الجرائم والجناة والضحايا المحتملين للميتافيرس والتقنيات الناشئة

بحث ميداني حول التصنيف، التنبؤ وأليات المواجهة

إعداد

د. أسماء جابر علي مهران

أستاذ علم اجتماع الجريمة المساعد

كلية الآداب - جامعة أسيوط

Email: asmaagabermahran@aun.edu.eg

DOI: 10.21608/aakj.2025.373973.2021

تاريخ الاستلام: ٩ /٣/ ٢٠٢٥م

تاريخ القبول: ١٣/ ٤/ ٢٠٢٥م

ملخص:

الغرض من البحث الراهن هو دراسة جرائم ومخاطر النظام البيئي للميتافيرس والتقنيات الناشئة، حيث يسعى البحث إلى تقديم تحليل سوسيولوجي عن الميتافيرس وتطبيقاته، ويستهدف استشراف والتنبؤ بالجرائم المرتبطة بالميتافيرس والتقنيات الناشئة، حيث يحاول البحث الإجابة عن الأسئلة التالية: ما سيناريوهات تهديدات الجرائم المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة؟ ما المخاطر الكامنة التي من المحتمل أن يتعرض لها الأطفال عبر الميتافيرس والتقنيات الناشئة؟ ما العوامل التي تدفع إلى ارتكاب الجرائم عبر الميتافيرس والتقنيات الناشئة؟ ما أليات وحلول مواجهة تلك الجرائم؟ ما مدى الاعتقاد بأن الميتافيرس والتقنيات الناشئة تؤدي إلى إساءة الاستخدام والتحرش؟ ما مدى القلق بشأن البيانات والخصوصية عبر الميتافيرس والتقنيات الناشئة؟ ما فئات الجناة المحتمل ارتكابهم للجرائم عبر الميتافيرس والتقنيات الناشئة؟ وما فئات الضحايا المحتملين لجرائم الميتافيرس والتقنيات الناشئة؟ واستنادًا إلى مراجعة منهجية الأدبيات السابقة، سعى البحث إلى الجمع بين الأسلوبين الأسلوب الكمي والكيفي لتحقيق التكامل المنهجي والشمولية في جمع البيانات؛ حيث استعانت الباحثة بمنهج المسح الاجتماعي على عينة عشوائية بسيطة من الشباب مستخدمي الميتافيرس بلغ عددهم (٤٠٤) مستخدم، كما عقدت مقابلات لعينة من الخبراء والنخب بلغ عددهم (٤١) خبيرًا في مختلف المهن، وممن لهم صلة بالميتافيرس والتقنيات الناشئة.

أظهرت نتائج البحث إنه بإجماع أراء الخبراء والمستخدمين من الشباب للميتافيرس؛ أن تهديد الجرائم المالية هي أقوى تهديدات الجرائم المحتمل ارتكابها عبر التقنيات الناشئة بمتوسط (٢.٧٣) للخبراء وبمتوسط (١.٨٥) للمستخدمين، يليها تهديدات الجرائم الجنسية في الترتيب الثاني عند الخبراء بمتوسط (٢.٧١)، وفي الترتيب الثالث عند المستخدمين بمتوسط (١.٧٩)، وجاءت تهديدات الجرائم ضد الأشخاص في الترتيب الثالث عند الخبراء بمتوسط (٢.٦٥) وفي الترتيب الثاني عند المستخدمين بمتوسط (١.٨٠)، وجاءت تهديدات الجرائم الأخرى في الترتيب الرابع عند الخبراء بمتوسط (٢.٦٣)، وفي الترتيب الثاني مكرر عند المستخدمين بمتوسط (١.٨٠)، وجاءت تهديدات جرائم الممتلكات في الترتيب الخامس عند الخبراء بمتوسط (٢.٦٢) وفي الترتيب الرابع عند المستخدمين بمتوسط (١.٨٠) من سيناريوهات تهديدات الجرائم المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة من وجهة نظر الخبراء والمستخدمين. حول سيناريوهات تهديدات المخاطر التي قد يتعرض لها الأطفال عبر الميتافيرس والتقنيات الناشئة، كشفت نتائج البحث أن تهديدات مخاطر المحتوى (وتعني المخاطر التي يتعرض فيها الطفل لمحتوى غير لائق أو قانوني، والمخاطر النفسية (الإحباط، القلق، الاكتئاب) أقوى تأثيرًا في المخاطر التي من المحتمل أن يتعرض لها الأطفال طبقًا لإجماع أراء الخبراء بمتوسط (٢.٨٥)، بينما من وجهة نظر المستخدمين، تبين أن تهديدات المخاطر النفسية (الإحباط، القلق، الاكتئاب) أقوى تأثيرًا طبقًا لإجماع أراء المستخدمين بمتوسط (٢.٠٧). وحول العوامل الدافعة إلى حدوث الجرائم عبر الميتافيرس والتقنيات الناشئة، أظهرت نتائج البحث أنه بإجماع أراء الخبراء والمستخدمين، أن العوامل العالمية هي أقوى العوامل الدافعة إلى حدوث الجرائم عبر الميتافيرس والتقنيات الناشئة بمتوسط (٢.٨٨) للخبراء، وبمتوسط (٢.٤١) للمستخدمين، يليها العوامل الفردية بمتوسط (٢.٧٦) عند الخبراء، وبمتوسط (٢.١٧) عند المستخدمين، وأخيرًا جاءت العوامل المجتمعية بمتوسط (٢.٧٠) عند الخبراء، وبمتوسط (٢.٠٨) عند المستخدمين. وحول الحلول والأليات المقترحة لمواجهة الجرائم والمخاطر المرتبطة بالميتافيرس والتقنيات الناشئة، أظهرت نتائج البحث أن الحلول القانونية والتقنية هي أقوى الحلول لمواجهة جرائم ومخاطر الميتافيرس والتقنيات الناشئة بمتوسط (٢.٩٧) من وجهة نظر الخبراء، وأن الحلول القانونية هي أقوى الحلول لمواجهة جرائم ومخاطر الميتافيرس والتقنيات الناشئة بمتوسط (٢.٨٠) من وجهة نظر المستخدمين من الشباب.

الكلمات المفتاحية: الجرائم، المخاطر، الجناة، الضحايا، الميتافيرس، التقنيات الناشئة.

Abstract :

The purpose of the current research is to study crimes and risks in the metaverse ecosystem and emerging technologies. The research seeks to provide a sociological analysis of the metaverse and its applications, and aims to anticipate and predict crimes related to the metaverse and emerging technologies. The research attempts to answer the following questions: What are the potential crime threat scenarios committed through the metaverse and emerging technologies? What are the potential risks that children are likely to be exposed to through the metaverse and emerging technologies? What are the factors that drive crimes through the metaverse and emerging technologies? What are the mechanisms and solutions to combat these crimes? To what extent is the belief that the metaverse and emerging technologies lead to abuse and harassment? What is the extent of concern about data and privacy through the metaverse and emerging technologies? What are the categories of potential perpetrators who commit crimes through the metaverse and emerging technologies? What are the potential victims of crimes related to the metaverse and emerging technologies? Based on a systematic review of previous literature, the research sought to combine quantitative and qualitative methods to achieve methodological integration and comprehensiveness in data collection. The researcher used the social survey method on a simple random sample of young people using the Metaverse, numbering (404) users. She also conducted interviews with a sample of (41) experts and elites in various professions, who are related to the Metaverse and emerging technologies.

The research results showed that, by consensus among experts and young users of the Metaverse, The threat of financial crimes is the strongest threat of potential crimes committed through emerging technologies, with an average of (2.73) for experts and an average of (1.85) for users. Sexual crimes threats are followed by experts, with an average of (2.71), and users, with an average of (1.79). Threats of crimes against persons came in third place for experts, with an average of (2.65), and users, with an average of (1.80). Other crime threats came in fourth place for experts, with an average of (2.63), and users, with an average of (1.80). Property crime threats came in fifth place for experts, with an average of (2.62), and users, with an average of (1.80) of the potential crime threat scenarios committed through the metaverse and emerging technologies, from the perspective of experts and users. Regarding the scenarios of risks that children may be exposed to through the Metaverse and emerging technologies, the research results revealed that the threats of content risks (meaning the risks in which the child is exposed to inappropriate or illegal content) and psychological risks (frustration, anxiety, depression) have the strongest impact on the risks that children are likely to be exposed to according to the consensus of experts' opinions with an average of (2.85), while from the users' point of view, it was found that the threats of psychological risks (frustration, anxiety, depression) have the strongest impact according to the consensus of users' opinions with an average of (2.07). Regarding the factors driving the occurrence of crimes through the Metaverse and emerging technologies, the research results showed that, by consensus of experts and users, global factors are the strongest factors driving the occurrence of crimes through the Metaverse and emerging technologies with an average of (2.88) for experts, and an average of (2.41) for users, followed by individual factors with an average of (2.76) for experts, and an average of (2.17) for users, and finally, societal factors came with an average of (2.70) for experts, and an average of (2.08) among users. Regarding the proposed solutions and mechanisms to address crimes and risks associated with the metaverse and emerging technologies, the research results showed that legal and technical solutions are the most powerful solutions to address crimes and risks associated with the metaverse and emerging technologies, with an average of (2.97) from the perspective of experts. Legal solutions are the most powerful solutions to address crimes and risks associated with the metaverse and emerging technologies, with an average of (2.80) from the perspective of young users.

