

الدرك ويب (Dark Web) الانترنت المظلم ودور الذكاء الاصطناعي في

التصدي ومكافحة الجرائم.

The Dark Web and the Role of Artificial Intelligence in Combatting and Preventing Cybercrimes.

بن غالم ايمن *

مخبر علم النفس العيادي

جامعة سطيف 2 الجزائر

i.benghalem@univ-setif2.dz

تاريخ القبول : 2025/06/30

تاريخ الاستلام: 2025/02/25

ملخص:

يشير الدارك ويب (Dark Web) إلى الجزء غير المفهرس من الإنترنت، والذي لا يمكن الوصول إليه عبر محركات البحث التقليدية، مما يجعله بيئة خفية تستخدم في العديد من الأنشطة غير القانونية، مثل الاتجار بالبشر، الاستغلال الجنسي، تجارة المخدرات والأسلحة، وتداول البيانات المسروقة. وبسبب خطورته المتزايدة على المجتمعات، أصبح التصدي لهذه الجرائم ضرورة ملحة. في هذا السياق، يلعب الذكاء الاصطناعي دورًا محوريًا في مكافحة الأنشطة غير القانونية على الدارك ويب، وذلك من خلال تقنيات التحليل المتقدم، والتعلم الآلي، والتعرف على الأنماط الإجرامية. يهدف هذا المقال إلى تسليط الضوء على دور الذكاء الاصطناعي في مكافحة الجرائم على الدارك ويب، من خلال مراجعة الأدبيات العلمية وتحليل أحدث التطورات في هذا المجال. الكلمات المفتاحية: الدارك ويب؛ الجرائم؛ الأنشطة غير القانونية؛ الذكاء الاصطناعي.

Abstract:

The Dark Web refers to the concealed portion of the internet that is not indexed and cannot be accessed through conventional search engines. This space has become a hub for illicit activities such as human trafficking, sexual exploitation, drug and arms trade, and the trafficking of stolen data, posing a significant threat to societies. In contrast, artificial intelligence plays a crucial role in combating these illegal activities. This paper seeks to examine the role of artificial intelligence in addressing unlawful activities within the Dark Web by reviewing the relevant scholarly literature on the subject.

Keywords: Dark Web; Cybercrime ; Illegal Activities; Artificial Intelligence.

مقدمة:

تُعدّ الإنترنت واحدة من أعظم الابتكارات التكنولوجية في العصر الحديث واصبحت جزءاً أساسياً من حياتنا اليومية. بدأت نشأتها في ستينيات القرن الماضي كجزء من مشروع لوزارة الدفاع الأمريكية ARPANET. لتبادل المعلومات بين الجامعات والمؤسسات البحثية وكانت كأول شبكة حاسوبية لنقل البيانات بتقنية تبديل الحزم، وبعدها وفي الثمانينات، تم تطوير بروتوكول TCP/IP، الذي مكّن أجهزة الكمبيوتر المختلفة من التواصل فيما بينها بسهولة. بعد ذلك وفي التسعينات ظهر ما يعرف بـ World Wide Web الشبكة العنكبوتية العالمية على يد تيم بيرنرز لي Sir Timothy John Berners-Lee الأمر الذي أحدث ثورة في العالم الرقمي الذي نعرفه اليوم وكان له تأثير عميق على جميع مجالات الحياة من الاتصالات والتعليم والعمل الاقتصاد... الخ. وهذا ما يعرف بالويب السطحي. بالمقابل ومع هذا التطور السريع الذي تزامن مع تطور محركات البحث، بدأ البعض في التفكير في طرق للحفاظ على خصوصية المعلومات أو جعل بعض البيانات غير مرئية للجميع. فظهر ما يعرف بـ Deep web. من جهة أخرى وفي نهاية التسعينات، أطلقت مؤسستان بحثيتان تابعتان لوزارة الدفاع الأمريكية مبادرة تهدف إلى تطوير شبكة مجهولة ومشفرة لحماية الاتصالات الحساسة لعملاء التجسس في البلاد. لم يكن لدى المستخدمين العاديين للإنترنت علم بهذه الشبكة السرية ولم يكن بإمكانهم الوصول إليها. إلا أن الهدف الأولي للسرية لم يتحقق بشكل كامل، كما اكتشف بعض الباحثين في هذا المشروع فرصة مثيرة لإنشاء نظام غير ربحي يركز على الحفاظ على الخصوصية، موجه للنشطاء في مجال حقوق الإنسان وحماية الحياة الشخصية. وهكذا وُلدت شبكة تور، TOR وهي اختصار لـ The Onion Router في إشارة إلى الطبقات العديدة من التشفير التي تحمي المعلومات التي تمر عبرها. تقع تور على هامش الإنترنت وتشكل التقنية الأساسية لما يعرف بـ الويب المظلم (Dark Web)، وهو مجموعة من المواقع المخفية التي لا يمكن الوصول إليها عبر المتصفحات التقليدية ولا يتم فهرستها بواسطة محركات البحث مثل جوجل. (Aditi Kumar, Eric Rosenbach, 2019, p 22) فدارك ويب، هو جزء من الإنترنت يسمح للناس بالبقاء مجهولين ويتيح لهم الاحتفاظ بأسرارهم. لكن للأسف، يُستخدم هذا الجانب من الإنترنت أيضاً في أمور غير قانونية مثل الاتجار بالبشر والاستغلال الجنسي وصناعة وتوزيع المحتوى الإباحي (Devi, G. G., & Radha, R, 2024, p2880) وتجارة الأسلحة والمخدرات وتداول البيانات المسروقة الأمر الذي جعل منه مصدراً متزايداً للقلق بسبب تزايد الجرائم والمخاطر الأمنية والأنشطة غير القانونية. فأصبح بذلك يشكل تحدي خطير وتهديد حقيقي للمجتمعات الإنسانية. وعلى جانب آخر يعد الذكاء الاصطناعي من أكثر التقنيات تقدماً في العصر الحديث، وقد أثر على جميع مجالات الحياة، بما في ذلك الفضاء المظلم للإنترنت Dark web. إلا أنه ومع تطور تقنيات الذكاء الاصطناعي، أصبح له دور مزدوج في تعزيز الأنشطة في الويب المظلم وفي مكافحة الجريمة والأنشطة الغير قانونية. ومن خلال هذا المقال سنحاول لقاء الضوء على دور الذكاء الاصطناعي في

مكافحة الأنشطة الغير قانونية في الدرك ويب من خلال مراجعة الادبيات العلمية في هذا المجال. وهذا ما يقودنا الى طرح التساؤل التالي:

ما هو الدور الذي يمكن أن يلعبه الذكاء الاصطناعي في مكافحة جرائم الدارك ويب، وكيف يمكن لهذه التقنيات أن تعزز من فعالية الكشف عن الأنشطة غير القانونية، وتتبع المجرمين، والتصدي لها؟

1. أهداف الدراسة:

- استكشاف دور الذكاء الاصطناعي في الكشف عن الأنشطة الإجرامية على الدارك ويب.
- التعرف وعرض أهم تقنيات الذكاء الاصطناعي المستخدمة في الكشف والتصدي للأنشطة الاجرامية على الدارك ويب.

2. منهج الدراسة:

في هذه الدراسة، اعتمدنا على المنهج الوصفي التحليلي، حيث قمنا بمراجعة الموروث العلمي المتعلق بالدراك ويب وتحليل الممارسات الإجرامية المرتبطة به، كما ركزنا بالاستناد على الادبيات العلمية على الأدوات والتقنيات التي يوفرها الذكاء الاصطناعي، في التصدي لهذه الأنشطة الاجرامية ومكافحتها.

3. مفهوم الدارك ويب:

3-1 تعريف الدارك ويب (الانترنت المظلم):

يمكن تعريفها بأنها: جزء من شبكة الانترنت، يسمح بإصدار المواقع الالكترونية ونشر المعلومات بدون الكشف عن هوية الناشر أو موقعه، ويحتاج الى برمجيات وضبط وتفويض خاص للوصول إليه، وهي جزء من الويب لا تفهرسه محركات البحث، ويمكن الوصول الى الانترنت المظلم من خلال خدمات معينة مثل خدمة Tor. (ياسر رجب، 2023، ص76)

يشترك هذا الجزء من الأنترنت من الانترنت العميق والذي يحتوي على عمليات هدفها السرية بشكل أساسي وبعبءة عن المراقبة والتجسس وغالبا ما يستخدمها الخارجون عن القانون. (رحاب سيد، 2019، ص73)

3-2 خصائص الدارك ويب:

1- السرية:

تتسم شبكة الدارك ويب بالسرية التامة التي يتمتع بها مستخدموها نتيجة التشفير الحاصل لأي بيانات تدخل إليها.

2- الخصوصية:

يحافظ مستخدمو شبكة الدارك ويب على خصوصيتهم بشكل كبير، نتيجة تعطيل أنظمة التشفير المستخدمة ضمنها لأي محاولات تعقب الكترونية لبيانات ومعلومات المستخدمين، حيث

تساعد شبكة التحويلات التي تمر عبرها الإشارة في حماية المستخدم من الوصول لمعلوماتهم الشخصية إلى أصحاب المواقع الإلكترونية المتواجدة على الدارك ويب.

(ياسر رجب، 2023، ص 73) فالخصوصية هي السبب الأساسي لتوجه العديد من الأفراد نحوها. ومع ذلك، فإن الخصوصية أيضاً تُشجع الأنشطة الإجرامية، مما يُفسر سمعة الويب المظلم المخيفة (Eyo, E, 2020, p109).

3-3 الفرق بين الويب المرئي (السطحي) والديب ويب (الويب العميق) والدرك ويب (الويب المظلم): ركز هذا العمل بشكل أساسي على الويب، وبالتحديد الأجزاء من الويب التي لا يمكن لمحركات البحث رؤيتها (المعروفة باسم الويب غير المرئي). ولكن لفهم ظاهرة الويب غير المرئي بشكل كامل، من المهم أولاً فهم الفروق الأساسية بين الإنترنت والويب. يميل معظم الناس إلى استخدام مصطلحي "الإنترنت" و "الويب" بشكل مترادف، ولكنهما ليسا مترادفين.

الإنترنت هو شبكة متصلة من الحواسيب وبروتوكولات الشبكات التي تسمح لجميع أنواع الحواسيب بالاتصال ببعضها البعض والتواصل عبر الإنترنت. يعود أصل الإنترنت إلى مشروع تم دعمه من قبل وكالة مشاريع البحوث المتطورة الدفاعية الأمريكية (DARPA) في عام 1969 كوسيلة للباحثين والمقاولين في مجال الدفاع لمشاركة المعلومات.

أما الويب، فهو بروتوكول برمجي يسمح للمستخدمين بالوصول بسهولة إلى الملفات المخزنة على أجهزة الكمبيوتر المتصلة بالإنترنت. تم إنشاء الويب في عام 1990 بواسطة تيم بيرنرز لي، مبرمج كمبيوتر يعمل لدى المنظمة الأوروبية للأبحاث النووية (CERN). قبل ظهور الويب، كان الوصول إلى الملفات على الإنترنت مهمة صعبة تتطلب معرفة ومهارات متخصصة. جعل الويب من السهل استرجاع مجموعة متنوعة من الملفات، بما في ذلك النصوص والصور والصوتيات ومقاطع الفيديو، من خلال (Trevino, A et al, 2023)



آلية بسيطة تعتمد على النقر على رابط نصي (Eyo, E, 2020, p107) . و فيما يلي شكل يوضح مستويات الويب

فالويب الواضح أو سطحي يكون بسطح الويب وهو بيئة صديقة للمستخدم، ويتكون من محتوى قام بإنتاجه المستخدم في البيانات التجارية، ويتم فهرسة المحتوى على الويب بواسطة محركات البحث مثل جوجل. يتكون الويب السطحي من صفحات ذات محتوى ثابت، بينما يتكون الويب العميق من صفحات ديناميكية. الصفحات الثابتة تعتمد على ملفات مُخزنة مباشرة على الخادم، ولا تستند إلى قواعد بيانات لتوليد محتواها. يتم تخزين هذه الملفات على الخادم لتكون جاهزة للاسترجاع، وأي تعديل يُجرى عليها يتطلب تعديل كود HTML مباشرةً وتحميل النسخة المُحدثة إلى الخادم (Eyo, E, 2020, p108).

