب فعله غير المشروع، وتتطلب توفر معرفة أو حد ادني من الثقافة التقنية لدى الجاني، وهي لا تخرج عن كونها سلوك إجرامي ينشأ بارتكاب فعل جرمه القانون أو الامتناع عن فعل أمر به القانون، وتتجه إرادة الجاني إليه، رغم وجود نص قانوني يجرم السلوك(مهدي 2021 ، ص 114.)

2- الجريمة الالكترونية ذات بعد دولي، أي أنها عابرة الحدود، فهي قد تتجاوز الحدود الجغرافية بسبب أن تنفيذها يتم عبر الشبكة المعلوماتية، وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية فنية، بل سياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية(عطايا ، 2015، ص 373)

1- نظرا للطابع الخاص الذي تتميز به الجرائم السيبرانية. فإن إثباتها يحيط به كثير من الصعوبات التي تواجه سلطة الإستدلال أو التحقيق الجنائي في استخلاص الدليل ، والتي تتمثل في صعوبة اكتشاف هذه الجرائم لأنها لا تترك أثرا خارجيا .فالجرائم السيبرانية لا عنف فيها ولا سفك دماء ولا آثار اقتحام لسرقة أموال ، وإنما هي أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسبات ،وليس لها أي اثر خارجي مرئي. بمعنى آخر إن الجرائم السيبرانية هي جرائم فنية تتطلب تكتيك معين في مجال الحاسبات الآلية، وهي جريمة هادئة لا تتطلب العنف (الزهراني، 2020، ص 779).

3- صعوبة الكشف عن مرتكب الجريمة السيبرانية إلا بأساليب أمنية وتقنية عالية (العنزي، 2022 ص 112)

4- مرتكب الجريمة الإلكترونية في الغالب شخص يتميز بالذكاء، والدهاء ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب وكيفية تشغيله، وكيفية تخزين المعلومات والحصول عليها، في حين أن مرتكب الجريمة التقليدية في الغالب شخص أمي بسيط متوسط التعليم. مرتكب الجريمة الإلكترونية قد يكون منسجماً اجتماعياً وقادراً مادياً، إلا أن باعثه على ارتكاب جريمته في كثير من الأحيان رغبته في قهر النظام .وهذه الرغبة قد تزيد عنده على رغبته في الحصول على المال. في حين أن مرتكب الجريمة التقليدية في الغالب يكون غير منسجم اجتماعياً ورغبته في الحصول على المال تفوق بكثير أي رغبة أخرى (عطايا ، 2015 ص 373)

5 - الخفاء والإستتار، فهذه الجريمة تتسم دائما بأنها خفية لا يلاحظها المجني عليه، وهي مستترة يستعصي على غير الخبير بالحاسب الآلي أن يكتشفها، مثل جريمة تدمير البرامج بواسطة الفيروسات ، أو التجسس على البيانات السرية أو اختراق المواقع، كما أنها تتسم بالهدوء ولا تحتاج إلى عنف ، وإنما تتطلب من مرتكبها قدرا من التمكن في مجال الحاسب الآلي والإنترنت الذي يمكنه من استخدام الأفعال غير المشروعة. (اسماعيل ، 2015، ص 274)

المطلب الثاني: الأنماط المستحدثة للجريمة السيبرانية

لم تتوقف الجريمة السيبرانية عن الإنتشار وخاصة في ظل الإستخدام الواسع النطاق للأنترنت والأجهزة والتطبيقات الذكية بمختلف أنواعها، وهو ما نجم عنه ظهور أنماط وصور مستحدثة من الجرائم السيبرانية، باتت تشكل تهديدا حقيقيا على مختلف الأصعدة، فظهور الأسواق الخفية والعملات المشفرة وأنظمة الذكاء الإصطناعي جعل المجرمين السيبرانيين يستفيدون إلى أقصى درجة مما توفره هذه الأدوات، وبات استخدامها واسع النطاق في تهريب البشر والإتجار بهم، والتعدي على حقوق وحريات الأفراد، بل والهجوم على الدول في إطار ما يعرف بالحروب السيبرانية، وهو ما سوف نتطرق إليه بشيئ من التفصيل في النقاط التالية

أولا - الحروب السيبرانية والإرهاب السيبراني:

غيرت التكنولوجيا من أشكال الحروب والصراعات البشرية على مدى العصور، فمن الحروب التقليدية التي كانت تعتمد على السيوف والرماح، ثم البنادق والرشاشات، ثم القنابل النووية والصواريخ العابرة للقارات ، إلى نوع جديد من الحروب هي الحروب السيبرانية التي تستخدم نوعا آخر من الأسلحة المتمثلة في فيروسات الكمبيوتر التي لها القدرة على إحداث دمار يوازي دمار الأسلحة التقليدية ، بل قد يفوقه في بعض الأحيان.(ايهاب ، 2019 ص 14)

