دور الذكاء الاصطناعي في مواجهة الجريمة المنظمة عبر العالم الافتراضي «دراسة تحليلية»

الدكتور/ عمار ياسر محمد زهير البابلي
محاضر بأكاديمية الشرطة. جمهورية مصر العربية

دور الذكاء الاصطناعي في مواجهة الجريمة المنظمة عبر العالم الافتراضي «دراسة تحليلية»

الدكتور/ عمار ياسر البابلي
محاضر بأكاديمية الشرطة. جمهورية مصر العربية

المُلخَّص

يأتي المجتمع الافتراضي بالتحديات والمخاطر والعمليات غير المشروعة والمجرمة عبر الإنترنت، وهنا يأتي دور الذكاء الاصطناعي والشبكات العصبية الاصطناعية للمساهمة في تأمين هذه البيئة الرقمية من التهديدات الإجرامية والإرهابية والتطرف في بيئة الإنترنت الافتراضية؛ كالاتجار بالبشر، وغسل الأموال، وتجارة المخدرات المصطنعة عبر طبقات الإنترنت، وتهريب المهاجرين، والابتزاز الإلكتروني، والاحتيال المالي للمنظمات الإجرامية، وغيره من الجرائم المستحدثة. ويتناول البحث دور الذكاء الاصطناعي (AI) في مواجهة العنف الرقمي والإرهاب عبر المنصات وخاصة مواقع التواصل الاجتماعي؛ حيث يعمل (AI) على رصد وتحليل وتتبع تلك الجرائم ومنفذيها وتحديد أماكن ارتكابها ومعرفة مساراتها، ومكافحة منصات الجماعات الإرهابية، وحظر المحتوى الإرهابي من تأثيره المتطرف على أمن المجتمع والأسرة، بالإضافة إلى التهديدات المستحدثة من الفضاء السيبراني مثل التجنيد الافتراضي، ويبرز دور الذكاء الاصطناعي والشبكات العصبية الاصطناعية والخوارزميات في رصد وتحليل الاتجاهات المتطرفة والإرهابية داخل المنصات الإلكترونية، فاستخدام الأنظمة الذكية يساهم في مواجهة الإجرام المستجد عبر الإنترنت. وقد استخدم الباحث المنهج الوصفي التحليلي في منهجية البحث، وأوصت الدراسة بتعزيز استخدام تطبيقات الذكاء الاصطناعي في إنفاذ القانون والتدابير الأمنية ومكافحة والتنبؤ بالجرائم المستحدثة؛ لمواجهة الإرهاب والعنف الرقمي والجرائم الافتراضية عبر الإنترنت، وتعزيز التوعية الدائمة في المجتمع والجامعات والمدارس ومواقع التواصل الاجتماعي والأخبار والرسائل الإلكترونية والمعرفة، وحماية الأمن السيبراني، فالذكاء الاصطناعي هو التكنولوجيا الناشئة المثالية في عصرنا؛ حيث يتمتع بقدرات متعددة تجعله قادرًا على مكافحة الجرائم المستحدثة؛ كالتطرف والإرهاب وغسل الأموال وتجارة المخدرات عبر المنصات الإلكترونية.

الكلمات المفتاحية: الذكاء الاصطناعي -الإرهاب-الفضاء الإلكتروني – الشبكات العصبية – التعلم الآلي والعميق – الخوارزميات -منصات التواصل الاجتماعي -غسل الأموال – المخدرات المصنعة.

ABSTRACT

The Role of Artificial Intelligence in Countering Organized Crime Through the Virtual World "Analytical Study"

Dr. Ammar Yasir Al-Babli

lecturer at the police academy. Arab Republic of Egypt

The Virtual Community Is Characterized By Vital Communication And Continuous Interactions Via The Internet, And Here Comes The Role Of Artificial Intelligence And Artificial Neural Networks To Contribute To Securing This Digital Environment From Criminal And Terrorist Threats And Extremism In The Virtual Internet Environment Such As Human Trafficking, Money Laundering, Artificial Drug Trade Through The Internet Layers, Migrant Smuggling, Electronic Extortion, Financial Fraud Of Criminal Organizations And Other New Crimes, And The Research Deals With The Role Of (Ai) In Confronting Digital Violence And Terrorism Through Platforms, Especially Communication Sites. Social, Where (Ai) Works To Monitor, Analyze And Track These Crimes And Their Perpetrators, Determine The Places Of Their Commission, Know Their Paths, Combat The Platforms Of Terrorist Groups, And Ban Terrorist Content From Its Extremist Impact On The Security Of Society And Family, In Addition To Threats Created From Cyberspace Such As Virtual Recruitment, And The Role Of Artificial Intelligence, Artificial Neural Networks And Algorithms Comes In Monitoring And Analyzing Extremist And Terrorist Trends Within Electronic Platforms, And That The Use Of Smart Systems Contributes To Confronting Emerging Crime Via The Internet, And The Use Of The Researcher Is The Descriptive Analytical Approach In The Research Methodology The Study Recommends Promoting The Use Of Artificial Intelligence Applications In Law Enforcement, Security Measures, Combating And Predicting New Crimes, Confronting Terrorism, Digital Violence And Virtual Crimes Via The Internet, Enhancing Permanent Awareness In Society, Universities, Schools, Communication Sites, News, Electronic Messages, Knowledge And Protecting Cybersecurity, And Artificial Intelligence Is The Ideal Emerging Technology In Our Time, As It Has Multiple Capabilities That Make It Able To Combat New Crimes. Such As Extremism, Terrorism, Money Laundering and Drug Trafficking Through Electronic Platforms.

Keywords: Artificial Intelligence, Terrorism, Cyberspace, Neural Networks, Machine and Deep Learning, Algorithms, Social Media Platforms, Money Laundering, Synthetic Drugs

المقدمة

تشكل أنشطة الشرطة عاملا مهمًا ضمن جهود الدول لتعزيز الأمن والاستقرار، ودعم جهودها لمواجهة التهديدات التي تفرضها الممارسات الجنائية، ويتطلب تزايد التهديدات الإرهابية، ونماذج الجرائم المتغيرة باستمرار، والاحتياج المتزايد لخدمات الشرطة، تجديدًا مستمرًا في الاستراتيجيات والأولويات والخطط والأساليب، ويعتبر نموذج الشرطة الاستخباراتية الجنائية المزودة بتقنيات الذكاء الاصطناعي خطوة مهمة على طريق مواجهة التحديات [1].

وتعمل الجرائم الإلكترونية عبر مجالات متميزة يمكن تصنيفها إلى ثلاث مساحات محددة: افتراضية ومختلطة في الفضاء الافتراضي، ترتكب الجرائم بالكامل عبر الإنترنت ويشمل العالم الهجين الجرائم التي تنتقل بين العالمين عبر الإنترنت وغير المتصل بالإنترنت، ويشير الفضاء المادي إلى المواقع الجغرافية الملموسة المرتبطة بالأنشطة الإجرامية، ويقدم كل مجال جريمة تحدياته وتعقيداته الخاصة، ويشير مصطلح مساحة الجريمة إلى البيئة التي تحدث فيها هذه الجرائم، بينما تشير المناطق الجغرافية إلى المواقع الملموسة المرتبطة بالجريمة، والتي قد تتطابق أو لا تتطابق مع مواقع الجناة أو الضحايا، ويخلق التفاعل المعقد بين هذه العوالم شبكة من التحديات القضائية والقوانين المتضاربة ومخاوف خصوصية البيانات وحقوق الإنفاذ القانوني، وتزيد هذه التعقيدات من الصعوبات في القبض على المجرمين وحماية الضحايا على حد سواء، ولا سيما عندما تمتد عبر مناطق جغرافية مختلفة. وستتناول الأقسام اللاحقة استكشافًا مفصلاً لفضاءات الجريمة الثلاثة والمواقع الجغرافية للجرائم.

وقد ظهرت الظواهر الإرهابية والإجرامية والأنشطة المتعلقة بالإرهاب في العصر الرقمي بشكل متزايد؛ حيث استغلت المنصات الرقمية ووسائل التواصل الاجتماعي لتنظيم وترويج أنشطتها وأصبح الإرهاب أكثر تنظيمًا وانتشارًا، وتطورت الوسائل والأسلحة التي تستخدمها هذه الجماعات؛ حيث باتت تستخدم الأسلحة الكيميائية والبيولوجية مستغلة في ذلك التكنولوجيا، وعملت الجماعات والتنظيمات الإرهابية على استغلال أجهزة الحاسوب الآلي وشبكة المعلومات الدولية (الإنترنت) والدارك ويب (dark web) في تنفيذ هجمات إرهابية عبر الفضاء الإلكتروني، وتشمل هذه الجرائم المعلوماتية إنشاء مواقع إلكترونية ذات اتجاهات دينية متطرفة ومتعصبة، والتي تستغل الدين أو تتاجر به، وتبادل الاتصالات والمعلومات بين أفراد الجماعات الإرهابية والإعداد والتخطيط لأنشطة معادية وهدامة، التي

(1) ممدوح عبد المطلب، خوارزميات الذكاء الاصطناعي وإنفاذ القانون، الجمعية الدولية للعلوم الشرطية، دار النهضة العربية، القاهرة، 2020، ص3

قد تصل إلى تنفيذ هجمات لاختراق المواقع الإلكترونية المهمة للدولة وتخريبها أو تعطيلها، أو استخدام شبكة الإنترنت ومنصات التواصل الاجتماعي في عمليات تجنيد واستقطاب الشباب ونشر الفكر المتطرف، والإعداد والتنظيم والتخطيط لتنفيذ العمليات الإرهابية تحت غطاء الدين. كما يشمل الاستغلال الإرهابي للإنترنت إنشاء مواقع إلكترونية ذات اتجاهات إثارية ومعارضة لأنظمة الحكم، واستخدام البريد الإلكتروني في تبادل الرسائل بين الجماعات المتطرفة[2]، وذلك بخلاف غسل الأموال وتجارة السلاح والمخدرات المصطنعة عبر شبكات الدارك ويب.

وعلى الجانب الجنائي ظهرت صور جديدة لأشكال متطورة وسريعة التطور من الاعتداءات، تتطلب استجابات فورية لمكافحة الابتزاز الجنسي والمالي وإكراه الأطفال، بالإضافة إلى مواد الاعتداء الجنسي على الأطفال التي تستفيد من تقنيات الذكاء الاصطناعي؛ حيث تسلط المحادثات عبر منصات الألعاب الاجتماعية الضوء على مواقف خطيرة يمكن أن تتطور في غضون 19 ثانية فقط بعد أول رسالة. ومن التحديات الناشئة التي تواجه شركات التقنية وصناع السياسات التصدي لمشكلة مشاهدة ومشاركة صور الأطفال غير المشروعة بهدف الاستغلال والابتزاز، وتظهر الأدلة الحديثة أن هناك ارتباطًا بين مشاهدة المواد الإباحية وارتكاب جرائم الاعتداء الجنسي على الأطفال، مما يبرز أهمية التصدي لهذه القضية بفعالية وسرعة.[3]

وتنتهج الجماعات الإرهابية والجريمة المنظمة استراتيجيات متقدمة عبر الإنترنت وشبكات الدراك ويب لتنظيم وتنفيذ أنشطتها الإجرامية بشكل فعال، ويستخدمون هذه الوسائل للاستفادة من الأفراد والأطفال والقصر، سواء من خلال استغلالهم مباشرةً أو من خلال تحقيق أهدافهم الإجرامية، كما تعتمد هذه الجماعات على تكنولوجيا الدراك ويب؛ حيث يصعب التسلل إلى طبقات تأمينها، مما يجعلها أكثر تحديًا للأجهزة الأمنية ويتيح لهم استخدام الإنترنت الظلام إجراء عملياتهم بشكل متسق وخفي، ويصعب على السلطات التعامل معها بفعالية، كما تشمل أنشطتهم الجرمية جرائم مثل الاتجار بالبشر، والإرهاب، وتجارة المخدرات، والاتجار بالرقيق، والنساء والأطفال، والابتزاز الإلكتروني والأخلاقي، وتمويل الإرهاب، وتهريب المهاجرين، والجرائم التي تندرج ضمن نطاق القتل المأمور، والتي تحدث في كثير من الأحيان داخل أوساط الإنترنت، خاصةً في شبكات الإنترنت المظلمة مثل الدارك ويب.

(2) أحمد محمد الجمال: «الإرهاب الفكري بين المواجهة المجتمعية والأمنية»، رسالة دكتوراه، كلية الدراسات العليا بأكاديمية الشرطة القاهرة، 2021، ص38

(3)The Annual Report 2022 (Internet Watch Foundation، 4792023) Accessed from: https://annualreport2022.iwf.org.uk/wp-content/uploads/202304//IWF-Annual-Report-2022_FINAL.pdf172023/08/

إشكالية الدراسة

أصبح من الصعب بشكل متزايد، البحث بالطرق التقليدية عن مرتكبي الجرائم داخل شبكات الإنترنت؛ مثل الاتجار بالبشر وغسل الأموال والجرائم ذات الأسلوب الإجرامي المستحدث، بخلاف التطرف الرقمي والإرهاب ونشر محتوى متطرف أو إجرامي عبر منصات التوصل الاجتماعي؛ لأن الإنترنت يحتوي على قدر هائل من المعلومات، مما يلزم الحكومات حول العالم بتطوير خوارزميات الذكاء الاصطناعي لمكافحة التطرف والجرائم الافتراضية والمستحدثة من خلال جمع وتحليل البيانات واسعة النطاق بالإنترنت، ونظرًا للتحديات التي تكمن في سرعة نشر المعلومات المضللة والمتطرفة بسبب تعدد المنصات الإلكترونية وصعوبة السيطرة عليها لما تشهده من أعمال التطرف والإرهاب ونشر المشاهد العنيفة وتبادل المواد المخدرة وقنوات غسل الأموال والاتجار بالبشر بمنصات التواصل الاجتماعي والاحتيال المعلوماتي والتحرش الجنسي بالأطفال.

أهمية الدراسة:

تزداد أهمية صناعة الإرهاب مع التطور التقني السريع توازيًا مع الجرائم المنظمة بأنواعها الإجرامية المتعددة كغسل الأموال والابتزاز الجنسي للأطفال وتهريب المهاجرين والاتجار بالبشر وغيرهم من الجرائم المستحدثة، ويتعين علينا تطوير خطوط الدفاع الإلكترونية والإعلامية والأمنية وحملات التوعية لمواجهة دواعي الإرهاب والتطرف الرقمي والإجرام في البيئة السيبرانية والحفاظ عليها، وتركز العديد من الدول على كيفية استخدام التكنولوجيا والذكاء الاصطناعي بشكل يرفع من فاعلية حصر البيانات المطلوبة وتوظيفها لخدمة الأهداف الأمنية وحماية المجتمعات، وخاصة مكافحة الإرهاب والتطرف العنيف على منصات التواصل الاجتماعي التي تنتشر بقوة في جميع أنحاء العالم وصولاً إلى 4.8 مليار مستخدم للإنترنت حول العام في مطلع 2024 ورصد المنظمات الإجرامية عبر شبكات الإنترنت المظلم، لذلك تتطلب المكافحة ضد الإرهاب وجرائم الطبقة الخفية من طبقات الإنترنت وبناء شراكات قوية بين شركات التكنولوجيا والأجهزة الأمنية والاستخباراتية، واستخدام خوارزميات الذكاء الاصطناعي في مواجهة تلك الأعمال الإرهابية والعدائية، بالإضافة إلى تطوير استراتيجيات الوعي ضد التطرف والإرهاب وجرائم الدراك ويب.

أهداف الدراسة

- التعرف على أهم تطبيقات التوصل الاجتماعي الأكثر انتشارًا بين المستخدمين حول العالم، وخاصة أعداد مستخدمي المنصات في الدول العربية ومدى خطورة التطبيقات على مستوي الأمن القومي.
- استخدام تقنيات الذكاء الاصطناعي في مكافحة الإرهاب ورصد المحتوى الإرهابي على منصات التواصل الاجتماعي، وذلك من خلال فهم مراحل ومكونات هذه التقنيات؛ مثل تعلم الآلة، والخوارزميات، ومعالجة اللغات الطبيعية، والشبكات العصبية الذكية، وتحديد محتوى التطرف العنيف ومحاربة انتشار خطاب الكراهية ونشر الأفكار المتطرفة والإرهابية على منصات التواصل الاجتماعي، بالإضافة إلى دور تلك الشبكات العصبية في رصد وتحليل وتتبع مصدر الخطر عبر شبكات الدراك ويب (ابتزاز الأطفال جنسيًا – تهريب المهاجرين – الاتجار بالبشر-...).
- التعرف على تحديات الأجهزة الأمنية الدولية لشبكات (VPN) في تمويل الإرهاب والجريمة المنظمة وقراءة بعض الجرائم وطرق تنفيذها وآليات رصدها على الدارك ويب.
- التعرف على مراحل الاستغلال الجنسي للأطفال عبر طبقات الإنترنت والدارك ويب، والتعرف على مخاطر غسل الأموال وآليات رصدها بأدوات الذكاء الاصطناعي في الجرائم المستحدثة، وهي الاتجار بالبشر وتهريب المهاجرين -ابتزاز واستغلال الأطفال الجنسي – الاحتيال الإلكتروني وإبلاغ السطات وإنفاذ القانون للمواجهة، والتعرف على آليات المواجهة الإعلامية والتقنية لمواجهة جرائم العنف الرقمي وخاصة جرائم الدارك ويب.

تساؤلات الدراسة

- ما هي الشبكات الافتراضية، وما علاقتها بطبقات الإنترنت، وما مفهوم الإنترنت المظلم، وما مخاطره الأمنية، وما علاقته بالجريمة المنظمة؟ وما طريقة تداول المعلومات داخل تلك الطبقات؟
- ما هي المخاطر الأمنية لمواقع التواصل الاجتماعي، وما أسباب زيادة نسب أعداد مستخدمي هذه المنصات، وما هي مراحل الاستغلال الجنسي للأطفال عبر الإنترنت، وما هي طريقة بيع المخدرات المصطنعة وغسل الأموال عبر طبقات الإنترنت، وما هي علاقة المنظمات الإجرامية بالاحتيال الإلكتروني؟
- ما هو مفهوم التطرف الرقمي، وما علاقته بالذئاب المنفردة، وما هي هي تحديات VPN في تمويل الإرهاب؟

- هل يمكن لمخرجات الذكاء الاصطناعي مساعدة الأجهزة الأمنية في مكافحة التطرف العنيف عبر المنصات الإلكترونية في الإزالة وتتبع آثارها وتقديم الأدلة الرقمية للجهات القضائية؟
- ما هي الفرص التي استغلتها المجموعات الإرهابية للذكاء الاصطناعي في الهجمات الإرهابية ونشر موجة الإرهاب والعنف؟

منهج البحث

فرض الموضوع محل الدراسة، الذي يهدف لتحديد دور الذكاء الاصطناعي في مواجهة الظواهر الإجرامية المستحدثة عبر طبقات الإنترنت بسبب تطور معدلات استخدام لتلك المنصات؛ حيث تقع بيئة افتراضية للجرائم المستحدثة كالإرهاب والمخدرات وتهريب المهاجرين واستغلال الأطفال جنسيًا والاحتيال الإلكتروني في عمليات الاتجار بالبشر، وبيان الآثار المترتبة عليها، وضرورة الاعتماد على المنهج الوصفي التحليلي للبحث عن الحلول التقنية؛ حيث توضح المقدمات وتأصيلها، واستعراض التقنيات الداعمة ضد التطرف والإرهاب، ثم تدعيم الوصف بالمنهج التحليلي.

خطة الدراسة

جاء المبحث الأول بعنوان تحديات ومخاطر المجتمع الافتراضي، ويضم مطلبين؛ المطلب الأول: تطور الجرائم الرقمية داخل المجتمع الافتراضي، والمطلب الثاني: التحديات الإجرامية والافتراضية عبر المنصات الرقمية. وجاء المبحث الثاني بعنوان تطبيقات الذكاء الاصطناعي في رصد ومكافحة الظواهر الإجرامية في المجتمع الافتراضي، وتناول مطلبين؛ المطلب الأول: تكنولوجيا الذكاء الاصطناعي في مكافحة الإرهاب والعنف الرقمي المستحدث، والمطلب الثاني: قدرة الشبكات العصبية الاصطناعية على مواجهة الجرائم.

المبحث الأول
تحديات ومخاطر المجتمع الافتراضي

التمهيد

تمثل ظاهرة الإرهاب الرقمي عبر المنصات الإلكترونية تحديات جديدة ومعقدة تواجه جهود مكافحة الإرهاب والأمن السيبراني، وتتضمن هذه الظاهرة استغلال التقنيات الرقمية لتنفيذ أعمال إرهابية أو نشرها، وتشمل هذه الظواهر مجموعة متنوعة من الأنشطة والتحديات، بدءًا من التواصل والترويج والتنسيق لشن هجمات سيبرانية، وصولاً إلى نشر الشائعات والأكاذيب واستخدام الروبوتات عبر المنصات الرقمية، وكل هذه الأنشطة تمثل خطرًا على خصوصية الأفراد من جهة، وعلى الأمن الاجتماعي والأمن القومي للدول من جهة أخرى.

وهناك تحدٍّ رئيس ضمن التحديات التي تواجه إنفاذ القانون الآن: التعقيدات المتزايدة وعبور الجريمة لما وراء الحدود وتواجه الشرطة، وإنفاذ قانون هذه التحديات من خلال تحديد الأولوية الأمنية والاستخباراتية والتأكيد عليها، ثم تحديد المهام والموارد المتاحة المتماشية مع الأولويات المحددة. وإن مواقع التواصل الاجتماعي قد أثرت بشكل كبير على الأمان المجتمعي نتيجة للمخاطر الأمنية والاجتماعية التي تنجم عنها، مثل التزييف العميق والتطرف العنيف وسوء الاستخدام وانتشار خطاب الكراهية واستخدام التكنولوجيا الذكية في تنفيذ أعمال ضارة وخبيثة، بالإضافة إلى ذلك فإن تقنية الميتافيرس والأخبار المضللة يمكن أن تسهم في خلق فوضى واضطراب في المجتمع، ونتناول تلك التحديات كالتالي

المطلب الأول: تطور الجرائم الرقمية داخل المجتمع الافتراضي
المطلب الثاني: التحديات الإجرامية والافتراضية عبر المنصات الرقمية

المطلب الأول
تطور الجرائم الرقمية داخل المجتمع الافتراضي

إن المجتمع الافتراضي، الذي يشمل التفاعلات والأنشطة الاجرامية عبر الإنترنت ومنصات التواصل الاجتماعي، له تأثير كبير على الأمان المجتمعي، وذلك من خلال زيادة الجرائم مثل الاتجار بالبشر وتداول المواد المخدرة والعقاقير المصطنعة وغسل الأموال، بالإضافة إلى استخدام المنصات الرقمية والدارك ويب «الإنترنت المظلم» في التواصل

والتخطيط لتلك الجرائم، ويشير هذا المصطلح إلى التفاعلات والتواصلات في العالم الرقمي؛ حيث يتيح للأفراد التفاعل والمشاركة بسهولة دون معوقات المسافات والزمان ويمكن المجتمع الافتراضي للأفراد من تبادل الأفكار والمعلومات بوسائل متنوعة، سواء عبر شبكات التواصل الاجتماعي، والمنتديات، ووسائل الدردشة، والمدونات، وغيرها من المنصات[4].

أولاً- تعريف تطبيقات التواصل الاجتماعي:

تعرف بأنها: «محتوى يمكن أن يكون على شكل نص مقروء أو مسموع أو مرئي في مجتمع افتراضي، ويشمل هذا المصطلح أيضًا كافة الاتصالات عبر شبكة الإنترنت والهواتف المتحركة ومنصات النشر المستخدمة في التفاعل الاجتماعي والحوار بين الكيانات المؤسسية والجمهور».

ويعرف أيضًا بأنه: مجموعة من المواقع على شبكة الإنترنت، ظهرت مع الجيل الثاني للويب «web 2»، تتيح التواصل بين الأفراد في بنية مجتمع افتراضي، يجمع بين أفرادها اهتمام مشترك أو شبه انتماء (بلد، مدرسة، جامعة، شركة)، يتم التواصل بينهم من خلال الرسائل، أو الاطلاع على الملفات الشخصية، ومعرفة أخبارهم ومعلوماتهم التي يتيحونها للعرض، وهي وسيلة فعالة للتواصل الاجتماعي بين الأفراد، سواء كانوا أصدقاء من الواقع الاجتماعي، أو أصدقاء تم التعرف إليهم من خلال السياقات الافتراضية، باعتبار أن هذه الشبكات الافتراضية لها مخاطر وتحديات أمنية كبرى.

ثانيًا- تزايد أعداد مستخدمي وسائل التواصل الاجتماعي وتزايد التحديات الأمنية:

إن ازدياد أعداد مستخدمي المجتمعات الإلكترونية E–Communities في كثافتهم السكانية على المجتمعات التقليدية يتجلى في زيادة عدد مستخدمي الإنترنت البالغين أكثر من ملياري نسمة؛ حيث تسيطر شبكات التواصل الاجتماعي على الوقت الذي يمضونه على الإنترنت، وبالتالي أسهمت هذه الظاهرة في إنشاء مجتمع افتراضي ذي حجم ضخم يتفوق حتى على أكبر دول العالم، مما يمكنه من تحشيد جموعه حول أي قضية في أي وقت، وتؤدي شبكات التواصل الاجتماعي دورًا فعالاً في دعوة الشعوب إلى المطالبة بحقوقها، كما هو واضح في

(4) عمار ياسر البابلي: آليات الذكاء الاصطناعي في مواجهة التطرف العنيف، مجلة العلوم الشرطية والقانونية بأكاديمية شرطة الشارقة، الشارقة، الإمارات، مجلة العلوم الشرطية والقانونية: دورية علمية، العدد الأول، المجلد 14، 2023، ص222.

تأثيرها في تنحية الرئيس الفلبيني عام 2001 وإسقاط رئيس وزراء إسبانيا عام 2004، وفي التحركات الاحتجاجية ضد الحزب الشيوعي في مولدوفيا والحراس السيخ في الهند والحركة الخضراء في إيران عام 2009، بالإضافة إلى حركة القميص الأحمر في تايلاند عام 2010، ويعتبر Facebook من بين المنصات التي تؤدي دورًا فعالاً في مجال التعبئة؛ إذ يستخدمه 4.62 مليار شخص، ممثلين أكثر من نصف سكان العالم، وتشكل 93.4٪ من الأشخاص المتصلين بالإنترنت [5].