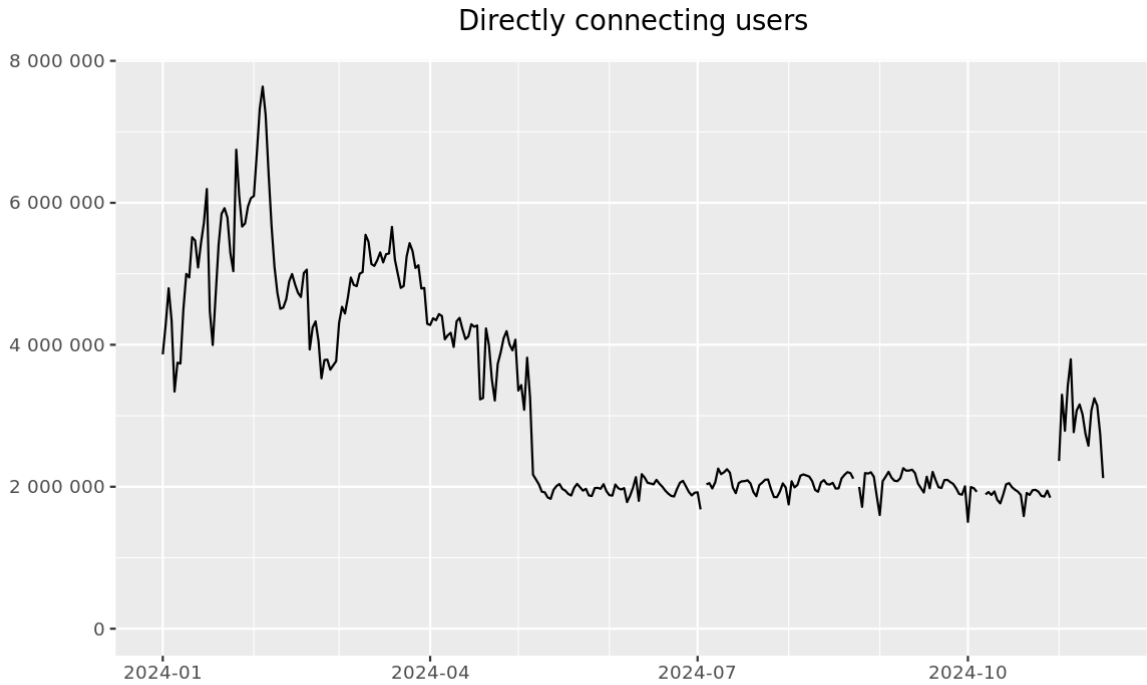
ونظرا للطبيعة غير المشفرة للويب الواضح، فيمكن لتقنية التعقب الرقمي تجميع أنشطة المستخدم المميزة، مثل سلوكيات التصفح، كما يطلب من المستخدمين أيضا تقديم معلومات شخصية عند التسجيل للحصول على الخدمة، إلا أن المعلومات التي يقدمه للمستخدمين والتي يتم الحصول عليها من سلوكهم عبر الانترنت، قد تستخدمها إحدى الشركات لاستهداف الاعلانات أو لأغراض البحث، كما يمكن بيع المعلومات لأغراض الدعاية والتسويق، أو تقديمها للجهات تنفيذ القانون لتعزيز المراقبة أو الملاحقة القضائية، وبالتالي، فإن استخدام بيئة الويب الواضحة تنطوي على خيارات حاسمة للمستخدمين، حيث يؤدي استخدام الخدمات المجانية الى فقدان الخصوصية، وقلة السيطرة على كيفية استخدام المعلومات الشخصية، فضلا على أن عملية المراقبة تتم عن طريق بيانات المواطنين الذين يستخدمون الويب الواضح، حيث تستخدم الحكومات هذه البيانات لفهم مواطنيها، وتستخدم الشرطة في تحديد الأنشطة غير القانونية، ويستخدمها متخصصي الصحة العامة في التنبؤ باندلاع المرض القادم ، ويمكن للمؤسسات التجارية فهم المستهلكين بشكل أفضل وتطوير أسواق جديدة.(رحاب السيد،2019،ص94)

غالبًا ما يتم الخلط بين مصطلحي "الدرك ويب الانترنت المظلم" و"الديب ويب الانترنت العميق" الا انهما يشيران إلى مفهومين مختلفين. (Fabien, T,2022)يشمل الديب ويب جميع صفحات الويب التي لا تتم فهرستها من قبل محركات البحث التقليدية مثل جوجل. وهذا يتضمن الصفحات التي يتطلب الوصول إليها مصادقة، والمحتوى المدفوع، وقواعد البيانات عبر الإنترنت غير المُفهرسة. على سبيل المثال، تشمل الأمثلة السجلات الطبية عبر الإنترنت، والمنتديات الخاصة، وصفحات الشركات المستخدمة داخلياً. (Mathieu B., 2022) على عكس الويب السطحي، يُمثل الديب ويب جميع المواقع غير المفهرسة بواسطة محركات البحث، وهو ما يمثل 96% من صفحات الإنترنت المتاحة (Viard, A, 2017, p3) .

أما الدرك ويب هو جزء محدد من الديب ويب مخفي عمداً وغير قابل للوصول عبر المتصفحات التقليدية. للوصول إليه، يُستخدم متصفح متخصص مثل Tor، الذي يتيح التصفح بشكل مجهول. غالبًا ما ترتبط مواقع الدرك ويب بأنشطة غير قانونية، مثل بيع المخدرات أو الأسلحة أو سلع أخرى

غير مشروعة. يتم تحقيق تخفي الدارك ويب من خلال أنفاق الحركة الظاهرية وبنية الشبكة العشوائية، بالإضافة إلى تطبيقات الأمان الإضافية مثل جدران الحماية وخوارزميات التشفير. يُصعب تقدير حجم الدارك ويب الفعلي، لكن يُقدَّر أنه يُشكل حوالي 5% من إجمالي الإنترنت. باختصار، الديب ويب يتضمن كل المحتوى غير المُفهرَس من قبل محركات البحث، بينما الدارك ويب هو جزء محدد ومخفي من الديب ويب يرتبط عادة بأنشطة غير قانونية ويمكن الوصول إليه فقط بواسطة وسائل محددة. (Mathieu B., 2022) من بين الـ 94% التي تمثل الديب ويب، حوالي 4% فقط هي جزء من الدارك ويب (Viard, A, 2017, p6).

4-3 تقديرات مستخدمي شبكة تور:



The Tor Project - <https://metrics.torproject.org/>

يوضح هذا الرسم البياني العدد التقديري للمستخدمين في كل انحاء العالم المتصلين مباشرة؛ أي أنه يستثني المستخدمين المتصلين عبر الجسور. تستند هذه التقديرات إلى عدد طلبات الدليل التي تم احتسابها على سلطات ومرايا الدليل (Directory Authorities Directory Mirrors)

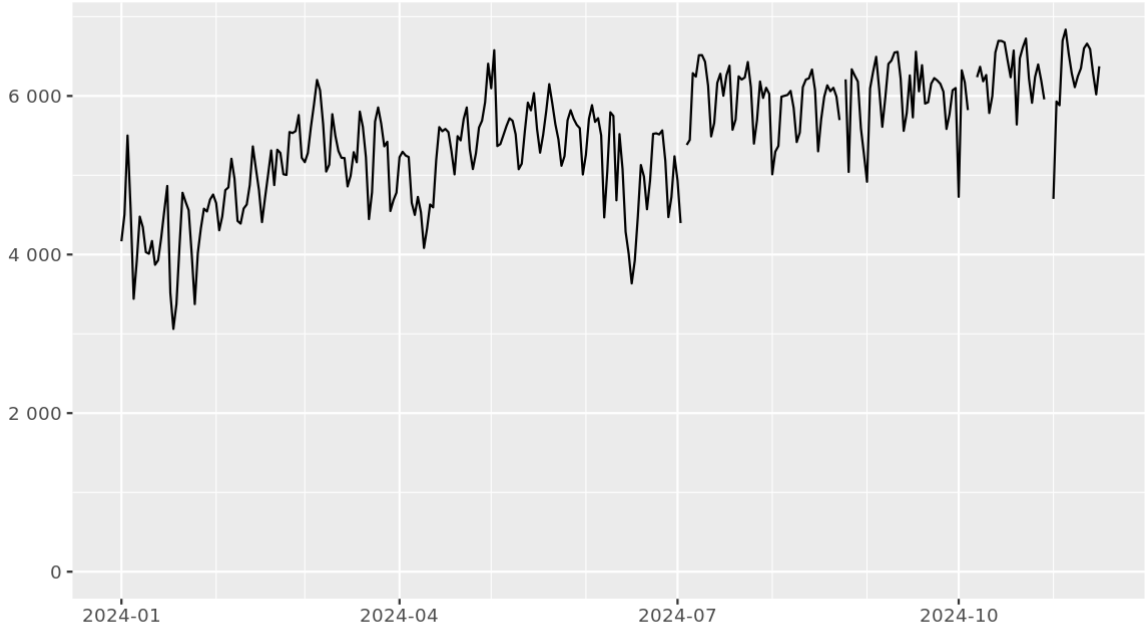
من 2024/01/01 إلى 2024/11/21

الرسم البياني يوضح عدد المستخدمين المتصلين مباشرة بشبكة "تور" من جميع أنحاء العالم في الفترة من يناير إلى نوفمبر 2024. يلاحظ أن هناك زيادة ملحوظة في عدد المستخدمين في بداية العام، تليها فترة انخفاض حاد بين منتصف العام (مايو-يونيو) حتى أغسطس. بعد فترة الانخفاض، يظهر الرسم البياني بعض الارتفاعات في عدد المستخدمين، مما يشير إلى انتعاش أو تزايد في نشاط استخدام شبكة

تور. هذه الزيادة قد تعكس عودة استخدام الشبكة التي يمكن أن تعزى الى تزايد الحاجة للخصوصية في الإنترنت في مناطق معينة.

البيانات تستند إلى عدد طلبات الدليل المرسل إلى سلطات ومرايا الدليل، مما يعني أن هذه الأرقام تعكس المستخدمين الذين يتصلون مباشرة بالشبكة وليس أولئك الذين يستخدمون الجسور للوصول إليها، مما يترك بعض الفروق في تقدير العدد الفعلي للمستخدمين.

Directly connecting users from Algeria



The Tor Project - <https://metrics.torproject.org/>

يوضح هذا الرسم البياني العدد التقديري للمستخدمين في كل الجزائر المتصلين مباشرة؛ أي أنه يستثني المستخدمين المتصلين عبر الجسور. تستند هذه التقديرات إلى عدد طلبات الدليل التي تم احتسابها على سلطات ومرايا الدليل (Directory AuthoritiesDirectory Mirrors)

من 2024/01/01 إلى 2024/11/21

الرسم البياني يعرض عدد المستخدمين المتصلين مباشرة من الجزائر عبر شبكة "تور (Tor)" خلال الفترة من يناير إلى نوفمبر 2024. يتضح من الرسم أن عدد المستخدمين يتقلب بشكل مستمر على مدار العام، حيث يظهر بعض الارتفاعات والانخفاضات التي تشير إلى تغييرات في حجم استخدام شبكة تور في الجزائر. هذه البيانات تعتمد على تقديرات عدد طلبات الدليل المرسل إلى سلطات ومرايا الدليل الخاصة بشبكة تور، وبالتالي فهي تعكس فقط المستخدمين الذين يتصلون مباشرة عبر الشبكة دون المرور عبر الجسور.