وتتميز الحروب السيبرانية عن الحرب التقليدية في أن المفهوم التقليدي للحرب ينطوي على استخدام الجيوش النظامية ، ويسبقها إعلان واضح لحالة الحرب، وميدان قتال محدد بينما تبدوا هجمات الفضاء الإلكتروني غير محددة المجال وغامضة الأهداف ، إضافة إلى اعتمادها ما يمكن وصفه بأسلحة إلكترونية جديدة تلائم طبيعة السباق الإلكتروني لعصر المعلومات، حيث يتم توجيهها ضد المنشآت الحيوية أو دسها عن طريق عملاء لأجهزة الإستخبارات (مسعود، 2018، ص 74)

تحتل الهجمات السيبرانية وعواقبها مكان الصدارة على جداول الأعمال في جميع أنحاء العالم. وما يثير القلق، ، هو أن العمليات العسكرية السيبرانية تتحول أيضاً إلى جزء من النزاعات المسلحة اليوم، ويمكنها أن تعطل عمل البنية التحتية بالغة الأهمية والخدمات الحيوية للسكان المدنيين. وعلى سبيل المثال، يزداد اعتماد نظم الرعاية الصحية على الرقمنة والاتصال بالإنترنت، ولكنها تفتقر إلى الحماية في غالب الأحيان، ولذلك، فهي معرضة بشكل خاص للهجمات السيبرانية. وفي كثير من الأحيان، تتضرر البنية التحتية للمياه والطاقة، أو المستشفيات، في النزاعات المسلحة جراء القصف، وتعمل الخدمات جزئياً فقط أو لا تعمل على الإطلاق، ولك أن تتخيّل أثر وقوع حادث

سيبراني كبير علاوة على هذا! فقد يترتب على ذلك عواقب وخيمة. ويكفي المدنيين العالقين في براثن النزاع والعنف ما يعانونه أصلاً حتى يروا صعوباتهم تتفاقم أكثر فأكثر.(https://www.icrc.org/ar/)

كما أن هناك قلق متزايد إزاء تزايد استخدام الإرهابيين ومؤيديهم، في ظل مجتمع مُعَوْلم، لتكنولوجيا المعلومات والاتصالات، وبخاصة شبكة الإنترنت وغيرها من الوسائط، واستخدام هذه التكنولوجيات لارتكاب الأعمال الإرهابية أو التحريض عليها أو التجنيد لها أو تمويلها أو التخطيط لها" ، وقد اتخذ مكتب الأمم المتحدة لمكافحة الإرهاب عدة مبادرات في مجال التكنولوجيات الجديدة. ويروم برنامج أمن الفضاء الإلكتروني والتكنولوجيات الجديدة تعزيز قدرات الدول الأعضاء والمنظمات الخاصة على منع إساءة استعمال الإرهابيين والمتطرفين العنيفين التطورات التكنولوجية وتخفيف آثار إساءة الاستعمال هذه. ويشمل ذلك التصدي لخطر الهجمات الإلكترونية التي تشنها الجهات الفاعلة الإرهابية على البنى التحتية الحيوية، علاوة على تطوير استخدام وسائط التواصل الاجتماعي لجمع المعلومات من مصادر مفتوحة والأدلة الرقمية لمكافحة الإرهاب والتطرف العنيف على الإنترنت، في ظل احترام حقوق الإنسان. (الأمم المتحدة https://www.un.org/counterterrorism/ar/cct/programme-projects/cybersecurity)

ثانيا- الجرائم المرتبطة بتقنية الذكاء الإصطناعي:

أصبحت كيانات الذكاء الاصطناعي حقيقة وواقع فرض نفسه بعد أن كانت ضربًا من الخيال، حتى أننا بتنا نشاهد استخدام هذه التطبيقات الذكية في كثير من المجالات سواء الطبية أو الصناعية أو العسكرية، وكذلك التعليمية وغيرها من المجالات المختلفة ،ولأن القدرة البشرية لا تقف عند حد معين، بات تطور كيانات الذكاء الاصطناعي متسارعا ونجح الإنسان في صناعة الذكاء وتوطينه في الآلة ليحاكي السلوك البشري من خلال الحاسوب ،وما زال يسعى الإنسان بعلمه إلى تطوير هذا السلوك ليصل به إلى سلوك يحاكي السلوك البشري على نحو تام من خلال تمكين تلك الكيانات من القدرة على التواصل والإبداع والتعلم ومحاكاة العالم البشري(العدوان، 2021، ص 149)

وقد ظهر مصطلح الذكاء الاصطناعي للمرة الاولى في مؤتمرٍ عُقد في دارت موث كوليدج،هانوفر، نيوهامبشر في عام 1956 في إشارة إلى تفاؤل الباحثين باستخدام الخوارزميات القائمة على الكمبيوتر سوف يحقق تقدمًا سريعًا . ونجحوا في هذه المراحل المبكرة في كتابة كود لحل المشاكل؛ وتضمنت البرامج عناصر معينة لتحسين الأداء بالتعلم ،ثم توقف الاستثمار في أبحاثه وقل الاهتمام بها في ستينيات القرن الماضي ثم عاد للانتشار في العصر الحالي . حيث يعتبر هذا العصر عصر جديد من الفبركة والتزييف حيث تستخدم فيه التكنولوجيا والتقنيات والبرمجيات المعقدة وقد يستحيل فيه تمييز الحقيقة عن الكذب، إنه عصر التزييف العميق أو أن التزييف العميق أو الديب فيك تقنية تستخدم