ومع تسليط الضوء على دور منصات التواصل الاجتماعي كأداة حيوية، تظهر مشكلة الاستخدام السلبي لهذه المنصات؛ حيث تعد كأنواع من الأكسجين التي تمد الإرهاب بالحياة وتسمح هذه المنصات للتنظيمات الإرهابية بانتهاك المجتمعات والخصوصية، وتشجع على ترويج الأفكار الهدامة والعدوانية، بالإضافة إلى عرض مشاهد العنف، وتشير الملاحظات إلى استخدام العديد من تلك الجماعات الإرهابية لتلك المنصات لاستقطاب الشباب ونشر محتوى تحريضي؛ حيث تعتبر هذه المنصات بيئة مواتية لنشر وتعزيز معتقداتهم ومع تصاعد الأضرار الناجمة عن هذه الظاهرة في الدول المعرضة للتطرف والإرهاب، بما في ذلك زيادة التجارة في المواد المخدرة والاتجار بالبشر والعنف الرقمي وغسل الأموال، إلى جانب انتشار الألعاب المولة وظاهرة تهريب المهاجرين، الأمر الذي يصبح معه التصدي لهذه التحديات بأساليب تقنية ذكية ويظهر ما يتم بثه عبر مواقع التواصل الاجتماعي من أخبار وأنشطة لتلك المنظمات المتطرفة زيادة في دعائها واعترافها ومشروعيتها وترويجها، مما يشكل تحديًا يتطلب التدخل بأساليب تقنية وذكية لمواجهته بفعالية.

ثالثًا- نمو وتحليل البيانات داخل أوعية معلومات المنصات الرقمية [6]:

سكان العالم		مستخدمي الإنترنت	مواقع التواصل الاجتماعي	
8.01 مليار		5.16 مليار حول العالم	4.76 مليار من سكان العالم	
الذكور	الإناث	بنسبة 64.4% من سكان العالم	الذكور	الإناث
50.3%	49.7%		46.3%	53.7%

(5) FACEBOOK STATISTICS AND TRENDS: Essential Facebook statistics and trends for 2022 At: https://datareportal.com/ on 52023/

(6) Number of internet and social media users worldwide as of January 2024:= https://www.statista.com/markets/424/internet/

- أنتج العالم 94 زيتابايت من البيانات بنهاية ومن المتوقع إنشاء 181 زيتابايت من البيانات بحلول 2025.
- تظهر الأرقام الحديثة تفوقًا متزايدًا لمستخدمي التطبيقات الرائدة في مجال التواصل الاجتماعي على مستوى العالم حتى سبتمبر 2023، ويتجاوز عدد مستخدمي الإنترنت حول العالم 5.6 مليار شخص، مع إرسال ما يقارب من 42 مليون رسالة يوميًا عبر تطبيق الواتساب، وتنفذ ما يصل إلى 2 مليون مكالمة صوتية ورسالة يوميًا عبر منصة فيسبوك، بالإضافة إلى نحو 99,000 عملية بحث في الثانية الواحدة على هذه المنصة، كما تصل عمليات البحث اليومية على جوجل إلى ما يقرب من 8.5 مليار عملية بحث. ويتم نشر أكثر من 700 مليون تغريدة جديدة يوميًا على تويتر، فيما يصل عدد رسائل البريد الإلكتروني إلى 400 مليون رسالة يوميًا.
- وفيما يتعلق بتطبيقات التواصل الاجتماعي، يتفوق YouTube بـ 2.96 مليار مستخدم، بينما يبلغ عدد مستخدمي Instagram 2.51 مليار، ولدى TikTok 1.32 مليار مستخدم، ولدىWhatsApp 1.05 مليار مستخدم. وعن توزيع الجنسين، تظهر الأرقام أن نسبة الإناث تمثل أغلبية المستخدمين في Instagram وTikTok، بينما يظهر WhatsApp توزيعًا أكثر توازنًا بين الجنسين[7].

وتتزايد خطورة الجرائم الرقمية المتنامية في الفضاء الإلكتروني نتيجة للارتفاع الملحوظ في أعداد وإحصائيات مستخدمي منصات التواصل الاجتماعي على مستوى العالم؛ حيث يجد هؤلاء المستخدمون أنفسهم عرضة لمجموعة من المخاطر التي تتنوع وتظهر بشكل متزايد في هذا البيئة الرقمية. ومن بين هذه المخاطر يتصاعد التطرف والإرهاب، فضلاً عن مشاكل مثل غسل الأموال والاتجار بالبشر والعنف الرقمي، وتظهر أخطار أخرى أيضًا، مثل تجارة البغاء والتحرش الإلكتروني الجنسي بالأطفال وابتزازهم، والتضليل الإعلامي، ونشر الشائعات. ومن ضمن هذه المخاطر يتجلى التحريض على الكراهية والعنف داخل منصات التواصل الاجتماعي كمصدر للقلق؛ إذ يمكن أن يؤدي ذلك إلى زيادة في انتهاكات المجتمعات والبشرية بشكل عام.

(7) https://wearesocial-net.s3.amazonaws.com/wp-content/uploads/202105-/01/Time-Spent-on-Social-by-Country-DataReportal-20210126-Digital-2021-Global-Overview-Report-Slide-90.png تاريخ الزيارة 2024/3/1

رابعًا– أثر وسائل التواصل الاجتماعي على الأمن المجتمعي والفكري:

- يعتبر الأمن الفكري الأساس الذي يرتكب إليه فكرة الحفاظ على الأمان والمنع من الانجراف الفكري نحو التطرف والإرهاب، ويتعلق الأمن الفكري بالقدرة على المحافظة على استقرار الأفكار والمعرفة في المجتمع والحماية والوقاية من الجرائم المستحدثة، والتقليل من انتشار الأفكار المتطرفة والمواقف الصارمة التي قد تفضي إلى العنف والإرهاب.
- إن استخدام مواقع التواصل الاجتماعي يمكن أن يؤثر على الأمن الفكري للأفراد، فعلى سبيل المثال يؤثر على الأمن الفكري للفرد من خلال الاطلاع المستمر على البيانات والمعلومات المنشورة على مواقع التواصل الاجتماعي، ويؤثر على الإدراك والتفكير والقدرة على التحليل النقدي، وبالتالي قد يؤثر على الأمن الفكري للفرد[8].
- تستخدم العديد من التنظيمات الإرهابية والمتطرفة وسائل التواصل الاجتماعي للتواصل مع بعضها البعض ونشر الدعاية والتحريض على العنف والإرهاب وتبادل الخبرات والتكتيكات والتخطيط للعمليات الإرهابية، ويعد تنظيم الدولة الإسلامية وحركة الشباب من أبرز المستخدمين لوسائل التواصل الاجتماعي، وخاصة على تويتر[9].
- ويمثل استخدام هذه التنظيمات والجماعات المتطرفة لوسائل التواصل الاجتماعي تحديًا كبيرًا للأمن الفكري والأمن الدولي بالإضافة إلى موقع اليوتيوب، لنشر الدعاية والتحريض على العنف والإرهاب، وتبادل الخبرات والتكتيكات والتخطيط للعمليات الإرهابية والترويج للمواد المتطرفة باعتبارها وظيفة الدعاية الرئيسة والمورد المالي الأساسي، وتظهر البحوث أن الإنترنت يعمل كقناة للتطرف والإرهاب بثلاث وسائل([10]):
- **التفسير والتعزيز**: يستخدم الإنترنت ووسائل التواصل الاجتماعي في توضيح وتعزيز الأيديولوجيات المتطرفة عبر الرسائل والسرديات المرسلة عبر الفضاءات الزرقاء والإنترنت.

(8) خالد كاظم أبو دوح، دور وسائل التواص الاجتماعي في نشر الإرهاب، مجلة آفاق استراتيجية، مركز المعلومات واتخاذ القرار، رئاسة مجلس الوزراء المصري، القاهرة، العدد (2)، أكتوبر 2021، ص 79.

(9) شبكات ومواقع ومنصات التواصل الاجتماعي وتجنيد الذئاب المنفردة ونشر فكرهم المتطرف العنيف، دراسة مقدمة من مرصد الفتاوى التكفيرية والآراء المتشددة، دار الإفتاء المصرية، بتاريخ 2019/1/14. للمزيد انظر الموقع الإلكتروني الآتي: https://www.facebook.com/InfedilizingFatwas تاريخ الزيارة 2020/9/13

(10) إليسا أوروفينو؛ التطرف عبر الإنترنت: كيفية اكتشاف المحتوى المتطرف والتعامل معه (المملكة المتحدة نموذجًا)، تقرير موقع عين أوروبية على التطرف، 19 سبتمبر 2022 متاح على https://eeradicalization.com/exploring-online-radicalization-how-to-spot-extremist-content-and-what-to-do-about-it/

- **العضوية والاندماج:** يوظف الإنترنت ووسائل التواصل الاجتماعي في إنشاء مسارات سهلة للأفراد المتشابهين في التفكير، للانضمام معًا وتشكيل شبكات لدمج المزيد من الأشخاص.
- **تطبيع الآراء والسلوك غير المقبول:** يستخدم الإنترنت في إنشاء غرف افتراضية للنقاش والمحاكاة لوجهات النظر والأفكار المتطرفة، التي يتم من خلالها تطبيع السلوكيات غير المقبولة.
- أجرت اليونسكو دراسة حول استخدام شبكات التواصل الاجتماعي، ووجدت أنها تستخدم في إنشاء منصات تفاعلية ونشر محتوى عنيف ومتطرف، وتحديد الأعضاء الجدد المحتملين وإنتاج معلومات كاذبة، وتعزيز الحوار الفردي وتكوين علاقات مع الأفراد، بهدف التجنيد أو كسب التعاطف، وأشار «إيفان هولمان»، الخبير في مجال مكافحة الإرهاب الإلكتروني، إلى أن 90% من النشاط الإرهابي على الإنترنت يتم من خلال استخدام مواقع التواصل الاجتماعي[11].
- وتشير الدراسات الحديثة إلى أن الجماعات الإرهابية تسعى جاهدة إلى استخدام التقنيات الحديثة والذكاء الاصطناعي في تحقيق أهدافها الإرهابية عبر الإنترنت، ويعد الروبوت (وهو تطبيق أو برنامج يعمل بشكل مستقل عبر الإنترنت) [12]واحدًا من أهم الأدوات التي تستخدمها هذه الجماعات للتواصل مع المجندين المحتملين وإرسال رسائل الدعاية ونشر المحتوى الإرهابي.
- ابتكر «محمد بهرون نعيم» الإرهابي المعروف بـ «أبي محمد الإندونيسي» Bahrun Naim روبوتًا لتواصل المجندين المحتملين، يستخدم هذا الروبوت رسائل آلية باللغة الإندونيسية للتواصل مع المستخدمين، ثم يشاركهم فيديوهات ورسائل دعائية، ويقدم لهم أدلة على تصنيع المتفجرات المحلية الصنع، وهو ما يتيح للجماعات الإرهابية البقاء على اتصال مع متابعيها، كما استخدمت حركة الشباب المجاهدين روبوتًا على تطبيق التليجرام، ويرسل هذا الروبوت روابطًا لآخر أخبار الحركة، مما يتيح لها البقاء على اتصال دائم مع متابعيها[13].

(11) تقرير منظمة اليونيسكو بشأن المعلومات المضللة على شبكة الإنترنت: اليونسكو تكشف خطة عملها الرامية إلى تنظيم عمل منصات التواصل الاجتماعي، بتاريخ 6 نوفمبر 2023 ومتاح على الموقع الإلكتروني
https://www.unesco.org/ar/articles/almlwmat-almdllt-ly-shbkt-alantrnt-alywnskw-tkshf-khtt-mlha-alramyt-aly-tnzym-ml-mnsat-altwasl

(12) الروبوت (بالإنجليزية: Robot) عبارة عن آلة صممت من خلال نظام هندسي يجعلها تعمل كبديل للأيدي العاملة البشرية رغم مظهرها غير الشبيه بمظهر البشر، إلا أنها قادرة على أن تؤدي الوظيفة المطلوبة منها بالطريقة التي يؤديها البشر، وهو آلة ميكانيكية قادرة على القيام بأعمال مبرمجة

(13) خالد كاظم أبو دوح، دور وسائل التواصل الاجتماعي في نشر الإرهاب والتطرف، مجلة درع الوطن الإماراتية مجلة عسكرية واستراتيجية تصدر عن مديرية التوجيه المعنوي في القيادة العامة للقوات المسلحة الإماراتية بتاريخ 1 مارس 2022 ومتاح على الموقع الإلكتروني: https://www.nationshield.ae/index.php/home/index/en

- فإن هناك بعض الدول شهدت ارتفاعًا في عدد الشباب الذين انضموا إلى الفكر المتطرف والإرهاب عبر شبكات التواصل الاجتماعي خلال السنوات الأخيرة.

التطرف الفكري عبر المنصات الرقمية:

- مصطلح «التطرف الفكري الرقمي» يعبر عن المعتقدات والأفعال التي يتبناها أنصار أو مستخدمون للعنف، وذلك بهدف تعزيز أهداف إيديولوجية أو دينية أو سياسية ذات طابع تطرفي، وتشمل الجرائم المرتبطة بالإرهاب استخدام العنف لأغراض سياسية، مثل خطف الطائرات واستهداف السفن البحرية، واستخدام الأسلحة الكيميائية أو النووية ضد الدولة والمدنيين، واختطاف الأفراد، وغيرها من أشكال استهداف المدنيين. ويتميز الإرهاب بكونه ظاهرة ليست جديدة، ويظهر هذا الأمر في سياق الأفعال والتنظيمات الإرهابية في تخطيطاتها وعملياتها[14].
- ذكرت شبكة «سي إن إن» (CNN) الإخبارية الأميركية أن الأطقم الفنية في منصات التواصل الاجتماعي «فيسبوك» و«يوتيوب» و«تويتر» استغرقت وقتًا طويلًا لحذف مقاطع فيديو تظهر الهجوم الإرهابي الذي وقع في مسجدين بمدينة كرايست، والذي أسفر عن مقتل 51 شخصًا وإصابة العشرات كما وقع هجوم في 14 مايو 2022؛ حيث قتل مهاجم 10 أشخاص في سوبرماركت في بافالو، نيويورك، وأصاب ثلاثة آخرين؛ حيث بث الجاني، الذي يبلغ من العمر 18 عامًا، هجومه مباشرة على منصة البث «تويتش» ونشر رابطًا لبيان يوضح دوافعه للهجوم على تطبيق «مستندات جوجل» قبل وبعد إطلاق النار، وقد اكتشفت السلطات مذكرات الجاني على الإنترنت عبر منصة الألعاب «ديسكورد».
- وتم استخدام منصة تويتش مثلًا لبث هجوم كرايستشيرش في نيوزيلندا عام 2019[15]، وكذلك لبث هجوم بوفالو في تكساس في وقت لاحق من عام 2022، وكلا الهجومين الإرهابيين كان لهما مرجع أيديولوجي يميني متطرف، وعند تحميل «رفع» upload مقاطع الفيديو الخاصة بتلك الأحداث على الإنترنت يصعب حذفها؛ حيث يتابع آلاف الأشخاص مشاهدتها حول العالم، ما يؤدي إلى إلهام بعضهم لارتكاب أعمال إرهابية في المستقبل[16].

(14) عمار ياسر البابلي، الذكاء الاصطناعي في مواجهة الشائعات وجرائم تمويل الإرهاب في البيئة السيبرانية «التداعيات وسبل المواجهة»، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، القاهرة، 2023، ص 124.

(15) تقرير الأمم المتحدة بشأن إدانة الهجوم الإرهابي على مسجدين في نيوزيلندا، وقع في مسجدي النور ولينوود في مدينة كرايست تشيرتش في نيوزيلندا اليوم الخامس عشر من مارس 2019، مما أدى إلى مقتل 49 شخصا وإصابة الكثيرين بجراح (تاريخ الزيارة 2024/1/15) https://news.un.org/ar/story/2019/03/1028961

(16) ماري شروتر، الذكاء الاصطناعي ومكافحة التطرف العنيف: كتاب تمهيدي، (لندن، تقرير صادر من الشبكة العالمية للتطرف والتكنولوجيا GNET المملكة المتحدة، 2022) ص 23- 34.

- الذئاب المنفردة عبر البث المباشر وتهديد الإنسانية: حدثت الهجمات الإرهابية التي تبث لحظيًا في الولايات المتحدة وألمانيا ونيوزيلندا في السنوات الأخيرة على شبكة الإنترنت وتطبيقات التواصل الاجتماعي، مثل هجوم برينتون تارانت، الذي هاجم مسجدًا في كرايستشرش في 15 مارس 2019، ما أسفر عن مقتل 51 مسلمًا وإصابة 49 آخرين وقام ببث الحدث على الهواء مباشرةً، وأصبح بيانه «الاستبدال العظيم» نوعًا من الكتابة المقدسة في الحركة، لتستشهد به وتشير إليه سلسلة القتلة المقلدين التي تلت ذلك، وعلى الرغم من أن عددًا قليلًا شاهدوا البث المباشر، فسرعان ما أنتج الحدث ما لا يقل عن 722 ألفًا و295 تغريدة، والتي اشتملت على تعليقات منها المؤيد ومنها المعارض لما حدث، وسرعان ما دشن أصحاب الفيديو المقطع في الذاكرة السحابية[17].

خامسًا - تحديات الأجهزة الأمنية الدولية لشبكات (VPN) في تمويل الإرهاب والجريمة المنظمة:

- تعني VPN «شبكة خاصة افتراضية virtual private network»، وتقدم وصفًا لكيفية إنشاء اتصال شبكي محمي عند استخدام الشبكات العامة، وتقوم شبكات VPN بتشفير حركة البيانات الخاصة بك على الإنترنت وإخفاء الهوية الإلكترونية، مما يجعل تتبع الأنشطة عبر الإنترنت وسرقة بياناتك أمرًا في غاية الصعوبة بالنسبة للغير؛ حيث يتم التشفير في الوقت الفعلي.... وهي شبكة مجهولة الأطراف، وأنها متعددة الدول[18].
- تخفي شبكات VPN عنوان IP الخاص بالمستخدم من خلال السماح للشبكة بإعادة توجيهه عبر خادم مهيأ خصيصًا ويعمل عن بعد تحت إدارة مستضيف شبكة VPN، وهذا يعني أنه إذا قام المستخدم بالتصفح عبر الإنترنت باستخدام شبكة VPN، فإن خادم VPN يصبح مصدرًا للبيانات، وهذا يعني أن مزود خدمة الإنترنت (ISP) والأطراف الثالثة الأخرى لا يمكنهم معرفة مواقع الويب التي تزورها أو البيانات التي ترسلها وتستقبلها عبر الإنترنت، وتعمل شبكة VPN مثل عامل تصفية يحول جميع بياناتك إلى «بيانات مبهمة»، ولو نجح أي طرف في الوصول إلى هذه البيانات، فستكون بلا فائدة.

(17) المرجع نفسه، ص 23-34.

(18) خلدون غسان سعيد، أعماق «الإنترنت المظلم»، استئجار قتلة وخدمات غير سوية لقاء عملات رقمية مشفرة، جريدة الشرق الأوسط، جريدة العرب الدولية، رقم العدد [15351]، لندن، ديسمبر 2021، ص 15.

- بعض دول العالم تجيز استخدام خدمة VPN لحماية خصوصية شعبها، لكننا سنجد في الجانب الآخر أن هناك دولًا أخرى -مثل كوريا الشمالية- تجرم فعل التصفح باستخدام VPN، فهي تريد إحكام يد السيطرة على عملية مراقبة نشاطات مواطنيها عند تصفحهم للإنترنت من خلال إصدار قوانين تمنع استخدام VPN نهائيًّا لديها، بينما توجد دول أخرى تفرض رقابة على خدمات VPN دون منعها بشكل كامل كالصين[19].
- تزداد التحديات بصعود شبكة «6G» نقل وتداول البيانات والمعلومات بسرعة فائقة ومعدلات بيانات أعلى بكثير مقارنة بتقنية «5G»، ويمكن أن توفر معدلات ذروة للبيانات تقاس بوحدة تيرابايت في الثانية (Tbps)، ما يتيح البث عالي الجودة للغاية، وتجارب الواقع المعزز والافتراضي في الوقت الفعلي، ونقل البيانات بسرعة، كما أن شبكة «6G» تهدف إلى تقليل زمن الوصول إلى حدود الميكروثانية، ومن المرجح أن تستفيد من الترددات الأعلى، بما في ذلك طيف التيراهرتز (THz) [20].

المطلب الثاني
التحديات الإجرامية والافتراضية عبر المنصات الرقمية

يواجه مستخدمو مواقع التواصل الاجتماعي تحديات ومخاطر عديدة، من بينها التزييف الرقمي والشائعات التي يمكن أن تؤثر على صحة المعلومات، وتؤدي إلى تشكيك المستخدمين في الأخبار والمعلومات المنشورة، وبالرغم من أن وسائل التواصل الاجتماعي وسعت بدون شك فرص التفاعل الاجتماعي، فهي تستخدم أيضًا من الأفراد وجماعات الجريمة المنظمة عبر الوطنية للاتجار بالمخدرات، وجرى استخدام منصات وتطبيقات الشبكات الاجتماعية، مثل فيسبوك وإنستغرام وسناب تشات وغيرها، لتيسير الاتجار بالمخدرات بصورة غير مشروعة باستخدام الصور ومقاطع الفيديو، وكثيرًا ما يستخدم البائعون مجموعة متنوعة من الأيقونات التعبيرية (الإيموجي) وعلامات الهاشتاغ واللغة العامية للإعلان عن العقاقير المخدرة المتوفرة لديهم على وسائل التواصل الاجتماعي في الرسائل أو التغريدات أو بواسطة أسماء المستخدمين. ويمكن للأفراد البحث عن مجموعة متنوعة من المخدرات غير المشروعة والعثور على معلومات مفصلة عن أماكن وكيفية الوصول إليها بخلاف استغلال المنصات في غسل الأموال والاتجار بالبشر وسرقة الحسابات الإلكترونية والبنكية وإنتاج مواد اباحية للأطفال وتهريب المهاجرين للإرهاب والنصب والاحتيال عليهم.

(19) ماري شروتر، الذكاء الاصطناعي ومكافحة التطرف العنيف، مرجع سابق.

(20) نسيم رمضان . تقرير جريدة الشرق الأوسط الدولية: «إنتل» لـ«الشرق الأوسط»: التقنيات الجديدة تتطلب الجيل السادس من الإنترنت، لندن، 9 نوفمبر 2023 ومتاح على: https://aawsat.com/files/pdf/issue16419/

ومما سبق يمكن أن تستخدم طبقات الإنترنت والمنصات الرقمية ومنصات، ومنها مواقع التواصل الاجتماعي، في المخاطر الافتراضية والمستحدثة على النحو التالي:

أولًا– بيئة الإنترنت المظلمة وخطورتها على مختلف مستويات الأمن (The Dark Web):

إن الإنترنت العميق هو مجموع كافة المواقع الإلكترونية التي لم تدرج في محركات البحث، وبعض المواقع العميقة هي أسواق غير تقليدية تقدم مجموعة مقلقة من المنتجات أو الخدمات؛ حيث يمكنك شراء أو التوسط في شراء العقاقير غير المشروعة، والأسلحة، والسلع المقلدة، وبطاقات الائتمان المسروقة والبيانات المخترقة، أو العملات الرقمية، أو البرمجيات الضارة وبطاقات الهوية الوطنية او جوازات السفر. ويمكنك التعاقد مع الخدمات الرقمية أو الجنائية، بدءًا من حملات البريد المزعج (spam) إلى هجمات التعطيل المنتشر للخدمة (DDoS). ويمكن للمبتدئين حتى شراء الكتب الإلكترونية التي تشرح كيفية مهاجمة المواقع، وسرقة الهويات أو خلاف ذلك الربح من الأنشطة غير المشروعة، فإن 80٪ من حركة مرور الويب على الشبكة تتعلق باستغلال الأطفال في المواد الإباحية، وتشمل عمليات البيع والشراء على الإنترنت المظلم بيع بيانات بطاقة الائتمان المسروقة، والأبحاث الطبية بما في ذلك معلومات حول الأدوية والعلاجات الجديدة، والأسرار التجارية والسجلات المالية، و التقارير الاستخباراتية كما تشمل نشاطات الشبكة بيع الأسلحة والمخدرات والسلع المسروقة والآثار المنهوبة والسلع غير القانونية والحيوانات المهددة بالانقراض والعمل بالسخرة والمواد الإباحية للأطفال وبيع الأعضاء والاتجار بالبشر[21].

وما يحدث في عالم الإنترنت المظلم يشير إلى وجود أمور لا تقبل الجدل؛ حيث يمكن أن تكون هذه الشبكات الإرهابية غير قابلة للقبض عليها بسهولة، محصنة بشكل كامل من خلال شبكات وخبراء متخصصين، أو أن هناك جهات دولية تتجاهلها عمدًا، مما يؤدي إلى تشابك المصالح بين هذه الجهات والشبكات الإجرامية، ويعتبر الجانب المظلم من الإنترنت، المعروف أيضًا بـ «دارك ويب»، متصلاً بكل ما هو غير قانوني وضد الأخلاقيات. ففي هذا السياق، تأسس موقع «طريق الحرير» في 2011، وكان يختص في توفير ممنوعات مثل المخدرات والأسلحة حيث ألقي القبض على مؤسس موقع «سيلك رود» في 2013، والذي أغلق نهائيًا في 2015، لكن ظهرت بعد ذلك مواقع بديلة لتلبية الطلب على المواد غير القانونية.

(21) علي القحيص، تقرير جريدة الرياض الدولية، سوق رائجة للمخدرات والأعضاء البشرية والرقيق الأبيض، تاريخ الزيارة 13 نوفمبر 2023 ومتاح على: https://www.alriyadh.com/1569663

وكان موقع «طريق الحرير» يسمح بشراء المخدرات والأسلحة باستخدام العملة الرقمية «بيتكوين» مع ضمان السرية التامة حول هوية المتعاملين. يذكر أن مؤسس موقع « طريق الحرير» حكم عليه بالسجن مدى الحياة في نيويورك بتهم غسل الأموال والاتجار بالمخدرات وتشكيل عصابة إجرامية والقرصنة المعلوماتية.