5-3 استخدامات الدارك ويب:

ان استخدام الويب المظلم بحد ذاته أمر قانوني ، لكن الأمر يعود للأنشطة التي تقوم عليه، فمنها ما هو قانوني وغير قانوني. (رحاب السيد، 2019، ص 95)

-الأنشطة المشروعة:

ينتقل المستخدمون الشرعيون من الشبكة السطحية إلى الشبكة المظلمة لحماية هوياتهم ومصادرهم وخصوصياتهم من خلال الإخفاء والأمان والسلامة التي توفرها بيئة الشبكة المظلمة. (Akhgar, B. et al, 2021, p29) فهناك العديد من المجموعات من المستخدمين الشرعيين من قطاعات مختلفة، بما في ذلك أولئك الذين يتعاملون مع مكافحة الجريمة، الذين يصبحون مستخدمين للشبكة المظلمة لأغراض محددة. من خلال الاستفادة من ميزاتها. وتتضمن:

• المستخدمين العاديون (العامة):

يستخدم الأشخاص العاديون الشبكة المظلمة لأسباب متنوعة، ولكن بشكل أساسي لتصفح الإنترنت دون أن يتم تتبعهم، وبالتالي حماية خصوصيتهم من المخاطر المختلفة. يدرج مشروع تور بعض هذه الأسباب أدناه ويوصي المستخدمين باستخدام متصفح تور لهذه الحالات:

- لحماية خصوصيتهم وبياناتهم الشخصية.
- لحماية موقعهم الجغرافي الحالي من خلال عدم الكشف عن عنوان IP الخاص بهم.
- للوصول إلى موضوعات بحث حساسة التي تكون محجوبة في بعض البلدان على الشبكة السطحية.
- للوصول إلى الإنترنت ومنصات التواصل الاجتماعي مثل فيسبوك ويوتيوب التي يتم حظرها من قبل الحكومات في بعض الدول من وقت لآخر.
- لحماية خصوصيتهم من المراقبة عبر الإنترنت من خلال جعل من الصعب للغاية على المراقب ربط المواقع التي تمت زيارتها بالهوية في العالم الواقعي. (Akhgar, B., 2021, p30)
- -الناشطون:

حرية التعبير ليست حقًا عالميًا في جميع البلدان. يساعد تصفح الويب العميق المواطنين في الدول التي تقيد حرية التعبير على إخفاء هوياتهم للتعبير عن آرائهم بحرية (Eyo, E, 2020, p110). تتيح الشبكات المظلمة للناشطين في مجال حقوق الإنسان الفرصة لرفع أصواتهم والإبلاغ عن الانتهاكات مثل العمل القسري وأشكال أخرى من الانتهاكات، فضلاً عن تمكينهم من تنظيم حملات أو تحركات تدعو إلى احترام حقوق الإنسان وفقاً لما نص عليه الإعلان العالمي لحقوق الإنسان (Akhgar, B. et al, 2021, p30) كما قد يساعد الويب العميق في النشاط السياسي. (Eyo, E, 2020, p110)

• الاتصالات الحساسة:

يمكن للأفراد استخدام أداة تور للوصول الى غرف المحادثة أو المنتديات ويرغبون في إجراء الاتصالات الحساسة لأغراض شخصية أو تجارية، ويستخدم هذا لحماية الأطفال أثناء تصفح الانترنت لتجنبهم من أنشطة الاساءة، عن طريق إخفاء عناوين بروتوكولات الانترنت IP بأجهزتهم، كما يمكن للشركات استخدام هذه الأداة لحماية مشاريعها. كما يمكن للصحفيين من استخدام أداة تور للتواصل بشكل آمن مع المخبرين والمعارضين (رحاب السيد، 2019، ص98)

• الاستخدام الحكومي:

هناك عدة مجالات مفيدة يوفرها استخدام الويب المظلم، بحيث لا يسعى الأفراد والشركات فقط للحصول على الخصوصية عبر الانترنت، ولكن يستخدمها بعض القطاعات الحكومية، مثل هيئات انفاذ القانون والجيش والمخابرات. بحيث تقوم هيئات انفاذ القانون بإخفاء الهوية على الويب المظلم، (رحاب السيد، 2019، ص107) وذلك لتبادل الوثائق السرية، (مرجع سابق، 96) لتنفيذ عمليات المراقبة عبر الانترنت للحفاظ على خطوط المعلومات المجهولة، وعلى رغم من أنه يمكن لبعض الافراد تحديد هوية الأنشطة، إلا أن هذه الهيئات قد تكهنات بالوسائل التي يمكن من خلالها فرض القانون وتتبع الأنشطة الضارة. فلقد قام مكتب التحقيق الفيدرالي بوضع موارد لتطوير البرمجيات الضارة التي يمكن أن تؤثر على الخوادم في محاولة لتحديد بعض مستخدمي أداة TOR. (رحاب السيد، 2019، ص107) وفيما يلي جدول يوضح المستخدمين الشرعيين الذين يستخدمون الشبكة المظلمة، بالإضافة إلى الجمهور العادي من المستخدمين.

جدول(1): يوضح المستخدمين الشرعيين الذين يستخدمون الشبكة المظلمة.

الفئة	الغرض من استخدام الشبكة المظلمة
الناشطون السياسيون والمبلغون عن المخالفات	يعملون anonymously في الأنظمة الديكتاتورية؛ يكشفون عن الظلم المتعلق بالأعمال أو الحكومة مما يقلل من خطر الانتقام.
الصحفيون	يحمون المصادر ويحمون أنفسهم أثناء نشر المقالات التي لا تخضع لرقابة الدولة.
رجال إنفاذ القانون	يتلقون نصائح مجهولة الهوية حقًا، ويستخدمون الإنترنت أثناء المراقبة، ويحميون الموظفين السريين.
الشركات	يدعمون التجسس الصناعي وعمليات مسح السوق.
الجيش	يشاركون البيانات السرية، ويحميون هوية العملاء الميدانيين، ويجمعون المعلومات الاستخبارية.

(Akhgar, B. et al , 2021, p29)

-الأنشطة غير القانونية الشائعة على الدارك:

الوصول إلى الدارك ويب بحد ذاته ليس غير قانوني، ولكن بسبب مستوى السرية الذي يوفره، يتم استخدامه لأغراض إجرامية. (Children's Society, 2020) وهنا ستغل خاصية إخفاء الهوية التي يوفرها الإنترنت المظلم في تنفيذ أنشطة غير قانونية. والمقلقة. ويُعدّ منصة غير قانونية تُستخدم في أنشطة متعددة تشمل الإرهاب، والقرصنة الإلكترونية، وتقديم خدمات الاحتيال، والاحتيال المالي، واستغلال الأطفال في المحتويات غير القانونية، (Kaur, S., & Randhawa, S., 2020,p3) وغيرها من

الأنشطة المشبوهة.فالتغيير التكنولوجي ادى الى خلق بيئة جديدة اتاحت ظهور أشكال مبتكرة من الجرائم، بالإضافة إلى انتقال الجرائم التقليدية إلى العالم الرقمي، مما يضع هذه الجرائم في سياق مختلف تمامًا عن الجرائم التقليدية المعتمدة على الأماكن ويتطلب مناهج جديدة لمكافحة المخاطر المرتبطة بها.

فالجرائم الرقمية، أو ما يُطلق عليها الجرائم الإلكترونية تُعرف على أنها تشمل الجرائم التي تستهدف أنظمة تكنولوجيا المعلومات والاتصالات (مثل الحواسيب والشبكات)، أو الجرائم التي يكون نظام تكنولوجيا المعلومات والاتصالات جزءًا أساسيًا في تنفيذها. وتنوع دوافع هذه الجرائم بين النفسية- الاجتماعية والجيوسياسية؛ فالجرائم النفسية-الاجتماعية مثل التتبع والمضايقات الإلكترونية ونشر المواد المتعلقة باستغلال الأطفال تُركز على الأفراد، مما يتسبب بأضرار نفسية طويلة الأمد على الضحايا. في المقابل، تأخذ الجرائم الجيوسياسية طابعًا عامًا يشمل خطاب الكراهية الإلكتروني والتخريب الرقمي، مما يعكس تأثيرها على المجتمعات ككل. (Scanlan, J. et al ; 2022,p2)

ومن أبرز أشكال هذه الأنشطة غير القانونية على الدارك ويب نجد:

• بيع المحتوى الحميم والمعلومات الشخصية:

يسهل الإنترنت المظلم بيع الصور والفيديوهات والمعلومات الشخصية، وغالبًا ما يتم ذلك دون إذن الضحايا أو تحت التهديد. غالبًا ما تكون النساء والأطفال الفئة الأكثر استهدافًا، حيث تُستخدم بياناتهم الشخصية في الابتزاز، التحرش، أو الاستغلال. توفر السرية التي يتميز بها الإنترنت المظلم للجنة فرصة لتحقيق مكاسب مالية على حساب انتهاك خصوصية ضحاياهم، مما يؤدي إلى أضرار نفسية واجتماعية مستمرة.

• الاتجار بالبشر:

يُعد الاتجار بالبشر من أخطر الجرائم المنتشرة على الإنترنت المظلم، حيث يستغل المتاجرون خاصية السرية التي يوفرها هذا الجانب الخفي من الإنترنت لشراء وبيع الأشخاص، خاصة النساء والأطفال، لأغراض متعددة. وغالبًا ما يتم خداع الضحايا أو إجبارهم على الانخراط في أوضاع استغلالية تشمل العمل القسري، العبودية الجنسية، أو حتى الاتجار بالأعضاء، مما يسبب لهم معاناة جسدية ونفسية شديدة. تواجه السلطات الأمنية تحديات كبيرة في التصدي لهذه الجرائم بسبب صعوبة كشف هوية المتورطين في الإنترنت المظلم. ونتيجة لذلك، يعاني الضحايا من أضرار طويلة الأمد على المستويين الجسدي والنفسي (Devi, G. G., & Radha, R, 2024, p2882).

• استغلال الأطفال والمواد الإباحية المتعلقة بالأطفال:

يُعد الإنترنت المظلم بيئة خصبة لاستغلال الأطفال، خاصة من خلال إنتاج وتوزيع المواد الإباحية المتعلقة بهم. يتم استغلال الأطفال الأبرياء على الإنترنت المظلم، مما يساهم في استمرار تعرضهم للانتهاكات. يستخدم المجرمون المنتديات المشفرة والأسواق الإلكترونية لمشاركة الصور ومقاطع الفيديو غير القانونية التي توثق الاعتداءات الجنسية على الأطفال. وتساهم خاصية إخفاء الهوية التي يوفرها

الإنترنت المظلم في تمكين هؤلاء المجرمين من التهرب من رقابة السلطات وإنفاذ القانون، مما يزيد من معاناة الضحايا. لمكافحة استغلال الأطفال على الإنترنت المظلم، هناك حاجة ملحة لتوظيف تقنيات متقدمة، وتعزيز التعاون الدولي، واتخاذ إجراءات استباقية تضمن حماية الأطفال من الأذى.

• الاتجار الجنسي:

يعرف "الاتجار بالجنس" بأنه تجنيد الأشخاص ونقلهم واستغلالهم بهدف الاستغلال الجنسي التجاري، وهو أحد فروع الاتجار بالبشر. على الإنترنت المظلم، حيث يقوم المتاجرون بالإعلان عن أنشطتهم الإجرامية والبحث عن عملاء، تكون النساء والأطفال أكثر عرضة لأن يصبحوا ضحايا للاتجار بالجنس. يُحرم الضحايا من استقلالهم وكرامتهم، ويُدفعون إلى الدعارة أو صناعة المواد الإباحية، ويتعرضون للاعتداءات النفسية والجسدية. لمكافحة الاتجار بالجنس على الإنترنت المظلم، هناك حاجة إلى دعم شامل للضحايا، وتدخلات فعالة، واستراتيجيات وقائية. كما أن تطبيق تدابير قانونية صارمة أمر ضروري لمحاسبة الجناة.