Keywords: Crimes, Risks, Perpetrators, Victims, Metaverse, Emerging Technologies.

أولًا: المقدمة:

يتوسع الإنترنت في مختلف دول العالم بشكل متسارع، ونقل المجتمعات إلى عوالم مذهلة من الخدمات بمختلف أنواعها وأحجامها **(تقييم التهديد العالمي،٢٠٢٣ :٣)**.

ونلاحظ إنه خلال العقدين الأخيرين طرأت تحولات مهمة لشبكة الإنترنت عبر أجيال ثلاثة، كان الجيل الأول يتسم بوجود درجة من افتقاد المرونة والتركيز على مجرد نقل المعلومات وإتاحتها للاطلاع من مكان إلى آخر فقط، وكان أبرزها المواقع الإلكترونية والمنتديات وغرف الدردشة والمدونات، وجاء الجيل الثاني ليتيح القدرة على التفاعل مع البيئات والمحتوى الذي يمكن الاطلاع علية ونشرة بسرعة كبرى مع التطور في الخوادم ومراكز البيانات، مثل تطبيقات الشبكات الاجتماعية واليوتيوب والهواتف الذكية، وجاء الجيل الثالث للشبكة عبر التحول إلى الإنترنت اللامركزي، وعدم الاعتماد على احتكار الشركات التقنية الكبرى وإدارتها من قبل أشخاص أو مشغلين أخرين والاعتماد بشكل أكبر على تطبيقات الذكاء الاصطناعي والطابعات ثلاثية الأبعاد وتطوير نظارات الواقع الافتراضي ودمج الحواس في التفاعل عبر المنصات الرقمية.

وأصبح واقع شبكة الإنترنت يعاني من وجود تحديات تتمثل في وجود درجة من التعقيد التقني الذي يحول دون فهم طبيعة التحديات واتجاهاتها، وتصاعد دور الشركات التقنية الكبرى، والهيمنة على البيانات الشخصية للملايين والتعرض لحملات تخريبية واسعة الحدود**(عبدالصادق، ٢٠٢٢: ١-٢)**.

وتتمثل أحدث التقنيات في الذكاء الاصطناعي (Artificial Intelligence) والحوسبة السحابية (Cloud Computing) وإنترنت الأشياء (Internet of things) وسلسلة الكتل (Block chain) والواقع الافتراضي (Visual Reality) والواقع المعزز (Augment Reality) وغيرها من التقنيات المتكاملة ذات الإمكانيات الهائلة.
(القنبري، ٢٠٢١: ٢).

ويأت إلى جانب ذلك حقيقة تحول العالم الافتراضي إلى واقع وليس مجرد خيال علمي، حيث جاء ذلك مدفوعًا بالتطور الهائل في شبكات الاتصالات مثل الجيل الخامس

والجيل السادس، والتي تمثل بنية تحتية رقمية تستطيع أن توفر السرعة والكفاءة والاستيعاب للخدمات البشرية كافة، والتعامل بشكل أسرع مع معالجة الجرافيك والصور الرقمية والرسوم في الوقت الفعلي والخدمات السحابية وتطبيقات التتش فير والهوية الرقمية ومواجهة المشكلات التقنية أمام توسع شبكة الإنترنت، وتطور مشروع استخدام المعدات أو الأجهزة كوسيط لعملية الاتصال من خلال تطوير نظام اتصال فعال قائم على عملية الدمج بين الجهاز العصبي والأفكار والأجهزة التكنولوجية، ما من شأنه توظيف الحواس في عملية الاستخدام داخل الميتافيرس **(عبدالصادق،٢٠٢٢ :١-٢)**.

وتجدر الإشارة إلى أن الميتافيرس هو آخر ما توصلت إليه مسيرة البحث والاستكشاف للجمع بين التقنيات الحديثة والقديمة لبناء عالم (Metarerse) الذي أُعلن عنه في ٢٨ أكتوبر عام ٢٠٢١ من قبل أحد أكبر رجال الأعمال والمبرمجين في العالم (Mark Zuckerberg) مؤسس الرئيس التنفيذي لشركة (Face Book) وجاء في الإعلان إلى أنه سيتم تغيير اسم شركة (Face Book) إلى (Meta) وتستهدف ميتافيرس تحت هذا الاسم الجديد المساعدة في بناء إنترنت يوطد العلاقات الاجتماعية ويجسد التجارب، ويجعل المستخدم عنصرًا بداخلها وليس مجرد مشاهدًا لها **(القنبري، ٢٠٢١م:٢)**. إلى جانب تطوير بيئة رقمية تفاعلية تجري بالتوازي مع العالم المادي، ويأتي هذا في ظل تصاعد اتجاه الدمج بين البعد المادي والرقمي والبيولوجي للإنسان وتحويل ذلك إلى معطيات وبيانات ذات أبعاد استراتيجية **(عبدالصادق، ٢٠٢٢: ١)**.

حيث تعد تقنية الميتافيرس في الوقت الحالي واحدة من أبرز الموضوعات المتداولة في المجتمع التقني، وتعمل مجموعة من الشركات على تطوير هذه التقنية، وتشكيل مستقبلها، وتسعى عدة حكومات إلى اطلاق مبادرات للدخول إلى عالم الميتافيرس بما يتوائم مع توجيهات كل دولة وريادتها التقنية **(التقنيات الحديثة المعتمد على البيانات والذكاء الاصطناعي، ٢٠٢٣ :٥٨)**.

وناهيك عن ذلك لقد تم وصف الميتافيرس على إنه التكرار التالي للإنترنت، كما كان الحال مع ظهور الإنترنت، ولكن لا نعرف الاتجاه الذي سيتخذه الميتافيرس مثل

الإنترنت، فمن المرجح أن يستمر في التطور بشكل دوري متخذًا اتجاهات جديدة مع الأخذ في الاعتبار أن تطبيق القانون تاريخيًا كان بشكل عام أبطأ في تطوير القدرات والأدوات المتعلقة بالجرائم المرتكبة رقميًا، ومن ثم يجب علينا أن نبدأ في أقرب وقت ممكن في الاستعداد لظهور التحول الرقمي من منظور إنفاذ القانون.

ومع الاطلاق الأخير لمنصة Meta's Horizon Worlds في فرنسا وإسبانيا تقدم الشركة تجربتها العالمية الغامرة أو تجربة Metverse إلى أوروبا، فقد جلب مفهوم الميتافيرس انتباه الجمهور لتقوم كلًا من Google و Microsoft والعديد من الشركات الأخرى باستثمارات كبيرة في هذه التكنولوجيا ومع توقع تقرير الاقتصاد العالمي بقيمته (١.٦) تريليون يورو بحلول عام٢٠٣٠، ومع توقع أن يقضي (٢٥%) من الأشخاص ما لا يقل عن ساعة يوميًا في الميتافيرس، فمن المؤكد أن يكون لها تأثير على عدم آمن المواطنين وتكون شيئًا يجب على جهات إنفاذ القانون النظر فيه.**(Europol, 2022: 5)**

- **مبررات إجراء البحث الراهن:**

ويمكن الإشارة إلي أهم مبررات إجراء البحث الراهن علي النحو التالي:

- تزايد استخدام الإنترنت، ففي أبريل ٢٠٢٣م أصبح هناك (٥.١٨) مليار شخص بنسبة (٦٤.٦) من سكان العالم مستخدمين نشطين للإنترنت، وأن (٤.٨٩) مليار شخص منهم (٥٩.٩%) من سكان العالم مستخدمين نشطين لشبكات التواصل الاجتماعي بعد ما كان عددهم (٤.٢٦) مليار شخص عام ٢٠٢١.
- لقد أظهرت دراسة أجراها الاتحاد الدولي للاتصالات أن الشباب هم أصحاب السهم الأكبر في هذا الاتصال؛ حيث أصبحت نسبة (٧٥%) من الأشخاص الذين تتراوح أعمارهم بين (١٥و٢٤) عامًا في عام ٢٠٢٢ متصلين بالإنترنت مقاربة بنسبة (٦٨%) من بقية الفئات.
- تتجلى الفجوات بين الأجيال بشكل أوضح في أفريقيا حيث نسب المستخدمين المذكورة (٥٥% و٣٦%) على التوالي **(تقييم التهديد العالمي ٢٠٢٣ : ١٠)**.

- لقد جذبت مشاركة المستخدمين في العالم الافتراضي جمهورًا كبيرًا على مستوى العالم بما يتجاوز (٤٠٠) مليون مستخدم شهريًا كمتوسط فريد.
- أن (٥١%) من المستخدمين المذكورين تبلغ أعمارهم ١٣ عامًا أو أقل، وهو الأمر الذي يؤكد بدورة أن تقنية الميتافيرس تحظى بشعبية كبيرة بين جيل الشباب.
- إن نسبة هائلة تبلغ (٨٣.٥%) من مستخدمي تقنية الميتافيرس تقل أعمارهم عن ١٨ عامًا، ويعكس ذلك هيمنة الفئة السكانية الأصغر عمرًا، على إنه كلما زاد تبني تقنية الميتافيرس شيئًا فشيئًا؛ زادت هذه التقنية زخمًا وجاذبية بشكل كبير.