ومن بين القضايا المروعة كانت قضية «شانون ماكول» في عام 2012؛ حيث ظهر موقع يستغل الأطفال على الشبكة السوداء وكان يطلب من الأعضاء المشاركة بمواد فاضحة للأطفال للحصول على إذن للدخول إلى الموقع وتمكنت جهود التحقيق المشتركة من عدة دول من كسر دائرة الصمت، واكتشاف هوية المتهم «شانون ماكول»، الذي حكم عليه بالسجن لمدة 35 عامًا بتهم استغلال الأطفال وتوزيع مواد فاضحة.[22]

ثانيًا– الاستغلال الجنسي للأطفال عبر طبقات الإنترنت:

استغلال الأطفال جنسيًا يتنوع في أشكاله وأنماطه بشكل واضح ويمكن تقسيم هذا الاستغلال وفقًا لما جاء في الاتفاقية الأوروبية لحماية الأطفال من الاستغلال والاعتداء الجنسي إلى عدة أصناف مختلفة وأحد هذه الأصناف هو الاعتداء الجنسي، والذي يشمل أي تصرف يتضمن ممارسة الجنس مع الأطفال، سواء كان ذلك مرتبطًا بالإكراه، أو التهديد، أو خرق الثقة، أو سوء استخدام السلطة، أو القدرة لاستمالة الطفل كما يمكن أن ينجم الاعتداء الجنسي عن حالات مرض عقلي أو جسدي للطفل[23].

بالإضافة إلى ذلك، يعتبر إنتاج واستخدام الصور والمقاطع الجنسية التي تظهر الأطفال أمرًا آخر يعد من أشكال الاعتداء الجنسي عليهم، ويتم ذلك بهدف تحقيق مكاسب جنسية أو مالية أو أية منافع أخرى. يمكن للجناة في هذا النوع من الجرائم أن يكونوا بالغين أو أطفالاً أنفسهم، وغالبًا ما يتم إنتاج مواد الاعتداء الجنسي على الأطفال عن طريق خداع الضحية للمشاركة في إنتاج تلك المواد الإباحية.

(22) كفاية أولير، تقرير عربية independent الدولية، ألمانيا تفكك «دارك ويب» أكبر سوق لاستغلال الأطفال في العالم، تاريخ الزيارة 17 مارس 2024 ومتاح على: https://www.independentarabia.com/

(23) حسام نبيل الشرنقاوي، التعاون الدولي في مكافحة استغلال الأطفال جنسيًا، مجلة الأمن والقانون، أكاديمية شرطة دبي، العدد الأول، يناير 2020، ص 201. ومتاح على: https://dubaipolice.ac.ae/dpacademy/ar/sada_acadmey/show_doc.jsp?doc_type=sum_file&book_id=137

وفي مجال دراسات حقوق الطفل والتحقيقات القانونية المتعلقة بالاستغلال الجنسي للأطفال، يعتبر استغلال الأطفال في المواد الإباحية ظاهرة معقدة ومتنوعة، كما يتضمن هذا الاستغلال توثيق الأطفال بواسطة الصور ومقاطع الفيديو والتسجيلات الصوتية، سواء بتمثيل وهمي أو بتجربة جنسية حقيقية، بهدف تحقيق الرغبات الجنسية للآخرين كما يشمل ذلك إنتاج وتوزيع وعرض واحتفاظ بالمواد الإباحية للأطفال، وكذلك تسهيل الوصول إليها[24].

ويرى الباحث أنه تتنوع المواد الإباحية في الصور بشكل كبير؛ حيث يمكن تقسيمها إلى عدة مستويات تتراوح بين الإرشادي والعراة والشبقية والتظاهر والإثارة الجنسية والجنس الصريح والنشاط الجنسي الصريح والاعتداء والاعتداء الجسيم والسادية أو البهيمية واستغلال الأطفال في عروض إباحية وإفساد الأطفال واستدراج الأطفال لأغراض جنسية.

وإن استخدام الأطفال في هذه المواد الإباحية يعد انتهاكًا صارخًا لحقوقهم ويعرضهم لخطر كبير ويجب على المجتمع الدولي والسلطات القانونية اتخاذ إجراءات حازمة لمكافحة هذه الظاهرة الشنيعة، بما في ذلك تشديد القوانين وتوعية الجمهور وتعزيز الرقابة على الإنترنت، وهذه الجهود المشتركة تسعى إلى حماية الأطفال وضمان نموهم وتطويرهم في بيئة آمنة وصحية؛ حيث يمكن للأطفال العيش والازدهار بحرية دون أي تهديد من هذه الظواهر الضارة.

وعلى سبيل المثال كان عدد الأطفال الفلبينيين الذين وقعوا ضحايا الاستغلال الجنسي 500 ألف طفل في عام 2022، وهو ما يوازي طفل لكل 100 طفل وجزء منها من خلال منصات الفيديو والبث المباشر لتحقيق مكاسب مالية وتجارية لدى المنظمات الإجرامية والأشخاص المريضة نفسيًا، وكشف تقرير نشره تحالف «WeProtect Global Alliance» عن ارتفاع بنسبة 87 في المائة في الحالات المتعلقة بالاعتداءات الجنسية المبلغ عنها عند الأطفال في عام 2023 مقارنة بعام 2019، وبلغ عدد الحالات أكثر من 32 مليون حالة عالميًا بحسب المركز الوطني للأطفال المفقودين والمستغلين[25].

(24) المرجع السابق.

(25) UK Safety Tech Sector: 2022 analysis (UK Government، 2023) 352Accessed from: https://www.gov.uk/government/publications/safer-technology-safer-users-the-uk-as-a-world-leader-in-safety-tech/uk-safety-tech-sector-2022-analysis 182023/08/

وقد كشف التقرير الذي يقدم نظرة معمقة وجوهرية حول التهديدات التي يواجهها الأطفال عبر الإنترنت في عام 2023 عن ارتفاع بنسبة 360 في المائة في الصور الجنسية التي يلتقطها الأطفال لأنفسهم ضمن الفئة العمرية من 7 إلى 10 سنوات بين عام 2020 وعام 2022، بحسب مؤسسة مراقبة الإنترنت، وأظهر التقرير أن المحادثات التي يجريها الأطفال على المنصات الاجتماعية للألعاب مع المعتدين يمكن أن تتحول إلى محادثات خطرة في غضون 19 ثانية فقط من محاولات الاستمالة، في حين يبلغ المعدل العام لوقت عملية الاستمالة 45 دقيقة فقط، وتساهم بيئات الألعاب الجماعية الإلكترونية عبر الإنترنت في تسهيل الاختلاط بين البالغين والأطفال، وتبادل الهدايا الافتراضية وأنظمة التصنيف العامة، في ارتفاع هذه المخاطر إلى حد كبير.

مراحل الاستغلال الجنسي للأطفال عبر طبقات الإنترنت والدارك ويب:

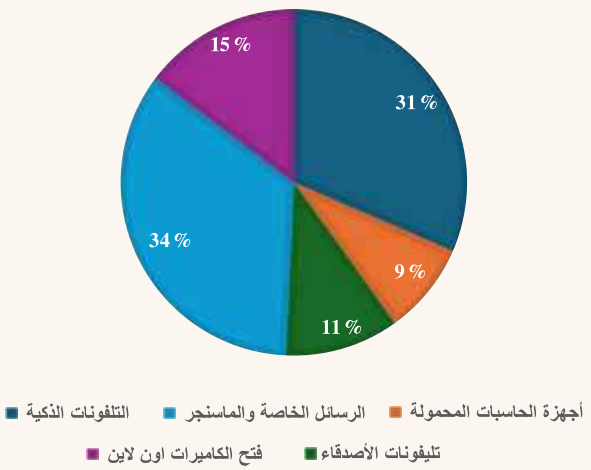
- **إنتاج المواد الإباحية:** في هذه المرحلة، يقوم الجناة بإنشاء صور إباحية، سواء عن طريق تحرير صور موجودة أو تسجيل محتوى إباحي جديد يظهر فيه الأطفال بشكل واضح ويستفيد الجناة من التطور التكنولوجي السريع؛ حيث يمكنهم إنتاج صور ومقاطع فيديو عالية الجودة باستخدام الكاميرات الرقمية وكاميرات الويب المتقدمة، كما يستخدمون الأماكن العامة ووسائل التواصل الاجتماعي لالتقاط الصور دون علم الأطفال.

- **توزيع المواد الإباحية للأطفال:** تتضمن هذه المرحلة نشر المحتوى الإباحي للأطفال على الإنترنت ويقوم الجناة بتحميل هذه المواد على خوادم المواقع أو استخدام مجموعات في وسائل التواصل الاجتماعي لطلب المحتوى الإباحي للأطفال وتشمل هذه العمليات تبادل المحتوى عبر الرسائل المباشرة أو الدردشة والمنتديات. تقوم السلطات بمراقبة الأنشطة عبر الإنترنت والمواقع المشبوهة، ولذا يستخدم الجناة تقنيات متقدمة للحفاظ على سرية هويتهم وتجنب الكشف عن هويتهم.

- **تنزيل وتحميل الصور الإباحية للأطفال:** تتعلق هذه المرحلة بالحصول على المواد الإباحية للأطفال عبر الإنترنت؛ حيث يمكن للجناة الوصول إلى هذه الصور دون الحاجة لتخزينها على الأجهزة الخاصة بهم ويتم ذلك عبر روابط بريد إلكتروني غير مرغوب فيها أو عن طريق الانتقال إلى مواقع إباحية عن طريق الخطأ ويحتاج الجناة إلى مهارات تقنية متقدمة للبحث عن هذه المواقع والوصول إليها، وقد يتطلب الأمر دفع رسوم أو استخدام كلمات مرور للوصول إلى المحتوى الإباحي للأطفال، وتظل هذه الأنشطة الإجرامية مستمرة وتتطلب تكامل الجهود بين الجهات القانونية ومقدمي خدمات الإنترنت للقضاء على هذه الجرائم وحماية الأطفال من التعرض لها.

صورة توضح الوصول إلى الاعتداء الجنسي على الأطفال وإمكانية المشاهدة والمشاركة[26]:

التعرض للتحرش والابتزاز الجنسي للأطفال من خلال [27]:



(26) تقرير WeProtect Global Alliance، تقييم التهديد العالمي، تقييم حجم الاستغلال والاعتداء الجنسي للأطفال 2023، مرجع سابق، ص27

(27) الأضرار الجنسية عبر الإنترنت، تقييم التهديدات العالمية، الاطلاع بتاريخ 2024/3/8:
/https://www.weprotect.org/economist-impact-global-survey

تقرير يكشف ارتفاع أخطار الاستغلال والاعتداء الجنسي على الأطفال عبر الإنترنت[28]

32 مليون	بلاغ عن مواد اعتداء جنسي للأطفال في عام 2023
360%	زيادة عدد الصور والمنشورات الإباحية لاستغلال الأطفال لأعمار 7-10 عامي 2021 – 2023
60%	من حالات الاعتداء كان فردًا معروفًا للطفل

من: مواد الاعتداء الجنسي على الأطفال الموجودة على شبكة الإنترنت المظلمة Darstellungen Sexuellen Kindesmissbrauchs Im Darknet

I also find it alarming that this appears to be a case where showing the child's face is what lead to the conviction, unless I'm misunderstanding the story or something got lost in translation. They say that it happened at the same time they decided the girl lived in [redacted], so I don't know if that means they narrowed it down to the city and then checked social media photos, or if they identified her photo and also identified her location independently.

I have repeatedly told people that it's OK to show the child's face because you NEVER year of that being the factor that gets people caught. Producer shows a face – they're done. Show something that gives away your location? Done. But never based on just the girl's face.

(28)https://arabic.cnn.com/science-and-health/article/062023/11//children-online-sexual-abuse-infographic
https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-AR.pdf

ثالثًا – بيع والاتجار بالمواد والعقاقير المخدرة والمصنعة من خلال المنصات الرقمية عبر طبقات الإنترنت:

تعد مشكلة المخدرات مشكلة عالمية وواحدة من أصعب المسائل التي يواجهها العالم، ولها آثار واسعة النطاق على صحة ورفاهية الأفراد والأسر والمجتمعات وعلى أمن الدول وتنميتها المستدامة، وإن معالجة التحديات المتعلقة بالمخدرات بكل تعقيداتها تعد أمرًا جوهريًّا لكل دول العالم.

وتزايد استخدام المنصات الإلكترونية في تسويق وبيع المخدرات الاصطناعية وتنوع على مر السنوات، مما وفر للمجرمين وسيلة فعالة للإعلان عن منتجاتهم والوصول إلى جمهورهم المستهدف. وليس ذلك فقط، بل ساعدت هذه المنصات في تمويه أعمالهم غير المشروعة بطرق متنوعة، بالإضافة إلى ذلك ساهمت هذه المنصات في تعزيز احترافية بيع المخدرات والعقاقير من خلال توفير وسائل للمعلنين لتقديم وصف مفصل للمنتجات، مع إرفاق صور ومعلومات حول توفرها وتتضمن هذه المنصات أسواق الشبكة الخفية، ووسائل التواصل الاجتماعي، وتطبيقات المراسلة، وخدمات الاتصالات، وأنظمة الدفع، كما ساعدت هذه المنصات أيضًا في بناء سمعة جيدة عبر الإنترنت بين الزبائن والمشترين، مما أدى إلى تعزيز تبادل المعلومات والتجارب بين أفراد الجمهور.

ووفقًا لتقارير منظمة الصحة العالمية، فإن تعاطي الكحول على نحو ضار هو ثالث أهم عوامل الخطر فيما يتعلق بالوفيات المبكرة وحالات الإعاقة في العالم ويؤدي كل عام إلى وفاة مليوني ونصف المليون شخص، منهم عدد كبير من الشباب يبلغ 320000 شاب وشابة تتراوح أعمارهم بين 15 و29 عامًا، كما أن تعاطي الكحول وحده يعد أحد أهم العوامل الرئيسة ذات العلاقة بتردي الوضع الصحي في العالم، وهناك مجموعة كبيرة من المشكلات ذات العلاقة بالكحول يمكن لها أن تحدث آثارًا مدمرة على الفرد وعلى الأسرة، ويمكن أيضًا أن يكون لها واقع فادح خطير على حياة المجتمع، وتعاطي الكحول على نحو ضار هو أحد عوامل الخطر الأربعة الأكثر شيوعًا، والتي يمكن تغييرها حتى يتم اتقاء شر الإصابة بالأمراض غير السارية الرئيسية [29].

(29) نقلًا عن عبد الحفيظ يحيى خوجة، تقرير دولي حول مشاكل الإدمان، مروجو المخدرات يستغلون وسائل التواصل الاجتماعي لنشرها بين الشباب، جريدة الشرق الأوسط "صحيفة العرب الاولي"، الرياض، 9 يوليو 2020 ومتاح على: https://aawsat.com/home/article/2380571/

وتتضح الزيادة الملحوظة في استخدام الأفراد وجماعات الجريمة المنظمة لشبكة الإنترنت كمنصة للتجارة بالمخدرات الاصطناعية، ويعتبر دور الإنترنت في تسهيل التجارة بالمخدرات موضوعًا للقلق نظرًا لإغلاق العديد من المواقع الظاهرة والمخفية، المعروفة أيضًا بالأسواق وتمتاز المخدرات الاصطناعية بأنها تباع عبر وسائل التواصل الاجتماعي والمواقع الإلكترونية على الإنترنت، سواءً كانت ظاهرة أو مخفية، مما يزيد من انتشار هذه الظاهرة ويؤثر على التجارة بالمخدرات بشكل عام.

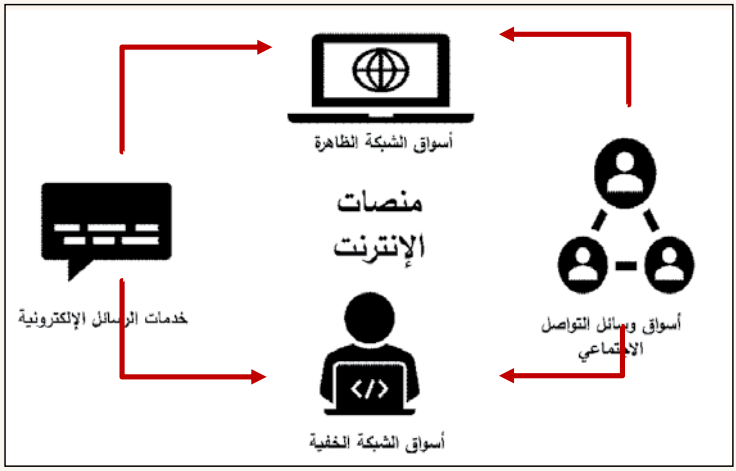
وبناءً على ما سبق نستطيع القول إن الأسباب الرئيسية لتفضيل التجارة بالمخدرات المصنعة Synthetic Drugs [30] عبر الإنترنت هي:

1. إخفاء الهوية بشكل أفضل: مثل التشفير والشبكات الخاصة الافتراضية وخوادم البروكسي البديلة، يمكن للجرائم تجنب الكشف القانوني بسهولة، مما يجعل من الصعب تتبع الجناة وتحديد هويتهم.
2. القدرة على التواصل عالميًا: يتيح الإنترنت للمجرمين الوصول إلى جمهور أوسع وتسويق المنتجات بفعالية بالإضافة إلى ذلك، فإنه يسهل التواصل دون الكشف عن الهوية بين البائع والمشتري، مما يزيد من التحايل على التحقيقات القانونية [31].
3. منصة لتبادل المعرفة والخبرات: يوفر الإنترنت كميات هائلة من المعلومات حول المخدرات، بما في ذلك إرشادات تصنيع المخدرات ووسائل الحصول على المكونات الكيميائية غير المشروعة وخدمات التوزيع والتحويل المالي وكيفية تجنب الاكتشاف من قبل الجهات القانونية.

ويرى الباحث أنه يزداد معدل الخطر بزيادة تلك الأنشطة الجرمية وتأثيرها السلبي على المجتمع، وتتطلب مكافحة هذه المشكلة تنسيق الجهود بين السلطات والقطاع الخاص وزيادة التوعية بمخاطر تعاطي المخدرات وترويجها عبر الإنترنت.

(30) التي تستخرج من المخدر الطبيعي، بعد أن تتعرض لبعض العمليات الكيماوية، التي تحولها إلى صورة أخرى غير صورتها الطبيعية، المخدرات المحظورة المثيرة للنشوة تمثل خطرًا جسيمًا ومتزايدًا على صحة وسلامة الأشخاص حول العالم نظائر الفنتانيل (الأفيونات الاصطناعية).

(31) مجموعة أدوات الأمم المتحدة بشأن مكافحة المخدرات الاصطناعية، تقرير بشأن منصات البيع عبر الإنترنت،، 9 نوفمبر 2023 ومتاح على: https://syntheticdrugs.unodc.org/syntheticdrugs/ar/cybercrime/onlinetrafficking/onlinesalesplatforms.html



4. يستخدم تجار المخدرات أنواعًا مختلفة من خدمات الرسائل الإلكترونية المزودة بتشفير من طرف إلى طرف للإعلان عن منتجاتهم وبيعها، وكذلك للتواصل مع المشترين الذين يطلعونهم على بيانات تحديد الموقع الجغرافي، وتستخدم خدمات الرسائل الإلكترونية أيضًا من قبل التجار السريين في العملات المشفرة لترتيب عمليات تبادل العملات المشفرة [32].

5. من خلال البنية الخفية على الإنترنت، التي تمثل جزءًا من البنية العالمية للشبكة، والتي لا يمكن الوصول إليها باستخدام المتصفحات القياسية مثل Internet Explorer أو Firefox أو Edge أو Chrome، يتم تشغيل شبكات مشفرة متخصصة لإتاحة إخفاء الهوية، بشكل مشابه للشبكة المرئية؛ حيث تستضيف الشبكة الخفية آلاف الصفحات الشبكية ولكن هذه الصفحات لا يمكن الوصول إليها إلا عند الاتصال بشبكة خفية، وتمثل المخدرات أوسع فئات المنتجات تداولًا على الشبكة الخفية، بما في ذلك ميثيلين ديوكسي ميثامفيتامين (MDMA)، والأمفيتامين، والميثامفيتامين، والقنب بجميع أشكاله، والكوكايين، والمؤثرات الأفيونية بجميع أشكالها، وثنائي إيثيلاميد حمض الليسرجيك (LSD)، والفطر المهلوس، والكيتامين، والعقاقير المبيعة بوصفة طبية (معظمها بنزوديازيبينات) [33].

(32) What Is the Dark Web and Should You Access It? 474(Investopedia، 2022) Accessed from: https://www.investopedia.com/terms/d/dark-web.asp 212023/08/

(33) Election Security Spotlight – The Surface Web، Dark Web، and 475 Deep Web (Center for Internet Security، n.d.) Accessed from: https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-the-surface-web-dark-web-and-deep-web 212023/08/.

6. تمكنت الإنتربول في 2022 في أكبر عملية ضبط لها؛ من خلال تحليل وفحص المنصات الرقمية وتتبع الشبكات الخفية، من الكشف عن حجم هائل لتهريب المخدرات في مدينة ليون بفرنسا. وتم ضبط كميات كبيرة من المخدرات غير المشروعة والسلائف الكيميائية، بلغت قيمتها 717 مليون دولار أمريكي. وتم اعتقال 1,333 شخصًا يشتبه في ضلوعهم في هذه العمليات على مستوى العالم.[34]

7. تمت عملية «ليون فيش V" في الفترة من 23 يونيو إلى 31 يوليو؛ حيث استهدفت الاتجار بالمخدرات غير المشروعة عبر الطرق الجوية والبرية والبحرية في 22 بلدًا حول العالم، واعتمدت نهجًا منسقًا عبر الحدود. وتم ضبط أكثر من 291 طنًا من السلائف الكيميائية و35.5 طنًا من المخدرات خلال هذه العملية، بينما تظل المخدرات الشائعة مثل الكوكايين والقنب تشكل نسبة كبيرة من سوق المخدرات غير المشروعة، وتعزز هذه العملية الانتباه إلى زيادة إنتاج وتداول المخدرات الاصطناعية مثل الميثامفيتامين والكبتاغون والكيتامين[35].

8. ألقت الشرطة الأوروبية القبض على حوالي 150 فردًا حول العالم كانوا يشترون أو يبيعون مخدرات وأسلحة عبر الإنترنت المظلمة، المعروفة أيضًا باسم «دارك ويب»، وتعتبر هذه العملية واحدة من أضخم العمليات التي تستهدف هذا الجانب الخفي من الإنترنت، وفقًا لإعلان من مسؤولين في شرطة الاتحاد الأوروبي «يوروبول» ووزارة الخارجية الأميركية، وأكدت يوروبول أن العملية «دارك هانتور» (DarkHunter) تمت عبر سلسلة من الخطوات المنفصلة، وشملت عدة دول، من بينها أستراليا، وبلغاريا، وفرنسا، وألمانيا، وإيطاليا، وهولندا، وسويسرا، وبريطانيا، والولايات المتحدة[36].

9. تأتي هذه العملية بعد تفكيك منصة «دارك ماركت» (DarkMarket) في يناير بقيادة الشرطة الألمانية، والتي وصفت حينها بأنها «أوسع نقطة شراء في السوق السوداء

(34) الإنتربول، عملية مكافحة لتهريب المخدرات تتيح ضبط كميات غير مسبوقة منها وتوقيف 1333 شخص.
https://www.interpol.int/ar/1/1/2022/1333 (تاريخ الزيارة 2024/3/1)

(35) تقرير منظمة الإنتربول، عملية مكافحة لتهريب المخدرات تتيح ضبط كميات غير مسبوقة منها وتوقيف 1333 شخصًا، وتقدر قيمة المخدرات المضبوطة بنحو ثلاثة أرباع مليار دولار أمريكي في 2022 - ومتاح على الموقع الرسمي للإنتربول:
https://www.interpol.int/ar/1/1/2022/1333

(36) لاهاي (أ ف ب) عملية واسعة ضد الإنترنت المظلم والشرطة الأوروبية توقف 150 شخصًا – قناة فرنسا 24 نشرت في 2021/10/26 - ومتاح على: https://www.france24.com/en/live-news/20211026-police-arrest-150-in-joint-us-europe-dark-web-sweep

الإلكترونية» وتم تنفيذ العملية في عدة دول؛ حيث أدت إلى توقيف حوالي 65 شخصًا في الولايات المتحدة، و47 شخصًا في ألمانيا، و24 شخصًا في بريطانيا، و4 أشخاص في إيطاليا، و4 أشخاص في هولندا، إضافة إلى آخرين. [37]

10. سجلت يوروبول أيضًا مصادرة تقدر بملايين اليورو نقدًا وباستخدام البيتكوين، بالإضافة إلى مخدرات وأسلحة. وفي إيطاليا، تم إغلاق سوقين غير قانونيتين تسميان «ديب سي» (DeepSea) و«برولوسكوني» (Berlusconi)؛ حيث كانتا تعرضان أكثر من مئة ألف إعلان لمنتجات غير قانونية.

11. تعد عملية تفكيك «دارك ماركت» في يناير، حين اعتقل المشغل الرئيسي للمنصة، الذي يشتبه في توفيره للمحققين معلومات قيمة، خطوة مهمة في مواجهة الجرائم عبر الإنترنت. ويشير محللون إلى أن هذه العملية تمثل تحولًا في استراتيجية الشرطة في مواجهة الجرائم الإلكترونية.

وفي تقرير صادر عن الأمم المتحدة في ديسمبر 2023، تم استعراض عدة نقاط مهمة:

- استخدام الإنترنت ووسائل التواصل الاجتماعي على نطاق عالمي: يمتلك ثلثا سكان العالم (66%) وصولًا إلى الإنترنت، ويستخدم أكثر من نصفهم (59%) وسائل التواصل الاجتماعي [38].
- العملات المشفرة في المعاملات غير القانونية: كانت نسبة 0.24% من جميع معاملات العملات المشفرة في عام 2022 مرتبطة بأنشطة غير قانونية، وخاصة تلك المتعلقة بأسواق الويب المظلمة التي تشمل أنشطة المخدرات وتمثل 0.02% من مجموع المعاملات.
- اتجاهات في مبيعات المخدرات عبر الويب المظلم: شهدنا زيادة كبيرة في نسبة المستهلكين الذين يشترون المخدرات عبر الويب المظلم، ولكن تراجعت المبيعات في عام 2022 بعد سنوات من النمو وإيرادات أسواق الويب المظلم: وصلت الإيرادات المجمعة لأسواق الويب المظلم إلى مستويات قياسية في عام 2021، لكنها انخفضت بشكل كبير في عام 2022 [39].