• الاتجار بالأعضاء:

يعتبر الاتجار بالأعضاء نشاطًا آخر من أنشطة الاستغلال على الإنترنت المظلم، حيث قد يُجبر أو يُخدع الأفراد لبيع أعضائهم من أجل عمليات زرع الأعضاء. غالبًا ما تستهدف النساء والأطفال، حيث يستغل المجرمين ظروفهم الصعبة أو فقرهم لتحقيق الربح. تسهل سرية الإنترنت المظلم هذه التجارة غير المشروعة، مما يجعل من الصعب على السلطات إيقافها أو تتبعها.

• التبني غير القانوني وخدمات تأجير الأرحام:

يُستخدم الإنترنت المظلم أيضًا لتوفير خدمات التبني غير القانونية وتأجير الأرحام، حيث قد يواجه الراغبون في التبني أو تنظيم خدمات الأمومة البديلة ممارسات استغلالية. غالبًا ما تُجبر النساء، خاصة اللواتي يعانين من صعوبات مالية أو يواجهن حالات ضعف، على المشاركة في هذه المخططات غير القانونية.

• التسول القسري والعروض في الشوارع Street Performances :

قد يساهم الإنترنت المظلم أيضًا استغلال النساء والأطفال من خلال التسول القسري والأداء في الشوارع، حيث يُجبر الضحايا على التسول أو الأداء في الأماكن العامة لتحقيق مكاسب مالية للمستغلين. قد يتعرض النساء والأطفال، لا سيما من يعيشون في فقر أو ظروف هشة، للتجارة أو الاستغلال من أجل التسول القسري أو الأداء في الشوارع، مما يعرضهم للأذى الجسدي والنفسي.

• الإتجار للعمل القسري:

بالإضافة إلى الاستغلال الجنسي، يُعد الإنترنت المظلم أيضًا منصة لتهريب الأشخاص، بما في ذلك النساء والأطفال، لاستغلالهم في العمل القسري. قد يتم خداع الضحايا أو تهديدهم، ثم إجبارهم على العمل في ظروف قاسية في صناعات مثل الزراعة، والبناء، والأعمال المنزلية، والتصنيع. تتيح

الطبيعة الخفية للإنترنت المظلم للمتاجرين الإعلان عن هذه الأنشطة وترتيب الصفقات، مما يصعب على السلطات إيقافها.

• السياحة الجنسية واستغلال المسافرين:

يُستخدم الإنترنت المظلم في سياحة الجنس واستغلال المسافرين، حيث يُستغل الأشخاص، بما في ذلك النساء والأطفال، في ممارسة الجنس في دول مختلفة. قد يقوم المتاجرون بالإعلان عن باقات سفر تشمل الوصول إلى الأشخاص المستضعفين لاستغلالهم جنسيًا، مُدعين أن ذلك جزء من السياحة العادية. قد يُعد الضحايا بوظائف أو فرص تعليمية، لكنهم ينتهي بهم المطاف في الوقوع في فخ الاستغلال الجنسي في الخارج. بسبب سرية الإنترنت المظلم، يمكن للمتاجرين العمل عبر الحدود، مما يصعب على الشرطة القبض عليهم. (Devi, G. G., & Radha, R, 2024, p2882-2883)

• صناعة البورنوغرافيا:

غالبًا ما تُستغل النساء اللواتي يتعرضن للاتجار بالبشر والاتجار بالجنس في صناعة البورنوغرافيا، حيث يُجبرهن المهربون على إنتاج المواد الإباحية تحت تهديد القتل، بعد توقيع اتفاقيات بين الرجال والنساء لتنفيذ الأفعال المطلوبة. قوم مهربو الجنس بتسجيل الفيديوهات دون موافقة الضحايا، ثم يقومون بتوزيع هذه الفيديوهات على الأطراف المهتمة عبر صناعة البورنوغرافيا. كما يقوم المهربون بنشر التسجيلات والصور على مواقعهم الإلكترونية.

العديد من المواقع المتعلقة بصناعة البورنوغرافيا يتم استضافتها على الشبكة المظلمة (Dark Web) ومثلما يفعل مهربو البشر والاتجار بالجنس، تستخدم صناعة الإباحية الشبكة المظلمة ووسائل التواصل الاجتماعي والمنديات الإلكترونية لتجنيد أو اختطاف الضحايا، مخفية هوياتهم. تظهر أشكال جديدة من الجرائم ومستويات عالية من العنف في الفيديوهات والصور الإباحية الخاصة بالدعارة على الإنترنت. ومع الاستخدام الواسع لوسائل التواصل الاجتماعي، أصبحت الدعارة أكثر تطورًا وتعقيدًا. ومن منظور تحقيقي، فإن إجراء مقابلات مع الضحايا والشهود وتتبع السلوك، وبالتالي مراقبة نشاط الدعارة، أصبح أمرًا بالغ الصعوبة وفعالته محدودة (S. Nazah et al., 2020).

• الاتجار بالمخدرات:

أغلب تجارة المخدرات في الوقت الراهن تتم عبر الإنترنت المظلم. فالويب المظلم يعد بمثابة منصة غير قانونية لتوزيع المواد المحظورة والخطيرة التي تُباع مقابل العملات المشفرة مثل البيتكوين، والإيثريوم، والريبيل وغيرها. على سبيل المثال، طريق الحرير (Silk Road) هو أحد أشهر الأسواق على الويب العميق، التي كانت مخصصة لتجارة المخدرات والعقاقير غير المرخصة. حيث يُمكن شراء أي نوع من الأدوية بأي كمية مرغوبة، ويتم توصيل المشتريات مباشرة إلى المنزل بطرق تخفي طبيعة المنتج. (Eyo, E, 2020, p109) والذي أنشئ من قبل مواطن كندي، وفي عام 2013، أغلق مكتب التحقيقات الفيدرالي (FBI) هذا الموقع. من بين المواقع الأخرى، كان Agora أحد هذه الأسواق وأُغلق أيضًا العام الماضي. حاليًا، يُعد Alpha Bay أكبر سوق للمخدرات على الشبكة المظلمة، بالإضافة إلى مواقع أخرى

مثل Dream Market، وValhalla، وWall Street Market، التي تُعتبر منصات لتجارة المخدرات. هناك العديد من المواقع المماثلة التي لا تزال تعمل عبر الويب المظلم لتسويق وشراء المخدرات بشكل غير قانوني، (Kaur, S., & Randhawa, S, 2020,p10).

وهنا يتم العثور عادةً على نوعين من أسواق المخدرات في الويب المظلم. النوع الأول هو الأسواق المتخصصة في نوع واحد من المخدرات مثل الهيروين. وبفضل الخبرة في المنتج والعلاقة بين البائع والعميل، تعد هذه الأسواق أكثر شعبية. أما النوع الثاني فهو الأسواق العامة التي توفر جميع أنواع المنتجات غير القانونية مثل الأسلحة، الإباحية، المجوهرات المسروقة، السجائر في السوق السوداء، وبطاقات الائتمان. وتعد مجموعة المخدرات الواسعة، بما في ذلك المعدات والمواد الكيميائية المستخدمة في تصنيع المخدرات، من العناصر الأكثر شيوعًا. لقد ساعدت خصوصية الويب المظلم على زيادة كبيرة في معاملات المخدرات عبر الإنترنت، مما أسهم في إنشاء سوق سوداء رقمية للمخدرات. وبما أن المعاملات لا تتطلب تواصلًا وجهًا لوجه، يستخدم البائعون غير الشرعيين الويب المظلم لشراء وبيع المخدرات. (S. Nazah et al.,2020)

• الاتجار بالأسلحة:

يُعتبر الويب المظلم منصة للاتجار غير القانوني بالأسلحة. وفقًا لدراسة أجرتها مؤسسة RAND، فإن الشبكة المظلمة تزيد بالفعل من توفر الأسلحة النارية بأسعار مشابهة لتلك الموجودة في الأسواق السوداء على الأرض (Kaur, S., & Randhawa, S, 2020, p12).

علاوة على ما تقدم تشجع السرية والخصوصية العالية لمستخدمي الدارك ويب على القيام بالكثير من الأنشطة غير المشروعة: كبيع المخدرات والأسلحة والأجهزة الإلكترونية المسروقة، وتزوير الهويات الشخصية وجوزات السفر، بسبب صعوبة تعقب المستخدمين وكشف هويتهم وأماكن تواجدهم. كما توفر بعض مواقع الدارك ويب خدمات لتوظيف مخترقين، ومزورين وحتى قتلة مأجورين، فهناك قتلة مأجورون، يعملون بإرسال صورة الضحية إلى القاتل والاتفاق على سعر معين، وبعد إرسال صورة الضحية مقتولا يستلم نقوده من مشتري هذه الخدمة، علاوة على استئجار مخترقي حسابات البنوك والحسابات الشخصية، أو حتى إن اردت سرقة شيء ثمين، فهناك لصوص محترفون يتقاضون أجرا مقابل عمليات السطو، كما ان هناك مواقع خاصة لبيع المسروقات على الانترنت. (ياسر رجب، 2023، ص78)

بالإضافة إلى ما تم ذكره يواجه مستخدموا الدارك ويب خطرا كبيرا لإصابة أجهزة الكمبيوتر الخاصة بهم بواسطة البرمجيات الخبيثة، (Malware) وتبرز خطورة استخدام الشبكة المظلمة في أنها تشكل بيئة خصبة وعالما خاصا للمجرمين المعلوماتيين، لا يخضعون فيه لأي رقابة (لتعذر وصول السلطات واستحالة تعقبه أو تعقب مستخدميه إذا استعملوه بطريقة صحيحة). فهو يستخدم كسوق سوداء ويمكن لتبادل المعلومات الممنوعة التي يعاقب عليها القانون، ومن بين هذه الأمور: تعليم صناعة واستخدام الأسلحة والمتفجرات وحتى الأسلحة البيولوجية منها، تعليم اختراق وتبادل البرمجيات

الممنوعة كالفيروسات والثغرات والتطبيقات الخبيثة، مواقع مختصة بالتزوير والمعاملات المزيفة، مواقع تبادل الكتب والفيديوهات المسروقة. (ياسر رجب، 2023، ص79) كما يتم استنساخ مواقع Onion يشبه أسلوب خداع الوكيل. يقوم المحتال بنسخ الموقع أو الصفحة الحقيقية، ثم يُحدث الروابط بحيث يتم إعادة توجيه المستخدم إلى مواقع احتيالية خاصة به بهدف سرقة الأموال من المستخدم (Kaur, S., & Randhawa, S., 2020, p13) وهنا وفي هذه المواقع الاحتيالية يتم بيع أرقام الحسابات البنكية، وبطاقات ائتمانية مسروقة بعمليات الاختراق بأسعار أقل نسبياً من الرصيد المتوفر فيها وفي بلدان غير بلدانها الأصلية. ومواقع الخدمات الخاصة بالعملات الإلكترونية، ومواقع مجموعات الاختراق المأجورة لتحقيق الكسب المادي بنشر البرامج الخبيثة أو اختراق الحسابات البنكية وبطاقات الائتمان، ومواقع غسيل الأموال لتمويه مصدر المال الأصلي بحيث يبدو وكأنه أتى من مصدر شرعي أو من مصدر غير معروف على الأقل لقطع صلته بالنشاط الإجرامي الذي أدى له. ومواقع خدمات البريد الإلكتروني لما يقدمه من ميزات إضافية مثل الرسائل التي تقوم بحذف نفسها بعد وقت من استلامها وبعد قراءتها مباشرة، ومواقع الخداع والاحتيال لصنع واجهات متاجر وهمية تسمح للمستخدمين بطلب العديد من المنتجات والخدمات، لكنها لا تقوم بإيصالها أو توفيرها بل تأخذ الأجرة فقط، ومع كون التعامل بالعملات الرقمية لا يمكن التراجع عنها، فالمستخدمون سيجدون أنفسهم في دائرة احتيال بدون أن يستطيعوا التصرف حيال الأمر. (رحاب سيد، 2019، ص105)

جدول (2): الأنشطة الإجرامية على الإنترنت المظلم ضد النساء والأطفال.