(سليمان وأخرون،٢٠٢٣ : ٢٢).

- يعتمد المجتمع الناجح بشكل كبير على استخدام التكنولوجيا من خلال شبكة الإنترنت، لقد تطور الإنترنت من Web 1.0 إلى Web 3.0 إلى أحدث تطور وهو الميتافيرس.
- إنه في عام ٢٠٢٢ تفاعل (١.٩٦) مليار مستخدم يوميًا عبر Meta، وتمسك كل مستخدم بـ ٣٣٨ صداقة في المتوسط، حيث حظى الميتافيرس باهتمام متزايد على نطاق عالمي مدفوعًا بالطلب المتزايد على تطبيقات Roblox, Micrsoft, Epic Games
- كما إنه بحلول عام ٢٠٢٦ سيقضي أكثر من (٢) مليار شخص ما يقرب من ساعة واحدة يوميًا على الأقل في الميتافيرس. **(Wang& Su &Yan, 2023)**
- بالإضافة إلى ذلك وجدت دراسة استقضائية أجراها مركز بيو للأبحاث وجامعة إيلون أن (٥٤%) من الخبراء يعتقدون أن Metverse سيصبح مكونًا يعمل بشكل جيد لنصف مليار مستخدم للإنترنت على مستوى العالم بحلول عام ٢٠٤٠

(Stavola, J&Choi, K, 2023: 3).

- وطبقًا لتقرير صادر عن شركة ديلونت بتكليف من شركة ميتا، يتوقع إنه في إطار زمني أطول يصل مداه لعام ٢٠٣٥، يمكن أن يؤدي اعتماد تقنية الميتافيرس إلى مساهمات سنوية بالأرقام التالية في الناتج المحلي الإجمالي العربي نتيجة المبادرات الحالية لاعتماد تقنية الميتافيرس، حيث في مصر تقدر بقيمة (١١.٦- ٢٢) مليون

دولار أمريكي، في الأردن بقيمة (٠.٩- ١.٧) مليار دولار أمريكي، في المغرب بقيمة (٢.٦ – ٥) مليارات دولار أمريكي، وفي الأمارات العربية المتحدة بقيمة (٨.٨ – ١٦.٦) مليار دولار أمريكي، في المملكة العربية السعودية بقيمة (٢٠.٢ – ٣٨.١) مليار دولار أمريكي، بالإضافة إلى مساهمات أخرى في دول أخرى.**(سليمان وأخرون،٢٠٢٣ : ٢٢)**.

- لقد كشف الصحفيون الاستقصائيون والآباء والجهات الفاعلة في مجال إنفاذ القانون عن خطورة إساءة الاستخدام على منصات الألعاب الاجتماعية ومنصات الميتافيرس؛ فقد تضمن التقارير عمليات اختطاف واستمالة جنسية وإساءة استخدام الصور الرمزية للأطفال، مع الإشارة إلى العديد من الحوادث على منصات Roblox, Minecraft. ففي الولايات المتحدة أُتهم مستخدم بالإتجار بالحبس واختطاف واغتصاب فتاة تبلغ من العمر ١٣ عامًاعلى منصة Roblox، وجاء هذا الحادث المأساوي بعد فترة وجيزة من تقارير أكدت أن المستخدمين على Roblox أنشأوا غرف جنسية صريحة تسمح بممارسة نشاط غير مناسب بين الأطفال والكبار.
- أن الأطفال يلعبون Roblox أكثر من غيرهم، وأن (٦٧%) منهم تقل أعمارهم عن ١٦ عامًا.
- في عام ٢٠٢٢م تم توثيق التحرش الجنسي بالقاصرين وترويجهم لمحتوى غير لائق على المنصات الافتراضية ومنها VR CHAT أحد التطبيقات الأكثر شعبية داخل متجر Metas Oculus Quest Store.
- كما وجد مركز مكافحة الكراهية الرقمي أن المستخدمين بما في ذلك القُصر يتعرضون لسلوك مسيء كل سبع دقائق على منصة VRCHAT.

(Gaming and the Metaverse, 2019:16-17).

- بالإضافة إلى ما سبق أظهرت النتائج زيادة عدد الحوادث المبلغ عنها بين عامي ٢٠٢٠ و٢٠٢٢، حيث تم إجراء مراجعة للمقالات الإخبارية من يناير ٢٠٢٠ إلى

يونيو ٢٠٢٢، وركزت المراجعة على ٨٠ كلمة رئيسة،وقد تم استخدام منصة أخبار Google، وقد أظهرت النتائج زيادة واضحة في عدد تقارير الوسائط حول إساءة الاستخدام على منصات الألعاب الاجتماعية ومنصات الميتافيرس سنويًا، وبينما تم العثور في عام ٢٠٢٠ على ستة تقارير إخبارية فقط فقد ارتفع العدد إلى ١٧ في عام ٢٠٢١، مع نشر ٤٦ تقريرًا في النصف الأول من عام ٢٠٢٢ وحده. هذا بالإضافة إلى إن شركة ميتا قد تلقت (٨٣.١) مليون حادثة تتعلق بمحتوى استغلال جنسي للأطفال على فيسبوك وانستغرام بين أبريل ٢٠٢١ ومارس ٢٠٢٢ وهو ما يمثل أكثر من ٢٣٠ ألف حالة يوميًا.

ثانيًا: إشكالية البحث وتساؤلاته:

لسوء الحظ عندما يتم تقديم خدمات جديدة فمن الشائع أن يتم تجاهل آثارها الإجرامية والأمنية أو معالجتها بشكل غير كاف، ويمكن أن يؤدي هذا إلى ما يشير إليه "بينز" باسم "حصاد الجريمة" حيث يستغل الجناة فرص الجريمة التي توفرها التكنولوجيا الجديدة، وقد لوحظ حصاد الجريمة للعديد من الخدمات في العقود الأخيرة، بما في ذلك المركبات في التسعينات، والهواتف المحمولة في العقد الأول من القرن العشرين، والعملات المشفرة، ومؤخراً يمكن إضافة الميتافيرس إلى هذه القائمة.

(Gomez–Quintero, [et.al], 2024: 2).

لقد أشار "مارشال وكلاركسون" إلى أن الجرائم المرتكبة ليست جديدة على الرغم من أن الطرائق قد تكون كذلك، كما خلصت دراسة سابقة إلى أن التكنولوجيا قد تسهل أو حتى توسع نطاق عمل إجرامي معين، فاستخدام التكنولوجيا هو امتداد وليس إنشاء أنشطة إجرامية. وقد أظهرت الأحداث الأخيرة مثل قضية (كامبريدج انا ليتيكا) وادعاءات التدخل في الانتخابات، أن الخدمات الجديدة عبر الإنترنت لا تسبب أنواعًا جديدة من السلوك المسيء أو الجريمة ولكنها تسهلها ببساطة بطريقة مشابهة لتلك التي شوهدت في وسائل الإعلام القديمة قبل ظهورها. ومع ذلك فإن الاستخدام الإجرامي أو التعسفي للتكنولوجيا ليس ظاهرة جديدة؛ ففي حالة الإنترنت هناك دودة موريس عام ١٩٨٨وتجربة

(كليفورد تسول) في تعقب المتسللين، اثنين من أكثر الأمثلة المعروفة لإساءة استخدام الكمبيوتر، ولكن ليس هناك شك في إن التكنولوجيا تعمل على زيادة القدرة على الوصول للمعلومات، أو تجعل التواصل بين الناس أسهل، أو تتلاعب بشيء ذي قيمة للبشر، سوف يتم فحصها من قبل أصحاب النوايا السيئة، وإذا أمكن سيتم تخزينها لتحقيق أهدافهم الخاصة. تشمل الأمثلة الأخرى على ذلك الاستخدام الإجرامي لتطبيق What's app وبرامج الاتصالات الأخرى، واعتماد تغذيات إدارة رسوم مكالمات الهاتف المحمول للتعتيم على العلاقات بين المتصلين، واستمرار إساءة الاستخدام الإبداعي لوسائل التواصل الاجتماعي لإخفاء هوية المتصلين، واستهداف الضحايا المحتملين واعتماد استخدام الويب المظلم، وما إلى ذلك، والحقيقة هي إنه منذ اصبح الوصول إلى الإنترنت متاحًا لعامة الناس فقد أصبح جذابًا للمجرمين بسبب العدد الكثير من الضحايا المحتملين الذي يقدمه، إلى جانب احتمال قيام المجرمين بإخفاء هوياتهم الخاصة بدرجات متفاوتة من النجاح **(Marshall & Tompstt, 2023: 12)**.