.»Deep fake« ما يعرف بالديب فيك ، وقد استُخدمت تقنيّة التزييف العميق لتشويه صورة بعض السياسيين المعروفين (أحمد محمد فتحي الخولي، المسؤولية 2021، ص 256)

يشير مصطلح الذكاء الاصطناعي (AI) إلى الأنظمة أو الأجهزة التي تحاكي الذكاء البشري لأداء المهام والتي يمكنها أن تحسن من نفسها استنادًا إلى المعلومات التي تجمعها. يتجلى الذكاء الاصطناعي في عدد من الأشكال. ومن أمثلتها أن تستخدم روبوتات المحادثة الذكاء الاصطناعي لفهم مشكلات العملاء بشكل أسرع وتقديم إجابات أكثر كفاءة، كما أن القائمون على الذكاء الاصطناعي يستخدمونه لتحليل المعلومات الهامة من مجموعة كبيرة من البيانات النصية لتحسين الجدولة يمكن لمحركات التوصية تقديم توصيات مؤتمتة للبرامج التلفزيونية استنادًا إلى عادات المشاهدة للمستخدمين(https://uomus.edu.iq/NewDep.aspx?depid=14&newid=9532)

فالذكاء الاصطناعي يتعلق بالقدرة على التفكير الفائق وتحليل البيانات أكثر من تعلقه بشكل معين أو وظيفة معينة. وعلى الرغم من أن الذكاء الاصطناعي يقدم صورًا عن الروبوتات العالية الأداء الشبيهة بالإنسان التي تسيطر على العالم، فإنه لا يهدف إلى أن يحل محل البشر. إنه يهدف إلى تعزيز القدرات والمساهمات البشرية بشكل كبير. مما يجعله أصلاً ذا قيمة كبيرة من أصول الأعمال.(/https://www.oracle.com/ae-ar/artificial-intelligence/what-is-ai)

تعتبر جرائم الذكاء الاصطناعي هى جرائم المستقبل القريب إن لم يكن بدأ بعضها الآن، فقد ساعد التطور التكنولوجى خلال السنوات الماضية - والذى تسارعت وتيرته في الفترة الحالية - في ظهور العديد من تلك الجرائم، حيث أعطت البرمجة المتطورة لبعض الآلات التى تعمل بالذكاء الاصطناعي قدرات تصل خطورتها إلى بناء خبرة ذاتية تمكنها من اتخاذ قرارات منفردة في أية مواقف تواجهها مثل الإنسان البشري ، ويثير الموضوع إشكاليات متعددة ترتبط بإشكالية أساسية وهى إذا ارتكب الذكاء الاصطناعي جريمة جنائية من سيكون المسئول جنائيا عن تلك الجريمة؟، مما يترتب على ذلك عدد من الإشكاليات مثل منح الشخصية الاعتبارية لكيانات الذكاء الاصطناعي، وعدم قدرة القوانين العادية على مواكبة هذا التطور (دهشان، 2019، ص 5.)

بيد أن الذكاء الاصطناعي هو إلى حد كبير جدا سلاح ذو حدين، لأنه يمكن أن يؤدي إلى تغيرات كبيرة في الطريقة التي تتعامل بها أجهزة إنفاذ القانون مع مهمة حفظ الأمن، ولكنه يعزز أيضاً أساليب عمل الجماعات الإجرامية والإرهابية، بل ويمكن أن ييسّر ظهور أشكال جديدة من الجريمة والأولوية في ذلك الصراع، الذي يمكن تشبيهه استعاريا بمعركة بين خصمين سيكتب فيها "البقاء للأقوى هي بعبارة موجزة تعزيز حفظ الأمن بالاستعانة

بتقنيات الذكاء الاصطناعي لمكافحة الجرائم القائمة على الذكاء الاصطناعي. (الأمم المتحدة، chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.unodc.org/documents/Cybercrime/IEG_Cyber_website/A_CONF.234_11_A.pdf، تم الإطلاع بتاريخ 2022/02/13 . 17:54.)