الأداة	التفاصيل	طبيعة الجريمة الإلكترونية	التعاون الدولي	الحصيلة
مرحباً بكم في الفيديو Welcome to video	تم كشف قضية «Welcome to Video» في عام 2019 وهي منصة إلكترونية ضخمة على الإنترنت المظلم. تم انشائها بين 2015 و 2018 ومقرها كوريا الجنوبية والتي تداولت مواد استغلال جنسي للأطفال (CSAM)، حيث شكلت سوقاً ضخمة. بقيادة سون جون-وو، جمعت المنصة أكثر من 250,000 مقطع فيديو و1.2 مليون عضو من مختلف أنحاء العالم، مما جعلها الأكبر من نوعها التي تم اكتشافها في ذلك الوقت.	الاعتداء الجنسي على الاطفال تداول المواد على منصة الويب المظلم	التعاون الدولي بين وكالات تطبيق القانون أدى إلى إسقاط المنصة، وإنقاذ الضحايا، واعتقال الجناة.	تم اعتقال أكثر من 300 شخص وإنقاذ ما لا يقل عن 23 ضحية.
تفكيك منصة بلايين Playpen Takedown	عملية «Playpen Takedown» عام 2017 كانت علامة فارقة في تفكيك سوق سوداء على شبكة الإنترنت المظلم لتداول مواد استغلال الأطفال جنسياً (CSAM)	توزيع مواد استغلال الأطفال جنسياً عبر سوق على الشبكة	قادت مكتب التحقيقات الفيدرالي العملية بتعاون دولي، والذي يظهر الجهود المشتركة لمكافحة استغلال	تم اعتقال ما يقرب من 900 على مستوى العالم، وإنقاذ ما يقرب عن 300

والمعروفة باسم «Playpen» بإشراف الـ FBI و بالتعاون مع الجهات الدولية.	المظلمة.	الأطفال وإنقاذ الضحايا.	طفل، وتم الحكم بالسجن لمدة 30 عامًا على على مؤسس المنصة.
عملية بايسيفير Operation Pacifier	تم إطلاق عملية "بايسيفير" في عام 2015 لاستهداف منصة الويب المعروفة باسم "بلايين" في الويب المظلم، وهي مركز سيء السمعة لنشر مواد الاعتداء الجنسي على الأطفال (CSAM) بدلاً من إغلاق الموقع فور اكتشافه في عام 2014، اختارت إدارة التحقيقات الفيدرالية الأمريكية (FBI) السيطرة على خوادم بلايين. سمح هذا التحرك الاستراتيجي لهم بالاستمرار في تشغيل الموقع من منشأة حكومية مع جمع الأدلة الهامة ضد مستخدميه ومديره.	التوزيع عبر الإنترنت لمواد الاعتداء الجنسي على الأطفال والأنشطة المتعلقة بها.	نسق مكتب التحقيقات الفيدرالي (FBI) مع وكالات تطبيق القانون الدولية لاستهداف وتفكيك المنصة، مؤكدة على الطبيعة العالمية للجريمة الإلكترونية.
تفكيك منصة "بويس تاون" Boystown Takedown	في عام 2020، اكتشفت السلطات الألمانية منصة «Boystown» وقامت بتفكيكها، وهي منصة على الويب المظلم مخصصة لتوزيع وتبادل مواد الاعتداء الجنسي على الأطفال (CSAM) مع وجود أكثر من 400,000 مستخدم مسجل، عملت «Boystown» كمركز لتوزيع المواد الإباحية التي تشمل الأطفال.	توزيع مواد الاعتداء الجنسي على الأطفال منصة الويب المظلم	أدى التعاون بين السلطات الألمانية والشركاء الدوليين باتخاذ إجراءات سريعة وجهود منسقة للتعامل مع القضية.
طريق الحرير Silk road	قضية "سيلك رود" التي كانت لحظة محورية في عالم الجرائم الإلكترونية. بدأت في عام 2011 مع ظهور سوق على الويب المظلم يُعرف باسم "سيلك رود". تم تأسيسه بواسطة روس أولبريخت تحت الاسم المستعار "دريد بايرت روبرتس"، وكان سيلك رود يعمل كمنصة مجهولة يمكن الوصول إليها فقط عبر شبكة تور، ميسرة تجارة السلع والخدمات غير القانونية باستخدام عملة البيتكوين.	سوق غير قانوني عبر الإنترنت يسهل بيع المخدرات والسلع غير القانونية الأخرى.	أدى التعاون بين وكالات تطبيق القانون المتعددة على مستوى العالم، بما في ذلك مكتب التحقيقات الفيدرالي (FBI)، إلى اعتقال وإدانة مؤسس الموقع.
ألفاباي Alphabay	قضية ألفاباي حدثت في عام 2017، والتي تُعتبر حدثاً بارزاً في معركة مكافحة الجرائم الإلكترونية، أين تم إغلاق واحدة من أكبر	سوق إلكتروني غير قانوني يسهل بيع	ساهم التعاون بين وكالات تطبيق القانون الدولية في إغلاق

(Devi, G. G., & Radha, R, 2024, p2885)

تستدعي الآثار النفسية للديناميكيات الاجتماعية في الدارك ويب دراسة معمقة، خصوصًا فيما يتعلق بمفهوم الهوية المجهولة. وبالاستناد إلى النموذج البنيوي للنفس لدى فرويد الذي يتألف من الأنا، الأنا العليا، وهو يمكننا استكشاف كيفية تأثير التفاعلات المجهولة على السلوك البشري في هذا العالم الرقمي. تمثل الأنا القوة العقلانية والوسيلة في نفس الإنسان، وغالبًا ما تكون في صراع مع الهو المندفع والأنا العليا الأخلاقية. في أروقة الدارك ويب المجهولة، تواجه الأنا ضغوطًا اجتماعية أقل، مما يسمح لكل من الهو والأنا العليا بأن يكون لهما تأثير أكبر.

ومع ذلك، فإن غياب العواقب في العالم الواقعي قد يؤدي إلى تشويه هذه الديناميكيات النفسية. فعند غياب تأثير الأنا الوسيط، قد يتضخم تأثير كل من الهو والأنا العليا، مما يؤدي إلى سلوكيات متطرفة قد لا تظهر في بيئات أكثر تنظيمًا). ففهم الأسس النفسية للتفاعلات على الدارك ويب يضيف بُعدًا من التعقيد لدراستنا لديناميكياته الاجتماعية. فهو يتيح لنا فهم الدوافع الكامنة وراء مختلف

الأنشطة، بدءًا من الأعمال الإجرامية وصولًا إلى الأفعال الإيثارية، ويساعدنا في استيعاب كيفية تأثير الهوية المجهولة في تحرير النفس البشرية أو تقييدها. (Karim, M, 2024).

4. الذكاء الاصطناعي كأداة مكافحة:

طور المجرمون في أساليبهم بشكل ملحوظ، ويهدف التفوق على السلطات وتحقيق غاياتهم، لجأوا إلى استخدام الذكاء الاصطناعي في أنشطتهم الإجرامية. ومع الانتشار الواسع للتكنولوجيا واعتمادها في مختلف جوانب الحياة، أصبح بإمكان المجرمين إنشاء مساح جريمة جديدة في العالم الرقمي. (Ndikaru wa Teresia, J, 2024, p222)

4-1 تعريف الذكاء الاصطناعي ومجالات استخدامه:

يعد الذكاء الاصطناعي أحد ركائز التكنولوجيا في العصر الحديث، وأصبح جزء طبيعي من حياتنا. "فتطبيقات الذكاء الاصطناعي تتعدد وتزايد بصورة يصعب حصرها، فهي تقريبا تدخل في كافة المجالات الإنسانية كالطب والاقتصاد والتعليم... الخ. (بن غالم ايمان، 2023، ص84) ويُعرف الذكاء الاصطناعي بأنه "خوارزمية قادرة على أداء وظيفة كان يُعتقد سابقًا أنها حصرية للذكاء البشري" يشمل هذا التعريف مجموعة واسعة من الخوارزميات المستخدمة لوظائف متعددة، بما في ذلك التنبؤ، والتصنيف، والاستدلال السببي (Spivak, B. L., Shepherd, S. M. 2021).

يُعتبر الذكاء الاصطناعي من أبرز ثمار الثورة الرقمية في العصر الحديث، حيث أسهم بشكل كبير في إحداث تحولات جوهرية في العديد من المجالات. نذكر منها:

- البيئة: التنوع البيولوجي وتغير المناخ المياه، الزراعة.
- الصحة: الطب التنبؤي والجراحة المدعومة بالتقنيات Technology-Assisted Surgery
- الدفاع والطيران: الأمن السيبراني. (يُستخدم للكشف عن الأنشطة الخبيثة أو الهجمات السيبرانية وتحليل البيانات)
- السياحة: السياحة الإلكترونية والمساعدات الشخصية.
- الخدمات المصرفية والمالية: الدردشة الآلية (Chatbot) والمستشارين الآليين (Robo-advisors) لتقديم الاستشارات المالية أو الإجابة على استفسارات العملاء، لتحليل البيانات المالية والتنبؤ بالأداء الاقتصادي للأسواق.
- التجارة: خدمة العملاء، التسويق المستهدف، وكشف الاتجاهات.
- التعليم: التوجيه المستهدف والتعليم المخصص. (منصات التعليم المدعومة بالذكاء الاصطناعي، التعلم التكيفي...)

- الصناعة :الصيانة التنبؤية. تحسين الإنتاجية. بالإضافة الى الرعاية الاجتماعية (الذكاء الاصطناعي في دعم ذوي الاحتياجات الخاصة، مراقبة كبار السن) وغيرها من المجالات الاخرى. (M. Eugène C. Ezin ,2023)

وفيما يلي جدول يوضح الأنشطة الإجرامية على الإنترنت المظلم ضد النساء والأطفال

2-4 استخدام الذكاء الاصطناعي في علم الجريمة إمكانيات الذكاء الاصطناعي في مكافحة الجريمة:



أصبحت التكنولوجيا جزءاً لا يتجزأ من جميع جوانب الحياة، جالبةً معها تأثيرات إيجابية وسلبية على حد سواء. ولم يكن مجال علم الجريمة بمنأى، حيث يسعى علماء الجريمة إلى تطوير أدوات تكنولوجية مبتكرة، بما في

المصدر (Thabault, B ,2024)

ذلك نماذج الذكاء الاصطناعي، للكشف عن الأنشطة الإجرامية ومكافحتها والوقاية منها. تُعد هذه الجهود خطوة بالغة الأهمية، خاصة في ظل استغلال المجرمين للتكنولوجيا كوسيلة لتسهيل أنشطتهم الإجرامية (Ndikaru wa Teresia, J., 2024, p221). تشير الأدبيات الحديثة إلى أن الذكاء الاصطناعي يُستخدم في علم الجريمة بطرق متنوعة، تشمل التنبؤ بالجريمة وتقييم المخاطر واتخاذ القرارات وكذلك تحديد الضحايا وتقديم المساعدة لهم.