وتجدر الإشارة إلى إنه يتم ارتكاب الإساءة بواسطة مستخدمي الميتافيرس أو أولئك الذين يملكون البنية التحتية أو يقدمون خدمات الميتافيرس على سبيل المثال (في حلقة الألعاب من سلسلة مستقبل) يشير مقدم العرض إلى أنه إذا رغب المستخدمون في ممارسة العاب الواقع المعزز من منازلهم، فيستعين عليهم تقديم بيانات مكانية مفصلة حول هذه المساحات الخاصة، في هذا السيناريو هناك سؤال مهم يتعلق بالاستخدامات التي سيتم وضع هذه الأنواع من البيانات فيها من قبل أولئك الذين يجمعونها. ومن ناحية أخرى قد يتخبط مستخدموا الميتافيرس بأنفسهم في أنشطة ضارة مثل أشكال الجرائم الإلكترونية التي نراها تحدث بالفعل عبر الإنترنت والشبكات الاجتماعية مثل (عمليات الاحتيال والمضايقة واستخدام الروبوتات أو التنمر) ففي تقرير (Sum of Us) يصف المؤلفون العديد من الحوادث التي ابلغ فيها المستخدمون الذين يختبرون منصة (Meta's Horizon world) أن الصور الرمزية التي يتحكم فيها مستخدمون آخرون قد استخدمت مفردات عنيفة ومسيئة جنسيًا لمضايقتهم أو إجبارهم على ذلك، بالإضافة إلى

التفاعلات الجنسية الافتراضية وغير التوافقية (على سبيل المثال الاقتراب عن كثب من الصور الرمزية الانثوية ومحاكاة الأثارة) في حين أن العديد من الجرائم قد تكون ممكنة على الإنترنت كما نشهدها اليوم، فإن الطبيعة الغامرة للتحول من المحتمل أن تجعل تجربة بعض هذه الأضرار مثل جرائم الكراهية في الجرائم الجنسية أكثر صدمة.

(Gomez–Quintero,[et.al], 2024:4).

ونلاحظ إنه قبل تطوير الميتافيرس، كانت الجرائم الشخصية تهاجم شبكة الإنترنت السطحية؛ لقد القي القبض على أحد الأشخاص (٥٠ عامًا) بتهمة التنمر عبر الإنترنت ووجهت إليه ثلاث تهم تتعلق بالتحرش الإلكتروني بطفلة، والتحرش بها في مارس ٢٠٢١ لنشرها وسائط تم التلاعب بها لثلاثة أعضاء من فرقة التشجيع لأبنتها على الويب، حيث قامت سلطات إنفاذ القانون بمراجعة وسائل الإعلام وقررت إنها من إنتاج التزييف العميق، ومن ثم أمرت المحكمة بإكمال تقييم الصحة العقلية لتحديد أي مرض نفسي أدى إلى سلوكه الإجرامي، بالإضافة إلى ذلك حدثت مؤخرًا حالة من الجرائم المالية المتعلقة بالتزييف العميق؛ ففي شهر مايو٢٠٢٣ في الصين، حيث تبين إن الجاني استخدم تقنية التزييف العميق لمواجهة تبادل الصور وانتحال شخصية صديق الضحية أثناء مكالمة فيديو مما أدى إلى الاحتيال على الضحية لدفع (٤.٣) مليون يوان أي ما يقرب من (٦٢٢ ألف دولار) بالعملة الأمريكية، ويمكن توقع حدوث ذلك في الميتافيرس حيث يمكن استخدام التزييف العميق لانتحال شخصية أفراد آخرين أو صور رمزية، ارتكاب عمليات احتيال مالي مماثلة. **(Stavola, J & Choi,K, 2023: 4)**

ليس هذا فحسب بل أن الجرائم الشخصية آخذه في الارتفاع بالفعل في الميتافيرس وفي مقابلة مع قناة (CNBC TV 18) ذكرت "نيناجين باتيل" ٤٣ عامًا وهي معالجة نفسية أجرت بحثًا عن التأثير النفسي والفسيولوجي للميتافيرس، إنها تعرضت للتحرش اللفظي والنفسي من قبل أربعة تجسيدات ذكورية في الميتافيرس، وقد قاموا بعد ذلك باغتصاب الصورة الرمزية الخاصة بها، وأكدت الضحية على أن ردود أفعالها النفسية والفسيولوجية كانت واقعية مما جعلها تشعر وكأن الإساءة تحدث في العالم المادي. وأكدت

إنها تهدف إلى استخدام تجربتها لجعل الميتافيرس مكانًا أكثر أمانًا للأطفال، حيث يمكن أن يصبحوا الأطفال أهدافًا رئيسية للجرائم الإلكترونية عبر الميتافيرس.

(Stavola,J & Choi,K, 2023:4).

وعلى الرغم من أن تهديدات الجرائم السيبرانية قد تم دراستها إلا أن هناك الكثير من عدم اليقين بشأن الجرائم الفعلية التي يمكن حدوثها أو تنفيذها بواسطة الميتافيرس والتقنيات الناشئة، حيث هناك فجوة بحثية في توفير إطار نظري وميداني شامل لهذه الجرائم والمخاطر المحتملة الحدوث، إلى جانب أن توقع التهديدات المحتملة الحدوث أمر بالغ الأهمية في الوقت الحالي، بالإضافة إلى معرفة من هم فئات الجناة والضحايا المحتملين لتلك الجرائم، ومن ثم فإن ذلك سوف يساهم في تحديد آليات التصدي لها بشكل استباقي؛ الأمر الذي يساعد صُناع القرار وأصحاب المصلحة والجهات المعنية على الاستعداد لما قد يحدث ومعالجة مثل هذه التهديدات بشكل منضبط قبل انتشارها وظهور جرائم جديدة أخرى.

وبناءً على ما سبق تتمثل إشكالية البحث الراهن في الإجابة على التساؤل الرئيسي: ما أنماط الجرائم والمخاطر التي قد يتم ارتكابها عبر الميتافيرس والتقنيات الناشئة؟

ويتفرع من هذا التساؤل الرئيس التساؤلات الفرعية التالية:

- ما سيناريوهات تهديدات الجرائم التي قد يتم ارتكابها عبر الميتافيرس والتقنيات الناشئة؟
- ما سيناريوهات المخاطر الكامنة التي قد يتعرض لها الأطفال عبر الميتافيرس والتقنيات الناشئة؟
- ما العوامل الدافعة إلى حدوث الجرائم عبر الميتافيرس والتقنيات الناشئة؟
- ما الحلول والأليات المقترحة لمواجهة الجرائم والمخاطر عبر الميتافيرس والتقنيات الناشئة؟

- ما مدى الاعتقاد بأن المجال الافتراضي ومنصات التواصل الاجتماعي قد تؤدي إلى إساءة الاستخدام والتحرش؟
- ما مدى الشعور بالقلق بشأن الخصوصية عبر الميتافيرس والتقنيات الناشئة؟
- من هم فئات الجناة والضحايا المحتملين للجرائم التي قد يتم ارتكابها عبر الميتافيرس والتقنيات الناشئة؟

ثالثاً: أهداف البحث:

يتمثل الهدف الرئيسي للبحث الراهن في: التعرف على أنماط الجرائم والمخاطر التي قد يتم ارتكابها عبر الميتافيرس والتقنيات الناشئة.

ويتفرع من الهدف الرئيس الأهداف الفرعية التالية:

- رصد سيناريوهات تهديدات الجرائم التي قد يتم ارتكابها عبر الميتافيرس والتقنيات الناشئة.
- رصد سيناريوهات المخاطر الكامنة التي من المحتمل أن يتعرض لها الأطفال عبر الميتافيرس والتقنيات الناشئة.
- رصد العوامل الدافعة إلى حدوث الجرائم عبر الميتافيرس والتقنيات الناشئة.
- الوقوف على الحلول والأليات المقترحة لمواجهة المخاطر والجرائم المحتملة الحدوث عبر الميتافيرس والتقنيات الناشئة.
- تبيان مدى الاعتقاد بأن المجال الافتراضي ومنصات التواصل الاجتماعي قد تؤدي إلى إساءة الاستخدام والتحرش؟
- رصد مدى الشعور بالقلق بشأن الخصوصية عبر الميتافيرس والتقنيات الناشئة.
- الوقوف على فئات الجناة والضحايا المحتملين للجرائم التي قد يم ارتكابها عبر الميتافيرس والتقنيات الناشئة.