وعلى الرغم من أهمية الذكاء الإصطناعي التي تتمثل أهميته في المساعدة على كشف الجرائم المستقبلية والتنبؤ بنسب الإجرام ونوع الجرائم، إلا أن ذلك صاحبه ظهور وتعدد وتنوع جرائم الذكاء الإصطناعي في الواقع والعالم الإفتراضي (العدوان، ص 153)، ولعل أهم مثال لذلك استخدام **تقنية التزييف العميق (بالإنجليزية:)** Deepfake هي تقنية تقومُ على صنعِ فيديوهات مزيّفة عبر برامج الحاسوب من خِلال تعلّم الذكاء الاصطناعي. تقومُ هذهِ التقنيّة على محاولة دمجِ عددٍ من الصور ومقاطع الفيديو لشخصيّةٍ ما من أجلِ إنتاج مقطع فيديو جديد – باستخدام تقنية التعلم الآلي – قد يبدو للوهلة الأولى أنه حقيقي لكنّه في واقع الأمر مُزيّف. استُعمِلت هذه التقنيّة في إنشاءِ مقاطع فيديو إباحيّة مزيفة لعددٍ من المشاهير كما استُخدمت في أحيان أخرى لخلق أخبار كاذبة ومُحاولة خدع القُرّاء والانتقام الاباحي (https://ar.wikipedia.org)

فعلى سبيل المثال لا الحصر استُبدل وجه الرئيس الأرجنتيني ماوريسيو ماكري بوجه أدولف هتلر كمَا استعيض عن وجه أنجيلا ميركل بقلم دونالد ترامب. في نيسان/أبريل 2018؛ نشرَ جوردان بيل وجوناه بريتي فيديو على شكلِ إعلان خدمى عامّة يظهرُ فيه الرئيس الأمريكي السابق باراك أوباما وهوَ يتحدث حولَ خطر التزييف العميق. وفي كانون الثاني/يناير 2019، بثت شبكة فوكس التلفزيونية هي الأخرى فيديو مصنوع بتقنيّة التزييف العميق «بنيّة حسنة» للرئيس ترامب خلال خطابه في المكتب البيضاوي (https://www.aljazeera.net/news/scienceandtechnology/2020/10/18)

كما أن هناك تساؤلات عديدة تفرض نفسها أهمها ، كيفية التحقيق مع الروبوت، بما في ذلك سؤاله واستجوابه، وتفتيشه، ومعاينة مسرح الجريمة، ورفع بصمات الروبوت، وتحليلها، والحصول على الدليل الجنائي الذي هو محور اهتمام العدالة الجنائية، وكذلك حضور الجلسات، والحبس المؤقت والكفالة، وعناصر الركن المادي للجريمة المتمثلة في السلوك الإجرامي للروبوت، والنتيجة الإجرامية لفعل الروبوت، وعلاقة السببية بين السلوك الإجرامي للروبوت والنتيجة الإجرامية، والركن المعنوي للجريمة بما في ذلك إرادة ارتكاب الجريمة والعلم بعناصرها، وهل ينسب للروبوت عنصر الإرادة والعلم بالجريمة؟ وهل الروبوت هو المسؤول مباشرة أم هناك شخص آخر مسؤول؟ وقواعد المساهمة الجنائية في جرائم الروبوت، والدفاع عن الروبوت، والظروف المخففة والمشددة والأعذار القانونية، وإجراءات المحاكمة والتحقيق النهائي، وتنفيذ العقوبة، وهل الروبوت هو من سينفذ

العقوبة أم هناك أشخاص آخرون سيتم التنفيذ عليهم، وقواعد الإسناد والمسؤولية الجنائية؟ أليست هذه تساؤلات باتت الإجابة عليها عصيبة في ظل . التشريعات الجنائية القائمة التي شرعت من أجل الإنسان البشري، وليست من أجل الإنسان الآلي(حسكر، 2022، ص 198)

ثالثا- جرائم العملات المشفرة:

ظهرت في السنوات الأخيرة العملات المشفَّرة والموجودات الافتراضية وجذبت استثمارات لإقامة بنى تحتية لنظم للدفع باستخدام بروتوكولات برمجية خاصة بتلك العملات والموجودات، وقد يستصوب البعض استعمال العملات المشفَّرة لمجموعة متنوعة من الأسباب، وربما يحتفظ بها في الوقت نفسه لاستثمارها في المضاربات. ويسعى البعض إلى الاستفادة من طابع السرية المرتبط بما توفره من مستويات عليا من حجب الهوية في المعاملات، في حين أن كل ما يريده آخرون هو تجنب خضوع معاملاته القانونية للإشراف و/أو المراقبة من جانب الدولة أو المصارف، ويشير مؤيدو العملات المشفَّرة إلى أن رسوم المعاملات بها تقل عن الرسوم التي تفرضها البنوك التقليدية على العملات الوطنية، وإن كان من المحتمل أن تقلِّل أيُّ خسارة في أسعار الصرف وارتفاع الرسوم المرتبطة بمقدمي خدمات العملات المشفَّرة من وفورات التكلفة.(الامم المتحدة، الأمم المتحدة، مؤتمر الأمم المتحدة لمنع الجريمة والعدالة الجنائية، https://undocs.org/ar/A/CONF.234/11 تم الإطلاع بتاريخ 2020/05/08، ص 3.)