• التنبؤ بالجريمة:

اعتمد علماء الجريمة الذكاء الاصطناعي في أداء العديد من مهامهم الأساسية، لا سيما في مجالي الكشف عن الجرائم والتحقيق فيها. ففي فيتنام، تم استخدام أدوات مدعومة بالذكاء الاصطناعي مثل تقييم المخاطر، وتقنيات تخزين وربط البيانات، والتحليلات التنبؤية لتحديد الأنشطة الإجرامية والتحقيق فيها. وقد أثبتت هذه الأدوات فعاليتها، حيث ساهمت في تسريع عمليات الكشف والتحقيق، مما أدى إلى خفض التكاليف والوقت وتحقيق نتائج أكثر دقة وفعالية في العمل الجنائي. تُعد أدوات الذكاء الاصطناعي أيضاً أساسية في تحسين التنبؤ بالجريمة، وهو مفهوم يقوم على استخدام البيانات والخوارزميات لتوقع الأنشطة الإجرامية. يهدف التنبؤ بالجريمة إلى تحديد المكان والزمان الأكثر احتمالاً لوقوع الجرائم المستقبلية، مستنداً إلى الأنماط المكانية والزمانية. وفقاً لبرك (2021)، يمكن بناءً على هذه التوقعات تخصيص موارد الشرطة بشكل استباقي للتعامل مع الجرائم المحتملة ومنع وقوعها، مما يعزز من فعالية استراتيجيات منع الجرائم في سياقات مختلفة (Ndikaru wa Teresia, J., 2024, p222). لا تزال هناك مخاوف بشأن مشاركة البيانات، ومواءمة هذه التقنيات مع القوانين الحالية، واحتمالية التمييز ضد فئات معينة، مما يستدعي تنظيمًا أخلاقياً وتشريعياً لضمان الاستخدام العادل والمسؤول (Ndikaru wa Teresia, J., 2024, p223).

• تقييم المخاطر واتخاذ القرارات:

اعتمد علماء الجريمة استخدام الذكاء الاصطناعي في تقييم المخاطر واتخاذ القرارات المتعلقة بالقضايا الجنائية. يميز Berk (2021) بين تقييم المخاطر والتنبؤ الشرطي، حيث يهدف الأخير إلى تنبؤ بالجرائم بناءً على المكان والزمان، بينما يركز تقييم المخاطر على خصائص الأفراد لتوقع احتمال ارتكابهم للجرائم. يُعد تقييم المخاطر عملية إحصائية تركز على تحديد السمات المرتبطة بالسلوك الإجرامي، وهو مشابه لتوقع مخاطر صحية أو أداء وظيفي.

في الولايات المتحدة، استُخدم تقييم المخاطر في النظام القضائي منذ عشرينيات القرن الماضي، حيث أثر بشكل مباشر في قرارات الإفراج المشروط. كما تم دمج الذكاء الاصطناعي في هذه العمليات حتى قبل ظهور التنبؤ الشرطي. يُوظف تقييم المخاطر لتوجيه العديد من القرارات الجنائية، مثل إصدار الأحكام، والإفراج المشروط، والإشراف على المفرج عنهم، والإفراج المؤقت، وتحديد مستويات الأمان داخل السجون. أشار Spivak & Shepherd (2021) إلى وجود أوجه تشابه بين طرق تقييم المخاطر التقليدية وتلك القائمة على الذكاء الاصطناعي، حيث يعتمد كلاهما على نماذج الانحدار. إلا أن الذكاء الاصطناعي يوفر نطاقاً واسعاً من الخوارزميات، مثل التعلم تحت الإشراف والتعلم التعزيزي، مما يحقق دقة تنبؤية أعلى. ومع ذلك، شددوا على ضرورة وجود إشراف بشري لتجنب تجاهل العوامل الديناميكية المؤثرة على النتائج.

في فيتنام، توصل علماء الجريمة إلى أن الذكاء الاصطناعي يُعد أداة ضرورية في تقييم المخاطر المرتبطة ببعض الجرائم، مما يُسهم في تعزيز عملية اتخاذ القرارات. ومع ذلك، أكدوا على أهمية استخدام الذكاء الاصطناعي كوسيلة مساعدة بدلاً من الاعتماد عليه كبديل للحكم البشري، لتجنب القضايا الأخلاقية المرتبطة بتطبيق هذه التكنولوجيا (Ndikaru wa Teresia, J, 2024, p224).

• التعرف على الضحايا وتقديم المساعدة:

أحدث استخدام الذكاء الاصطناعي تحولاً جذرياً في مجال التعرف على الضحايا وتقديم الدعم لهم. تُعد تقنيات مثل التعرف على الوجه والتحليل البيومتري أدوات فعّالة لتحسين الكفاءة والدقة في تحديد هوية الضحايا. حيث يقوم الذكاء الاصطناعي بتحليل كميات هائلة من البيانات ومقارنتها بمصادر متعددة، مثل وسائل التواصل الاجتماعي، ولقطات المراقبة، والسجلات الرسمية، مما يُسرّع عملية التعرف على الضحايا مقارنة بالأساليب التقليدية.

إلى جانب ذلك، يُسهم الذكاء الاصطناعي في دعم الضحايا من خلال تمكين السلطات من التعرف على الأشخاص المحتمل تعرضهم للإساءة أو الاستغلال. وتُعد روبوتات الدردشة المدعومة بالذكاء الاصطناعي والمساعدات الافتراضية جزءاً أساسياً من هذا الدعم، حيث توفر معلومات حول الحقوق القانونية، وخطط السلامة، وموارد الدعم العاطفي، مما يضمن للضحايا إمكانية الوصول إلى المساعدة بشكل مستمر وعلى مدار الساعة (Ndikaru wa Teresia, J, 2024, p226).

في أمريكا تستخدم وزارة الأمن الداخلي والمحللون الجنائيون في جهاز الخدمة السرية أدوات الذكاء الاصطناعي التي طورتها وزارة الأمن الداخلي للعلوم والتكنولوجيا، مثل أداة الكلام واللغة، وأداة PinPoint، وأداة HORUS للتعرف على الوجوه. تعتمد هذه الأدوات على الذكاء الاصطناعي وتعلم الآلة (ML) لتحديد واستعادة ضحايا الأطفال ومحاسبة المعتدين. في عام 2023، نفذت إدارة التحقيقات الأمنية عملية "الأمل المتجدد"، التي استخدمت الذكاء الاصطناعي ونماذج تعلم الآلة لتحديد وتحديد موقع 311 حالة استغلال جنسي على الإنترنت كانت مجهولة سابقًا. تم تحسين الصور القديمة باستخدام التكنولوجيا المتقدمة، واستُخدمت الأدوات البيومترية لتقديم خيوط جديدة للمحققين. أسفرت العملية التي استمرت ثلاثة أسابيع عن تحديد وإنقاذ أكثر من 100 ضحية للإساءة واعتقال العديد من المشتبه بهم (Homeland Security).

• تعزيز خدمات المؤسسات الإصلاحية:

أصبح استخدام الذكاء الاصطناعي في المؤسسات الإصلاحية حول العالم قوة تحويلية تُسهم في تحسين الكفاءة التشغيلية، وتعزيز السلامة، وتحقيق نتائج إيجابية في إعادة التأهيل. يُستخدم الذكاء الاصطناعي في مجالات متعددة داخل الأنظمة الإصلاحية، تشمل الأمن، وإدارة النزلاء، وبرامج التأهيل، حيث تنشر الدول هذه التقنيات بدرجات متفاوتة من التعقيد والنجاح، مواكبةً للاتجاهات العالمية التي تدعو إلى بناء مرافق إصلاحية أكثر ذكاءً وكفاءة.

في الولايات المتحدة، أثبتت نماذج الذكاء الاصطناعي فعاليتها في تحسين الأمن والكفاءة داخل السجون. على سبيل المثال، تُستخدم تقنيات التعرف على الوجه وتحليل السلوك لمراقبة النزلاء والتنبؤ بالتهديدات الأمنية المحتملة التي قد تصدر عنهم تجاه أنفسهم أو الآخرين. تعتمد هذه الأنظمة على تحليل الأنماط السلوكية وحركات النزلاء لاكتشاف أي نشاط غير اعتيادي، مما يمكنها من تنبيه الموظفين بسرعة إلى المخاطر المحتملة قبل تفاقمها.

تسهم هذه القدرات التنبؤية في تعزيز السلامة من خلال تمكين السلطات من تخصيص الموارد بشكل أكثر كفاءة. إذ يتم نشر الموظفين استراتيجيًا استنادًا إلى البيانات اللحظية التي توفرها أنظمة الذكاء الاصطناعي، مما يحسّن الاستجابة للأحداث ويعزز الأمن داخل المؤسسات الإصلاحية.

في أوروبا، استكشفت المملكة المتحدة استخدام نماذج الذكاء الاصطناعي لتحسين إعادة تأهيل النزلاء وتقليل معدلات العودة إلى الجريمة. ونتيجة لذلك، طُوّرت واختُبرت برامج تعليمية تعتمد على الذكاء الاصطناعي، بالإضافة إلى أنظمة لدعم الصحة النفسية، بهدف توفير جلسات تعليمية وعلاجية مخصصة. تتميز هذه الأنظمة بقدرتها على تكييف المحتوى التعليمي والعلاجي وفقًا لتقدم واحتياجات كل نزيل، مما يضمن تقديم دعم فعال ومخصص. علاوةً على ذلك، تُستخدم القدرات التنبؤية للذكاء الاصطناعي لتقييم مخاطر العودة للجريمة، مما يساعد لجان الإفراج المشروط على اتخاذ قرارات مستنيرة وتحديد الاحتياجات الفردية للنزلاء. كما تُساهم هذه النماذج في تصميم خدمات دعم ما بعد

الإفراج تتناسب مع كل حالة على حدة، مما يعزز فرص الاندماج الناجح في المجتمع ويقلل من احتمالية العودة إلى الجريمة (Ndikaru wa Teresia, J, 2024, p227-228).

• الكشف عن البرمجيات الخبيثة:

غالبًا ما يتم استهداف خوادم الشبكة من قبل المجرمين الإلكترونيين للهجمات كوسيلة لنشر البرمجيات الخبيثة عبر الشبكة أو اختراق النظام. مراقبة حركة مرور الشبكة هي طريقة فعالة أخرى لمراقبة أنشطة المجرمين في شبكة الويب المظلم TOR في هذا السياق، تم اقتراح استخدام تقنية Honeypots لاكتشاف الهجمات الإلكترونية وسلوكيات المجرمين في حركة مرور الشبكة في العديد من الدراسات. تم تطبيق تقنيات Honeypots كطريقة للكشف عن البرمجيات الخبيثة مثل Ransomware حيث يقوم Honeypot بخداع المهاجمين من خلال التظاهر بأنه جهاز كمبيوتر مزيف، ويمكن من خلال هذه التقنية اكتشاف الوصول غير المشروع. (S. Nazah et al., 2020)

كما تم تصميم مصيدة إلكترونية (Honeypot) استخدمت لعرض رسائل تحذيرية للمستخدمين الذين حاولوا الوصول إلى موقع إباحي وهمي. يعرض محتوى مشابه لمواد استغلال الأطفال. هذه البرامج تسعى بشكل استباقي لردع المجرمين المحتملين عن الانخراط في سلوك محظور على الإنترنت من خلال تثقيفهم وزيادة وعيهم بالمخاطر والأضرار المرتبطة بهذا السلوك. (Scanlan, J et al ; 2022,p2)

وفيما يلي جدول يوضح مختلف تقنيات الذكاء الاصطناعي المستخدمة في التصدي للجرائم على المستوى العالمي. جدول من اعداد الباحثة بالاستناد الى دراسة (Ndikaru wa Teresia, J, p2024)

جدول (3): يوضح مختلف تقنيات الذكاء الاصطناعي المستخدمة في التصدي للجرائم

على المستوى العالمي

البلد	وصف الاستخدام	التقنية المستخدمة
الولايات المتحدة	Predpol - يستخدم للتنبؤ بالنشاط الإجرامي باستخدام بيانات الجرائم السابقة.	Predpol, COMPAS, Thorn
	COMPAS - يُستخدم لتقييم مخاطر العودة للجريمة وتحديد قرارات الإفراج المشروط والإفراج بكفالة.	
	Thorn - يستخدم الذكاء الاصطناعي للكشف عن الاتجار بالبشر وتحليل الإعلانات عبر الإنترنت.	
ألمانيا	Precobs - يستخدم لتنبؤ بالسراقات السكنية بناءً على بيانات الجرائم السابقة.	Precobs, Red Cross AI Chatbots
	-الصليب الأحمر الألماني يستخدم روبوتات دردشة مدعومة بالذكاء الاصطناعي لتقديم الدعم القانوني والنفسي للاجئين.	
المملكة المتحدة	HART - يستخدم للتنبؤ بمخاطر ارتكاب الجرائم الخطيرة.	HART, National Data