رابعًا: أهمية البحث:

الأهمية العلمية (النظرية):

- **فهم الأنماط الإجرامية:** إن دراسة الجرائم المحتمل ارتكابها في الميتافيرس والتقنيات الناشئة تساعد الباحثين على فهم الأنماط والتوجهات الإنسانية مما يساهم في تطوير نظريات جديدة في علم الجريمة.
- **نقطة قوة:** يعد البحث الراهن بمثابة نقطة قوة نتيجة الافتقار إلى الأدبيات السابقة حول هذا للموضوع؛ فهذا أول بحث يُجري على مستوى عربي – على حد علم الباحثة– لاستشراف سيناريوهات الجرائم المحتمل ارتكابها والمرتبطة بالميتافيرس والتقنيات الناشئة ودوافعها واليات التخفيف منها من منظور سوسيولوجي، ومن ثم يسد البحث فجوة نقص البحوث حول جرائم الميتافيرس.
- **مقابلة الخبراء والمستخدمين:** تعد مقابلة الخبراء والمستخدمين من الشباب للميتافيرس ومعرفة آرائهم حول التقنيات الناشئة والجرائم المرتبطة بها من الجوانب المهمة ونقاط القوة كذلك، حيث أن شهادات الخبراء سوف تكون بمثابة إطار قوي للتنبؤ والوقاية، حيث أن مصر مثل بقية دول العالم تشهد ارتفاعًا في عدد مستخدمي التطبيقات والتقنيات، الأمر الذي حظى باهتمام متزايد على نطاق عالمي مع بدء استخدام (Roblex).
- **على الرغم من الأبحاث الكثيرة العالمية حول الميتافيرس،** والتي ركز جزء منها على التطبيقات المرتبطة بها، وركزت أخرى على الجوانب الإيجابية المرتبط بها في مجالات التعليم والعمل والصناعة، وركزت ثالثة على الآثار الاقتصادية للميتافرس، وركز القليل على الأضرار والجوانب السلبية لها؛ جاء البحث الراهن ليسعى لمحاولة رصد سيناريوهات الجرائم والمخاطر المحتمل ارتكابها عبر الميتافيرس، وتسليط الضوء الجناة على الضحايا المحتملين لتلك الجرائم.
- **بناء إطار مفاهيمي:** يسعي البحث الراهن إلي بناء إطار مفاهيمي للمصطلحات والمفاهيم والمتغيرات التي يرتكز عليها، ويكون بمثابة أساساً نظرياً للبحث، ويساهم في

تصميم بحث مُنظم ومُنضبط من الناحية النظرية والمنهجية، كما يضمن أن البحث يقيس ما يراد قياسه، كما يساعد على تحديد الثغرات في المعرفة العلمية، وتطوير رؤي ونظريات جديدة.

- **من خلال توظيف نظرية الأنشطة الروتينية**، يسعى البحث الراهن إلى التوصل إلى مجموعة من الحلول والتوصيات بشأن التصدي للجرائم والمخاطر عبر الميتافيرس والتقنيات الناشئة.

الأهمية العملية (التطبيقية):

- **تطوير أدوات تحليل البيانات:** تتطلب التقنيات الناشئة توافر أدوات متقدمة لتحليل البيانات والتحقيق في الجرائم، ومن ثم نأمل أن تسهم نتائج البحث الراهن في تطوير برمجيات وأنظمة تعتمد على الذكاء الاصطناعي لكشف الجرائم قبل وقوعها مما يساعد في تدعيم القدرات الأمنية وتحقيق العدالة وحماية المستخدمين.
- **تحقيق الأمان السيراني:** من خلال دراسة الجرائم في البيئات الافتراضية يمكن توفير حلول فعالة لمواجهة التهديدات السيرانية، مما يسهم في تحسين إجراءات الأمان وتطوير استراتيجيات لحماية البيانات الشخصية والمؤسسية.
- **تدريب أجهزة إنفاذ القانون:** نأمل أن تسهم نتائج وتوصيات هذا البحث في تطوير برامج تدريبية لأفراد الشرطة وجهاز الأمن، حيث أن التعامل مع الجرائم في الميتافيرس يجب أن يتضمن معرفة شاملة بالتقنيات الجديدة وآليات التعامل مع الجرائم وكيفية التحقيق فيها.
- **تشريع قوانين جديدة وتعديل القوانين الحالية:** نأمل أن تساهم نتائج وتوصيات هذا البحث في سن قوانين وتشريعات جديدة تناسب البيئة الرقمية والتطورات التكنولوجية بالإضافة إلى وجوب تعديل القوانين الحالية، حيث تبرز الحاجة الملحة لقوانين مستحدثة تحمي الأفراد من النشاطات غير الأخلاقية أو الإجرامية التي يمكن أن تحدث عبر الميتافيرس والتقنيات الناشئة.

- تأتي أهمية هذا البحث في تعزيز الوعي المجتمعي حول المخاطر الموجودة في الفضاء الإلكتروني، وذلك عبر التعليم والإعلام حتى يتمكن الأفراد من حماية أنفسهم وفهم كيفية التفاعل بشكل آمن في البيئات الافتراضية.

خامسًا: مفاهيم البحث:

ارتكز البحث الراهن على عدة مفاهيم رئيسة يمكن تناولها على النحو التالي:

(١) مفهوم الجريمة الافتراضية والإجرام الميتافيرسي:

لا يوجد إجماع على تعريف الجريمة الافتراضية من حيث كيف تُعرف أو ماهي الجرائم التي تتضمنها الجريمة الافتراضية، حيث يقول (فان دير هلست ونيف) هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة.... وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية والرقمية وكلها تعكس فجوات مهمة في التعريف **(البداينة، ٢٠١٤ : ٣)**.

ويرجع عدم وجود تعريف جامع مانع للجريمة السيبرانية إلى عدد من الأسباب منها: تاريخ التطورات الإجرامية المصاحب لتطور تكنولوجيات المعلومات ونظم الاتصالات منذ بدايتها في القرن الماضي، حيث عرفت في أول الأمر على إنها جريمة إلكترونية تستهدف أجهزة نظم المعلومات، ثم عرفت على إنها جريمة معلوماتية، تستهدف البيانات والمعلومات المخزنة على نظم المعلومات، ثم عرفت أخيرًا بأنها جريمة سيبرانية بعد ما تم ربط نظم المعلومات بشبكة المعلومات الدولية وبالفضاء السيبراني. ويمكننا تتبع تطور المفهوم من خلال تسليط الضوء على الدور المزدوج للتطور التكنولوجي واختراق الشبكات لأطول فترة ممكنة،على النحو التالي **(الزنط،٢٠٢٢: ٢٠٣-٢٠٤)**:

- **استهداف نظام التلغراف السلكي عام (١٨٣٤):** إن الظهور الأول للإجرام الإلكتروني كان عام ١٨٣٤، حيث قام اثنان من اللصوص باختراق نظام التلغراف الفرنسي وسرقة معلومات خاصة بالسوق المالية الفرنسية، وكان ذلك أول هجوم إلكتروني عرفه العالم.

- **استهداف المكالمات الهاتفية:** في عام (١٨٧٠) قام مراهق بقطع الاتصالات وإعادة توجيه المكالمات الهاتفية بأسلوب **Switchboard Hack** واستخدام خطوط الهاتف الحكومية للاستخدام الشخصي في أمريكا، ويذكر أنه وبعد عامين من اختراع الكسندر جراهام بيل للهاتف (١٨٧٨) قامت الشركة في نيويورك بطرد عدد من العمال المراهقين بالشركة لقيامهم وبشكل متعمد قطع الاتصالات وإعادة توجيه المكالمات للاستخدام الشخصي.
- **استهداف نظام التليغراف اللاسلكي:** في عام (١٩٠٣) وأثناء عرض "جون أمبروز فليمنج" لاختراع التليغراف اللاسلكي – تكنولوجيات ماركوني Marconis للتليغرافات الأمنة– قام شخص يدعي "نيفيل ماسكلين "Nevil Maskelyne بإرسال رسائل مسيئة من شفرة مورس كان الغرض منها تشويه سمعة ومصداقية اختراع ماركوني.
- **أول استهداف للتشفير العسكري:** في عام (١٩٣٩) قام مخترع الحاسب الألي "آلان تورنج وجورج ويلشمان Gordon Welchman & Alan turing" باختراق شفرة النجمة Enigma codes الألمانية أثناء الحرب العالمية الثانية وذلك باختراع آلة كهروميكانيكية وقاما بفك رموز الشفرة مما ساعد الإنجليز على الانتصار في الحرب.
- **أول اختراق أخلاقي:** في عام (١٩٤٠) اكتشف "رينيه كارميل"Rene Carmille" عضو المقاومة في فرنسا التي احتلها النازيون وخبير الكمبيوتر بالبطاقات المثقوبة الذي يمتلك الآلات التي تستخدمها حكومة فيشي الفرنسية لمعالجة المعلومات، أن النازيون يستخدمون الآت البطاقات لمعالجة وتعقب اليهود والمتطوعين والسماح لهم باستخدامه، ومن ثم اختراقهم لإفشال خطتهم.
- **أول اختراق هاتف:** في عام (١٩٥٥) قام David Condon باختبار نظرية حول كيفية عمل أنظمة الهاتف Davy Crockett Cat ليكون أول جهاز Phone Hacker حيث يقوم نظامه على فكرة الرمز السري Password ويفترض أنه يمكن ربط أي هاتف متصل بنظام تشغيل ما بمشغل المسافات الطويلة وتوصيلة بأي رقم يطلبه مجانًا بعج ما يتم معرفة شفرة تشغيل نُظم الهواتف في مكان ما.

- **أول مُخادع عبر الهواتف:** في عام (١٩٥٧) قام صبي أعمى يُدعى "Joe Engressia " يبلغ من العمر ٧ سنوات باختراع طبقة صوت مثالية "صفير" يسمع من خلالها نغمة عالية على خط الهاتف ويبدأ في بثها عبر إشارة موجة طولها بتردد ٢٦٠٠ هرتز، مما يمكنه من التواصل مع خطوط الهاتف وأصبح أول مخترق هاتف مخادع في الولايات المتحدة.