وقدأفرز الإنتشار السريع لاستخدام العملات المشفرة إلى ظهور العديد من التحديات المرتبطة باستخدامها في ارتكاب العديد من الجرائم الخطيرة ، ونظرا لأهمية هذه المسألة فقد أدرجتها الأمم المتحدة ، ممثلة في لجنة منع الجريمة والعدالة الجنائية ضمن أهم الأشكال المستجدَّة من الجريمة على الصعيد العالمي التي سيتم مناقشتها ضمن فعاليات مؤتمر الأمم المتحدة الرابع عشر لمنع الجريمة والعدالة الجنائية.

إن الدرجة العالية من إغفال الهوية التي تتيحها العملات المشفَّرة، مقترنة بانخفاض مستويات انكشاف مستعمليها، تتسبب في تلاشي الكثير من المخاطر المرتبطة بأنشطة غسل الأموال وتمويل الإرهاب، مما يسهل ارتكاب تلك الأنشطة داخل البيئات الافتراضية. وبالإضافة إلى ذلك، يمكن أن تسهِّل العملات المشفَّرة ارتكاب جرائم أخرى مثل الابتزاز والاحتيال. ونتيجة لذلك، فإنَّ استغلال العملات المشفَّرة ينطوي على اختبار لمقدرة السلطات المختصة على توفير تدابير التصدي من خلال التنظيم الرقابي وتعزيز التعاون الدول، تتيح الشبكة المظلمة الحاسوبية فرصا

جديدة للاتجار بالمخدِّرات لأهنا تتيح للمستعملين شراء المخدِّرات بالعملة المشفرة مع تسليم المشتريات إليهم بطريقة مخفية (الأمم المتحدة، 2020، ص 54)

تزيد العملات المشفَّرة من السهولة التي يتمكن بها المهرّبون من تلقِّي الأموال وإخفائها ونقلها. ويمكن لهذه العملات أن تساعد على غسل الأموال ، وأن تعين المهرّبين على تجنب التعرض للتحقيق أو التوقيف من خلال حجب هويتهم والحد من الحاجة إلى حمل مبالغ نقدية كبيرة (الأمم المتحدة، مؤتمر الأمم المتحدة 14 لمنع الجريمة، ص 12)

فقد ساهم غياب رقابة الدولة واخفاء هوية المتعامل في تشجيع المجرمين في جرائم غسل الاموال على استخدام العملات المشفرة ، ففي هذه الجرائم يحاول الجاني أن يعثر على طريقة يسبغ بها المشروعية على دخله فيقلبه من دخل غير مشروع الى دخل ظاهره مشروع ،يمكن استخدامه من أجل غايه أخرى في كافه مجال الاقتصاد، فهذه الجريمة تتشكل من إخفاء الأصول ومصادر الدخل غير المشروعة مصدرها، حتى تبدو مشروعة، وهذه الجرائم يمكن ارتكابها بسهوله كبيره باستخدام العملات الإفتراضية مثل البيتكوين، فكون المستخدم مجهولا أو يستخدم إسما مستعارا ، ما يسمح لأي شخص القيام بتحويل الأموال فورا بينما يظل أطراف التعامل غير معروفين(توفيق شرف شمس الدين، 2019 م ، ص 673)

أكدّت مجموعة العمل المالي FATF أنّ هذه العملات تُستعمل لتمويل الإرهابيين وإخفاء محاصيلهم الجرمية، فقد تمّ الكشف عن عمليات تمويل لتنظيم الدولة الإسلامية ومجموعات إرهابية أخرى(مارلين، 2019، ص 77)

كما يشكل استغلال الأطفال في المواد الإباحية على شبكة الإنترنت معضلة عالمية، فقد كان من آثار تطور الوسائل التكنولوجية الجديدة، مضاعفتها إلى حد كبير لإمكانيات الحصول على هذه المواد الإجرامية ونشرها وبيعها، تشجيع نمو هذه الظاهرة (إبراهيم، 2013، ص 1116). وقد أشارت اليونيسف في تقريرها الصادر سنة 2017 حول حالة الأطفال أن التحدي الذي يواجه مكافحة الجرائم الجنسية على الإنترنت ضد الأطفال هو الإستخدام المتنامي للعملات المشفرة ومنصات التشفير ضمن الشبكة المظلمة التي توفر عدم الكشف عن الهوية ، مع استغلال عصابات الإساءة للأطفال لهذه النظم، ما يشكل معضلة بالنسبة لأجهزة إنفاذ القانون التي تسعى لجمع الأدلة حول هذه الجرائم

(اليونيسف، 2017، ص 79)

رابعا - الجرائم المرتبطة بأسواق الشبكة الخفية:

تهيئ الإنترنت فرصاً جديدة لبيع السلع وشرائها بصورة غير مشروعة، سواء عبر الشبكة الواضحة أو الشبكة الخفية ("الداركنت"). وعلى عكس الشبكة الواضحة (التي تسمى أيضاً "الشبكة السطحية")، التي تحيل إلى

معلومات متاحة للجمهور وتفهرسها محركات البحث الشائعة التوافر، فإن الشبكة الخفية تتكون من شبكات خفية مشفَّرة، مما يسمح لمالك الموقع ومستخدميه على السواء بإبقاء هويتهم مجهولة مع صعوبة تعقبها نسبيًّا (رامي متولي القاض، 2021، ص 48)

وتتيح أسواق الشبكة الخفية (التي توصف أيضاً باسم "الأسواق المشفَّرة") للمشترين والبائعين عدم الكشف عن هويتهم، وفي تلك الأسواق، تُستخدم العملات المشفَّرة أساساً لدفع ثمن المشتريات لتيسير بيع وتداول سلع من قبيل الأسلحة والمخدِّرات غير المشروعة.(الأمم المتحدة، مؤتمر الأمم المتحدة 14 لمنع الجريمة والعدالة الجنائية،2021، ص 30).