Analytics Solution (NDAS), Face Recognition Technology	NDAS -يستخدم لتحليل بيانات الجرائم لتحديد الأفراد المعرضين للعنف.	
	-تكنولوجيا التعرف على الوجه تُستخدم للتعرف على الأشخاص المفقودين والمشاركين في الأنشطة الإجرامية.	
ShotSpotter, AI Facial Recognition, Missing Children South Africa, Smart Policing	ShotSpotter -يُستخدم للكشف عن إطلاق النار باستخدام أجهزة استشعار صوتية.	جنوب أفريقيا
	-تقنيات التعرف على الوجه تُستخدم لتحديد ضحايا الجرائم والجناة في الأماكن العامة.	
	-منظمة Missing Children South Africa تستخدم الذكاء الاصطناعي لتحديد أماكن الأطفال المفقودين.	
CAS (Crime Anticipation System)	CAS -يُستخدم لتنبؤ بالمناطق الأكثر عرضة للجريمة بناءً على البيانات الديموغرافية والاجتماعية.	هولندا
Precobs	Precobs -يُستخدم للتنبؤ بالسرقات السكنية استناداً إلى بيانات الجرائم التاريخية.	ألمانيا
تقنيات التنبؤ بالجريمة	-دول مثل فرنسا ورومانيا تتبنى تقنيات التنبؤ بالجريمة باستخدام بيانات مختلفة.	فرنسا، رومانيا
Integrated Joint Operations Platform (IJOP)	IJOP -يُستخدم لجمع البيانات من مصادر متعددة لتحليل المخاطر وتحديد السلوكيات المشبوهة.	الصين
	-تستخدم أنظمة الذكاء الاصطناعي في التعرف على ضحايا الجرائم وتقديم الدعم لهم، مثل تحليل حالات العنف المنزلي.	المملكة المتحدة
Safe City Project	-مشروع Safe City يستخدم أنظمة الذكاء الاصطناعي لرصد الأنشطة غير الطبيعية مثل الانتهاكات المرورية.	رواندا
Crime Mapping, Police Prediction	-تقنيات رسم الخرائط الجنائية تُستخدم لتحليل البيانات وتحديد أنماط الجرائم في كينيا.	كينيا
Social Media AI Analysis, Smart Policing, Risk Assessment Tools in Prisons	-الشرطة الفيدرالية تستخدم الذكاء الاصطناعي لتحليل وسائل التواصل الاجتماعي لاكتشاف علامات الإساءة.	أستراليا
Traffik Analysis Hub	-منصة Traffik Analysis Hub تستخدم الذكاء الاصطناعي لرسم خرائط طرق الاتجار بالبشر ودعمه.	الهند

3-4 تطبيقات الذكاء الاصطناعي على الدارك ويب:

يمكن للذكاء الاصطناعي أن يلعب دورًا هامًا في مراقبة وتحليل الأنشطة في الدرك ويب. باستخدام خوارزميات تعلم الآلة، يمكن اكتشاف الأنماط المشتبه بها التي تشير إلى أنشطة غير قانونية أو مشبوهة. للذكاء الاصطناعي وتحليل البيانات الضخمة القدرة على تقديم مساهمات كبيرة في عمل وكالات إنفاذ القانون. (Akhgar, B., 2021, p146) وذلك من خلال :

- تحليل ودمج البيانات:

أحرزت تقنيات الذكاء الاصطناعي والتعلم الآلي تقدما كبيرا كمثال على ذلك، يُذكر نظام "COPLINK"، وهو نظام متكامل لإدارة المعلومات تم تطويره من قبل جامعة أريزونا. يسمح بإجراء عمليات بحث متقدمة في قواعد البيانات وتبادل المعلومات بين وكالات إنفاذ القانون. (Op cite, p146) بهدف دعم عمليات التحقيق في الجرائم وتعزيز الكفاءة في تحليل البيانات الأمنية.

- التحليل التنبؤي:

أصبح التنبؤ بالجريمة تقنية قوية وشائعة الاستخدام. لذلك، تقضي أقسام الشرطة وقتًا كبيرًا وتستثمر موارد هائلة لاكتشاف الاتجاهات الإجرامية والتنبؤ بها. ومع التحول المتزايد نحو التكنولوجيا وتطورات الذكاء الاصطناعي (AI)، يمكن لتقنيات التعلم الآلي (ML) تقليل هذا الجهد من خلال تحليل كميات كبيرة من البيانات بسرعة لاستخراج أنماط الجرائم (Dakalbab, F., et al, 2022, p2).

- تقنيات تحليل النصوص واكتشاف المحتوى غير القانوني:

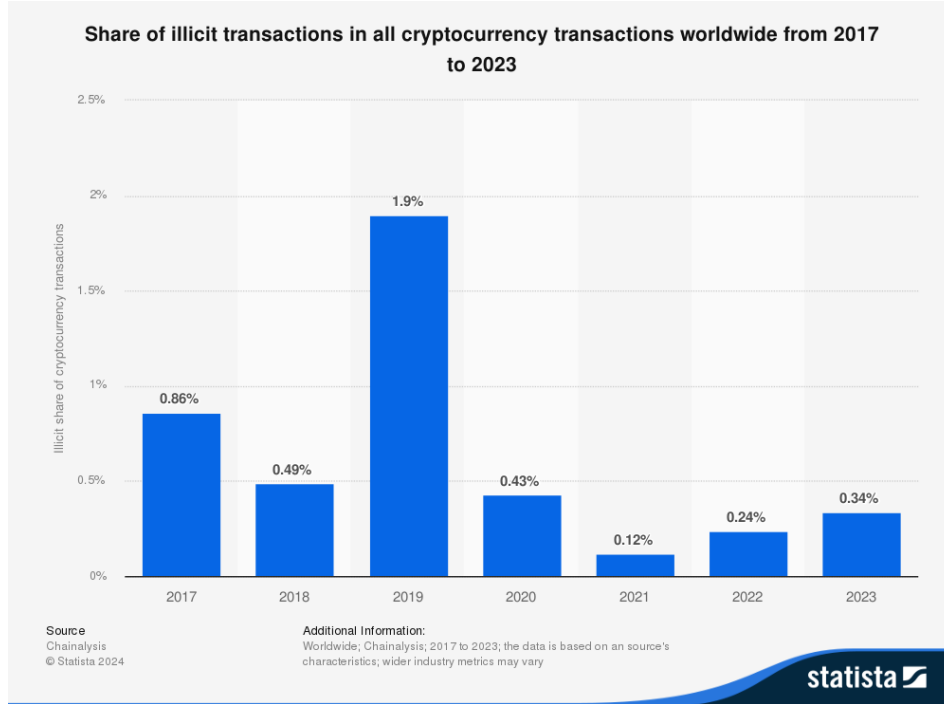
يتم استخدام نماذج مثل Naive Bayes أو BERT للمحتويات ومواد استغلال الأطفال جنسيًا (Child Sexual Abuse Material - CSAM) والذي يعتمد على تقنيات التعلم الآلي والتعلم العميق. يمكن استخدام نموذج للكشف عن CSAM ومراقبة وإزالة نصوص CSAM من المنصات الإلكترونية في الوقت الفعلي وبدقة عالية، مما يوفر حماية أفضل للأطفال. Ngo, V. M., McKeever, S., & Thorpe, C. (2023)

- برامج تتبع النشاطات المجهولة:

هناك واجهة برمجة تطبيقات تجارية (API) تُعرف بـ Webhose.io، والتي تُستخدم لجمع وتلخيص بيانات الويب المظلم. هذه الخدمة مدفوعة وتوفر حماية لهوية الطلاب وأعضاء هيئة التدريس أثناء البحث في الويب المظلم (Bagavathi, A., et al, n.d, p3). لأغراض أكاديمية وبحثية لدراسة الأنشطة غير القانونية أو الجرائم الإلكترونية. كما تستخدم أنظمة الذكاء الاصطناعي لاكتشاف عمليات الاحتيال والاختراق، (البيانات الشخصية، بطاقات الائتمان أو الحسابات البنكية، الاختراق الموجه للشركات والمؤسسات)

• تتبع العملات المشفرة:

العديد من الشركات بدأت في تطوير حلول تعتمد على الذكاء الاصطناعي لتتبع العملات الرقمية وتحليل سلوكيات المستخدمين. هذه الحلول قد تساعد السلطات في تعقب الأموال غير المشروعة ومنع الجرائم قبل حدوثها. في عام 2020، قامت شركة Chainalysis بتطوير أدوات تحليل جنائي رقمي تعتمد على الذكاء الاصطناعي لمساعدة السلطات على تعقب المعاملات المشبوهة عبر البلوك تشين. هذه الأدوات كانت حاسمة في تفكيك شبكات إجرامية متورطة في غسيل الأموال. (يوسف، 2024) وفيما يلي تمثيل بياني يوضح نسبة المعاملات غير القانونية من إجمالي معاملات العملات المشفرة على مستوى العالم



الرسم البياني يعرض نسبة المعاملات غير القانونية في جميع معاملات العملات المشفرة على مستوى العالم من عام 2017 إلى 2023. يوضح الرسم أن النسبة كانت في تزايد ملحوظ في عام 2019، حيث وصلت إلى 1.9% من إجمالي المعاملات المشفرة، وهو أعلى مستوى خلال هذه الفترة.

ثم شهدت السنوات التالية انخفاضاً مستمراً في النسبة:

- في عام 2020، كانت النسبة 0.43%.
- في عام 2021، انخفضت النسبة بشكل كبير إلى 0.12%.
- في عام 2022، ارتفعت بشكل طفيف إلى 0.24%.
- في عام 2023، استقرت النسبة عند 0.34%.

يلاحظ أن هناك تراجعاً عاماً في معاملات العملات المشفرة غير القانونية من 2019 حتى 2023. على الرغم من هذا التراجع، إلا أن النسبة لا تزال تمثل جزءاً من المعاملات المشفرة على مستوى العالم،

مما يشير إلى وجود نشاط غير قانوني في هذا المجال يستدعي المزيد من الرقابة والتشديد في السياسات التنظيمية.

- تحليل البيانات الضخمة من الويب المظلم: تعدّ التقنيات المبتكرة، وخاصة في الذكاء الاصطناعي وتحليلات البيانات الضخمة، جذابة بشكل متزايد في مجال مكافحة الجريمة نظرًا لقدرتها على تعزيز الفعالية والكفاءة. مما يجعلها واحدة من التقنيات الاستراتيجية الواعدة في القرن الحادي والعشرين. (Singh, D. 2022, p41)
- الأمن السيبراني ومكافحة الجرائم الرقمية: في ظل التطور المستمر في القدرات الحاسوبية والتقنيات والتكتيكات المتقدمة التي يستخدمها مجرمو الإنترنت، أصبح من الواضح أن الأنظمة التقليدية للكشف عن التسلسل ومنع التهديدات. تم دمج تقنيات الذكاء الاصطناعي مع منصات معلومات التهديدات السيبرانية الحل الأمثل لمواجهة هذا التحدي. (Dutta, A., & Kant, S. 2020, p81)

4-4 التحديات المرتبطة باستخدام الذكاء الاصطناعي في مكافحة والتصدي للجريمة:

يواجه استخدام الذكاء الاصطناعي في مكافحة الجريمة على الدارك ويب تحديات كبيرة بسبب طبيعة هذا الفضاء الرقمي مما يعقد عملية التصدي للجرائم فيه.