وعلى امتداد تلك الفترة لم يكن ثمة تشريع يُجرم هذه الأفعال، وكان يُنظر إليها تارة على إنها ابتكارات جديدة في مسيرة تطور تكنولوجيا المعلومات والاتصالات وشغف الإنسان بها. أو ينظر إليها على إنها سلوك غير أخلاقي تارة أخرى؛ حيث أن الأمور بدأت تتغير منذ منتصف القرن العشرين. ولكن كانت الجرائم الحاسوبية جرائم محلية عمومًا، فقد حولت شبكة المعلومات الدولية الإنترنت Internet الجرائم الإلكترونية إلى جريمة دولية غير وطنية. وقد أتسم العقد الأول من القرن الحادي والعشرين بانتشار أساليب جديدة ومعقدة للغاية في ارتكاب الجرائم مثل التصيد الاحتيالي والاستخدامات لمستجدات الكمبيوتر مثل الحوسبة السحابية وغيرها من الشبكات والتطبيقات التي تخلق صعوبات أمام إنفاذ القانون.

كذا من العوامل التي أدت إلى عدم اتفاق على تعريف جامع مانع للجريمة السيبرانية، هو أن التعاريف وبصفة عامة تتوقف في المقام الأول على الغرض من استخدام المصطلح، فالجريمة الأساسية تتمثل في عدد محدود من الأعمال التي تمس سرية البيانات أو النظم المعلوماتية، الحاسوبية وسلامتها وتوافرها، أو الأعمال المرتكبة بواسطة الحواسيب لتحقيق مكاسب شخصية او مالية أو إحداث أضرار معينة بالضحية، بما في ذلك أشكال الجرائم المتصلة بالهوية وبمحتوى الحواسيب وغيرها، ومن ثم لا يمكن تطويعها بسهولة لتندرج ضمن تعاريف قانونية لمصطلح جامع لمفهوم الجريمة المعلوماتية **(الزنط، ٢٠٢٢: ٢٠٧).**

ويمكن تعريف الجريمة السيبرانية بأنها "كل سلوك غير مشروع و/ أو غير أخلاقي يستهدف النظم الألية أو الاجتماعية أو الإنسانية" ويستخدم الحاسب الآلي في

ارتكابه، سواء كان محاولة نسخ أو حذف أو إتلاف برامج الحاسب الآلي للغير، أو أي جريمة يكون تنفيذها ذي صلة بالقواعد المعلوماتية ومتعلق بالمعالجة الآلية للبيانات، والتي تلعب فيها نظم تكنولوجيا المعلومات وشبكات الاتصالات دورًا أساسيًا في ارتكابها. **(الزنط، ٢٠٢٢: ٢٠٩).**

فالجريمة الإلكترونية هي فعل ينتهك القانون، والذي يُرتكب باستخدام تكنولوجيا المعلومات والاتصالات (ICT) لإستهداف الشبكات والأنظمة والبيانات والمواقع الإلكترونية و/أو التكنولوجيا أو تسهيل ارتكاب جريمة. تختلف الجرائم الإلكترونية عن الجريمة التقليدية من حيث أنها "لا تعرف حدودًا مادية أو جغرافية" ويمكن تنفيذها بجهد أقل وسهولة أكبر وبسرعة أكبر من الجريمة التقليدية (على الرغم من أن هذا يعتمد على نوع الجريمة الإلكترونية) ويفرّق اليوروبول (٢٠١٨) بين الجرائم الإلكترونية والجرائم التي تعتمد على الإنترنت (أي الجريمة لا يمكن ارتكابها إلا باستخدام أجهزة الحاسوب أو شبكات الحاسوب أو غيرها من أشكال تكنولوجيا اتصالات المعلومات)، والجرائم الإلكترونية (أي الجرائم التقليدية التي تسهلها الإنترنت والتقنيات الرقمية).والفرق الرئيسي بين هذه الفئات من الجرائم الإلكترونية؛ هو دور تكنولوجيا المعلومات والاتصالات في الجريمة – سواء كانت هدف الجريمة أو جزءًا من طريقة العمل (modus operandi) للجاني. وعندما تكون تكنولوجيا المعلومات والاتصالات هدفًا للجريمة، فإن هذه الجريمة الإلكترونية تؤثر سلبًا على سرية وسلامة و/أو توافر بيانات أو أنظمة الحاسوب. كما تشكل السرية والنزاهة والتوافر ما يُعرف باسم "CIA Triad" ببساطة، يجب أن تظل المعلومات الخاصة خاصة، ولا يجب تغييرها دون إذن من المالك، ويجب أن تكون البيانات والخدمات والأنظمة في متناول المالك في جميع الأوقات. وعندما تكون تكنولوجيا المعلومات والاتصالات جزءًا من "M.O"، فإن الجريمة الإلكترونية تنطوي على جريمة تقليدية (مثل الاحتيال والسرقة) يتم تسهيلها بطريقة ما عن طريق الإنترنت والتقنيات الرقمية. كما يتم استكشاف هذه الفئات وأنواع الجرائم الإلكترونية التي تندرج تحتها بمزيد من التفصيل في الوحدة التعليمية الثانية للجرائم الإلكترونية حول الأنماط العامة للجرائم

الإلكترونية. وعلاوة على ذلك، يمكن ارتكاب الجرائم الإلكترونية من قبل الأفراد والجماعات والشركات والدول القومية. ففي حين أن هؤلاء الفاعلين قد يستخدمون تكنيكات مماثلة (على سبيل المثال، استخدام البرامج الضارة) ويهاجمون أهدافًا مماثلة (على سبيل المثال، نظام الحاسوب)، فإن لديهم دوافع مختلفة ونية لارتكاب الجرائم السيبرانية.
(Unodc,2013:13-15).

وتأسيسًا على ما سبق يمكن تعريف الإجرام الميتافيرسي الجديد بأنه "الأنشطة الإجرامية التي من الممكن ارتكابها من خلال العالم الافتراضي أو الانشطة الإجرامية المرتبطة بعالم الميتافيرس الافتراضي المستقبلي والذي بدأ بالفعل منذ أول تجربة له"، ونتيجة لظهور هذا النوع الجديد من الإجرام أصبح هذا العالم يمثل تحديًا حقيقيا في ميدان الضبط الاجتماعي المؤثرة في ارتكاب الجريمة الافتراضية.
(إبراهيم،٢٠٢٣: ٣١-٣٢)

ويستخدم مفهوم الإجرام الميتافيرسي إجرائيًا في البحث الراهن للإشارة إلى:

- الأفعال والممارسات والسلوكيات الغير قانونية أو غير الأخلاقية؛
- التي تنتهك القوانين المعمول بها سواء كانت محلية أو اقليمية أو دولية؛
- التي تحدث داخل البيئات الافتراضية من خلال واجهات تفاعلية؛
- مثل شبكات التواصل الاجتماعي أو الألعاب الإلكترونية؛
- والمنصات الاقتصادية الافتراضية؛
- والتي تعتمد على تفاعلات المستخدمين؛
- ويستخدم الجناة في هذه البيئة أدوات وتقنيات تكنولوجية؛
- مثل العملات الرقمية والتشفير لتنفيذ جرائمهم؛
- والتي تتراوح بين السرقات والتلاعب والتحرش؛
- إلى الجرائم الأكثر تعقيدًا كالنصب والتصيد الاحتيالي والاعتداء على الخصوصية.

(٢) مفهوم الميتافيرس:

يعود مفهوم العالم الافتراضي الذي يشار إليه حاليًا باسم Metavers إلى فترة من الزمن، وقد بدأ مع ظهور مجالات أو أبعاد متعددة المستخدمين المعروفة بوجودها منذ أواخر التسعينيات في ذلك الوقت وكانت تعرف باسم (MUDS) وكانت العوالم الافتراضية تأخذ شكل الألعاب النصية وقد تطورت (MUDS) لاحقًا إلى (Moos Mud Object Oriented) وهي تفاعلت اجتماعية افتراضية قائمة على النص بين المستخدمين، ثم تقديم الرسومات في الثمانينات وبدأت تكتسب شعبية في منتصف التسعينات. ومع ظهور الإنترنت وارتفاع شعبيته، ظهر شكل آخر من العوالم الافتراضية إلى الحياة، العاب لعب الأدوار متعددة اللاعبين عبر الإنترنت، العاب (M MOPRG) ومن الأمثلة البارزة (World of Warcraft) أو (UHIMA Online) وقد بدأت ألعاب (M MOPRG) هذه تتراكم شعبيتها في بداية القرن الحادي والعشرين حيث توفر للمستخدمين بيئة أكثر تعقيدًا ورسومات ثلاثية الأبعاد (شبيه بالواقع) ثم تقديم ألعاب. (M MOPRG) هذه بموضوع محدد، مثل الخيال أو الخيال العلمي، بينما كان بعضها موجهًا نحو الأطفال وتستمر الألعاب هذه في الازدهار اليومي مع أمثلة بارزة مثل عوالم (Minecraft, Epic, Games, Fortnite) و (Roblex) من (Microsoft) في حين أتاحت التكنولوجيا في بداية القرن الحادي والعشرين تجربة ألعاب أكثر حيوية، فقد حاولت بعض الشركات أن تأخذها إلى ما هو ابعد من تجريده اللعبة من خلال إنشاء عالم افتراضي، وربما كان ابرزها هو فيلم Linden الذي يتم إطلاقه رسميًا في أبريل ٢٠٠٣ وكان Second Life عبارة عن لعبة ثلاثية الأبعاد. **(Haber,2024:845–846)**