(37) الشرطة الأوروبية توقف 150 شخصًا في عملية دولية ضد الإنترنت المظلم، أكتوبر 2021 ومتاح على: https://www.alghad.tv/

(38) Robin van der Sanden et al.، "'Choice' of Social Media Platform or Encrypted Messaging App to Buy and Sell Illegal Drugs،"International Journal of Drug Policy 108 (October 2022): 103819

(39) نقلًا عن د. عبد الحفيظ يحيى خوجة، تقرير دولي حول مشاكل الإدمان، مروجو المخدرات يستغلون وسائل التواصل الاجتماعي لنشرها بين الشباب، جريدة الشرق الأوسط "صحيفة العرب الأولى"، الرياض، 9 يوليو 2020 ومتاح على: https://aawsat.com/home/article/2380571/

- استخدام وسائل التواصل الاجتماعي لشراء المخدرات: أظهرت الدراسات أن نسبة كبيرة من عمليات شراء المخدرات عبر الإنترنت تتم عبر منصات وسائل التواصل الاجتماعي وتوزيع الجنس بين المشترين للمخدرات عبر الإنترنت، ويتمثل غالبية المشترين للمخدرات عبر الإنترنت في الذكور، ويفضلون استخدام أسواق الويب المظلم بشكل أكبر من وسائل التواصل الاجتماعي.
- وهناك علاقة لترابط بين الويب المظلم ووسائل التواصل الاجتماعي: هناك دلائل تشير إلى أن بعض البائعين يحصلون على المخدرات من الويب المظلم ويعيدون بيعها عبر منصات وسائل التواصل الاجتماعي، مما يبرز الارتباط الوثيق بين هذين المجالين في مجال المبيعات المخدرات.

رابعًا- استغلال المنظمات الإجرامية للإنترنت بغرض الاحتيال الإلكتروني كأحد أساليب الاتجار بالبشر:

1. رصدت الأجهزة الأمنية – ومنها الإنتربول- بعناية شديدة تصاعد الجرائم من هذا النوع؛ حيث يشهد الاتجار بالبشر على نطاق واسع استهداف الضحايا من خلال إعلانات عمل كاذبة، تقودهم إلى مراكز احتيال إلكتروني؛ حيث يتم ضغطهم لارتكاب جرائم مالية عبر الإنترنت بشكل واسع وهذا الاتجاه، الذي شهد انتشارًا واسعًا للاتجار بعشرات الآلاف في جنوب شرق آسيا واحتياًلا يفوق ذلك بكثير على مستوى العالم، جذب انتباه وسائل الإعلام وحث الحكومات والمجتمع المدني على التصدي له[40].

2. ومع ذلك، يحذر الإنتربول من التفاقم السريع لهذا الاتجاه الإجرامي الذي اتخذ بعدًا عالميًا جديدًا، مشيرًا إلى أنه من المرجح أن يكون أوسع انتشارًا مما كان يعتقد وقد أصدرت المنظمة تحذيرًا عالميًا للدول حول هذا التهديد الخطير والوشيك للسلامة العامة.

3. كانت مراكز الاحتيال الإلكتروني في البداية متركزة في كمبوديا، ولاحقًا تم اكتشاف مراكز أخرى للاتجار في لاوس وميانمار وفي الوقت الحالي، تم تحديد وجودها في على الأقل أربع دول آسيوية إضافية، مع دلائل على تكرار أسلوب العمل هذا في مناطق أخرى تشهد بالفعل جرائم مالية عبر الإنترنت، كما في غرب أفريقيا، وشهد التنوع الجغرافي لفئات الضحايا زيادة حادة أيضًا؛ حيث تم تجارة الأفراد الناطقين بالصينية الأصليين من الصين أو ماليزيا أو تايلاند إلى المنطقة، وأيضًا من مناطق بعيدة مثل جنوب أمريكا وشرق أفريقيا وغرب أوروبا.

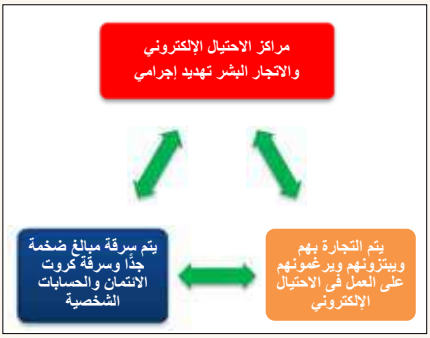
4. يوضح تقرير الأمم المتحدة الصادر في أغسطس 2023: أن معظم الأفراد الذين اتجروا بهم في عمليات الاحتيال عبر الإنترنت هم من الرجال، ورغم ذلك يكون النساء والمراهقين ضمن فئة الضحايا أيضًا وأن هؤلاء الضحايا الذكور ليسوا غالبًا من

(40) رامي متولى القاضي، مكافحة الإجرام المنظم عبر شبكة الإنترنت المظلمة: دراسة تحليلية في التشريع المصري، المجلة الجنائية القومية، المركز القومي للبحوث الجنائية والاجتماعية، القاهرة، نوفمبر 2022، المجلد 64، العدد 3، ص47.

مواطني الدول التي تشهد عمليات الاتجار، وأن الكثير من الضحايا يتمتعون بمستوى تعليميٍّ عالٍ ومستوى ثقافي مرتفع؛ حيث يأتون بعضهم من خلفيات وظيفية وتعليمية متقدمة، بمًا في ذلك حملة شهادات جامعية وما بعد الدراسات العليا، ويتقنون استخدام الحاسبات الآلية وتشمل الضحايا مناطق متنوعة، بدءًا من دول رابطة أمم جنوب شرق آسيا مثل إندونيسيا وجمهورية لاو الديمقراطية الشعبية وماليزيا وميانمار والفلبين وسنغافورة وتايلاند وفيتنام، وصولًا إلى البر الرئيسي للصين وهونغ كونغ وتايوان، وكذلك من أفريقيا وأميركا اللاتينية [41].

5. وقال الأمين العام للإنتربول يورغن شتوك: «ما بدأ كتهديد إجرامي إقليمي أصبح الآن أزمة اتجار بالبشر على الصعيد العالمي، أي شخص في العالم قد يكون ضحية للاتجار بالبشر أو لعمليات الاحتيال الإلكتروني التي تنفذ عبر هذه المراكز الإجرامية، والتعاون الشرطي الدولي أمر حاسم لمنع انتشار هذا الاتجاه الإجرامي على نطاق واسع» [42].

ويري الباحث أن خطورة مراكز الاحتيال الإلكتروني تتمثل في تشكيل تهديد جريمي؛ حيث تستهدف من الضحايا وفي سياق اتجار البشر ويتم إكراه ضحايا الاتجار على العمل القسري من خلال استخدام أساليب استرقاق بالدين، إضافةً إلى سوء المعاملة الجسدية والاستغلال الجنسي والتعذيب، بل قد يصل الأمر في بعض الحالات إلى نزع الأعضاء، ومن جهة أخرى يتم استخدام العمال المتاجر بهم في تنفيذ مجموعة متنوعة من عمليات الاحتيال الإلكتروني التي تستهدف طبقة أخرى من الضحايا المنتشرين بشكل متزايد في جميع أنحاء العالم، وتشمل هذه العمليات الاحتيال في ميدان الاستثمار، والاحتيال الرومانسي، والاحتيال المرتبط بالاستثمار في العملات المشفرة، بالإضافة إلى الأنشطة الإلكترونية للمقامرة.



(41) تقرير منظمة الأمم المتحدة بشأن الاتجار بمئات الآلاف من الأشخاص وإشراكهم في عمليات احتيال عبر الإنترنت بجنوب شرق آسيا، أغسطس 2023 ومتاح على الموقع الرسمي للإنتربول بالإنترنت
hundreds-thousands-trafficked-work-online-scammers-/08/https://www.ohchr.org/ar/press-releases/2023
se-asia-says-un-report

(42) دراسة أمنية للإنتربول، الاتجار بالبشر للعمل في مراكز احتيال إلكتروني قد تحول من اتجاه إجرامي إقليمي إلى تهديد عالمي، بتاريخ 7 يونيو 2023 ومتاح على الموقع الرسمي للإنتربول بالإنترنت: https://www.interpol.int/
20/2023/1/ar/1

خامسًا- نشر الكراهية والتحريض على العنف والتزييف الرقمي عبر منصات التواصل الاجتماعي:

هي ظاهرة ومشكلة معقدة ومزمنة تواجه المجتمعات اليوم، وتستخدم هذه الجماعات منصات التواصل الاجتماعي لنشر أفكارها وأيديولوجياتها المتطرفة، وتستهدف الشباب الذين يشعرون بالضياع والتهميش وعدم الانتماء؛ من خلال الآتي:

1. **صناعة الصورة:** تؤدي صناعة الصورة دورًا مهمًّا في تجنيد الشباب للجماعات الإرهابية ونشر رسائلها المتطرفة، وتستخدم هذه الجماعات وسائل متنوعة لجذب الأفراد وإقناعهم من خلال ما يلي:

- استخدام الفيديوهات والصور: تنتج الجماعات الإرهابية مواد إعلامية مثيرة وجذابة تظهر المقاتلين وهم يتدربون ويشاركون في المعارك، مما يجعل الجهاد يبدو مغامرة مثيرة وجذابة للشباب [43].
- استخدام نماذج زعماء الإرهاب وتنظيم القاعدة وداعش كنماذج: تحتفي الجماعات الإرهابية بزعماء الإرهاب وتقدمهم كنماذج للتقليد مشجعة الشباب على التضحية بأنفسهم من أجل القضية.
- استخدام الألعاب والمحتوى التفاعلي: تستغل الجماعات الإرهابية شعبية الألعاب الإلكترونية والمحتوى التفاعلي لنشر رسائلها وجذب الشباب.

2. **عمليات الاستقطاب:**

- استخدام شبكات التواصل الاجتماعي في التجنيد، سواء عن طريق وسطاء، أو عن طريق إرسال الشخص بنفسه رسائل إلى حسابات خاصة بالجماعات الإرهابية عبر حسابات الفيسبوك وتويتر وتليجرام وتطور الاتصال؛ من خلال منصات الدارك ويب dark web أخطر طبقات الإنترنت لصعوبة تتبع الأجهزة الأمنية تلك المنصات، أو يتم التواصل مع الشخص إلكترونيًّا عبر قريب أو صديق من داخل تلك الجماعات [44].

(43) تقرير الإنتربول عن الإرهاب الصادر في نوفمبر 2023:
https://www.interpol.int/ar/1/2023/1/Illegal-wildlife-trade-has-become-one-of-the-world-s-largest-criminal-activities

(44) خالد كاظم أبو دوح، دور وسائل التواصل الاجتماعي في نشر الإرهاب، مرجع سابق، ص 79.

3. **تكوين خلية التجنيد والتغذية الفكرية للتطرف:**

- تستخدم الجماعات الإرهابية خلايا التجنيد لتجنيد المستهدفين الشباب الجدد وتعميق الأفكار المتطرفة والتكفيرية في عقولهم، وتتمثل مهمة خلايا التجنيد في استخدام الخطاب الديني والأيديولوجي والأساليب النفسية لجذب الشباب المستهدف وتحريضهم على الانضمام إلى التنظيم.
- استخدام شفرة معينة خلال حديثهم، ويتم تركيب عبارات بطريقة معينة لاختبار المجندين من الشباب الجدد في التنظيمات، وتتضمن معرفة حالته النفسية، ثم التركيز على مسائل مثل التوحيد والحاكمية والولاء وأهمية الحكم بالقرآن والسنة، والتأكيد أن الجهاد هو الحل، ثم يتم زرع الأفكار التكفيرية والمتطرفة في عقل المستهدف، ودفعه إلى الاستماع إلى الخطب الحزينة والأناشيد الحماسية وتطبيق ما يمكن أن نسميه «التنويم المغناطيسي»، وذلك باعتماد فكرة أن الإسلام الموجود في المجتمع هو إسلام بعيد عن الإسلام الحقيقي [45].

4. **المرحلة التنفيذية:** يمكن تمييز هذه المرحلة بالنمط التقليدي لتشكيل الفكر المتطرف والانجذاب نحو الاتجاهات الطردية، ويظهر أن منصات ومواقع التواصل الاجتماعي قد تؤدي دورًا مهمًّا في تسهيل تلك العملية. وتتضمن الخطوات التالية مراحل الانضمام الفعلي إلى الجماعات الإرهابية المتطرفة:

- تزويد الفكر المتطرف عبر وسائل التواصل الاجتماعي: يستغل المتطرفون والجماعات الإرهابية منصات ومواقع التواصل الاجتماعي لنشر الأفكار المتطرفة، ويتم تداول المحتوى المتطرف مثل الفتاوى والمقالات والفيديوهات، مع تسليط الضوء على التفسيرات الأكثر تشددًا للنصوص.
- تعزيز الإيمان والقناعة: يمكن أن تسهم منصات التواصل الاجتماعي في تعزيز الأفكار المتطرفة عندما يقابل الأفراد الذين يشاركون في نفس الأفكار، وذلك من خلال التفاعل والتعليقات والمشاركات المشابهة، وهذا يمكن أن يؤدي إلى تعزيز الانتماء والاقتناع بالفكر المتطرف.
- الانخراط الفعلي والتواصل المباشر: يمكن للمنصات الاجتماعية أن تسهل التواصل المباشر بين المتطرفين المحتملين وأعضاء الجماعات الإرهابية، ويمكن تبادل المعلومات والدعوات للانضمام تحت شعارات مثل الهداية والالتزام وطلب الجنة.

(45) شريفة كلاعة، ظاهرة تجنيد الشباب في الجماعات الإرهابية من خلال استخدام شبكات التواصل الاجتماعي، مجلة مدارات سياسية، مجلة دولية محكمة نصف سنوية، العدد السادس، المجلد 2، الجزائر 2018، ص14.

5. **نشر الأنشطة العملياتية ودعوة الانضمام**: تمكن وسائل التواصل الاجتماعي الجماعات الإرهابية من نشر أنشطتها العملياتية وتشجيع الأفراد على المشاركة فيها، ويتم تبادل الخطط والتفاصيل وتشجيع الأفراد على الانخراط في الأدوار العملياتية، وهذا الأمر يمثل جزءًا من ديناميات التهديد الإرهابي عبر المنصات الإلكترونية من خلال[46]:

- تجنيد الشباب وغسيل الأدمغة: يعد تجنيد الشباب وتأثير الجماعات الإرهابية عليهم من خلال منصات التواصل الاجتماعي والدارك ويب (الإنترنت المظلم) جزءًا أساسيًا من ديناميات التهديد الإرهابي للدول، ويستغل الإرهابيون هذه المنصات للترويج للأيديولوجيات المتطرفة وجمع المعلومات وتوجيه الشباب نحو الأنشطة الإرهابية، بالإضافة إلى ذلك تستخدم الجماعات الإرهابية المنصات الإلكترونية لنشر أنشطتها ومحاولة تحقيق التأثير النفسي على الجمهور، ومن ضمن هذه الجوانب ما يلي:
- ترويج الأيديولوجيات المتطرفة: يستخدم التواصل الاجتماعي والإنترنت المظلم لنشر وتعزيز الأيديولوجيات المتطرفة وتبرير الأعمال العنيفة.
- جمع المعلومات والتجسس: تستخدم الجماعات الإرهابية المنصات الإلكترونية لجمع معلومات استخباراتية والتجسس على أهدافها المحتملة.
- توجيه الأفراد نحو العمل الإرهابي: يتم استغلال وسائل التواصل لتوجيه الشباب نحو تنفيذ أعمال إرهابية من خلال توفير التعليمات والتوجيهات.
- تكوين شبكات: يمكن للجماعات الإرهابية استخدام المنصات الإلكترونية لتكوين شبكات جديدة وتواصل أعضائها ومناصريها.

6. **التحريض والتأثير النفسي**: يستخدم التواصل الإلكتروني لتحريض الأفراد على تنفيذ هجمات ولزيادة الخوف والذعر بين الجمهور لذلك، منصات التواصل الاجتماعي تشكل مساحة مهمة لنشر الأنشطة الإرهابية وتأثير الجماعات الإرهابية على الشباب، مما يستدعي التعامل الجاد مع هذه التهديدات على مستوى السياسات والأمن الإلكتروني [47].

(46) حسنين توفيق إبراهيم، في تفسير استمرارية التنظيمات الجهادية الإرهابية: "داعش" نموذجًا، ترندز للبحوث والاستشارات، أبو ظبي، الإمارات، 2023، ص 11.

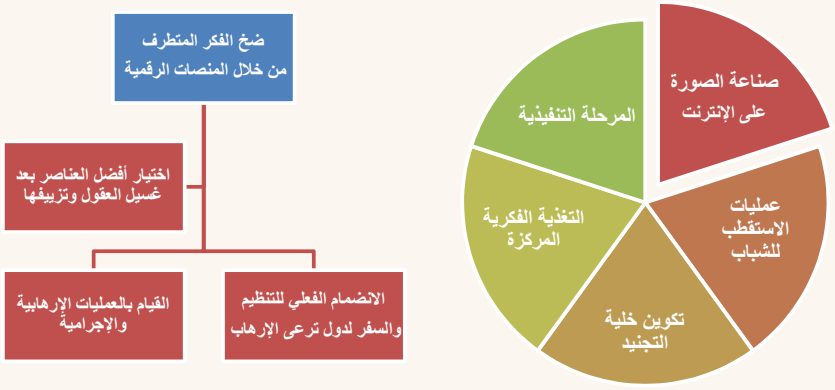
(47) محمد إبراهيم داود، سياسات ردع التهديدات غير التقليدية للأذرع الإرهابية، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، 2023، ص 111.

7. **الوصول إلى المعلومات:** توفر منصات التواصل الاجتماعي والدارك ويب dark web بيئة مناسبة للإرهابيين للوصول إلى المعلومات المطلوبة، ويمكنهم الحصول على معلومات عن الأساليب الإرهابية وصناعة المتفجرات والهجمات المحتملة وغيرها من التفاصيل الحساسة [48].

8. **تأثير الثقة والترويج للتطرف:** يسعى الإرهابيون إلى إقامة علاقة ثقة مع الشباب وإقناعهم بأفكارهم المتطرفة، ويستخدمون التلاعب النفسي والمناورات العاطفية لجذب الشباب وتجنيدهم في صفوفهم، كما يتم ترويج الأفكار المتطرفة من خلال منشورات ومقاطع فيديو محفزة تستقطب الشباب المستهدفين.

9. **جمع المعلومات والاستهداف:** تستخدم الجماعات الإرهابية منصات التواصل الاجتماعي والدارك ويب «الإنترنت المظلم» لجمع المعلومات حول الشرطة والقوات المسلحة والأهداف السياسية، وتستخدم هذه المعلومات للتخطيط وتنفيذ الهجمات الإرهابية والاغتيال [49].

يوضح الشكل: استغلال المنصات الرقمية وتطبيقات التواصل الاجتماعي في تجنيد الأفراد لدى الجماعات والتنظيمات الإرهابية



(48) المنهج المرجعي لمكافحة الإرهاب، تقرير حلف الناتو لمكافحة الإرهاب، إصدار 2020، ص 33، ومتاح على:
pdf/2012-DEEP-CTRC-arabic.PDF/12/https://www.nato.int/nato_static_fl2014/assets/pdf/2020

(49) Marie-Helen Maras and Alex Alexandrou. (2019). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. International Journal of Evidence & Proof، 23(3): 255–262.

سادسًا – تصاعد خدمات التهريب الافتراضية عبر المنصات الرقمية وتطبيقات التواصل الاجتماعي:

1. شهدت خدمات التهريب الرقمي عبر المنصات الرقمية زيادة ملحوظة، وفقًا لتحليلات المفوضية الأوروبية، وسجل ازدياد كبير في عدد المهاجرين غير الشرعيين الوافدين إلى دول الاتحاد الأوروبي خلال عام 2023؛ حيث بلغ إجمالي هؤلاء المهاجرين من دول خارج الاتحاد حوالي 1.08 مليون شخص، وهو ارتفاع بنسبة 59% مقارنة بالعام السابق 2022 وفي نفس الفترة، تم تنفيذ أكثر من 422 ألف أمر ترحيل، مسجلة زيادة نسبية بنسبة 23% عن عام 2021.

2. تؤدي وسائل الاتصال الرقمية، وعلى وجه الخصوص وسائل التواصل الاجتماعي، دورًا كبيرًا في تسهيل وتنظيم هذه الأنشطة غير المشروعة. وتؤكد خطة الاتحاد الأوروبي لمكافحة تهريب المهاجرين للفترة من 2021 إلى 2025، التي اعتمدتها المفوضية الأوروبية في سبتمبر 2021، أن الجانب الرقمي يشكل تحديًا جديدًا يواجه السلطات القانونية والقضائية [50].

3. يستخدم المهربون بشكل متزايد الخدمات والأدوات الرقمية لتنظيم أنشطتهم، من خلال توظيف وسائل التواصل الاجتماعي وتطبيقات الهواتف المحمولة في التجنيد والتواصل وتحويل الأموال، بالإضافة إلى تنظيم عمليات تسليم المهاجرين وتوجيههم.

4. يقومون أيضًا بتقديم إرشادات للطرق والمسارات، ويشاركون محتوىً مرئيًّا مثل الصور ومقاطع الفيديو للوثائق وتذاكر السفر، مما يضعهم تحت مراقبة نشاطات إنفاذ القانون. ولا سيما في سياق التطورات الأخيرة، وقد شهدت وسائل التواصل الاجتماعي تغييرًا جذريًّا في الأساليب المستخدمة في تسهيل تهريب المهاجرين؛ حيث قدمت أدوات غير مسبوقة لتوجيه وتنسيق الأنشطة المهربة. هذا السيناريو تم توثيقه من خلال دراسة نشرتها منظمة الهجرة الدولية في بداية عام 2023، وأظهرت الدراسة استخدام المهربين للشبكات الاجتماعية وتطبيقات الرسائل الفورية للترويج لخدماتهم غير المشروعة؛ من خلال نشر مقاطع فيديو توثق عمليات العبور الناجحة. وقد تم أيضًا استغلال هذه الوسائل للتفاعل وتبادل المعلومات وتسهيل عمليات الرحلة والتخطيط لها. وتجاوزت مدى الدراسة الحدود الجغرافية؛ حيث تضمنت عينة من 531 مهاجرًا عابرًا من منطقة مكسيك وأمريكا الوسطى وجمهورية الدومينيكان [51].

(50) فاطمة الزهراء عبد الفتاح، تقرير التهريب الرقمي: كيف تسهل وسائل التواصل الاجتماعي الهجرة غير الشرعية، مركز المستقبل للأبحاث والدراسات المستقبلية، أبو ظبي، 22 أغسطس 2023، ومتاح على https://futureuae.com/en-US/Home/Index/2/%D8%A7%D9%84%D8%B1%D8%A6%D9%8A%D8%B3%D9%8A%D8%A9

(51) شروع الاتحاد الأوروبي HTSM، تقرير مكافحة الاتجار بالبشر وتهريب المهاجرين في الاتحاد الأوروبي، 2023، ومتاح على: https://www.interpol.int/ar/4/10/HTSM

5. زيادة أعداد المهاجرين غير الشرعيين إلى دول الاتحاد الأوروبي تفتح أبوابًا للتحديات المرتبطة بالوسائط الرقمية ووسائل التواصل الاجتماعي، مما يتسبب في زيادة خطر العمليات الإرهابية في المنطقة، ويمكن تلخيص العلاقة بين التهريب غير الشرعي للمهاجرين والإرهاب على النحو التالي:

- انتقال المقاتلين الأجانب وتمويل الارهاب: ييسر تدفق المهاجرين غير الشرعيين انتقال المقاتلين الأجانب الذين ينضمون إلى جماعات إرهابية، مما يزيد من التهديد الإرهابي في الدول المستقبلة، ويمكن أن يوفر ازدياد أعداد المهاجرين غير الشرعيين مصادر تمويل إضافية للجماعات الإرهابية؛ حيث يستخدم المهربون والجماعات الإرهابية نفس الشبكات لتحويل الأموال أو تمويل عملياتهم [52].
- استخدام وسائل التواصل للتجنيد والترويج للإرهاب: يستخدم وسائل التواصل الاجتماعي لتجنيد المهاجرين وترويج الأيديولوجيات الإرهابية؛ حيث يستغل الإرهابيون هذه الوسائل لجذب المزيد من الأفراد إلى صفوفهم.
- التشبيك والتواصل بين الجماعات الإرهابية: ييسر استخدام وسائل التواصل الاجتماعي التشبيك والتواصل بين مختلف الجماعات الإرهابية، مما يعزز انتشار الأفكار والتكتيكات الإرهابية.

يوضح الجدول التالي استغلال وسائل التواصل في تنظيم الهجرة [53]:

2019	**كشفت السلطات الإيطالية عن شبكات تهريب تستخدم وسائل التواصل الاجتماعي، وخاصةً فيسبوك، لتنظيم وتسهيل عمليات الهجرة غير الشرعية، وتم اكتشاف صفحات تروج لخدمات التهريب وتقديم إرشادات حول كيفية تجنب الرصد والقبض.**
2020	**اكتشفت الشرطة الفرنسية شبكة تهريب تستخدم تطبيقات المراسلة مثل WhatsApp وTelegram لتنظيم وتنسيق وتوجيه المهاجرين عبر الحدود، وكانت هذه الشبكة تستفيد من التشفير للتحايل على إجراءات مراقبة الاتصالات.**
2022-2021	**رصدت السلطات الأمريكية حملة عبر وسائل التواصل الاجتماعي تروج لعمليات الهجرة غير الشرعية إلى الولايات المتحدة، وتم استخدام منصات مثل TikTok وFacebook لمشاركة محتوى يوجه الأفراد إلى طرق تجنب إجراءات الرصد والتوجه إلى الحدود.**

(52) محمد إبراهيم داود، سياسات ردع التهديدات غير التقليدية للأذرع الإرهابية، مرجع سابق.