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

ويتزايد استخدام الشبكة الخفية في عمليات التلاعب بنتائج المباريات وأنشطة القمار لدعم دروب غسل الأموال، ولا سيما من جانب الجماعات الإجرامية المنظمة عبر الوطنية. وفي مجال المخدِّرات، ذكر تقرير المخدِّرات العالمي 2019 أن مشتريات المخدِّرات عبر الشبكة الخفية آخذة في الازدياد على المدى الطويل، على الرغم من أنها ربما تكون قد انخفضت من عام 2018 إلى عام 2019. وتشير البيانات المستمدة من الدراسة الاستقصائية العالمية للمخدِّرات لعام 2019 إلى أن شراء المخدِّرات عن طريق الشبكة الخفية لا يزال ظاهرة حديثة جدًّا، حيث إن 48 في المائة من الأشخاص الذين أبلغوا عن شراء المخدِّرات عن طريق الشبكة الخفية في عام 2019 بدأوا في استخدامها لتلك الأغراض في العامين السابقين، وإن نسبة 29 في المائة أخرى بدأت في ذلك في العامين السابقين عليهما.(رامي متولي القاضي، ص 54)

خامسا- استخدام التكنولوجيا بغرض تيسير الاتجار بالأشخاص :

يعد الاتجار بالبشر أحد أبرز أشكال الجريمة المنظمة عابرة الحدود، التي اتسع نطاقها بشكل ملحوظ خلال الآونة الأخيرة، باعتبارها جريمة عابرة للقارات، حيث لا توجد أي منطقة جغرافية في العالم بمنأى عن هذه الجريمة كشكل جديد من أشكال العبودية التي جرمتها العديد من الاتفاقيات والمعاهدات الدولية (امحمد اقبلي، 2020، ص.57.)

وتتضح الخطورة الكبيرة لجريمة الاتجار بالبشر في أن هذا النشاط الإجرامي تعتبره جماعات الجريمة المنظمة ضمن الجرائم المحققة لأرباح طائلة وبأخطار أقل (بالنسبة لها) من جرائم أخرى كتهريب السلاح أو تجارة المخدرات(شريف سيد كمال، 2001 ص.139.)

تبيّن البحوث التي أجريت على مدى السنوات الماضية والأدلة المباشرة أن المتَّجرين بالبشر يستخدمون التكنولوجيا خلال جميع مراحل الجريمة، بما في ذلك تصيُّد الضحايا ومراقبتهم واستغلالهم. وأحد الأسباب التي تجعل المتَّجرين يستخدمون التكنولوجيا في عملهم هو أنها تمكِّنهم من العمل دون الكشف عن هويتهم، كما أن العملة المشفَّرة تسمح لهم بإجراء معاملات مالية ونقل العائدات الإجرامية دون الكشف عن هويتهم. أما السبب الثاني، فهو أن التكنولوجيا تيسِّر لهم تصيُّد الضحايا واستغلالهم، حيث يمكن استخدام مواقع الإعلانات المبوبة على الإنترنت وشبكات التواصل الاجتماعي كقنوات للاتِّجار بالبشر (رامي متولي القاضي، ص 73)

وعلاوة على ذلك، فإن إساءة استخدام التكنولوجيا يمكن أن تيسِّر على المتَّجرين إبرام معاملات مع زبائنهم، ودخول أسواق جديدة، وتوسيع نطاق العمليات الإجرامية. ويمكن للمتَّجرين استخدام تطبيقات البث المباشر للوصول إلى سوق أوسع لزبائن ربما لم يسبق لهم قط أي اتصال فعلي بالضحية، فضلا عن أن إساءة استخدام التكنولوجيات يمكن أن تساعد المتَّجرين على مراقبة الضحايا وإكراههم. ويمكن للمتجرين أن يستفيدوا من تطبيقات تتبع الحركة وتحديد المكان لتيسير استغلال الضحايا. وحتى بعد أن يفلت الضحايا من قبضة المتَّجرين، يظل من الممكن تعقُّبهم حيث يكتشف الجناة أماكن وجود ضحاياهم باستخدام تطبيقات تتبع الحركة وتحديد المكان الموجودة في الهواتف النقالة للضحايا(الأمم المتحدة، مؤتمر الأمم المتحدة 14 لمنع الجريمة والعدالة الجنائية، 2020، ص 11)

الخاتمة:

يتضح من خلال ما تم دراسته حول موضوع الجريمة السيبرانية والإستخدامات المعاصرة والمستحدثة لها التزايد الرهيب والغير معقول لحجم الجرائم والأضرار الناجمة عنها، مع بروز أشكال متجددة ، إذ كلما ظهرت تقنية جديدة بمنافعها المختلفة، إلا وصاحبها ظهور طائفة من الجرائم التي بات محترفوا الجريمة المنظمة يستغلونها لتحقيق منافعهم المادية، والأرباح الخيالية، مع بروز تحديات كبيرة أصبحت تشكل عقبة أمام التعاون الدولي لهذا النوع من الجرائم، خاصة تلك المرتبطة بالجريمة المنظمة

فالاختلافات في التشريعات المنظمة للجرائم الإلكترونية الوطنية عبر العالم، وكذا الاختلافات في قواعد الإثبات والإجراءات الجنائية شكل أحد أهم العقبات في سبيل قمع هذه الجرائم السيبرانية المعاصرة، كما أن

انعدام الثقة بين الأجهزة والدول ، أدى إلى غياب مشاورات مجدية وجدية بخصوص تقديم الطلبات الخاصة بالمساعدة المتبادلة بين أجهزة إنفاذ القانون لهذه الدول، وفي المقابل نجد أن تنظيمات الجريمة المنظمة باتت أكثر تنسيقا فيما بينها، وهو ما أدى إلى فشل وتقويض الكثير من الجهود،

ومما ساهم أيضا في الإنتشار الواسع والرهيب لمنظومة الجرائم السيبرانية عدم التوصل إلى حد الآن إلى تبني صك دولي حديث بخصوص الجريمة السيبرانية، حيث وافقت الجمعية العامة للأمم المتحدة يوم الجمعة، على قرار سيبدأ عملية صياغة معاهدة دولية جديدة لمكافحة جرائم الإنترنت "الجريمة السيبرانية"

ومما يلاحظ أيضا أن مسألة جمع الأدلة القضائية من الخارج بات تشكل إحدى أهم الصعوبات بالمطروحة أمام الدول النظر إلى وجود صعوبات في هذا المجال ، كما لوحظ أيضا سرعة زوال الأدلة الإلكترونية، وفي المقابل تأخر الردود على طلبات المساعدة.

كما أثارت مسألة مكافحة الجريمة السيبرانية مشاكل مرتبطة بحقوق الإنسان على اعتبار أنه قد يؤدي سن تشريعات مكافحة الجريمة المعلوماتية إلى استخدامها لتقييد الحريات كحرية التعبير، وقد بدى جليا تعرض الكثير من أصحاب الرأي والمعارضة في العديد من الدول إلى المضايقات والسجن، باسم مكافحة الجرائم الإلكترونية، وقد يصل الأمر في بعض الأحيان إلى التصفية الجسدية من أصحاب المصالح.

ومن أهم التحديات التي تواجه مكافحة الجرائم السيبرانية تلك التحديات التقنية التي تحتاج إلى خبراء على قدر كبير من الإحترافية ، على اعتبار أنه يمكن للمجرمين استخدام مجموعة متنوعة من الأدوات للتهرب من الاكتشاف من قبل وكالات إنفاذ القانون وإخفاء الوصول ، مع صعوبة تحديد مصداقية الأدلة الرقمية.

قائمةالمراجع:

-إبراهيم رمضان إبراهيم عطايا ،الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية، دراسة تحليلية تطبيقية مجلة كلية الشريعة و القانون بطنطا ، المجلد 30، العدد 2 أبريل 2015.

-امحمد اقبلي، عابد العمراني الميلودي، القانون الجنائي الخاص المعمق في شروح، الطبعة الأولى، دار الرشاد، المغرب 2020.

-السيد عطية شحاته، الجريمة الإلكترونية وعلاقاتها بالميل للجريمة لدي طلاب الجامعة، مجلة مركز الخدمة للاستشارات البحثية ، 2019، المجلد 21، العدد 60 جويلية 2019.

-الأمم المتحدة، أنظر ورقة معلومات أساسية عن حلقة العمل بشأن تعزيز تدابير منع الجريمة والعدالة الجنائية للأشكال المتطورة للجريمة مثل الجريمة السيبرانية والاتجار بالممتلكات الثقافية ، بما في ذلك الدروس المستفادة

والتعاون الدولي، ضمن وثائق مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية، الدوحة، قطر، 12-19 أبريل، 2015.

-ايهاب خليفة ، مجتمع ما بعد المعلومات تأثير الثورة الصناعية الرابعة على الأمن القومي، العربي للنشر والتوزيع، 2019.

-أحمد محمد فتحي الخولي،المسؤولية المدنية الناجمة عن الإستخدام غير المشروع لتطبيقات الذكاء الإصطناعي، الديب فيك نموذجا، مجلة ، مجلة البحوث الفقهية والقانونية، العدد 36، أكتوبر 2021.