كمفهوم حديث لا يزال قيد التحديد ما هو أو ما سيكون عليه Metaverse حيث تميل المناقشات الأكاديمية إلى التركيز بشكل أكبر على الواقع الافتراضي، وقد استخدم الأكاديميين مصطلحات مثل العوالم الافتراضية، منصة تكنولوجية، فالميتافيرس مزيج من الواقع الافتراضي والمختلط ومساحة افتراضية مشتركة، وكنموذج جديد سينجح الإنترنت إنه يجمع بين العديد من هذه المصطلحات ليجادل بأن الميتافيرس هو" تقارب العوالم

المادية والرقمية في التطور التالي للإنترنت والشبكات الاجتماعية باستخدام برامج ثلاثية الأبعاد في الوقت الفعلي" **(Gomez–Quintero,[et.al], 2024:1)**، فمصطلح (Metaverse) هو اسم مركب لأحدث تطورات شبكة الويب العالمية.
.(Stavola,J & Choi,K, 2023:4)

ولا يفوتنا أن ننوه إلى أن الميتافيرس مصطلح صاغة في الأصل "نيل سيتفنسون Neal Stephenson" لروايته (Snow Crash) عام ١٩٩٢ والتي تصف منصة اجتماعية ثلاثية الأبعاد، لم تكن هذه المرة الأولى التي يتم فيها وصف مثل هذا الواقع الافتراضي، حيث سبق أن تم الدفاع عنه من قبل "دانييل جالوي" في (Simulacron–3) كمشروع اقتصادي، وقد تم تعريف الميتافيرس من قبل "ماثيو بول" بأنه مستمر ومتزامن ومباشر، مما يوفر لكل مستخدم إحساسًا فرديًا بالحضور واقتصاد يعمل بكافة طاقته، وجسر العوالم الافتراضية والمادية مما يوفر إمكانية التشغيل البيئي غير المسبوق للبيانات والعناصر والأصول الرقمية والمحتوى، مع مقارنتها بوسائل التواصل الاجتماعي الحالية؛ يظهر الميتافيرس على شكل بيئة ثلاثية الأبعاد مع صورة رمزية يتحكم فيها المستخدم **(Henz,2022:3)**.

وطبقًا لرواية (Snow Crash) تم وصف عالم الواقع الافتراضي (VR) الذي يتواصل فيه بطل الكتاب هيرو مع الآخرين ويتسوق ويهزم أعداء العالم الحقيقي من خلال صورته الرمزية، يصل هيرو إلى Metaverse باستخدام زوج من نظارات الواقع الافتراضي، وسماعة الرأس ويظهر داخل العالم الرقمي العالم كصورة رمزية. إن المساحات الافتراضية ستسمح للأشخاص بالاستكشاف والتفاعل مع عوالم افتراضية ضخمة باستخدام الصور الرمزية (على الرغم من استبعاد تجربة الواقع الافتراضي الغامرة التي تمثل حجر الزاوية في (Snow Crash) فهي موجودة بالفعل ومعظمها في شكل ألعاب الأدوار متعددة اللاعبين مثل (M MOPRGS) **(Huq, [et. al], 2022: 3)**.

إن كلمة (Metaverse) تجمع ما بين الكلمة الأولى وهي ميتا (Meta) وتعني ما وراء، أما الكلمة الثانية فيرس (Verse) وهي كلمة مصاغة من العالم أو الكون وبذلك يكون الاسم الكامل (الكون الماورائي) أو ما بعد الكون **(القنبري، ٢٠٢١: ٤)**.

ولا يوجد تعريف متفق عليه لتقنية الميتافيرس حتى الآن، إذ تحاول كل شركة مطورة لهذه التقنية تعريفها وفقًا لتطور الشركة ونتائجها. فعلى سبيل المثال تصف شركة ميتا (Meta) تقنية الميتافيرس بأنها: "انترنت مجسد يكون فيه المستخدم داخل التجربة وليس متفرج" بينما تصفها شركة مايكروسوفت بأنها "مشروع يتكون من توائم رقمية وبيئات محاكاة وواقع مختلط" **(التقنيات الحديثة المعتمدة على البيانات والذكاء الاصطناعي، ٢٠٢٣: ٥٨)**.

كما يعرف الميتافيرس بأنه عبارة عن بيئة تشغيل سحابية موزعة ومتعددة البائعين وتفاعلية وغامرة يستخدمها المستخدمون ويمكن الوصول إليها من خلال فئات مختلفة من الأجهزة المتصلة (سواء الثابتة والمتنقلة) وتستخدم ويب ٢.٠ وتقنيات الويب ٣.٠ لتوفير طبقة تفاعلية فوق الإنترنت المتاح. وهي منصة مفتوحة للعمل واللعب داخل بيئة (VR – AR- MR- XR) وهذا المفهوم مشابه لمنصات (M MOPRG) الحالية ولكن في حين أن كل لعبة من (M MOPRG) تمثل عالمًا افتراضيًا واحدًا خاصًا فإن الميتافيرس سيسمح للاعبين بالتنقل بسلاسة بين المساحات الافتراضية مع أصولهم الافتراضية **(Huq, [et. al], 2022: 5)**.

ومن المفاهيم الأكثر انتشارًا للميتافيرس مفهوم كلًا من Meta platforms ومفهوم Microsoft، حيث يشير مفهوم "Meta platforms" إلى أن الميتافيرس منصة مستخدم عالمية تدمج عددًا كبيرًا من الخدمات المعروفة من مواقع الويب الأخرى والعالم المادي في الميتافيرس لتعظيم وقت المستخدم الذي يقضيه على النظام الأساسي، وخلافًا لذلك تركز على الاستخدام المهني، وربط الشركات والتقنيات والعمليات والموظفين.

ويأتي مفهوم الميتافيرس مختلفًا من Microsoft وهو يستهدف بشكل أقل المستهلكين والشركات، بما في ذلك مشاركة بيئة Digital Twi ومنصة اتصالات الشركة Teams، حيث توفر التوائم الرقمية في الميتافيرس قدرة المتعلمين على تجربة نسخة تجريبية من الألة الفعلية وتعلم كيفية التعامل معها،ودراسة التأثير على التغيرات المحتملة، إن جسر العالم المادي والرقمي يمكن الموظفين من تشغيل آلة عن بعد داخل الميتافيرس، في حين أن هذه التغيرات تؤدي إلى أداء التؤام المادي.**(Henz, 2022: 3)**

كما يعرف الميتافيرس بأنه عبارة عن بيئة تفاعلية مبنية على تكنولوجيا blockchain والإنترنت التي تجمع بين الواقع الافتراضي والواقع المعزز والواقع الرقمي والواقع الفعلي، حيث سيتمكن الأشخاص في العالم المادي من التفاعل مع بعضهم البعض من خلال الصور الرمزية، هذه الصور الرمزية عبارة عن اشخاص افتراضيين ثلاثي الأبعاد تم إنشاؤهم ليصبحوا التوأم الرقمي ويمكنهم تقليد مشاعرنا ومظهرنا وتعبيرات الوجه والخصائص الشخصية باستخدامات التعلم الآلي.