- التحديات التقنية: الدارك ويب هو أحد الوسائط الأكثر تحديًا وصعوبة في تتبعها التي يعتمد عليها المجرمون لتحقيق أهدافهم غير القانونية. الجرائم الإلكترونية التي تحدث داخل الدارك ويب تشبه الجرائم في العالم الواقعي. ومع ذلك، فإن الحجم الكبير، والنظام البيئي غير المتوقع، والسرية التي توفرها خدمات الدارك ويب تعد من التحديات الأساسية التي تواجه عملية تتبع المجرمين وذلك لصعوبة تعقب الأنشطة المشفرة وتطور أساليب المجرمين باستخدام الذكاء الاصطناعي مما يشكل تحديات كبيرة بالنسبة لوكالات إنفاذ القانون والأمن، فالحجم الكبير للويب المظلم يتطلب أساليب أكثر فعالية لتقليل التهديدات المحتملة من الدارك ويب. يجب تتبع الأسواق السوداء والمعاملات التي تحدث هناك لاكتشاف المجرمين باستخدام أساليب متقدمة. إن الهيكل غير المفهرس، المجزأ، والمتعدد الطبقات للدارك ويب يجعل من الصعب أكثر اكتشاف الجرائم. كما أن النظام البيئي للدارك ويب غير قابل للتنبؤ، حيث تختفي المواقع القديمة يوميًا بينما تظهر مواقع جديدة، مما يتطلب جمع أدلة رقمية قوية للوكالات الجنائية لضمان التغلب على العقبات في القبض على المجرمين ومصادرة المواقع غير القانونية (S. Nazah et al., 2020).

• التحديات الأخلاقية والقانونية:

لقد أثبتت نماذج الذكاء الاصطناعي فعاليتها في تقييم المخاطر، (Ndikaru wa Teresia, J, 2024, p- 225) ومع ذلك، وسط الإشادة بهذه التقنيات، تبرز مجموعة متزايدة من الأبحاث التي تسلط الضوء

على المخاطر التي تنطوي عليها تطبيقات الذكاء الاصطناعي على الحقوق الإنسانية الأساسية والمصلحة العامة. (Singh, D. 2022,p41) مما يجعل ان هناك حاجة ملحة للإشراف البشري لضمان دقة النتائج وتجنب المخاوف الأخلاقية (Ndikaru wa Teresia, J, 2024, p-225). فالذكاء الاصطناعي يحتوي على البيانات الحساسة، مما يثير قلقًا بشأن الخصوصية والمراقبة المستمرة. ورغم فوائده في مكافحة الجريمة، فإن البيانات الشخصية تصبح عرضة لمجرمي الإنترنت، مما يزيد من خطر سوء استخدامها. لذلك فمن المهم تحقيق توازن بين استخدام الذكاء الاصطناعي لمكافحة الجريمة وحماية حقوق الأفراد، مع ضمان الشفافية والإنصاف وتبني تدابير أمنية قوية لضمان الخصوصية والسلامة الرقمية. فقد يؤدي استخدام تقنيات الذكاء الاصطناعي الى انتهاك خصوصية الأفراد. وبشكل آخر يمكن استخدام خوارزميات الذكاء الاصطناعي لتحليل كميات هائلة من البيانات لأغراض إنفاذ القانون، مما يسهم في تحديد الأنشطة الإجرامية بشكل أكثر كفاءة. ومع ذلك، فإنها تحمل مخاطر مثل النتائج الخاطئة، واتخاذ قرارات متحيزة، وممارسات مراقبة تنتهك الخصوصية. (Karim,M ., 2024) فمثلا في جنوب أفريقيا، تمت الموافقة على استخدام المراقبة في الأماكن العامة من قبل المحاكم، وهنا أشارت (SAIIA (2021 إلى أن المراقبة العامة ستكون قانونية لأنها تهدف إلى حماية سلامة وأمن الأشخاص المعنيين وهي في المصلحة المشروعة لأولئك الذين يتم مراقبتهم. ومن وجهة نظر معارضة، أشاروا الى أن الأماكن العامة تخص المواطنين والجمهور بشكل عام. هذا النوع من المراقبة يجب أن يُحظر لأن العديد من حقوق الإنسان يمكن انتهاكها. (Singh, D. 2022, p48)

خاتمة:

أصبح اعتماد الذكاء الاصطناعي في مجال علم الجريمة، وخصوصًا في مكافحة الجرائم على الدارك ويب، ضرورة ملحة في ظل التحول الرقمي المتسارع الذي يشهده العالم اليوم. يتطلب هذا التركيز على تطوير تقنيات الذكاء الاصطناعي والابتكار في أساليب مواجهة هذه الجرائم، إلى جانب تعزيز التعاون الدولي للاستفادة من التقنيات المتقدمة بشكل أكثر فعالية. وعلى الرغم من الفوائد الكبيرة التي تقدمها هذه التقنيات واهتمام المجتمع بدمجها في هذا المجال، إلا أن هناك تحديات تواجه الحكومات والجهات الأمنية، منها صعوبة تعقب المجرمين، والحصول على بيانات دقيقة لتدريب الأنظمة الذكية، بالإضافة إلى التحديات المرتبطة بحماية الخصوصية أثناء جمع البيانات. ومع ذلك، فإن تقنيات الذكاء الاصطناعي تُعد سلاحًا ذا حدين؛ فقد تساهم إما في تخفيف تداعيات العالم الرقمي أو في تعقيدها إذا لم تُستخدم بشكل صحيح. لذا، تبرز الحاجة إلى معالجة القضايا القانونية والاجتماعية والأخلاقية المرتبطة بهذه التقنيات بشكل شامل، لضمان استخدامها بشكل مسؤول وفعال يحقق الأمن ويعزز العدالة في البيئة الرقمية.

المراجع:

- بن غالم ايمان، (2023): الانعكاسات والتداعيات السلبية لذكاء الاصطناعي على الصحة النفسية. (تقنية التزييف العميق مثالا)، المجلة العربية للطب النفسي، المجلد 34 العدد 2.
- رحاب فايز أحمد سيد، (2019): أدبيات الويب المظلم بمرصد بيانات شبكة العلوم، المجلة العربية للأرشيف وتوثيق المعلومات، س23، ع46.
- ياسر محمد عبد السلام رجب، (2023): دور الضبط الإداري الالكتروني في مواجهة الانترنت المظلم والانترنت العميق-دراسة مقارنة-مجلة القانون والتكنولوجيا تصدرها كلية القانون بالجامعة البريطانية بمصر، المجلد 3 العدد 2.
- يوسف، (2024): الجرائم المنظمة والتمويل غير المشروع عبر العملات الرقمية: تحليل قانوني ودولي، <https://easylaweg.com/2024/10/10/%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D9%85%D9%86%D8%B8%D9%85%D8%A9-%D9%88%D8%A7%D9%84%D8%AA%D9%85%D9%88%D9%8A%D9%84-%D8%BA%D9%8A%D8%B1-%D8%A7%D9%84%D9%85%D8%B4%D8%B1%D9%88%D8%B9> (تاريخ الاسترجاع، 01-11-2024)
- Akhgar, B., Gercke, M., Vrochidis, S., & Gibson, H. (2021). Dark Web Investigation (Security Informatics and Law Enforcement). Springer
- Bagavathi, A., Muppalla, S. E. P., Krishnan, S., & Cukic, B. (n.d.). A inventory of open and dark web marketplace for identity misrepresentation. Department of Computer Science, University of North Carolina at Charlotte.
- Children's Society. (2020). Online Safeguarding: The Dark Web - What is it? Retrieved from <https://www.childrenssociety.org.uk/sites/default/files/2020-12/What-Is-The-Dark-Web.pdf>.
- Dakalbab, F., Abu Talib, M., Abu Waraga, O., Bou Nassif, A., Abbas, S., & Nasir, Q. (2022). Artificial intelligence & crime prediction: A systematic literature review. Social Sciences & Humanities Open, 6. Elsevier.
- Dutta, A., & Kant, S. (2020). An overview of cyber threat intelligence platform and role of artificial intelligence and machine learning. In Information Systems Security: 16th International Conference, ICISS 2020, Jammu, India, December 16–20, 2020, Proceedings (pp. 81-86).
- Eugène, M. E. (2023). Intelligence artificielle et ses domaines d'applications. Retrieved from https://www.researchgate.net/publication/367525222_INTELLIGENCE_ARTIFICIELLE_ET_SES_DOMAINES_D'APPLICATIONS.
- Eyo, E. E. (2020). Relevance of the Deep Web to Academic Research. International Journal of Natural and Applied Sciences, 12(Special Edition), 107–113.
- Fabien, T. (2022). Deep web vs dark web: Quelles différences? Retrieved from <https://www.expressvpn.com/fr/blog/deep-web-vs-dark-web-quelles-differences/#:~:Acc%C3%A9der%20au%20deep%20web%20ne,web%20reste%20par%20d%C3%A9faut%20anonyme>.
- Homeland Security. (2024). Artificial intelligence and combatting online child sexual exploitation and abuse. Retrieved from https://www.dhs.gov/sites/default/files/2024-04/24_0408_k2p_genai-bulletin.pdf.
- Kaur, S., & Randhawa, S. (2020). Dark Web: A Web of Crimes. Wireless Personal Communications.

- Kumar, A., & Rosenbach, E.,. (2019). La vérité du dark web: Conçu pour protéger les dissidents politiques, il dissimule aussi des activités illicites. Finances & Développement.
- Karim, M. (2024). The Dark Web: A Comprehensive Handbook. Must Read.
- Mathieu, B. (2022). Dark Web: Définition, quel risque de cybersécurité? Retrieved from <https://www.cyberuniversity.com/post/dark-web-definition-quel-risque-de-cybersecuri>.
- Nazah, S., Huda, S., Abawajy, J., & Hassan, M. M. (2020). Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach. IEEE Access, 8.
- Ndikaru wa Teresia, J. (2024). Criminology and Social Impact in the Age of Artificial Intelligence [AI]. East African Journal of Information Technology, 7(1).
- Scanlan, J., Watters, P. A., Prichard, J., Hunn, C., Spiranovic, C., & Wortley, R. (2022). Creating Honeypots to Prevent Online Child Exploitation. Future Internet, 14, 121.
- Ngo, V. M., McKeever, S., & Thorpe, C. (2023). Identifying online child sexual texts in the dark web through machine learning and deep learning algorithms. In APWG.EU Technical Summit and Researchers Sync-Up (APWG.EU-Tech 2023) (pp. 1-6). CEUR Workshop Proceedings. <https://doi.org/10.21427/WFN5-RT72>
- Singh, D. (2022). Policing by Design: Artificial Intelligence, Predictive Policing and Human Rights in South Africa. Just Africa, 7(1), 41–52.
- Spivak, B. L., & Shepherd, S. M. (2021). Ethics, Artificial Intelligence, and Risk Assessment. Journal of the American Academy of Psychiatry and the Law Online.
- Thabault, B. (2024). L'intelligence artificielle au service de la sécurité publique: Décryptage des avantages et défis actuels. Retrieved from <https://www.lacreme.ai/post/intelligence-artificielle-securite-publique>
- Trevino, A., Cutler, A., & Guccione, D. (2023). Deep Web vs Dark Web: Quelle est la différence? Retrieved from <https://www.keepersecurity.com/blog/fr/2023/06/28/deep-web-vs-dark-web-whats-the-difference/>.
- Viard, A. (2017). Les défis et conséquences du Deep Web sur notre environnement et notre économie. Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES, Haute école de gestion de Genève.

مواقع الكترونية:

<https://metrics.torproject.org/userstats-relay-country.html>

<https://www.statista.com/statistics/1410685/illicit-crypto-transactions-worldwide/#:~:text=In%202023%2C%200.34%20percent%20of,volume%20was%20identified%20as%20illicit>