(53) Annual Report 2022 (INHOPE، 2023) Accessed from: https://inhope.org/media/pages/articles/annual-reports/14832daa351687272590-/inhope-annual-report-2022.pdf 032024/3/17 (تاريخ الزيارة 2023/07/)

المبحث الثاني
تطبيقات الذكاء الاصطناعي في رصد ومكافحة الظواهر الإجرامية في المجتمع الافتراضي

التمهيد

تؤدي تكنولوجيا الذكاء الاصطناعي دورًا حيويًّا في جهود مكافحة التطرف والإرهاب عبر المنصات الإلكترونية، فمن خلال الذكاء الاصطناعي يمكن القيام بتحليلات ضخمة وقدرة حسابية هائلة، مما يمكنه من معالجة كميات هائلة من البيانات وتحليلها بسرعة ودقة، وباستخدام تطبيقات الذكاء الاصطناعي يمكن رصد الأنشطة المشبوهة والمحتملة؛ مثل غسل الأموال ومنصات الاتجار بالبشر الخفية وتسويق المخدرات المصنعة وتهريب المهاجرين، وكذلك مكافحة هجمات الإنترنت المتنقلة؛ مثل التصيد الإلكتروني وسرقة بيانات البطاقات الائتمانية لصالح المنظمات الإجرامية والتطرف عبر المنصات الإلكترونية ووسائل التواصل الاجتماعي والمنتديات والمواقع الإلكترونية و يعتمد هذا النهج على تقنيات التعلم الآلي وتحليل اللغة الطبيعية لفحص المحتوى المنشور وتحديد الأنماط والسلوكيات المشبوهة للرصد والمواجهة وبهذا، يصبح تطوير استراتيجيات الذكاء الاصطناعي في مكافحة الإرهاب في المجتمع الافتراضي أمرًا بالغ الأهمية لتعزيز جهود الكشف والوقاية من الأنشطة الإرهابية والإجرامية عبر الإنترنت.

لا شك أن التقنيات الرقمية الحديثة، مثل الذكاء الاصطناعي(AI) Artificial Intelligence تمثل أفقًا جديدًا غير محدود، وبالنظر إلى تقنيات الذكاء الاصطناعي يتبين أن حكومات الكثير من الدول خصصت استثمارات ضخمة، ووضعت أجندات سياسية شاملة لدعم تطوير هذه التقنيات واستخدامها؛ ففي الصين – على سبيل المثال- أعلنت الحكومة خطة تطوير الجيل الجديد من الذكاء الاصطناعي، في شتى المجالات والقطاعات الحكومية الخدمية والأمنية، ويتوقع أن تنفق 150 مليار دولار لتعزيز ريادة الصين للعالم في مجال الذكاء الاصطناعي[54].

إنَّ تعبير مصطلح الذكاء الاصطناعي (AI) يشير إلى قدرة الأجهزة والحواسيب الرقمية على تنفيذ مهام محددة تشبه تلك التي يقوم بها الكائنات الحية الذكية؛ مثل القدرة على التفكير والتخطيط، والتعلم والإبداع، والتكيف والتفاعل، وتحسين العمليات، واستخلاص المعرفة، والتنبؤ باستناد إلى البيانات الرقمية الكبيرة والمتنوعة، ومجموعة متنوعة من العمليات الأخرى التي تتطلب عمليات ذهنية دقيقة [55].

(54) انظر في ذلك؛ تقرير المعهد الأمني الصيني: (Future of Life Institute. AI Policy China)، من خلال الموقع الإلكتروني التالي: https://futureoflife.org/ai-policy-china1 2023/6/

(55) The Bold Impact of Technology and Artificial Intelligence in Law Enforcement: https://www.boldbusiness.com/digital/the-bold-impact-of-artificial-intelligence-in-law-enforcement/

ويرى خبراء في مجال مكافحة الإرهاب أن هناك منهجين لمنع الهجمات الإرهابية؛ الأول يتعلق بحماية البنية التحتية والأفراد وتنفيذ الإجراءات الأمنية، والثاني يتمثل في تقييد القدرة على تنفيذ الهجمات الإرهابية، وذلك من خلال القبض على المشتبه بهم ومنعهم من التخطيط والتنفيذ.

وسوف نستعرض تطبيقات الذكاء الاصطناعي وإنفاذ القانون في رصد ومكافحة الظواهر الإجرامية في المجتمع الافتراضي كالتالي

المطلب الأول: تكنولوجيا الذكاء الاصطناعي في مكافحة الإرهاب والعنف الرقمي المستحدث

المطلب الثاني: قدرة الشبكات العصبية الاصطناعية على مواجهة الجرائم

المطلب الأول
تكنولوجيا الذكاء الاصطناعي في مكافحة الإرهاب والعنف الرقمي المستحدث

يعد الذكاء الاصطناعي أحد أهم مخرجات الثورة الصناعية الرابعة والتي قامت على تطور تكنولوجيا الحاسب الآلي والإنترنت، فقد أدى ظهور هذا العلم لفتح آفاق جديدة للإنسان في المجالات الاقتصادية والطبية والتعليمية **والأمنية** والخدمية والعسكرية، نظرًا لاعتماده على الربط والدمج بين العلوم الفيزيائية والبيولوجية والرقمية، فالتطور الملحوظ في علوم الحاسب الآلي أدى إلى إعادة تشكيل العلاقات بين الأفراد؛ حيث سهلت هذه التكنولوجيا على الإنسان حياته، وأنتجت العديد من التطبيقات التي تساعد على اتخاذ القرارات دون تفكير، الأمر الذي دعا إلى ضرورة دراسة هذا العلم، ومحاولة تسخير تطبيقاته في المجال الأمني[56].

أولًا- الذكاء الاصطناعي من منظور أمني واستخباراتي:

الذكاء الاصطناعي – من منظور أمني واستخباراتي- هو تطبيق تقنيات حاسوبية تمكن من محاكاة القدرات العقلية البشرية، مثل الفهم، والتعلم، والتفكير الاستدلالي، واتخاذ القرارات. يشكل الذكاء الاصطناعي أداة ذكية يمكن من تحليل البيانات وتعلم الأنماط باستخدام الخوارزميات، ومن الناحية الأمنية والاستخباراتية يعتبر الذكاء الاصطناعي فعالاً

(56) المنهج المرجعي لمكافحة الإرهاب، تقرير حلف الناتو لمكافحة الإرهاب، مرجع سابق.

في تحليل البيانات الضخمة والكشف عن التهديدات الأمنية والأنشطة غير المشروعة عبر الشبكة يستخدم أيضًا لمراقبة سلوك المستخدمين والكشف عن أي تغيير غير عادي يشير إلى تهديد أمني. بالإضافة إلى ذلك، يمكن الذكاء الاصطناعي من تقنيات التحقق من الهوية، مثل التعرف على الوجوه وبصمات الأصابع[57].

ويتيح الذكاء الاصطناعي: مراقبة وتحليل وسائل التواصل الاجتماعي للكشف عن أنشطة ذات صلة بالأمان والاستخبارات يستخدم في فهم وتحليل اللغة الطبيعية في النصوص واستخراج المعلومات الاستخبارية. كما يستفاد منه في التنبؤ بالتهديدات المستقبلية وتطورات الأمان ويعتبر استخدام الذكاء الاصطناعي في مكافحة الإرهاب فرصة لتحقيق تحسينات كبيرة في العمليات الأمنية والمراقبة. وهذا الاستخدام يمكن أن يؤدي إلى عدة فوائد[58]:

- **تحسين التنبؤ والاستباق**: يمكن للذكاء الاصطناعي تحليل البيانات والمعلومات بشكل أكثر دقة وفعالية، مما يتيح التنبؤ بأنماط السلوك المشبوه والتحذير من تهديدات إرهابية محتملة. وهذا يمكن أن يقلل من الحاجة إلى إجراءات أمنية مكثفة وغير ضرورية.
- **تقليل الاحتمالات الكاذبة**: باستخدام تحليل البيانات والتعلم الآلي، يمكن للذكاء الاصطناعي التمييز بين النماذج الحقيقية للتهديدات والأنماط العادية للسلوك. وهذا يساعد في تقليل الاعتقادات الخاطئة والإجراءات غير المبررة.
- **تقوم نظم الذكاء الاصطناعي** بتحليل كافة المعلومات المتوافرة من الأقمار الصناعية، وكاميرات المراقبة، ومواقع التواصل الاجتماعي، ومواقع الإنترنت، وتطبيقات جمع المعلومات الشخصية والحسابات البنكية، وأجهزة الاستشعار Sensors الخاصة بجمع المعلومات المنتشرة في الشوارع والسيارات الذكية، فضلًا عن المعلومات المتوافرة في الصحف والدوريات، والقنوات التلفزيونية، ومحطات الراديو، والكتب، والمجلات [59].

(57) طه محمد أحمد يوسف: «مستقبل الإدارة في عالم الذكاء الاصطناعي – إعادة تعريف الغرض والاستراتيجية في الثورة الصناعية الرابعة»، دار حميثرا للنشر، الطبعة الأولى، القاهرة، 2022، ص24.

(58) سعاد أغانيم، «خوارزميات الذكاء الاصطناعي والعمل القضائي قراءة في محاولات التجربة المغربية»، مجلة القانون والأعمال، ع 20، الرباط، المغرب، 2018، ص 174.

(59) Zak Doffman، U.S. Military Satellites Likely Cyber Attacked By China Or Russia Or Both: Report، forbes، Jul 5، 2019، accessed 28 08، 2023 on https://www.forbes.com/sites/zakdoffman/201905/07//u-s-military-satellites-likely-cyber-attacked-by-china-or-russia-or-both-report/#28bd31e9dd32

وهناك تطبيقات أساسية لاستخدام الذكاء الاصطناعي في محاربة الإرهاب والتطرف وهي:

ويرتبط استخدام الذكاء الاصطناعي بثلاثة مجالات يتم فيها ضمان أمن الفرد والمجتمع والدولة؛ «الرقمية، والمادية، والأمنية»[60]:

1. **المجال الرقمي**: يتم استخدام الذكاء الاصطناعي لتحسين فعالية مواجهة الهجمات الإلكترونية، بما في ذلك تلك التي تتطلب موارد كبيرة «التصيد المستهدف»، كما يمكن استخدام الذكاء الاصطناعي للبحث عن نقاط الضعف البشرية «تركيب وتحليل الكلام»، والبرمجيات «القرصنة التلقائية».

2. **المجال المادي**: يرجع استخدام الذكاء الاصطناعي إلى شن هجمات بطائرات بدون طيار وأنظمة فيزيائية أخرى مثل الطائرة الصغيرة ذات التحكم الآلي المعقد «سرب».

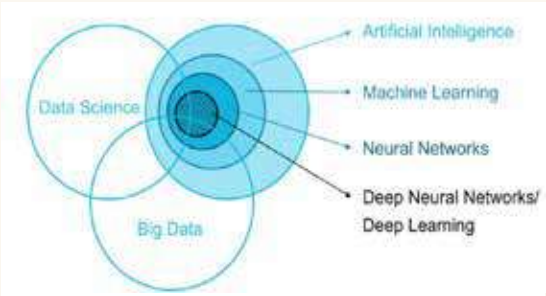
3. **المجال الأمني**: يمكن استخدام الذكاء الاصطناعي لحل مشاكل المراقبة «تحليل العمليات الأمنية»، والإقناع «الدعاية الرقمية»، ومواجهة المعلومات المضللة أو الخداع «إنشاء صوت رقمي، أو فيديو مزيف».

ثانيًا - الارتباط بين الذكاء الاصطناعي والبيانات الضخمة وعلاقتها بالدلائل الأمنية:

كان العالم غارقًا بالفعل فيما لديه من أحجام ضخمة من البيانات التي لا يدرك جدواها ثم حينما ظهر مصطلح البيانات الضخمة، انتبه الجميع إلى أن ما لديهم من البيانات المخزنة يمثل ثروة ضخمة، يمكن - إذا تم تحليلها بشكل صحيح- الاستفادة منها في إيضاح رؤى جديدة واتخاذ قرارات أكثر رشدًا للصناعة التي تنتمي إليها هذه البيانات، وسرعان ما أدرك أخصائيو المعلومات أن مهمة تحليل هذا الكم الضخم من البيانات لا يقدر عليها العقل البشري، وهو ما أوجد الحاجة إلى تطوير خوارزميات الذكاء الاصطناعي لإنجاز تلك المهمة.

(60) انظر في ذلك: Brundage، M.، Avin، S.، Clark، J.، Toner، H.، Eckersley، P.، Garfinke B.، & Amodei، D.The Malicious Use of Artificial Intelligence: Forecasting، Prevention، and Mitigation. Retrieved from. 2018.p56. http://ecai.raai.org/lib/exe/fetch.php?media=malicioususeofai.pdf

ولذا، فإنَّ قدرة الذكاء الاصطناعي على العمل بشكل يواكب متطلبات تحليل البيانات الضخمة هي السبب الرئيس الذي يجعل الذكاء الاصطناعي والبيانات الضخمة لا ينفصلان في كثير من التطبيقات، فالبيانات الضخمة هي شريان حياة الذكاء الاصطناعي، فهو يحتاج إلى التعلم منها ليتمكن من أداء وظيفته؛ أي لكي يكون أكثر ذكاءً، وعلى الجانب الآخر فإن البيانات الضخمة تزداد فائدتها إذا تم استخدامها في خوارزميات الذكاء الاصطناعي، ويبين الشكل التالي العلاقة بين الذكاء الاصطناعي بفروعه المختلفة والبيانات الضخمة.



ونظرًا لأن مصطلح «البيانات الضخمة» يشير إلى البيانات ذات الأحجام الكبيرة والتعقيد العالي، التي تصعب معالجتها وتحليلها باستخدام الأساليب التقليدية مثل نظم قواعد البيانات والتطبيقات الإحصائية، يصبح ضروريًا الاعتماد على برمجيات متقدمة قادرة على التعامل مع هذه التحديات.

يتيح تكامل أنظمة الذكاء الاصطناعي في معالجة هذه الكميات الهائلة من البيانات تحقيق فوائد كبيرة؛ حيث يتم تطوير أجهزة حاسبة ذكية عملاقة تستخدم خوارزميات متقدمة لسرعة تحديد البيانات المهمة وتحسين دقة الاستنتاج، وهذه البرمجيات تتعرف على أنماط السفر واللغة، وتحللها، وتربطها بالأفراد والأماكن والأحداث.

وتعد هذه الأجهزة والبرامج جزءًا حيويًا من نظم تقييم المخاطر، وقوائم المراقبة في المطارات ونقاط المراقبة الحدودية. وتتيح قدرة الذكاء الاصطناعي على تحليل وتفسير البيانات الضخمة رصد السلوكيات المشبوهة والتهديدات الأمنية، مما يسهم في تعزيز الأمان وتقديم إجراءات وقائية فعالة في مواجهة التحديات المعقدة للبيانات الكبيرة([61]).

وإنَّ الخوارزميات تقوم بتمييز الأشياء والأشخاص والمشاعر الإنسانية المعقدة والمعلومات والظروف بشكل يومي؛ حيث تقوم خوارزميات البرمجيات وأجهزة الحاسب الآلي، على سبيل المثال، بالتعلم الذاتي على مجموعات البيانات لفهم كيفية تحديد الأشخاص استنادًا إلى صورهم([62]).

(61) علي بن ذيب الأكلبي: «البيانات الضخمة واتخاذ القرار»، مشروع مستودع البيانات والجودة الإلكترونية «إتقان»، جامعة الملك سعود، الرياض، 2019، ص244-246.

(62) كريم محمد محروس: «تطبيقات شبكات الإنترنت في تقديم الخدمات الشرطية ودورها في الارتقاء بالأداء الأمني»، رسالة دكتوراه مقدمة لكلية الدراسات العليا بأكاديمية الشرطة، 2021، ص70.

كما أن البيانات الضخمة لديها القدرة على تعزيز دمج المعلومات وتنظيمها، مع ربطها بمصادر عدة: «مواقع التواصل الاجتماعي/ إنترنت الأشياء»، وتشكل البيانات المرتبطة بمصادر خارجية عاملاً فعالاً في المجال الأمني؛ إذ تعتبر البيانات الركيزة الأساسية للتحليل الأمني والذكاء الأمني، ولنمو فرص إنتاج المعارف الفعالة؛ حيث ترتبط البيانات الضخمة بمجموعة من الآليات التكنولوجية الجديدة المتعلقة بجمع البيانات، ونقلها، وتخزينها، وتنظيمها[63]. ولذا فإنَّ قدرة الذكاء الاصطناعي على العمل بشكل يواكب متطلبات تحليل البيانات الضخمة هي السبب الرئيس الذي يجعل الذكاء الاصطناعي والبيانات الضخمة لا ينفصلان في كثير من التطبيقات، فالبيانات الضخمة هي شريان حياة الذكاء الاصطناعي، فهو يحتاج إلى التعلم منها ليتمكن من أداء وظيفته؛ أي لكي يكون أكثر ذكاءً [64].

ثالثًا - التحولات الناجمة عن توظيف الذكاء الاصطناعي في مجال مكافحة الإرهاب:

إنَّ استخدام الذكاء الاصطناعي في مجال مكافحة الإرهاب استطاع أن يحقق بعض المميزات التي شكلت نقاط قوة واضحة استطاعت أن تحد من بعض الجرائم الإرهابية، وذلك من خلال إيجاد الفرص التالية أو بمعنى أدق النجاحات التي حققتها تلك الاستراتيجيات لمكافحة الإرهاب العنيف

- أسهمت عملية التحليل الآلي في تقليل انتهاك الخصوصية للمواطنين مقارنةً بالتحليل البشري، وكذا مكنت الشركات التكنولوجية العملاقة بالتعاون مع الأجهزة الأمنية من استخدام مقاييس ذكية؛ مثل: الاستدعاء والدقة، أو عدد الإنذارات الكاذبة باستخدام نماذج تنبؤية بالعمليات الإرهابية[65].
- قدم الذكاء الاصطناعي فرصًا جديدةً لتحليل البيانات الضخمة والتنبؤ بالمستقبل، ومن أهم الأدوات القائمة على الذكاء الاصطناعي محركات البحث وأنظمة التحليل والمعالجة اللغوية الطبيعية التي تمكن شركات التكنولوجيا والأجهزة الأمنية من فهم والتعرف على لغة الإرهاب والمتطرفين وترجمة الكتاب المشبوه، التي توفر إمكانية إدارة المحتوى عبر الإنترنت، خاصة فيما يتعلق باللغات التي تتواصل بها مجموعات من الأشخاص[66].

(63) مجدي الداغر: «دور الإعلام الجديد في تشكيل معارف واتجاهات الشباب الجامعي نحو ظاهرة الإرهاب على شبكة الإنترنت: دراسة ميدانية»، مجلة الآداب والعلوم الاجتماعية، الكويت، العدد 36، 2016، ص88، 89.

(64) انظر في ذلك: Reinsel، David، John Gantz، and John Rydning. 2018. The Digitization of the World- From Edge to Core. IDC، November. Retreved from https://www. Seagate. Com/files/www-content/our-story/trends/files/idc-seagate-dataage-white-paper. pdf. (تاريخ الزيارة 2024/2/20)

(65) سامح محمد الشريف، تحليل البيانات الضخمة في تحليل مواقع التواصل الاجتماعي، مجلة رؤى استراتيجية، مجلة علمية محكمة، المجلد السابع، العدد (19)، يونيو 2020، ص11-18.

(66) علي بن إبراهيم العلوي، تطبيقات الذكاء الاصطناعي في علوم الأدلة الجنائية، المجموعة العلمية لعلوم الأدلة الجنائية، رخصة النشر الإلكتروني من وزارة الإعلام رقم: ٤٧٩٥٩٤.

- هناك منصات أخرى تدعم ما يعد تطرفًا بدعوى إتاحة حرية التعبير، بزعم أنها لا تريد تقييد المستخدمين، وهنا فقد أتاحت المعالجة اللغوية الطبيعية NLP المحسنة ترجمة المحتوى إلى لغات يجيدها المشرفون، ويمكنها اكتشاف أنماط دلالية غير عادية على المواقع الإلكترونية أيضًا بهدف التعرف على النشاط المتطرف والإرهاب ومروجيه ونوعية النشاط المتطرف عبر منصات التواصل الاجتماعي[67].
- تستخدم خوارزميات الذكاء الاصطناعي داخل برامج وكالة الأمن القومي الأمريكية (SKYNET) لتحليل البيانات الوصفية من 55 مليون مستخدم محلي للهاتف المحمول الباكستاني في عام 2007، وكانت النتيجة أنه تم تعريف نسبة خطأ 0.008% فقط من الحالات على أنهم إرهابيون محتملون؛ أي أن هناك نحو 15 ألف فرد من إجمالي سكان باكستان البالغ 200 مليون، ومن الممكن أن يكونوا إرهابيين محتملين، ليوضح القيمة التنبؤية للبيانات عند تحديد روابط وثيقة مع الإرهاب والتعرف على الارهابيين[68].

رابعًا - الاستدلال والكشف عن دلالات الإرهاب:

- يمكن استخدام الذكاء الاصطناعي والخوارزميات للتنبؤ بالإرهاب ولمكافحة الأعمال العدائية بطرق متعددة، وتحليل البيانات وتحديد الأنماط الشائعة في الأنشطة الإرهابية، وتحديد الأشخاص المشبوهين وتحليل تحركاتهم وأنشطتهم وتحديد المواقع الجغرافية المتوقعة للهجوم الإرهابي، وتقييم الخطر المحتمل للتهديدات الإرهابية وتحديد الارتباط القائم بين الارهابيين، واتخاذ إجراءات وقائية للحد من التهديدات
- تقنيات التعلم الآلي: مثل التصنيف والتجميع والتنبؤ لتحليل المعلومات الخاصة بالإرهاب وتحديد النماذج المحتملة للأنشطة الإرهابية.
- التحليل النصي: مثل النصوص المتعلقة بالإرهاب، وتحديد الكلمات والعبارات والأنماط المستخدمة في الاتصالات الإرهابية.
- تحليل السلوك: للمشتبه به والأنشطة الإرهابية المحتملة، وتحديد بيانات تساعد كيفية التعرف على المشتبه بهم ومنع الهجمات الإرهابية.
- توجد العديد من الأمثلة الواقعية للذكاء الاصطناعي والخوارزميات لمكافحة الإرهاب وتنبؤ العمليات الإرهابية، ومن هذه الأمثلة:

(67) Tigran Hovsepyan. How Machine Learning Algorithms Are Used in The Justice System ،https://plat.ai/blog/machine-learning-algorithms-used-in-justice-system/ ، at December 9، 2022

(68) Eling، M.; Wirfs، J. What are the actual costs of cyber risk events? Eur. J. Oper. Res. 2019، 272، 1109–1119. www.scopus.com (تاريخ الزيارة 2024/1/1)

1. تحليل المعلومات الخاصة بالأفراد وتحديد الأشخاص المشبوهين وتحليل تحركاتهم وأنشطتهم، كسجلات الهاتف والبريد وتطبيقات الشبكات الاجتماعية وتطوير نظام تحليل الصوت والتحدث الذي يمكن استخدامه لإيضاح الأمور الإرهابية من اتصالات الهاتف والمحادثات الصوتية والبيانات.

2. في عام 2019، استخدمت الشرطة الفرنسية الخوارزميات لتحليل بيانات تطبيقات التواصل والإنترنت للكشف عن المشتبه بهم في هجوم ستراسبورغ الإرهابي.

3. في عام 2020، استخدمت شركة «سيسكو» الخوارزميات لتحليل بيانات حركة المرور والتنقل في دبي، وقدمت توقعات بشأن المناطق التي يمكن أن تشهد هجمات إرهابية محتملة[69].

خامسًا: تكنولوجيا الذكاء الاصطناعي والخوارزميات واستخدام البيانات البيومترية في مكافحة الإرهاب:

استخدام البيانات البيومترية في مكافحة الإرهاب من خلال تطبيقات الذكاء الاصطناعي يمثل تقدمًا مهمًا في مجال أمن المجتمعات وتعتمد هذه الاستراتيجية على البيانات الفريدة للأفراد؛ مثل البصمات الوراثية، وهياكل الوجوه، ونمط الصوت، لتحقيق تحقق دقيق من هويات الأشخاص[70]، وتعتمد التقنيات البيومترية على مميزات جسمية وسلوكية صعبة التزييف، مما يزيد من موثوقيتها في تحديد الهويات، من خلال استخدام الذكاء الاصطناعي، يمكن تحسين عمليات التحليل والمعالجة للبيانات البيومترية بطرق أكثر فعالية ودقة. يمكن للتقنيات الذكاء الاصطناعي تمييز أنماط معقدة واستخدام نماذج تعلم الآلة لتحديد سلوكيات غير عادية قد تكون مؤشرًا على نشاطات إرهابية[71].

(69) John Villasenor، "Artificial intelligence، geopolitics، and information integrity"، in: Fabio Rugge، ed.، The Global Race for Technological Superiority: Discover the Security Implications، (Milano: ISPI and Brookings، November 2023)، PP. 131142-.

(70) Shenoy، P.، Arora، A.، & Singh، M. (2018). Brain fingerprinting: Emerging trends in forensic science. Egyptian Journal of Forensic Sciences، 8(1)، 22.

(71) إيمان رجب، سياسات مكافحة الإرهاب في مصر، مركز الدراسات السياسية والإستراتيجية، العدد 296، القاهرة، يناير 2019، ص 36.