-أميرة محمد محمد سيد أحمد، استراتيجيات مكافحة الجرائم الإلكترونية في العصر المعلوماتي تعزيزًا لرؤية مصر 2030: دراسة استشرافية، مجلة البحوث الإعلامية، كلية الإعلام، جامعة الأزهر، العدد 58، جويلية 2021.

-الأمم المتحدة، دليل المناقشة لمؤتمر الأمم المتحدة الرابع عشر لمنع الجريمة والعدالة الجنائية، كيوتو، اليابان، 20-27 أبريل 2020، ص 54.

- الأمم المتحدة، مؤتمر الأمم المتحدة لمنع الجريمة والعدالة الجنائية، البند 6 من جدول الأعمال المؤقَّت، التعاون الدولي وتقديم المساعدة التقنية من أجل منع الجرائم بجميع أشكالها والتصدي لها، حلقة العمل 4- الاتجاهات الراهنة للجريمة، والتطورات الأخيرة والحلول المستجدة، لا سيما التكنولوجيات الجديدة بوصفها وسائل لارتكاب الجريمة وأدوات لمكافحتها،و رقة معلومات أساسية أعدتها الأمانة.

-بن حسكر عودة مراد، إشكالية تطبيق أحكام المسؤولية الجنائية على جرائم الذكاء الاصطناعي، مجلة الحقوق والعلوم الإنسانية، المجلد، 15، العدد 1، 2022.

-توفيق شرف شمس الدين، مخاطر العملات الإفتراضية، كتاب وقائع المؤتمر الدولي الخامس عشر لكلية الشريعة والدراسات الإسلامية، جامعة الشارقة، حول العملات الإفتراضية في الميزان، يومي الثلاثاء والأربعاء 16 و 17 إبريل 2019.

-جمال زكي اسماعيل ، المسؤولية المدنية الناشئة عن الجريمة الإلكترونية، مجلة كلية الدراسات الإسلامية والعربية للبنات بالإسكندرية ، المجلد، 30 العدد 5، 2014 .

-روان بنت عطية الله الصحفي، الجرائم السيبرانية، المجلة الإلكترونية الشاملة متعددة التخصصات، العدد 24، ماي 2020.

-عبد الرحمان بن سالم بن فهاد الطريف، اتجاهات الشباب السعودي نحو الجريمة السيبرانيةوخطورتها، مجلة بحوث كلية الآداب، جامعة المنوفية، المجلد31، العدد 123.

-نبيل ادريس الجريمة السيبرانية بين المفاهيم والنصوص التشريعية، مجلة القانون والمجتمع، المجلد 5، العدد 2، 2017.

الإنتربول: https://www.interpol.int/ar/4/6 تم الإطلاع بتاريخ 2022/06/03 الساعة 19:39.

-مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إليزا للبحوث والدراسات، المجلد 6، العدد 2، 2021.

-شيخه حسني الزهراني ، الطبيعة القانونية للهجوم السيبراني وخصائصه، يونيو 2020م مجلة جامعة الشارقة للعلوم القانونية المجلد 17 العدد 1.

-زينب طرقي العنزي، الجريمة الإلكترونية في ميزان الفقه والقانون، مجلة الدراسات الإسلامية والبحوث الأكاديمية ، العدد 99.

https://www.icrc.org/ar/

-يحي ابراهيم دهشان، المسؤولية الجنائية عن جرائم الذكاء الإصطناعي، مجلة الشريعة والقانون، جامعة الإمارات، العدد 2019.

-يحي ياسين مسعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، جامعة القاهرة، المجلد 4، العدد 4، 2018،.

https://uomus.edu.iq/NewDep.aspx?depid=14&newid=9532
https://www.oracle.com/ae-ar/artificial-intelligence/what-is-ai/

-ممدوح حسن العدوان، المسؤولية الجنائية عن أفعال كيانات الذكاء الاصطناعي غير المشروعة، دراسات، علوم الشريعة والقانون، المجلّد 48 ، عدد 4، 2021.

-ماريلين أورديكيان، العملات الافتراضية المشفّرة في الحقل الجنائي السيبراني، مجلة الدفاع الوطني، العدد 108، أبريل 2019.

-اليونيسف، تقرير حالة الأطفال لعام 2017، الأطفال في عالم رقمي، ص 79. للمزيد حول هذا التقرير أنظر الرابط الإلكتروني التالي:https://www.unicef.org/publications/files/SOWC_2017_AR.pdf ، تم الإطلاع بتاريخ: 2020/05/12، على الساعة 15:00.

-رامي متولي القاضي، مكافحة الإجرام المنظم عبر شبكة الإنترنت المظلمة، المجلة الجنائية القومية، المجلد 64، العدد 3 نوفمبر 2021.

-وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا، مجلة كلية الإقتصاد والعلوم السياسية، جامعة القاهرة، المجلد 23، العدد 1 - الرقم المسلسل للعدد 90، يناير 2022، الصفحة 151-178

-شريف سيد كمال، الجريمة المنظمة في القانون المقارن، الطبعة الأولى، دار النهضة العربية، مصر، 2001 ص.139.