وتستخدم هذه التقنيات في مجموعة متنوعة من المجالات، بما في ذلك مراقبة الحدود والمطارات والأماكن العامة؛ حيث يمكن استخدامها لتحسين عمليات الكشف عن الأفراد المشبوهين والممنوعين من السفر، والجدير بالذكر أن استخدام البيانات البيومترية يثير قضايا حول الخصوصية والحقوق الشخصية. ويجب ضمان حماية البيانات الشخصية وتطبيق سياسات صارمة للوصول إلى هذه البيانات واستخدامها[72]:

- **مراقبة الحدود والمطارات**: يمكن استخدام أنظمة AI والتحليل البيومتري لتحسين عمليات مراقبة الحدود والمطارات، ويمكن تطبيق تقنيات التعرف على الوجوه ومقارنة الصور مع قواعد بيانات لاعتراض المشتبه بهم، كما يمكن استخدام تقنيات التحليل السلوكي لاكتشاف أنماط غير طبيعية في تصرفات المسافرين[73].
- **معالجة الصور وتحليل الوجوه**: يمكن للذكاء الاصطناعي تحليل الصور والوجوه بدقة عالية لاستخراج السمات البيومترية المختلفة. ذلك يتضمن تحديد معالم الوجه وبصمات الأصابع والتعرف على السمات المميزة[74].
- **تعزيز قدرة التعرف وتحسين دقة التحقق**: الخوارزميات والشبكات العصبية يمكن أن تدعم التعرف على الوجوه والسمات البيومترية بشكل أسرع وأكثر دقة. ويساعد تعلم الآلة في تحسين أداء النظم مع مرور الوقت، كما تساهم الخوارزميات في تحسين دقة التحقق من الهويات المبنية على البيانات البيومترية، ويؤدي تحسين أداء هذه الخوارزميات إلى تقديم نتائج دقيقة وموثوقة.
- **تحليل البيانات الضخمة**: تحليل الكميات الهائلة من البيانات البيومترية يمكن أن يتم عبر خوارزميات تحليل البيانات الكبيرة والتعلم العميق، مما يساهم في اكتشاف الأنماط والتوجهات المشبوهة.
- **اكتشاف الأنماط غير العادية**: يمكن استخدام الخوارزميات لاكتشاف أنماط غير عادية في البيانات البيومترية، مثل الاختلافات في الوجوه أو بصمات الأصابع وذلك يمكن أن يساهم في التحذير من المحاولات المشبوهة.

(72) مكتب الأمم المتحدة المعني بالمخدرات والجريمة، التعاون الدولي في المسائل الجنائية المتعلقة بمكافحة الإرهاب سنة 2021.

(73) Elling، M.; Wirfs، J. What are the actual costs of cyber risk events? Eur. J. Oper. Res. 2019، 272، 1109–1119.www.scopus.com

(74) Judges now using Artificial Intelligence to Rule on Prisoners، Science & Technology. February 07، 2018، https://learningenglish.

- **مكافحة التزييف والتحريف**: تقنيات البيانات البيومترية صعبة التزييف بشكل كبير، مما يجعلها وسيلة فعالة للحد من التزوير والتحريف في الوثائق والهويات.
- **تحليل السلوك والكشف عن أنماط مشبوهة**: يمكن استخدام البيانات البيومترية لتحليل السلوك واكتشاف أنماط سلوكية غير عادية تشير إلى نشاطات مشبوهة أو إرهابية.

ويمثل منع تمجيد العنف والإرهاب، وانتشار المعلومات المضللة، وغيرها من صور المحتوى المتطرف عبر الإنترنت تحديات تواجهها الجهات الفاعلة السياسية ومنصات التكنولوجيا في جميع أنحاء العالم، وقد أصبح استخدام خوارزميات التعلم الآلي لتتبع المحتوى الإرهابي وكشفه واسع الانتشار، ويعزى ذلك إلى أنه سيكون من المستحيل تقريبًا على السلطات القضائية اكتشاف جميع بصمات الإرهابيين الرقمية يدويًا، وتبذل الحكومات كيفية استخدام خوارزميات التعلم الآلي لكشف اللغة المتطرفة، لأغراض الحفاظ على الأمن القومي للدول.

سادسًا- التنبؤ بالأنشطة الإرهابية المستقبلية باستخدام الشبكات العصبية العميقة عبر المنصات الإلكترونية:

- **مراقبة الاتصالات الرقمية**: يمكن للذكاء الاصطناعي مراقبة الاتصالات والمراسلات الرقمية للكشف عن محاولات تنسيق الأعمال الإرهابية. ويمكن تحليل النصوص والمحادثات بحثًا عن كلمات مفتاحية وأنماط تشير إلى التهديدات المحتملة [75].
- **المخالف للقوانين على المنصات الرقمية**: يمكن للخوارزميات تحليل الصور والنصوص والفيديوهات لتحديد المحتوى المحتمل للإرهاب وحجبه أو إزالته.
- **التعرف على الهويات المشبوهة**: يمكن استخدام تقنيات التعرف على الوجوه والبصمات البيومترية لتحديد الهويات المشبوهة على المنصات الرقمية، فهذا يمكن أن يسهم في تتبع الأفراد الذين قد يكونون مرتبطين بأنشطة إرهابية[76].
- **تحليل البيانات الكبيرة**: يمكن للذكاء الاصطناعي تحليل كميات ضخمة من البيانات المتعلقة بالأنشطة الإرهابية وتحديد الأنماط والاتجاهات، وهذا يساعد في توقع واكتشاف الأنشطة المشبوهة واتخاذ إجراءات وقائية[77].

(75) Mario Cannataro، Pietro Hiram Guzzi، Artificial Intelligence in Bioinformatics ،From Omics Analysis to Deep Learning and Network Mining،1st Edition - May 12، 2022 at: https://www.scopus.com/.

(76) عمار ياسر البابلي، الذكاء الاصطناعي في مواجهة الشائعات وجرائم تمويل الإرهاب في البيئة السيبرانية «التداعيات وسبل المواجهة»، مرجع سابق

(77) LUCAS ROPEK، New Orleans Declares State of Emergency After Ransomware Attack، govtech، DECEMBER 16، 2019 on https://www.govtech.com/security/New-Orleans-Declares-State-of-Emergency-After-Ransomware-Attack.html.

- **مراقبة المعاملات المالية الشبكية:** يمكن استخدام الذكاء الاصطناعي لمراقبة المعاملات المالية المشبوهة عبر المنصات الرقمية، فذلك يساعد في تحديد تمويل الأنشطة الإرهابية وقطع مصادر تمويلها.

سابعًا – استخدام الشبكات العصبية الاصطناعية في التعرف وحذف المحتوي الإرهابي:

يقصد بالشبكات العصبية الاصطناعي بأنها مجموعة من الخوارزميات، نموذجها مستوحى من الدماغ البشري، وتعد الشبكات العصبية الاصطناعية (Artificial Neural Networks) أحد الأدوات القوية المستخدمة للتعامل مع التحديات المتعلقة بحذف المحتوى الإرهابي من شبكات التواصل الاجتماعي، وتستند الشبكات العصبية الاصطناعية إلى عملية تعلم الآلة؛ حيث تتعلم من الأمثلة وتقوم بالتكيف تلقائيًا مع البيانات المقدمة لها[78].

تعمل الشبكات العصبية الاصطناعية على تحليل المحتوى الموجود على شبكات التواصل الاجتماعي وتصنيفه إلى فئات مختلفة، بما في ذلك الفئة المرتبطة بالمحتوى الإرهابي، وتستخدم الشبكات العصبية العديد من الطبقات (layers) والوحدات (units) المتصلة بشكل معقد لمعالجة المعلومات واستخلاص الأنماط والمعرفة من البيانات المدخلة وتعمل على العثور على العلاقات الأساسية بين المعلومات من خلال محاكاة عملية التفكير البشرية عبر المنصات الإلكترونية

ويتعرض صناع السياسات على الصعيدين الوطني والدولي، وكذلك شركات التكنولوجيا، لضغوط متزايدة للإسراع بإدارة المحتوى المتطرف وإزالته بفعالية أكبر، ومن الأسباب الداعية إلى ذلك وقوع أضرار فعلية ومأساوية، من حيث تكرارها واتساع نطاقها، نتيجة للمحتوى الضار عبر الإنترنت، مثل إطلاق النار على مسجد كرايستشيرش في مارس 2019، وإطلاق النار على كنيسة تشارلستون في الولايات المتحدة الأمريكية عام 2015، وإطلاق النار على مسجد مدينة كيبيك الكندية عام 2017، ولذلك فإنَّ صناع التكنولوجيا وصانعي السياسات الوطنيين ومتعددي الجنسيات بذلوا جهودًا حثيثة فيما بعد لإزالة بعض المحتوى المتطرف الذي ينتجه تنظيم الدولة الإسلامية والجماعات الجهادية العنيفة، فضلاً عن المحتوى الذي ينادي بالتعصب للبيض وكره النساء ومعاداة السامية وكراهية الإسلام.

(78) أحمد محمد صالح، تطبيقات الذكاء الاصطناعي ودورها في الإدارة الأمنية للحشود، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، 2022، ص 35.

من الممكن أن تساهم الشبكات العصبية الاصطناعية في حذف المحتوى الإرهابي من شبكات التواصل الاجتماعي بالطرق التالية[79]:

1. **التعرف على المحتوى الإرهابي**: تحليل المحتوى المنشور وتحديد العناصر التي تحتوي على محتوى إرهابي أو تطرفي، ويتم ذلك عن طريق تصنيف النصوص والصور والفيديوهات بناءً على السياق والمحتوى.
2. **الكشف عن الأنماط**: تحديد أنماط مشتركة في المحتوى الإرهابي، مثل الشعارات أو الألفاظ المستخدمة بشكل متكرر، وهذا يساعد في التعرف على محتوى إرهابي جديد وغير معروف.
3. **تصنيف المستخدمين**: تحديد المستخدمين الذين قد يكونون مرتبطين بالإرهاب أو التطرف، وبذلك يمكن اتخاذ إجراءات فعالة لحظرهم أو مراقبتهم.
4. **الترجمة والتفسير**: يمكن أن تقدم الشبكات العصبية الاصطناعية الدعم في ترجمة المحتوى المشتبه به إلى لغات مختلفة؛ لتمكين المراجعين من فهمه وتقييمه بشكل أفضل.

المطلب الثاني
قدرة الشبكات العصبية الاصطناعية على مواجهة الجرائم

تعد قدرة الشبكات العصبية الاصطناعية على مواجهة الجرائم الجنائية والرقمية المستحدثة مجالاً مثيرًا للاهتمام في مجتمعاتنا الحديثة، فمع تزايد التطور التكنولوجي وانتشار استخدام الإنترنت، أصبحت الجرائم الرقمية وسائل للتهديدات الجديدة والمتطورة، وتتيح الشبكات العصبية الاصطناعية استخدام الذكاء الاصطناعي لتحليل البيانات الكبيرة واكتشاف الأنماط والاتجاهات في السلوكيات الإلكترونية، ويمكن لهذه التقنيات تحديد الأنشطة غير المشروعة عبر الشبكات العنكبوتية، مثل اختراق الأنظمة، وسرقة البيانات الشخصية، والتزوير الإلكتروني، والاحتيال المالي، والتحرش الجنسي عبر الإنترنت، والكثير من الأنشطة الأخرى التي تهدد الأمن الرقمي والمجتمعات.

(79) The New Eyes of Surveillance: Artificial Intelligence and Humanizing Technology. Wired. accessed 23 Jan. 2020 https://www.wired.com/insights/201408//the-new-eyes-of-surveillance-artificial-intelligence-and-humanizing-technology/

وعندما يتم تدريب الشبكات العصبية الاصطناعية على مجموعة واسعة من البيانات، فإنها تصبح قادرة على التعرف على أنماط السلوك الطبيعي والغير طبيعي، وبالتالي يمكنها رصد وتحليل الأنشطة الجنائية بفعالية، بالإضافة إلى ذلك يمكن استخدام الشبكات العصبية لتطوير نماذج تنبؤية لتحديد الأنشطة المحتملة والتي قد تكون جرائم في المستقبل.

أولاً – استخدام الشبكات العصبية الاصطناعية في مكافحة جرائم الاستغلال الجنسي للأطفال:

كيفية استخدام تقنيات الذكاء الاصطناعي في مكافحة جرائم الاستغلال الجنسي للأطفال

- **تحليل الصور والفيديوهات:** يتيح استخدام تقنيات الذكاء الاصطناعي في تحليل الصور والفيديوهات إمكانية التعرف على المحتوى الإباحي الذي يشمل الأطفال، ويتم ذلك عن طريق تدريب النظام على مجموعة كبيرة من الصور ليتعلم التمييز بين المحتوى الآمن والمحتوى الضار، ثم تقوم الشبكات العصبية بتتبع مصدر المادة الإباحية وتتبع (IP) [80]: ورصد وإبلاغ السلطات والأجهزة الأمنية وشركات التكنولوجيا[81].
- **تحليل السلوك عبر الإنترنت:** يتيح الذكاء الاصطناعي مراقبة سلوك المستخدمين عبر الإنترنت والكشف عن أنماط مشبوهة على سبيل المثال، يمكن رصد تغييرات في نمط البحث أو التفاعل على وسائل التواصل الاجتماعي التي قد تشير إلى نشاط مريب.
- **استخدام تقنيات الشبكات العصبية:** يستخدم العمق في تحليل البيانات باستخدام الشبكات العصبية العميقة، مما يعزز قدرة النظام على التعرف على أنماط معقدة ومتطورة لجرائم الاستغلال الجنسي وتحليل الصور والفيديوهات ونمط تلك المواقع والجروبات.

(80) بروتوكول الإنترنت IP: إذ يعد هذا البروتوكول الطابع المميز لاستخدام الإنترنت، فأي شخص يحصل على بروتوكول الإنترنت يمكنه الولوج إلى الإنترنت ليصبح عضوًا فيها، يباشر الحركة خلالها، ويحصل على خدماتها، وهناك العديد من البرامج التي تقوم برصد بروتوكولات الإنترنت، وتتم عملية الرصد الإلكتروني بمنتهى الدقة والمهارة، وهي عملية فنية تقوم بها الأجهزة الأمنية، والمتخصصون في المجال التكنولوجي، أو الشركات التكنولوجية العملاقة، ويعتمد أسلوب عملها على استخدام برامج تقنيات المعلومات، وذلك عن طريق الاعتماد على أن لكل شخص يتعامل مع شبكة الإنترنت رقمًا للدخول على الشبكة يعرف بـ (IP)؛ حيث يمكن من خلال تتبع هذا الرقم معرفة مكان الشخص، عن طريق مزود خدمة الإنترنت، أو السنترال المقدم للخدمة أو أجهزة الراوتر الموزع منها الخدمة، والشبكات المقدمة لخدمات الاتصالات، وتقوم تلك العملية على تتبع الصفحات واتخاذ الإجراءات الفنية والقانونية لضبط المتهم وتحديد الأجهزة المستخدمة في عمليات دعم أو صناعة الإرهاب ونشر معلومات تضر الأمن القومي، أو تحرض على أعمال العنف و التخريب، ويتم الاستيلاء عليها والتحفظ على الصفحة «مواقع الإنترنت»، ويتم إحالته إلى النيابة التي تباشر التحقيق معه وتحيله إلى المحاكمة

(81) Sarah Brayne. 2020. Predict and surveil: Data، discretion، and the future of policing. Oxford University Press، USA

- **الكشف عن الهوية**:يمكن استخدام تقنيات الذكاء الاصطناعي للتحقق من هوية الأشخاص المشتبه بهم أو المشاركين في نشاط جنسي غير قانوني، سواء كان ذلك عبر الإنترنت أو في أي نشاط آخر وبالتالي التنبيه ابلاغ السلطات والأجهزة الأمنية وإنفاذ القانون[82].
- **مراقبة المحتوى عبر الويب**:تقوم التقنيات بفحص المحتوى عبر الويب، بما في ذلك المنتديات والمواقع الإباحية، للكشف عن أي نشاط يتعلق بجرائم الاستغلال الجنسي للأطفال، ويمكن للخوارزميات والشبكات العصبية الاصطناعية تحليل النصوص المتعلقة بجرائم الاتجار بالبشر، مثل الإعلانات غير القانونية أو الرسائل الإلكترونية أو المحادثات عبر وسائل التواصل الاجتماعي لتحديد أنماط وكلمات مفتاحية تشير إلى وجود جرائم. كما يمكن استخدام الخوارزميات والشبكات العصبية الاصطناعية لتحليل الصور والفيديوهات لتحديد علامات الاستغلال والإيذاء الجسدي والتعرف على الأشخاص المتورطين.
- **التعاون مع مزودي خدمات الإنترنت**: يجري التعاون مع مزودي خدمات الإنترنت لتحديد وتقديم تقارير حول المحتوى الإباحي الذي يتضمن الأطفال ومنع تلك المواقع من الخوادم الرئيسية ومنع وصولها للأسر والأطفال والمجتمعات ويمكن للشركات التكنولوجية الكبرى تطوير أدوات وأنظمة تبلغ عن هذا النوع من المحتوى[83].
- **حماية الخصوصية والبيانات**:يعطى اهتمام كبير لحماية خصوصية المستخدمين أثناء جمع وتحليل البيانات ويتم استخدام تقنيات التشفير وسائل أمان أخرى للحفاظ على سرية المعلومات.
- **التحليل النصي وتحليل المحتوى**:يستخدم التحليل النصي لمراقبة المحتوى النصي عبر الإنترنت، مثل المحادثات والتعليقات، لاكتشاف أي محتوى يشير إلى أنشطة غير قانونية.
- **التعاون مع السلطات الإنفاذ**:يتيح التكامل مع أنظمة السلطات الإنفاذ توجيه جهود محددة وفعالة لمكافحة الجرائم الجنسية ضد الأطفال.
- **تحليل البيانات الزمنية**:يمكن تحليل البيانات عبر الوقت لرصد التغييرات في أنماط السلوك واكتشاف اتجاهات جديدة في جرائم الاستغلال الجنسي.

(82) أنغوس كروفورد وتوني سميث، كيف يستخدم الذكاء الاصطناعي للاتجار بصور الاعتداء الجنسي على أطفال، تقرير لل BBC الدولية بتاريخ 28 يونيو 2023 ومتاح على: https://www.bbc.com/arabic/articles/clwd844084xo

(83) ضمن التحالف، تجتمع شركات كبيرة مثل «سناب» و«ديسكورد» و«ميغا»، وتعتبر الأخيرة منصة نيوزيلندية تركز بشكل خاص على الخصوصية. وفي سياق جهود التحالف، نجحت نسخة تجريبية من البرنامج في إزالة أكثر من عشرة آلاف حساب شخصي على فيسبوك وصفحات وحسابات في انستغرام بالتعاون مع «ميغا»؛ حيث قامت بمشاركة مجموعة من البيانات. ولتعزيز الأمان الرقمي أبلغت «ميتا» عن الحسابات المعنية إلى المركز الوطني للأطفال المفقودين والمستغلين، الذي يتخذ من الولايات المتحدة مقرًا له، كما شاركت النتائج مع منصات أخرى لتيسير إجراء تحقيقاتها الخاصة

باستخدام هذه التقنيات بشكل متكامل، يمكن تعزيز القدرة على رصد ومكافحة جرائم الاستغلال الجنسي للأطفال، وتحقيق مزيد من الكفاءة والفعالية في الحماية والتصدي لهذه الظاهرة الخطيرة.

وقد أعلنت شركة أبل (Apple)عن نظام جديد يسمح برصد مواد متعلقة بالإساءة الجنسية للأطفال (CSAM) في أجهزة آيفون، ويتيح النظام البحث عن مواد CSAM قبل تخزين الصور على نظام iCloud Photos، وفي حالة رصد تطابق، يقوم مراجع بشري بتقييم المحتوى والإبلاغ عنه لسلطات إنفاذ القانون، ورغم مخاوف من انتهاك الخصوصية، أكدت أبل أن النظام يحقق دقة عالية ونسبة خطأ تقل عن واحد في التريليون سنويًا، وستقوم أبل بمراجعة يدوية لتقارير الكشف عن التطابق وفي حالة التأكد، ستتخذ إجراءات لتعطيل حساب المستخدم والإبلاغ عنه للسلطات، مع تأكيد الشركة على فوائد هذه التقنية من حيث الخصوصية بناءً على تعلم النظام من صور المستخدمين للكشف عن وجود مواد CSAM في حساباتهم[84].

والجدير بالذكر أن الاتحاد الأوروبي أعد تطبيق جديد «بروتيك» يهدف إلى تقليل مشاهدة مواد الاعتداء الجنسي على الأطفال عبر الإنترنت، على تمويل بلغ 2.17 مليون دولار من الاتحاد الأوروبي، وسيخضع هذا التطبيق للاختبار عن طريق متطوعين الذين طلبوا المساعدة لمقاومة رغبتهم في مشاهدة صور اعتداء جنسي على الأطفال، وسيتم تثبيت التطبيق الجديد على أجهزة مثل الهواتف المحمولة؛ حيث سيقوم بتحديد الصور ومقاطع الفيديو المسيئة ومنع عرضها، ومن المأمول أن يؤدي هذا التطبيق دورًا في مكافحة «الطلب المتزايد» على صور الاعتداء الجنسي على الأطفال[85].

ثانيًا– دور الخوارزميات والشبكات العصبية الاصطناعية في رصد وكشف محتوي المخدرات والعقاقير المصطنعة خلال المنصات الرقمية عبر طبقات الإنترنت:

دور الذكاء الاصطناعي في التحقيقات عبر الإنترنت يعد طلبًا كبيرًا لدى الأجهزة الأمنية وإنفاذ القانون، ويكون الذكاء الاصطناعي عاملاً مضاعفًا للقوة؛ حيث يساعد المحققين في التغلب على التحديات المتنوعة التي تواجههم أثناء إجراء تحقيقاتهم عبر الشبكة. فيما يلي توضيح لبعض المجالات التي يمكن أن يؤدي فيها الذكاء الاصطناعي دورًا[86]:

(84) جيمس كلايتون، أبل ستفحص هواتف آيفون بحثًا عن أي محتوى مسيء جنسيًا للأطفال، تقرير لل BBC الدولية بتاريخ 6 أغسطس 2022 ومتاح على: https://www.bbc.com/arabic/science-and-tech-58086401

(85) كريس فالانس، تطبيق لحظر صور الاعتداء الجنسي على الأطفال يحصل على تمويل من الاتحاد الأوروبي، تقرير لل BBC الدولية بتاريخ 23 فبراير 2023 ومتاح على: https://www.bbc.com/arabic/science-and-tech-64734567

(86) Johnmichael O'Hare، Using AI to overcome the challenges of investigating digital narcotics supply chainsLaw enforcement agencies would do well to heed drug trafficking's technology-driven distribution systems، Police Drug Enforcement Software (Mar 30، 2021) at: https://bit.ly/3Vd9gCu

- **مراقبة أسواق الويب المظلمة**: يستطيع الذكاء الاصطناعي، بالتعاون مع ذكاء الويب، دعم المحققين وجهات انفاذ القانون في تنفيذ عمليات البحث في منتديات الويب المظلمة؛ حيث يروج لأسواق المخدرات وأمور أخرى، ويستخدم الذكاء الاصطناعي لتنفيذ عمليات بحث معقدة باستخدام معلمات مخصصة، مما يعزز كفاءة المحقق ودقة نتائج البحث.
- **تسريع عملية التحقيق**: تسريع عمليات البحث وجمع البيانات، ويوفر تحليلًا سريعًا وقويًا، ويمكنه استخدام قدراته في سحب البيانات من الويب السطحي والمظلم، مما يوفر وقتًا وجهدًا كبيرين يستخدمان عادةً في عمليات البحث اليدوية.
- **الكشف عن الجهات الفاعلة والشبكات التهديدية بسرعة**: تمكن قدرات التحقيق المدعومة بالذكاء الاصطناعي من تحديد هويات ممثلي التهديد بشكل سريع ودقيق، ثم الكشف عن شركائهم في سلاسل توريد المخدرات وربط البيانات المتنوعة المظهرة في التحقيق عبر الإنترنت لتحديد هويات الأطراف المعنية وكشف عن العلاقات بينها.
- بشكل عام، يسهم الذكاء الاصطناعي في تعزيز فعالية وكفاءة عمليات التحقيق، مما يساعد المؤسسات على مواجهة التحديات الأمنية والجنائية عبر الشبكة بشكل أفضل وأسرع.
- **العثور على أدلة على شبكة الإنترنت المفتوحة**: القدرة على اكتشاف البيانات الحيوية للتحقيقات في بيئة مفتوحة المصدر تعتبر ميزة إضافية لاستخدام تقنية الاستخبارات الويب (WEBINT) بدعم من الذكاء الاصطناعي كصور المخدرات والعقاقير والحبوب والمواد المشتبه فيها وبالرغم من أن العديد من جوانب سلسلة توريد الأدوية تعمل في الأماكن الظلمة على الويب، إلا أن بعض هذه الجوانب قد تتسلل إلى الويب العام، وعلى سبيل المثال: يعلن بعض أسواق الويب المظلمة عن وجودها من خلال وسائل التواصل الاجتماعي التقليدية، وقد تكون الصور المستخدمة للترويج على الويب المظلم متاحة أيضًا على الويب السطحي إذا لم يتم إزالة بيانات الصور القابلة للتبديل من قبل ممثل التهديد، ويمكن للمحققين الحصول على معلومات مهمة مثل الطوابع الزمنية وتحديد الموقع الجغرافي. (87)
- **دمج وتحليل الأدلة المادية**: يمكن لإنفاذ القانون في مجال مكافحة المخدرات استخدام التحقيق عبر الويب (WEBINT) لتقييم الأدلة المادية بجانب التنوع الرقمي، وعلى سبيل المثال: إذا تمت مصادرة أجهزة إلكترونية كجزء من التحقيق، يمكن للكاميرات أو

(87) United Nations Office of Drugs and Crime. 2020. 2020 UNODC Global Report on Trafficking in Persons

الكمبيوترات إنتاج صور على برامج التواصل الاجتماعي كالواتس أب والفيس بوك وغيرها من البرامج التي تتداول عليها صور لأنشطة وعقاقير المخدرات والتي قد تحتوي على أجزاء من البيانات ذات الصلة بالوقت والمكان، أو إذا تم اعتراض شحنة مخدرات[88]، فإن بطاقة الشحن توفر معلومات حول المنشأ والوجهة ويمكن للذكاء الاصطناعي أن يساعد في تحليل هذه النتائج وربطها بالبيانات الأخرى التي تم جمعها خلال التحقيق[89].

- **بناء القضية بثقة**: تساعد دقة وفعالية الذكاء الاصطناعي في تجميع وتحليل وتقديم بيانات موثوقة وجديرة بالثقة ويمثل مستوى الثقة الذي يتم الحصول عليه خطوة مهمة في التحقيق؛ حيث يمكن للبيانات الموثوقة تمكين موظفي إنفاذ القانون من اتخاذ الإجراءات الضرورية وضمان متابعة جهة التهديد المناسبة، والتأكد من أن البيانات يمكن أن تستخدم كدليل في المحكمة وتمكن البيانات المتحقق منها الوكالات من بناء قضية قوية ضد الأطراف الفاعلة في سلسلة توريد المخدرات، مما يؤدي إلى إصدار لوائح اتهام وتحسين معدلات المتابعة القانونية.

ويعزز ا ذكاء الاصطناعي قدرة وكلاء المخدرات على التعامل مع هذا التحدي الرقمي، وتحليل المعلومات الكبيرة بشكل أكثر فعالية. ويسرع الذكاء الاصطناعي عمليات التحقيق، ويعزز الجودة والدقة في جمع البيانات، مما يمكن وكالات إنفاذ القانون من بناء حالات قوية وموثوقة لمحاكمة الجهات الفاعلة في مجال التهديد.

ثالثًا– دور الخوارزميات والشبكات العصبية الاصطناعية في تهريب المهاجرين خلال المنصات الرقمية عبر طبقات الإنترنت:

تؤدي تقنية الذكاء الاصطناعي (الذكاء الاصطناعي) دورًا مهمًا في مراقبة ومكافحة الاتجار بالبشر وجرائم تهريب المهاجرين، ويكمن في تطوير نظم ذكاء اصطناعي قادرة على تحليل ومراقبة البيانات والسلوكيات على هذه المنصات، وفيما يلي بعض الطرق التي يتم بها استخدام الذكاء الاصطناعي لهذه الأغراض

(88) Suicide، Incels، and Drugs: How TikTok's deadly 112 algorithm harms kids (Eko، 2023) Accessed from: https://s3.amazonaws.com/s3.sumofus.org/images/eko_Tiktok-Report_FINAL.pdf 022023/08/

(89) Lauren Vollinger. 2021. Concretizing intersectional research methods: Incorporating social justice and action into United States sex trafficking research. Journal of Human Behavior in the Social Environment 31، 5 (2021)، 599–625.

- **تحليل البيانات والتعرف على الأنماط**: يمكن للخوارزميات (AI) تحليل كميات هائلة من البيانات من مصادر مختلفة، مثل مراقبة الحدود وكاميرات المراقبة وبيانات الهاتف المحمول، لتحديد الأنماط التي تشير إلى الاتجار بالبشر أو أنشطة تهريب المهاجرين، ويتضمن ذلك تحديد أنماط الحركة غير العادية أو ديناميكيات المجموعة أو السلوكيات المشبوهة، وتتعرف على أنماط التواصل والتفاعل على المنصات الرقمية التي تشير إلى وجود شبكات للاتجار بالبشر.
- **التعرف على الوجه**: يمكن استخدام تقنية التعرف على الوجه لتحديد الأفراد المتورطين في الاتجار بالبشر أو تهريب المهاجرين، ويمكن أن يساعد ذلك في تتبع حركة المشتبه بهم عبر مواقع مختلفة ومساعدة وكالات إنفاذ القانون على القبض عليهم.
- **تحليل النص ومراقبته**: يمكن استخدام تقنيات معالجة اللغة الطبيعية (NLP)، وهي مجموعة فرعية من (AI)، لمراقبة المحتوى والاتصالات عبر الإنترنت للكشف عن أي إشارات أو مناقشات تتعلق بالاتجار بالبشر أو تهريب المهاجرين، وهذا يساعد في تحديد الجناة أو الضحايا المحتملين وتحليلها والاستدلال عن أماكنهم والتعرف على أنماط التواصل والتفاعل على المنصات الرقمية التي تشير إلى وجود شبكات للاتجار بالبشر[90].
- **تحليل الشبكات الاجتماعية**: تستخدم خوارزميات (AI) في تحليل الشبكات الاجتماعية لكشف ورصد أنشطة الاتجار بالبشر وتهريب المهاجرين بكفاءة عالية. ويمكن لهذه التقنيات تحليل الروابط بين الأفراد والجماعات عبر المنصات الاجتماعية، مما يوفر نظرة شاملة عن الهياكل التنظيمية لتلك الشبكات الإجرامية ومراقبة سلوك المستخدمين وتحليل اللغة الطبيعية لاكتشاف أي أنماط تصرف غير طبيعية تشير إلى محاولات للاتجار بالبشر أو تهريب المهاجرين، ويساهم هذا النهج في رصد العلاقات والشبكات المشتبه بها، كما يتيح تقديم إشارات تحذيرية تلقائية للسلطات عند اكتشاف أنشطة مشبوهة، مما يسهم في الحد من هذه الجرائم بشكل فعال وفي الوقت الفعلي[91].
- **التكنولوجيا البيومترية**: يمكن أن تساعد التقنيات البيومترية، مثل مسح بصمات الأصابع وقزحية العين، في التحقق من هويات الأفراد واكتشاف الأنشطة الاحتيالية بشكل خاص عند المعابر الحدودية ونقاط تفتيش الهجرة و كشف ومراقبة جرائم الاتجار بالبشر وتهريب المهاجرين؛ حيث تعد البصمات وتقنيات التعرف على الوجوه

(90) M. Aschmann، L. Leenen، J. Jansen van Vuuren، The Utilisation of the Deep Web for Military Counter Terrorist Operations. (Academic Conferences and publish- ing limited، s.l.، 2022)

(91) EU Policy Cycle - EMPACTEMPACT 2022+ Fighting crime together Content type PAGE AT: https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact

أدوات تكنولوجية رئيسية ويتيح استخدام هذه التقنيات تسجيل معلومات بيولوجية دقيقة للأفراد، مما يساعد في التحقق من هوياتهم ورصد تحركاتهم عبر الحدود و تعمل هذه الأدوات على تعزيز الأمان وتقليل فرص التلاعب أو التزوير، مما يسهم في تحسين إدارة الحدود ومكافحة الجرائم بكفاءة، ومع ذلك يجب ضمان استخدام هذه التقنيات بمراعاة حقوق الإنسان والحفاظ على معايير الخصوصية خلال عمليات التنفيذ. (92)

- **الشرطة التنبؤية:** توقع ومنع أنشطة الاتجار بالبشر أو تهريب المهاجرين من خلال تحليل البيانات التاريخية وتحديد النقاط الساخنة المحتملة، ويمكن استخدام تقنيات تحليل الصوت والصورة بواسطة (AI) للكشف عن علامات الاستغاثة أو الأنشطة المشبوهة في مناطق تحتمل وقوع جرائم الاتجار بالبشر.
- **التعلم الآلي للكشف عن الحالات الشاذة والتحليلات التنبؤية:** يمكن تدريب خوارزميات التعلم الآلي على التعرف على الأنماط العادية للحركة والتواصل والمعاملات المالية، ويمكن اعتبار أي انحرافات عن هذه الأنماط حالات شاذة، مما قد يشير إلى الاتجار بالبشر أو أنشطة التهريب، ويمكن للنماذج الذكاء الاصطناعي، من خلال التحليلات التنبؤية، تحليل البيانات التاريخية للتنبؤ بالمناطق أو الطرق المحتملة التي قد يحدث فيها الاتجار أو التهريب، وهذا يساعد أجهزة إنفاذ القانون في نشر الموارد بفعالية والتصدي لهذه الجرائم بشكل استباقي. (93)
- **المراقبة في الوقت الحقيقي باستخدام أجهزة إنترنت الأشياء:** يمكن توصيل أجهزة إنترنت الأشياء (IoT)، مثل أجهزة الاستشعار وكاميرات المراقبة، بأنظمة الذكاء الاصطناعي للمراقبة في الوقت الفعلي، وهذا يمكن السلطات من اكتشاف الأنشطة المشبوهة والاستجابة لها على الفور.
- **معالجة اللغة الطبيعية (NLP) لاستخراج النصوص:** تستخدم تقنيات البرمجة اللغوية العصبية لتحليل البيانات النصية، بما في ذلك المنتديات عبر الإنترنت وسجلات الدردشة ووسائل التواصل الاجتماعي، لتحديد المناقشات المتعلقة بالاتجار أو التهريب، وهذا يساعد إنفاذ القانون على البقاء على اطلاع بالأنشطة الإجرامية المحتملة.

(92) REPORT OF UN about: Global Report on Trafficking in Persons 2020 https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf

(93) Julia Deeb-Swihart، Alex Endert، and Amy Bruckamn. 2022. Ethical Tensions in Applications of AI for Addressing Human Trafficking: A Human Rights Perspective. Proc. ACM Hum.-Comput. Interact. 6، CSCW2، Article 295 (November 2022)، 29 pages. https://doi.org/10.11453555186/

- **التعرف على الوجه والقياسات الحيوية**: تساعد تقنية التعرف على الوجه في تحديد وتتبع الأفراد عبر مواقع مختلفة، ويمكن استخدام البيانات البيومترية، بما في ذلك بصمات الأصابع ومسح قزحية العين، للتحقق وربط المشتبه بهم بالأنشطة الإجرامية.
- **يمكن للخوارزميات والشبكات العصبية الاصطناعية** تحليل البيانات الجغرافية واستخلاص الأنماط والتقارير التي تساعد في تحديد مناطق معينة تشهد نشاطًا مرتفعًا لجرائم الاتجار بالبشر، ويمكن أن تحلل هذه التقنيات البيانات المكانية مثل العناوين، والإحداثيات، والخرائط، والمعالم الجغرافية الأخرى لتوفير رؤى مفيدة، وعلى سبيل المثال: يمكن استخدام الخوارزميات والشبكات العصبية الاصطناعية لتحليل النمط المكاني لجرائم الاتجار بالبشر وتحديد المناطق التي تشهد نشاطًا غير طبيعيًا، ويمكن أيضًا استخدامها لتحليل التنقل والتحركات والمسارات المحتملة للمهربين والمهاجرين غير الشرعيين [94].
- **باستخدام الخوارزميات والشبكات العصبية الاصطناعية**، يمكن تحليل البيانات الجغرافية بطرق أكثر تعقيدًا وتفصيلًا، وبالتالي تعزيز القدرة على اكتشاف الأنماط والعلاقات الجغرافية المتعلقة بجرائم الاتجار بالبشر، ثم يمكن توجيه الجهود والموارد بشكل أفضل لمكافحة هذه الجرائم وتعزيز الأمان والعدالة.
- **التعاون مع جهات إنفاذ القانون:** يمكن استخدام الخوارزميات والشبكات العصبية الاصطناعية لتعزيز التعاون بين الجهات المعنية في مكافحة جرائم الاتجار بالبشر وتهريب المهاجرين. ويمكن لهذه التقنيات تحليل البيانات وتوفير تقارير ومعلومات مفيدة للجهات القانونية والأمنية لدعم عمليات التحقيق والقبض على المتورطين[95].

ويرى الباحث أن الذكاء الاصطناعي يدعم اكتشاف وتحقيق جرائم الاتجار؛ حيث يساعد في تحديد الضحايا من خلال تحليل المحتوى عبر الإنترنت ومواقع هذه الجرائم، وتشمل الحلول التكنولوجية تحليل صور الأقمار الصناعية، والتي تتبع حركة سفن الصيد التي تنقل ضحايا الاتجار بالبشر بين البلدان، وتشمل أيضًا جمع صور انتهاكات حقوق الأطفال من الويب للمساعدة في تعقب الضحايا، وخاصة الأطفال والمحتاجين إلى المساعدة العاجلة، كما تركز هذه التقنيات على رصد الكلمات المشتبه بها في رسائل النصوص بين أعضاء هذه الشبكات.

(94) Paolo Campana OF Online and technology-facilitated trafficking in human beings April 2022 ،Council of Europe at:
https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-full-rep/1680a73e49

(95) Ethical Tensions in Applications of AI for Addressing Human Trafficking: A Human Rights Perspective: Proceedings of the ACM on Human-Computer InteractionVolume 6Issue CSCW2Article No.: 295pp 1–29https://doi.org/10.11453555186/

وعلى سبيل المثال: يمكن لتقنيات معالجة الصور التعرف على الوجوه والأموال وعلامات الوشم الموضوعة على الضحايا، مما يمكنها من استخراج هذه المعلومات من الصور، ويتيح ذلك إنشاء روابط بين الصور التي تحتوي على جرائم والهواتف الذكية التي التقطتها وهويات الضحايا، ويمكن أيضًا تحليل الصور المعدلة بشكل كبير، وتقوم خوارزميات الذكاء الاصطناعي بتعلم آلاف الصور للضحايا وأماكن الجرائم، مما يتيح لها تحليلها والتنبؤ بالنتائج المرجوة. ويتم ذلك عبر تحديد أنماط المجرمين في مواقف مختلفة، مثل اختطاف الأفراد واختيار مواقع الجرائم وتوثيق انتهاكات حقوق الإنسان، وتساعد هذه التقنيات في التنبؤ بالحالات المستقبلية للاتجار في مناطق مختلفة حول العالم، وتحديد أولويات الحالات بناءً على تقييم المخاطر.

رابعًا- الآليات التوعوية لإنفاذ القانون والمؤسسات الإعلامية لجرائم الابتزاز الجنسي والتحرش الإلكتروني بالأطفال واستغلال الأطفال جنسيًا:

إنَّ توعية الجمهور وتعزيز الوعي بجرائم الابتزاز الجنسي والتحرش الإلكتروني بالأطفال واستغلال الأطفال جنسيًا يعد أمرًا حيويًا للحد من هذه الجرائم وحماية الأطفال. وهناك عدة آليات توعوية يمكن استخدامها من قبل إنفاذ القانون والمؤسسات الإعلامية لتحقيق هذا الهدف، منها

- **حملات التوعية العامة:** يمكن تنظيم حملات توعية عامة على نطاق واسع لزيادة الوعي بجرائم الابتزاز الجنسي والتحرش الإلكتروني بالأطفال واستغلال الأطفال جنسيًا. ويتم استخدام وسائل الإعلام المختلفة مثل التلفزيون والراديو والصحف ووسائل التواصل الاجتماعي لنشر رسائل التوعية وتوفير المعلومات المهمة للجمهور، ويجب أن تركز هذه الحملات على تعريف الجمهور بأنواع الجرائم وأعراضها والنصائح لحماية الأطفال. [96]
- **التعليم في المدارس:** يمكن تضمين مواضيع توعية حول جرائم الابتزاز الجنسي والتحرش الإلكتروني بالأطفال واستغلال الأطفال جنسيًا في المناهج المدرسية، ويتم توفير المعلومات اللازمة للأطفال والمراهقين حول الأخطار المحتملة وكيفية الحماية الذاتية والإبلاغ عن أي حالات مشتبه بها. ويجب تدريب المعلمين والمرشدين الطلابيين لتزويد الأطفال بالدعم والإرشاد المناسب [97].

(96) ضياء الدين محمد رضوان، التعاون المشترك بين الشرطة والجمهور وأثره على الأداء الأمني (دراسة مقارنة) العوامل وسبل الوقاية، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، 2018، ص 209.

(97) محمود راغب، «القومي للمرأة» يكشف عقوبة جريمة الابتزاز وكيفية حصول الضحية على حقها، تقرير مؤسسة اليوم السابع المصرية، بتاريخ 15 أبريل 2023 ومتاح على: https://www.youm7.com/story/2023/4/15/%D8%A7%D8%A7

- **الدور الإعلامي**: تؤدي المؤسسات الإعلامية دورًا مهمًا في نشر الأخبار والتقارير المتعلقة بجرائم الابتزاز الجنسي والتحرش الإلكتروني بالأطفال واستغلال الأطفال جنسيًا. يتم تسليط الضوء على القضايا المتعلقة بهذه الجرائم وتوفير المعلومات المهمة والتوضيح للجمهور حول الأسباب والتأثيرات والتدابير التي يمكن اتخاذها لمكافحتها. يجب أن تركز تلك المؤسسات على نشر القصص الناجحة للضحايا وتسليط الضوء على الخطوات العملية التي يمكن اتخاذها للحماية والإبلاغ.
- **التعاون مع المنظمات المجتمع المدني**: يجب تعزيز التعاون مع المنظمات غير الحكومية والجمعيات والمؤسسات المجتمعية المعنية بحماية الأطفال ومكافحة جرائم الابتزاز الجنسي والتحرش الإلكتروني. ويمكن تنظيم ورش عمل وندوات وبرامج توعوية بالتعاون مع هذه المنظمات لتوفير المزيد من المعلومات وتعزيز الوعي وتوجيه الجمهور بشأن الإجراءات المتاحة للمساعدة والدعم[98].
- **تشريعات وسياسات قوية**: يجب وضع تشريعات وسياسات فعالة وصارمة لمكافحة جرائم الابتزاز الجنسي والتحرش الإلكتروني بالأطفال واستغلال الأطفال جنسيًا، ويجب أن تتضمن هذه التشريعات عقوبات رادعة للمرتكبين وآليات سريعة وفعالة لتقديم العدالة للضحايا.
- **تعزيز التكنولوجيا الآمنة**: ينبغي تعزيز التكنولوجيا الآمنة وتطوير آليات فعالة لرصد وتتبع الجرائم المتعلقة بالابتزاز الجنسي والتحرش الإلكتروني بالأطفال. يجب تشجيع الشركات التكنولوجية على تطوير أدوات وتقنيات لاكتشاف ومنع هذه الجرائم والتبليغ عنها.

خامسًا– المواجهة الإعلامية لمكافحة المخدرات الرقمية والمصطنعة المتداولة بالمنصات الرقمية:

تتطلب المواجهة الإعلامية الأمنية لتداول المخدرات الرقمية والمصطنعة استراتيجية شاملة تشمل عدة جوانب كالتالي

- **التحديات الإعلامية**: يواجه مجتمعنا تحديات إعلامية في مواجهة انتشار المخدرات الرقمية والمصطنعة، وتشمل هذه التحديات تعقيدات التكنولوجيا الرقمية والتشفير والتمويل الرقمي، مما يجعل من الصعب تحديد مصادر وأساليب تداول هذه المخدرات. وبالتالي، يجب أن تركز الجهود الإعلامية على توفير المعلومات الدقيقة والتحذير من المخاطر بطرق فعالة ومبتكرة.

(98) آلاء برانية، «تقرير المخاطر الرقمية: كيف يمكن حماية الأطفال في ظل الفجوة الرقمية بين الأجيال؟»، المركز المصري للفكر والدراسات الاستراتيجية، القاهرة، 15 أكتوبر 2020 ومتاح على: https://ecss.com.eg/11708/

- **الأثر الصحي والاجتماعي:** يجب أن تركز الحملات الإعلامية على توضيح الأثر الصحي والاجتماعي السلبي لتداول المخدرات الرقمية والمصطنعة ويعتبر التوعية بالمخاطر الصحية المرتبطة بتلك المخدرات أمرًا حيويًا لتحقيق تأثير إيجابي، ويجب أن تركز الحملات على تبيين التأثيرات على الصحة العقلية والجسدية والأداء الوظيفي والعلاقات الاجتماعية.
- **الدور الشبابي:** يجب أن تركز الحملات الإعلامية على التواصل مع الشباب؛ حيث يكونون أكثر عرضة لتأثيرات المخدرات الرقمية والمصطنعة. يجب توفير المعلومات الموثوقة والموجهة لهذه الفئة العمرية بأسلوب يتناسب مع لغتهم واهتماماتهم. يمكن استخدام وسائل التواصل الاجتماعي والتقنيات الحديثة للوصول إلى الشباب وتوجيههم نحو اتخاذ قرارات صحية.
- **البحث والتطوير:** يجب أن يتم دعم البحث والتطوير في مجال مكافحة المخدرات الرقمية والمصطنعة. ويمكن أن يساهم التركيز على تطوير تقنيات الكشف والتحليل المتقدمة في تحديد ومراقبة نشاطات المخدرات الرقمية، كما يمكن أن يساعد التطوير في مجال الذكاء الاصطناعي وتحليل البيانات في تحليل الأنماط والاتجاهات والتنبؤ بالتطورات المستقبلية.

ويشير الباحث إلى ضرورة تطوير الأمن الرقمي على جميع المنصات الرقمية، مع التركيز على حماية الأشخاص الأكثر تأثرًا بالاستهداف الرقمي واستخدام المعلومات الرقمية كسلاح، ويجب أن تتحمل المنصات الرقمية مثل «ميتا» وتويتر وغيرها مسؤوليتها في منع تحول المساحات الرقمية إلى أدوات للقمع الحكومي، وهذا يتطلب اتخاذ إجراءات فعالة لحماية المستخدمين المعرضين للتهديدات الرقمية تحديدًا، يجب على هذه المنصات الرقمية الاستثمار في تعزيز الإشراف على المحتوى، بما في ذلك المحتوى باللغة العربية، من خلال تنفيذ إجراءات تشمل الإزالة الفورية للمحتوى المخالف لإرشادات المنصة أو المعايير المتعلقة بخطاب الكراهية والتحريض على العنف، وعلاوةً على ذلك يجب على هذه المنصات التدخل بسرعة لإزالة المحتوى الذي قد يعرض المستخدمين للخطر، وهذه الخطوات الوقائية تساعد في تقديم بيئة رقمية آمنة وموثوقة لجميع المستخدمين، مع تجنب استغلال المساحات الرقمية لأغراض سلبية مثل القمع أو التحريض على العنف.

الخاتمة

من الجدير بالذكر أن الذكاء الاصطناعي يعد أداةً فعالة داخل العمل الأمني ومكافحة الجريمة، وعلى الرغم من قدرته على تحويل طريقتنا في التصدي للنشاط الإجرامي، فإنَّ الحكمة البشرية واتخاذ القرارات البشرية لا تزال ذات أهمية حاسمة في مكافحة الجريمة، بوجود توازن مناسب بين الذكاء الاصطناعي والذكاء البشري، ويمكننا تحقيق تقدم كبير في بناء مجتمع أكثر أمانًا وحمايةً، وإنَّ دور الذكاء الاصطناعي في مواجهة الإرهاب والتطرف عبر المنصات الإلكترونية له أهمية كبيرة في العصر الحالي، ويعتبر الإنترنت ووسائل التواصل الاجتماعي منصات حيوية لانتشار العمليات غير مشروعة عبر الإنترنت العميق والأفكار المتطرفة والمحتوى الإرهابي، ولذلك فإنَّ استخدام الذكاء الاصطناعي يمكن أن يكون ذا تأثير إيجابي في مكافحة هذه الظاهرة.

النتائج

- يتميز المجتمع الرقمي بالتفاعل الحيوي والتواصل المستمر عبر شبكة الإنترنت. وفي هذا السياق يأتي الدور الحيوي للذكاء الاصطناعي والشبكات العصبية الاصطناعية في تعزيز أمان هذا البيئة الرقمية وحمايتها من التهديدات الجرمية والإرهابية والتطرف الذي ينشط في العالم الافتراضي، وتشمل هذه التهديدات مجالات متنوعة مثل تجارة البشر، وغسيل الأموال، وتجارة المخدرات الافتراضية، وتهريب المهاجرين، والابتزاز الإلكتروني، والاحتيال المالي الذي تمارسه الجماعات الإجرامية، وغيرها من الجرائم الرقمية الحديثة.
- يتم استخدام الذكاء الاصطناعي في تحليل الجريمة وأنماطها بشكل متزايد في العديد من المجالات الأمنية والقانونية. يمكن للذكاء الاصطناعي أن يقدم نصائح وتحليلات تساعد في تحديد الأنماط الجرمية وتوفير فهم أعمق للبيانات المتعلقة بالجرائم، وتستهدف الجرائم الإلكترونية في الغالب الأعم الأفراد والمنظمات أو حتى دولة بعينها، أما جرائم الإرهاب الإلكتروني فهي تستهدف المجتمع الدولي بأكمله، فعندما يقع الهجوم على دولة معينة فكأنه وقع على المجتمع كله وهناك الكثير من العمليات غير المشروعة تتم من خلال الطبقات المظلمة للإنترنت.
- يعمل الذكاء الاصطناعي والشبكات العصبية الاصطناعية على تحليل البيانات الكبيرة ورصد الأنشطة المشبوهة، ويتخذ التدابير الوقائية والردعية لمنع ومكافحة هذه الأنشطة الإجرامية. ويقوم هذا النهج بتوفير بيئة رقمية أكثر أمانًا للمستخدمين ويحد من انتشار الجرائم الرقمية والتهديدات ذات الصلة.

- إن الجريمة المنظمة في حالة تحول، فالهيكليات التقليدية التي يتزعمها أفراد نافذون يستأثرون بمجالات إجرامية محددة تختفي تدريجيًّا لتحل محلها شبكات إجرامية مرنة وفضفاضة تغير عملياتها وأساليب عملها وفقًا للفرص المتاحة ومستوى الأرباح والطلب، والأضرار الناجمة عن الجريمة عبر الوطنية في هذا العصر شديدة الوطأة، فهي تهدد سلامة الإنسان وأمن الدول والاقتصاد العالمي، ويصاحب ذلك تقويض لسيادة القانون ولثقة المواطنين في قدرة أجهزة إنفاذ القانون على حمايتهم.
- هناك العديد من الطرق والأساليب لمواجهة الإرهاب الإلكتروني، منها المواجهة الفنية بتأمين خطوط الدفاع الأمامية باستخدام تطبيقات الجدران النارية، وتأمين حسابات المستخدمين ونظم التحقق من الهوية، وخدمات الأدلة، وتقنية المفتاح العام، وإنشاء الشبكات الافتراضية والتركيز على أمن البرمجيات. وإلى جانب المواجهة الفنية هناك المواجهة الفكرية والمواجهة القانونية والمواجهات الاستخباراتية والعسكرية التي يجب ألا تغفل عن مواجهة جرائم الإرهاب الإلكتروني، إلا أنه يجب استخدام المواجهة العسكرية كحل أخير بعد استنفاد كافة الطرق والوسائل لمواجهة هذه الجرائم.
- استغلال التنظيمات الإرهابية لمواقع التواصل الاجتماعي أصبح أحد الأدوات الرئيسية التي يستخدمها هؤلاء التنظيمات في عمليات الاستقطاب وإدارة العمليات الإرهابية. وتعتبر مواقع التواصل الاجتماعي بمثابة ساحة افتراضية تسمح للتنظيمات الإرهابية بالتواصل مع جمهور واسع وتأثيرهم بسهولة، وأحد الأساليب الشائعة للاستقطاب هو استخدام محتوى مشوه ومتطرف لجذب وتأثير الأفراد المهتمين أو المعرضين للتأثر. وتستخدم التنظيمات الإرهابية تقنيات التوجيه المستهدف والخوارزميات لتحديد الأشخاص ذوي الاهتمامات المشابهة وعرض المحتوى الإرهابي المختلف عليهم، ويهدف هذا الأسلوب إلى تعميق الانتماء والولاء للتنظيم وتحفيز التجنيد والمشاركة في الأنشطة الإرهابية.

التوصيات

- تعزيز العمل على تبادل المعلومات في وقتها وحوكمة الجانب العملياتي؛ بهدف تحقيق الإدارة المتكاملة للحدود، مؤكدة في الوقت ذاته أهمية تشجيع التعاون الثنائي والدولي وتبادل المعلومات فيما بين الفاعلين في الإدارة المتكاملة للحدود (سلطات إنفاذ القانون، القوات البحرية، خفر السواحل، الجمارك، الصحة، والنقل...)، والعمل على إنشاء دليل استرشادي لإجراءات تشغيلية موحدة، وتكثيف التعاون العربي والدولي في عمليات البحث والإنقاذ لضحايا تهريب المهاجرين.

- العمل على جمع وتخزين وتبادل المعلومات ولاسيما المسافرين والركاب من أجل استجابة فعالة واستباقية ووقائية وفقًا للمنظومة القانونية الدولية وقرارات مجلس الأمن الدولي، التي أقرت تسوية وضعية المهاجر غير النظامي وغير الآمن وغير المنظم إلى وضعية نظامية وآمنة ومنظمة وفق الأنظمة الشاملة والأوضاع الإنسانية، ومنح الأولوية لبرامج إعادة القبول والعودة الطوعية للمهاجر.
- تعزيز التعاون الدولي والتفاعل بين المؤسسات على الصعيدين الوطني والإقليمي لأنه يشكل أساسًا لضمان نجاح الإدارة المتكاملة للحدود ويتضمن هذا التعاون تبادل الممارسات والخبرات؛ حيث يتم تحديد التحديات والفرص المشتركة في مجال إدارة الحدود المتكاملة، وخاصةً فيما يتعلق بالتحديات المتعلقة بتهريب المهاجرين والاتجار بالبشر، كما يؤكد هذا التفاعل أيضًا ضرورة تأمين الحدود بطرق تلبي متطلبات الأمان، مع مراعاة عدم التعارض مع سهولة تداول البضائع والسياحة، وضمان حقوق الإنسان.
- تبرز أهمية التزام الدول الأعضاء بتطوير استراتيجيات إدارة الحدود المتكاملة على الصعيد الوطني، بهدف تحقيق نهج إقليمي مشترك يشدد على ضرورة إقامة مراصد لرصد ومراقبة النظم الحدودية، مما يعزز التعاون الفعال ويساهم في تطوير نهج إقليمي موحد.
- مراكز الإعلام بوزارات الداخلية: استحداث وسائل حديثة للترويج لاستخدام الخدمات الإلكترونية في إنجاز المعاملات بحيث تكون قريبة من الاستخدام اليومي للمستفيدين، وذلك من خلال آليات مختلفة متمثلة في إرسال رسائل نصية SMS على جهاز الهاتف المتحرك، أو بعمل مجموعات إخبارية معينة للحصول على آخر الأخبار السياسية والرياضية والاقتصادية كخدمة مجانية تقتطع تكلفتها من ميزانية الحملات الإعلانية لاستقطاب فئات معينة لها ميول واهتمامات مشتركة من شرائح المجتمع المختلفة، بحيث تتضمن هذه الأخبار بعض الأخبار عن المزايا والخدمات الحديثة، التي يقدمها الموقع، وذلك من خلال المركز الإعلامي الأمني لوزارة الداخلية.
- ابتكار أساليب ووسائل للتثقيف المجتمعي، ونشر الوعي بالشراكة مع مؤسسات المجتمع المتخصصة بأهمية التحول الإلكتروني، واستخدام المواقع الإلكترونية أو الهاتف في إنجاز الخدمات بصفة عامة، والمعاملات المرورية بصفة خاصة، وذلك من خلال تطوير وسائل للحماية تبث الشعور بالأمان لدى الجمهور لوجود بياناتهم وإنجاز معاملاتهم عن طريق الإنترنت أو الهاتف، وكذا إيجاد وسائل للتداول النقدي الإلكتروني محلية معتمدة وموثوقة من قبل الحكومة لتشجيع الجمهور للإقبال على الدفع النقدي الإلكتروني، مثل بطاقة الدرهم الإلكتروني.

- السعي لامتلاك الروبوتات القادرة على القيام بالمهام الأمنية الخطرة، وتجنيب العناصر البشرية الأمنية العديد من المخاطر لتدعيم الإدارة العامة للحماية المدنية.
- تطبيق أساليب تحليل البيانات وسلوك مستخدمي مواقع التواصل الاجتماعي وشبكة الإنترنت لمعرفة التوجهات المتطرفة للعناصر المتشددة، واستخدام برامج التحليل الجنائي المعلوماتي، وبرامج الأونست الدولية، بالإضافة إلى التعاون الدولي بشأن تحليل نتائج تلك البرامج، وتبادل المعلومات والخبرات فيها.
- تعزيز الوعي الأمني وتشجيع المجتمع وأفراده وتحذيرهم من المخاطر والتهديدات الداخلية والخارجية التي يتعرضون لها، وتشجيعهم على تبليغ الجهات الأمنية عن أي معلومات، أو ملفات، أو صور، أو متعلقات تفيد في قضايا العنف والإرهاب وتساعد في حماية أمن المجتمع والبلاغ عن أي أعمال إجرامية أو أفراد مشبوهين مباشرة مع الجهات الأمنية لتلقي البلاغات والشكاوى والمعلومات المفيدة.
- تدريب النشء والشباب في على كيفية الاستخدام الآمن لمواقع التواصل الاجتماعي من خلال دورات متخصصة يشرف عليها الخبراء والمتخصصون الوطنيون، وتنمية الوعي لديهم بخطورة الفكر الذي تبثه الجماعات المتطرفة والإرهابية على هذه المواقع.
- إطلاق مواقع دينية على مواقع التواصل الاجتماعي تعكس مفاهيم إنسانية راقية يمكن أن يكون لها تأثير إيجابي في نشر قيم الحب والتسامح والتعاون، وتساهم في إبراز الجانب البناء والسلامي للثقافة الإسلامية ومكافحة الأفكار المتطرفة.
- يجب على منصات الإنترنت تعطيل المحتوى غير المشروع وغير القانوني أو إزالته في غضون ساعة واحدة من الطلب، وبناءً على ذلك سيكون مقدمو الخدمات هم المسؤولون عن تقييم مدى التهديد وطبيعته، وبالتالي يقررون ما إذا كانت المفردات أو التعبيرات المخالفة تندرج تحت الخطاب القانوني أو غير القانوني.
- أهمية التنسيق مع الشركات المالكة لتطبيقات التواصل الاجتماعي؛ لوضع مدونة الممارسات العربية بشأن المعلومات المضللة والمحتوى المتطرف وغير الأخلاقي المتداول عبر هذه التطبيقات، ومنها تطبيق «تيك توك»، على أن يكون الغرض من المدونة تحديد الإجراءات التي يمكن أن تتخذ لمواجهة التحديات الأمنية، والترويج لخطابات الكراهية والعنف.

قائمة المراجع

أولاً - المراجع العربية:

1. **الكتب والمؤلفات:**

- حسنين توفيق إبراهيم، في تفسير استمرارية التنظيمات الجهادية الإرهابية: «داعش» نموذجًا، ترينـدز للبحوث والاستشارات، أبو ظبي، الإمارات، 202.
- طه محمد أحمد يوسف، «مستقبل الإدارة في عالم الذكاء الاصطناعي – إعادة تعريف الغرض والاستراتيجية في الثورة الصناعية الرابعة»، دار حميثرا للنشر، الطبعة الأولى، القاهرة، 2022.
- علي بن إبراهيم العلوي، تطبيقات الذكاء الاصطناعي في علوم الأدلة الجنائية، المجموعة العلمية لعلوم الأدلة الجنائية.
- علي بن ذيب الأكلبي، «البيانات الضخمة واتخاذ القرار، مشروع مستودع البيانات والجودة الإلكترونية «إتقان»، جامعة الملك سعود، الرياض، 2019.
- عمار ياسر البابلي، الذكاء الاصطناعي في مواجهة الشائعات وجرائم تمويل الإرهاب في البيئة السيبرانية «التداعيات وسبل المواجهة»، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، القاهرة، 2023.
- ممدوح عبد المطلب، خوارزميات الذكاء الاصطناعي وإنفاذ القانون، الجمعية الدولية للعلوم الشرطية، دار النهضة العربية، القاهرة، 2020.

2. **رسائل الدكتوراه:**

- أحمد محمد الجمال: «الإرهاب الفكري بين المواجهة المجتمعية والأمنية»، رسالة دكتوراه، كلية الدراسات العليا بأكاديمية الشرطة القاهرة، 2021.
- أحمد محمد صالح، تطبيقات الذكاء الاصطناعي ودورها في الإدارة الأمنية للحشود، رسالة دكتوراه، كلية الدراسات العليا، اكاديمية الشرطة، القاهرة، 2022.
- رامي متولي القاضي، مكافحة الإجرام المنظم عبر شبكة الإنترنت المظلمة: دراسة تحليلية في التشريع المصري، المجلة الجنائية القومية، المركز القومي للبحوث الجنائية والاجتماعية، القاهرة، نوفمبر 2022، المجلد 64، العدد 3.
- ضياء الدين محمد رضوان، التعاون المشترك بين الشرطة والجمهور وأثره على الأداء الأمني (دراسة مقارنة) العوامل وسبل الوقاية، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، 2018.

- كريم محمد محروس، «تطبيقات شبكات الإنترنت في تقديم الخدمات الشرطية ودورها في الارتقاء بالأداء الأمني»، رسالة دكتوراه مقدمة لكلية الدراسات العليا بأكاديمية الشرطة، 2021.
- محمد إبراهيم داود، سياسات ردع التهديدات غير التقليدية للأذرع الإرهابية، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، 2023.

3. **الدراسات والتقارير:**

- أنغوس كروفورد وتوني سميث، كيف يستخدم الذكاء الاصطناعي للاتجار بصور الاعتداء الجنسي على أطفال، تقرير لل BBC الدولية بتاريخ 28 يونيو 2023 ومتاح على:

https//:www.bbc.com/arabic/articles/clwd844084xo

- آلاء برانية، «تقرير المخاطر الرقمية: كيف يمكن حماية الأطفال في ظل الفجوة الرقمية بين الأجيال، المركز المصري للفكر والدراسات الاستراتيجية، القاهرة، 15 أكتوبر 2020 ومتاح على: https://:eg.com.ecss/11708/

- شبكات ومواقع ومنصات التواصل الاجتماعي وتجنيد الذئاب المنفردة ونشر فكرهم المتطرف العنيف، دراسة مقدمة من مرصد الفتاوي التكفيرية والآراء المتشددة، دار الإفتاء المصرية، بتاريخ 2019/1/14. للمزيد انظر الموقع الإلكتروني الآتي: https:// www.facebook.com/InfedilizingFatwas تاريخ الزيارة 2020/9/13

- إليسا أوروفينو؛ التطرف عبر الإنترنت: كيفية اكتشاف المحتوى المتطرف والتعامل معه (المملكة المتحدة نموذجًا)، تقرير موقع عين أوروبية على التطرف، 19 سبتمبر 2022 متاح على: https://eeradicalization.com/exploring-online-radicalization-how-to-spot-extremist-content-and-what-to-do-about-it/

- تقرير منظمة ال اليونيسكو بشأن المعلومات المضللة على شبكة الإنترنت: اليونسكو تكشف خطة عملها الرامية إلى تنظيم عمل منصات التواصل الاجتماعي، بتاريخ 6 نوفمبر 2023 ومتاح على الموقع الإلكتروني:https://www.unesco.org/ar/articles/almlwmat-almdllt-shbkt-khtt-tkshf-alywnskw-alantrnt-ml-tnzym-aly-alramyt-mlha-altwasl-mnsat

- تقرير الأمم المتحدة بشأن ادانة الهجوم الإرهابي على مسجدين في نيوزيلندا، وقع في مسجدي النور ولينوود في مدينة كرايست تشيرتش في نيوزيلندا اليوم الخامس عشر من مارس 2019، مما أدى إلى مقتل 49 شخصا وإصابة الكثيرين بجراح:

https://news.un.org/ar/story/20191028961/03/

- ماري شروتر، الذكاء الاصطناعي ومكافحة التطرف العنيف: كتاب تمهيدي، (لندن، تقرير صادر من الشبكة العالمية للتطرف والتكنولوجيا GNET المملكة المتحدة، 2022) ص 23- 34.
- نسيم رمضان، تقرير جريدة الشرق الأوسط الدولية: «إنتل» لـ«الشرق الأوسط»: التقنيات الجديدة تتطلب الجيل السادس من الإنترنت، لندن، 9 نوفمبر 2023 ومتاح على:

https//:aawsat.com/files/pdf/issue16419/

- علي القحيص، تقرير جريدة الرياض الدولية، سوق رائجة للمخدرات والأعضاء البشرية والرقيق الأبيض، تاريخ الزيارة 13 نوفمبر 2023 ومتاح على:

https//:www.alriyadh.com1569663/

- عبد الحفيظ يحيى خوجة، تقرير دولي حول مشاكل الإدمان، مروجو المخدرات يستغلون وسائل التواصل الاجتماعي لنشرها بين الشباب، جريدة الشرق الأوسط «صحيفة العرب الأولى»، الرياض، 9 يوليو 2020 ومتاح على:

https://aawsat.com/home/article/2380571/

- مجموعة أدوات الأمم المتحدة بشأن مكافحة المخدرات الاصطناعية، تقرير بشأن منصات البيع عبر الإنترنت، 9 نوفمبر 2023 ومتاح على:

https//:syntheticdrugs.unodc.org/syntheticdrugs/ar/cybercrime/onlinetrafficking/onlinesalesplatforms.html

- تقرير منظمة الإنتربول، عملية مكافحة لتهريب المخدرات تتيح ضبط كميات غير مسبوقة منها وتوقيف 1333 شخصًا وتقدر قيمة المخدرات المضبوطة بنحو ثلاثة أرباع مليار دولار أمريكي في 2022 – ومتاح على الموقع الرسمي للإنتربول:

https//:www.interpol.int/ar1333/2022/1/1/

- تقرير منظمة الأمم المتحدة بشأن الاتجار بمئات الآلاف من الأشخاص وإشراكهم في عمليات احتيال عبر الإنترنت بجنوب شرق آسيا، أغسطس 2023 ومتاح على الموقع الرسمي للإنتربول بالإنترنت:

https//:www.ohchr.org/ar/press-releases/08/2023/hundreds-thousands-trafficked-work-online-scammers-se-asia-says-un-report

- دراسة أمنية للإنتربول، الاتجار بالبشر للعمل في مراكز احتيال إلكتروني قد تحول من اتجاه إجرامي إقليمي إلى تهديد عالمي، بتاريخ 7 يونيو 2023 ومتاح على الموقع الرسمي للإنتربول بالإنترنت: https://www.interpol.int/ar/1/1/2023/20

- تقرير الإنتربول عن الإرهاب الصادر في نوفمبر 2023:

- https://www.interpol.int/ar/1/1/2023/illegal-wildlife-trade-has-become-one-of-the-world-s-largest-criminal-activities

- المنهج المرجعي لمكافحة الإرهاب، تقرير حلف الناتو لمكافحة الإرهاب، إصدار 2020، ص 33، ومتاح على : https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2020/12/pdf/2012-DEEP-CTRC-arabic.PDF

- فاطمة الزهراء عبد الفتاح، تقرير التهريب الرقمي: كيف تسهل وسائل التواصل الاجتماعي الهجرة غير الشرعية، مركز المستقبل للأبحاث والدراسات المستقبلية، أبو ظبي، 22 أغسطس 2023، ومتاح على:

https://futureuae.com/en-US/Home
Index/2/%D8%A7%D9%84%D8%B1%D8%A6%D9%8A%D8%B3%D9%8A%D8%A9

- شروع الاتحاد الأوروبي HTSM، تقرير مكافحة الاتجار بالبشر وتهريب المهاجرين في الاتحاد الأوروبي، 2023، ومتاح علي:
https://www.interpol.int/ar/4/10/HTSM

- تقرير المعهد الأمني الصيني: (Future of Life Institute. AI Policy China)، من خلال الموقع الإلكتروني التالي: https://futureoflife.org/ai-policy-china1/6/2023

- جيمس كلايتون، أبل ستفحص هواتف آيفون بحثًا عن أي محتوى مسيء جنسيًا للأطفال، تقرير لل BBC الدولية بتاريخ 6 أغسطس 2022 ومتاح على:

https//:www.bbc.com/arabic/science-and-tech58086401-

- كريس فالانس، تطبيق لحظر صور الاعتداء الجنسي على الأطفال يحصل على تمويل من الاتحاد الأوروبي، تقرير لل BBC الدولية بتاريخ 23 فبراير 2023 ومتاح على:

https//:www.bbc.com/arabic/science-and-tech64734567-

- محمود راغب، «القومي للمرأة» يكشف عقوبة جريمة الابتزاز وكيفية حصول الضحية على حقها، تقرير مؤسسة اليوم السابع المصرية، بتاريخ 15 ابريل 2023 ومتاح على:

https://www.youm7.com/story/2023/4/15/%D8%A7

- لاهاي (أ ف ب) عملية واسعة ضد الإنترنت المظلم والشرطة الأوروبية توقف 150 شخصًا – قناة فرنسا 24 نشرت في 2021/10/26 – ومتاح على:

https://www.france24.com/en/live-news/20211026-police-arrest-150-joint-in-dark-web-sweep-europe-us

4. **المجلات والمقالات:**

- إيمان رجب، سياسات مكافحة الإرهاب في مصر، مركز الدراسات السياسية والاستراتيجية، العدد 296، القاهرة، يناير 2019.

- حسام نبيل الشرنقاوي، التعاون الدولي في مكافحة استغلال الأطفال جنسيًا، مجلة الأمن والقانون، أكاديمية شرطة دبي، العدد الأول، يناير 2020، ص 201. ومتاح على:

- https://dubaipolice.ac.ae/dpacademy/ar/sada__acadmey/show__doc.jsp?doc__type=sum__file&book__id=137

- خالد كاظم أبو دوح، دور وسائل التواصل الاجتماعي في نشر الإرهاب، مجلة آفاق استراتيجية، مركز المعلومات واتخاذ القرار، رئاسة مجلس الوزراء المصري، القاهرة، العدد (2)، أكتوبر 2021.

- خالد كاظم أبو دوح، دور وسائل التواصل الاجتماعي في نشر الإرهاب والتطرف، مجلة درع الوطن الإماراتية مجلة عسكرية واستراتيجية تصدر عن مديرية التوجيه المعنوي في القيادة العامة للقوات المسلحة الإماراتية بتاريخ 1 مارس 2022.

- خلدون غسان سعيد، أعماق «الإنترنت المظلم»، استئجار قتلة وخدمات غير سوية لقاء عملات رقمية مشفرة، جريدة الشرق الأوسط، جريدة العرب الدولية، رقم العدد [15351]، لندن، ديسمبر 2021.

- سامح محمد الشريف، تحليل البيانات الضخمة في تحليل مواقع التواصل الاجتماعي، مجلة رؤى استراتيجية، مجلة علمية محكمة، المجلد السابع، العدد (19)، يونيو 2020.
- سعاد أغانيم، «خوارزميات الذكاء الاصطناعي والعمل القضائي قراءة في محاولات التجربة المغربية»، مجلة القانون والأعمال، ع 20، الرباط، المغرب، 2018.
- شريفة كلاعة، ظاهرة تجنيد الشباب في الجماعات الإرهابية من خلال استخدام شبكات التواصل الاجتماعي، مجلة مدارات سياسية، مجلة دولية محكمة نصف سنوية، العدد السادس، المجلد 2، الجزائر 2018.
- عمار ياسر البابلي، آليات الذكاء الاصطناعي في مواجهة التطرف العنيف، مجلة العلوم الشرطية والقانونية بأكاديمية شرطة الشارقة، مجلة العلوم الشرطية والقانونية: مجلة دورية علمية، العدد الأول، المجلد 14، 2023.
- مجدي الداغر، «دور الإعلام الجديد في تشكيل معارف واتجاهات الشباب الجامعي نحو ظاهرة الإرهاب على شبكة الإنترنت: دراسة ميدانية»، مجلة الآداب والعلوم الاجتماعية، الكويت، العدد 36، 2016.

ثانيًا ـ المراجع الأجنبية:

- Annual Report 2022 (INHOPE, 2023) Accessed from: https://inhope.org/media/pages/articles/annual-reports/14832daa35-1687272590/inhope-annual-report-2022.pdf 03/07/2023
- AT: https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact At: https://datareportal.com/ on 5/2023
- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinke B., & Amodei, D.The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Retrieved from. 2018.p56.
- Election Security Spotlight – The Surface Web, Dark Web, and 475 Deep Web (Center for Internet Security, n.d.) Accessed from: https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-the-surface-web-dark-web-and-deep-web 21/08/2023
- Eling, M.; Wirfs, J. What are the actual costs of cyber risk events? Eur. J. Oper. Res. 2019, 272, 1109–1119. www.scopus.com

- Elling, M.; Wirfs, J. What are the actual costs of cyber risk events? Eur. J. Oper. Res. 2019, 272, 1109–1119.www.scopus.com
- Ethical Tensions in Applications of AI for Addressing Human Trafficking: A Human Rights Perspective: Proceedings of the ACM on Human-Computer InteractionVolume 6Issue CSCW2Article No.: 295pp 1–29https://doi.org/10.1145/3555186
- EU Policy Cycle - EMPACTEMPACT 2022+ Fighting crime together Content typePAGE
- FACEBOOK STATISTICS AND TRENDS: Essential Facebook statistics and trends for 2022
- http://ecai.raai.org/lib/exe/fetch.php?media=malicioususeofai.pdf
- https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-full-rep/1680a73e49
- https://wearesocial-net.s3.amazonaws.com/wp-content/uploads/2021/01/05-Time-Spent-on-Social-by-Country-DataReportal-20210126-Digital-2021-Global-Overview-Report-Slide-90.png
- https://www.boldbusiness.com/digital/the-bold-impact-of-artificial-intelligence-in-law-enforcement/
- https://www.police1.com/police-products/investigation/drug-enforcement-software/articles/using-ai-to-overcome-the-challenges-of-investigating-digital-narcotics-supply-chains-CB8DekvGssjJYcm7/
- John McDaniel, Ken Pease , Predictive Policing and Artificial Intelligence
- Johnmichael O'Hare , Using AI to overcome the challenges of investigating digital narcotics supply chainsLaw enforcement agencies would do well to heed drug trafficking's technology-driven distribution systems , Police Drug Enforcement Software (Mar 30, 2021) at:
- Judges now using Artificial Intelligence to Rule on Prisoners, Science & Technology. February 07, 2018, https://learningenglish.
- Julia Deeb-Swihart, Alex Endert, and Amy Bruckamn. 2022. Ethical Tensions in Applications of AI for Addressing Human Trafficking: A Human Rights Perspective. Proc. ACM Hum.-Comput. Interact. 6, CSCW2, Article 295 (November 2022), 29 pages. https://doi.org/10.1145/3555186
- Lauren Vollinger. 2021. Concretizing intersectional research methods: Incorporating social justice and action into United States sex trafficking research. Journal of Human Behavior in the Social Environment 31, 5 (2021).

- LUCAS ROPEK, New Orleans Declares State of Emergency After Ransomware Attack, govtech, DECEMBER 16, 2019 on https://www.govtech.com/security/New-Orleans-Declares-State-of-Emergency-After-Ransomware-Attack.html.
- M. Aschmann, L. Leenen, J. Jansen van Vuuren, The Utilisation of the Deep Web for Military Counter Terrorist Operations. (Academic Conferences and publish- ing limited, s.l., 2022)
- Marie-Helen Maras and Alex Alexandrou. (2019). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. International Journal of Evidence & Proof, 23(3).
- Mario Cannataro, Pietro Hiram Guzzi, Artificial Intelligence in Bioinformatics ,From Omics Analysis to Deep Learning and Network Mining,1st Edition - May 12, 2022 at: https://www.scopus.com/
- Paolo Campana OF Online and technology-facilitated trafficking in human beings
- April 2022 ,Council of Europe at:
- REPORT OF UN about: Global Report on Trafficking in Persons
- Sarah Brayne. 2020. Predict and surveil: Data, discretion, and the future of policing. Oxford University Press, USA
- Shenoy, P., Arora, A., & Singh, M. (2018). Brain fingerprinting: Emerging trends in forensic science. Egyptian Journal of Forensic Sciences, 8(1), 22.
- Suicide, Incels, and Drugs: How TikTok's deadly 112 algorithm harms kids (Eko, 2023) Accessed from:https://s3.amazonaws.com/s3.sumofus.org/images/eko_Tiktok-Report_FINAL.pdf 02/08/2023
- The Annual Report 2022 (Internet Watch Foundation, 4792023) Accessed from: https://annualreport2022.iwf.org.uk/wp-content/uploads/2023/04/IWF-Annual-Report-2022_FINAL.pdf 17/08/2023
- The Bold Impact of Technology and Artificial Intelligence in Law Enforcement:
- The New Eyes of Surveillance: Artificial Intelligence and Humanizing Technology, Wired, accessed 23 Jan, 2020 https://www.wired.com/insights/2014/08/the-new-eyes-of-surveillance-artificial-intelligence-and-humanizing-technology/
- Tigran Hovsepyan. How Machine Learning Algorithms Are Used in The Justice System ,https://plat.ai/blog/machine-learning-algorithms-used-in-justice-system/ , at December 9, 2022

- UK Safety Tech Sector: 2022 analysis (UK Government, 2023) 352Accessed from: https://www.gov.uk/government/publications/safer-technology-safer-users-the-uk-as-a-world-leader-in-safety-tech/uk-safety-tech-sector-2022-analysis 18/08/2023
- United Nations Office of Drugs and Crime. 2020. 2020 UNODC Global Report on Trafficking in Persons
- What Is the Dark Web and Should You Access It? 474(Investopedia, 2022) Accessed from: https://www.investopedia.com/terms/d/dark-web.asp 21/08/2023
- www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf
- Zak Doffman, U.S. Military Satellites Likely Cyber Attacked By China Or Russia Or Both: Report, forbes, Jul 5, 2019, accessed 28 08, 2023 on https://www.forbes.com/sites/zakdoffman/2019/07/05/u-s-military-satellites-likely-cyber-attacked-by-china-or-russia-or-both-report/#28bd31e9dd32