.(Stavola, J & Choi, K, 2023: 4)

وينص تعريف الإنتربول بشأن (Metaverse) على أنه يعتبر المرحلة التالية في تطوير الإنترنت مدفوعًا بمجموعة واسعة من التقنيات بما في ذلك الواقع الافتراضي (VR) والواقع المعزز (AR) والحوسبة المتطورة، ويهدف إلى تمكين الأشخاص في جميع أنحاء العالم من الوصول إلى البيئات الافتراضية ثلاثية الأبعاد المشتركة باستخدام اتصال بالإنترنت وأجهزة متخصصة مثل سماعات الواقع الافتراضي أو البدلات اللمسية (مما يسمح للبيئة الافتراضية بتوفير اللمس وإجبار ردود الفعل للمستخدم عبر الاهتزاز أو تقيد الحركة) يمكن للأفراد دخول هذه المساحة الافتراضية عبر الصورة الرمزية مما يخلق إحساسًا بالانتماء(الحضور الافتراضي). ووفقًا لشركة (Gartner Inc) فإن الميتافيرس هي مساحة مشتركة افتراضية جماعية، تم إنشاؤها من خلال التقارب بين الواقع المادي والرقمي المعزز افتراضيًا. كما يعرف بانه شبكة واسعة النطاق وقابلة التشغيل المتبادل من عوالم افتراضية ثلاثية الأبعاد معروضة في الوقت الفعلي، والتي يمكن تجربتها بشكل

متزامن ومستمر من قبل عدد غير محدود من المستخدمين بشكل فعال مع إحساس فردي بالوجود، ومع استمرارية البيانات، مثل الهوية، التاريخ، الاستحقاقات، الأشياء، الاتصالات والمدفوعات. يقترح الميتافيرس إنه يمكن الجميع من التجسيد في عالم افتراضي والتواجد داخل الإنترنت بدلًا من مجرد الوصول إليه، فالميتافيرس عبارة عن مزيج من التجارب المترابطة. كما يرى "لابورد" أن الميتافيرس هو نسخة مستقبلية من الإنترنت، حيث يمكن الوصول إلى المساحات الافتراضية والمستمرة والمشتركة من خلال التفاعلات ثلاثية الأبعاد. كما يعرف الميتافيرس بأنه عالم ما بعد الواقع، وهو بيئة دائمة ومستمرة متعددة المستخدمين تدمج الواقع المادي مع البيئة الافتراضية الرقمية. ويرى أخرون أن الميتافيرس نوع جديد من تطبيقات الإنترنت، والشكل الاجتماعي الذي يتضمن العديد من التقنيات فهو يجمع بين العالم الحقيقي والافتراضي. ويشير المتخصصون إلى إنه يقدم نوعًا من الديمقراطية والعدالة لأنها تلغي حدود الزمان والمكان. فالميتافيرس عالم رقمي محقق بالكامل موجود خارج العالم الذي نعيش فيه. بمعنى آخر يشير الميتافيرس إلى مجموعة متنوعة من التجارب والأصول والبيئات الموجودة في الفضاء الافتراضي، وهو يشمل وسائل التواصل الاجتماعي، والعاب الفيديو حيث يمكن للاعبين بناء عالمهم الخاص، والتطبيقات الافتراضية الأخرى بما في ذلك Nfts والعملات المشفرة والصور الرمزية الرقمية، والواقع المعزز، والواقع الافتراضي.

(Smailia & Raymond, 2022: 190- 191).

وخلاصة القول فإن التعريفات المشتركة للميتافيرس تتمحور حاليًا حول فكرة "بيئة الإنترنت ثلاثية الأبعاد التي يتفاعل فيها المستخدمون الممثلون بالصور الرمزية مع بعضهم البعض في مساحات افتراضية منفصلة من العالم المادي الحقيقي".

(Marshall& Tompsett, 2023: 1).

ويوجد تشابه بين ملابسات ظهور مصطلحي الميتافيرس والفضاء السيراني الذي كان ثمرة الخيال العلمي أيضًا، وظهر عام ١٩٨٣ في رواية الكاتب الأمريكي الكندي (ويليام جيبسون William Gibson) وعنوانها (نيورومانسر Neuromancer) وقصد به

ثورة في تكنولوجيا المعلومات، شملت الحاسب والمعلومات وقواعد البيانات والأنظمة والبرامج وشبكات الإنترنت المفتوحة، والجمهور المستخدم، وينطبق أيضًا على الشبكات المفتوحة العامة، أو المخصصة لقطاع معين من دون الاتصال بالإنترنت، إذ يشمل الفضاء السيراني العالمين المادي والافتراضي، يدمج بينهما، ويمكن النظر إليه من زاوية محددة بصفته وطنًا افتراضيًا جديدًا، لا يمت بصلة إلى الجغرافيا كاسرًا كل الحدود.

ويمكن الإشارة إلى أوجه الاختلاف والاتفاق بين الفضاء السيبراني والميتافيرس على النحو التالي (يحيي،٢٠٢٢ :٣١):

جدول رقم (١) أوجه التشابه بين ملابسات ظهور مصطلحي الفضاء السيبراني والميتافيرس

أوجه الاختلاف	الفضاء السيراني	الميتافيرس
ظهور المصطلح	عام ١٩٨٤	عام ١٩٩٢
مصدر المصطلح	رواية (نيورومانسر) (Neuromancer)	رواية تحطم الثلج (Snow crash)
التصنيف	خيال علمي	خيال علمي
اسم المؤلف	ويليام جيبسون William Gibson	نيل ستيفنسون Neal Stephenson
الجنسية	أمريكي – كندي	أمريكي
الاختلاف	لا يتطلب تقنيات قابلة للارتداء ولا يشترط البعد الثلاثي	يتطلب تقنيات قابلة للارتداء وهو ثلاثي الأبعاد

والفرق بين الفضاء السيراني والميتافيرس؛ هو أن التفاعل في الأخيرة يعتمد على بناء الأجسام الرقمية أو الصور الرمزية والأفاتار اعتمادًا على تكنولوجيا قابلة للارتداء تنتج تفاعلات متعددة الحواس مع البيئات الافتراضية والأشياء الرقمية والأشخاص، وقد ارتبط ظهور المصطلحين بنزعة عكستها أدبيات الخيال العلمي آنذاك، حملت طابعاً استشرفياً يعكس ثقافة مؤلفي الخيال العلمي، التي توقعت ظهور نماذج تدمج الأنظمة البيئية المادية في التكنولوجيا، وتصنع نظاماً بيئياً ثالثاً يدمج النظامين بفاعلية، ومن ثم يعد مصطلح ميتافيرس إمتداد لمصطلح الفضاء السيبراني، مع إضفاء بُعد ثالث عليه، ولا يُعد من هذة الزواية إبتكاراً قائماً بذاته؛ ويبقي المصطلحان علي صلة برؤية خيالية لمبدعين في مجال الخيال العلمي، حملت بُعدًا استشرافياً تحقق لاحقًا **(يحيى،٢٠٢٢:٣٢)**.

وتلعب هذه التقنيات دورًا حيويًا في توفير وهم الحضور وتمكين المستخدمين من التفاعل مع الأشياء والبيئات كما لو كانت حقيقية.

ويستخدم مفهوم الميتافيرس إجرائيًا في البحث الراهن للإشارة إلى:

- تكنولوجيا تتيح إنشاء بيئات ثلاثية الأبعاد؛
- مثل الواقع الافتراضي (VR) والواقع المعزز (AR) والواقع المختلط (MR)؛
- التي يمكن الوصول إليها باستخدام نظارات (VR)؛
- وتمكن للمستخدمين من التواصل والتفاعل مع بعضهم البعض؛
- عبر شخصيات افتراضية (أفتار)؛
- كما يمكنهم شراء وبيع الأصول الرقمية والعقارات الرقمية؛
- وارتكاب الجرائم عبر البيئات الافتراضية؛
- مثل التحرش، التنمر، الاحتيال والسرقة.

(٣) مفهوم التقنيات الناشئة:

تشمل التقنيات الناشئة على مجموعة واسعة من الأنظمة والخدمات بما في ذلك الواقع الافتراضي (VR) والواقع المختلط (MR)، والواقع المعزز (AR)، فالبيئات الغامرة هي عوالم تم إنشاؤها بواسطة الكمبيوتر حيث يمكن للمستخدم أن يشعر وكأنه موجود في حين أن البيئات الغامرة في أوسع نطاق لها، يمكن أن تشير إلى البيئات التي ينمكن الوصول إليها باستخدام مجموعة من التقنيات بما في ذلك وحدات التحكم في الألعاب **(DRCF, 2023:2)**.

ويمكن الإشارة إلى البيئات الافتراضية ومفاهيمها على النحو التالي:

- **مفهوم الواقع الممتد (Extended Reality):**

هو مصطلح شامل يستخدم لوصف التقنيات الغامرة للواقع الافتراضي والواقع المعزز والواقع المختلط.**(Unicef, 2023:10)**

- **مفهوم الواقع الافتراضي (Virtual Reality):**

يرجع مفهوم المجتمع الافتراضي إلى (هاوراره دينجولد) (HowarhDheingold) الذي وضع كتاب بعنوان المجتمع الافتراضي (Virtual Community) حيث عرف المجتمع الافتراضي بأنه تجمعات اجتماعية تشكلت من أفراد متفرقة في أنحاء العالم، يتقاربون ويتواصلون فيما بينهم عبر شاشات الكمبيوتر والبريد الإلكتروني.

(سليمان، ٢٠٢٣: ١٩٨).

فالواقع الافتراضي عبارة عن واجهة مستخدم رسومية مصممة للسماح للمستخدمين بالتفاعل مع بيئة افتراضية محاكاة لمساعدة أجهزة الواقع الافتراضي المختلفة وتستخدم تكنولوجيا التفاعل متعدد الحواس، تكنولوجيا عالية الدقة لإنشاء بيئة افتراضية محاكاة ثلاثية الأبعاد، فالبيئة الافتراضية التي يتفاعل معها المستخدم غامرة للغاية لدرجة إنها تخلق تجربة سريالية مما يجعل المستخدمون يعتقدون أنهم موجودين فعليًا في البيئة الافتراضية وأن جميع التفاعلات التي تحدث في العالم المحاكي تحدث في الوقت الفعلي، وتستخدم تقنية الواقع الافتراضي أجهزة إدخال مصممة خصيصًا لذلك، مثل سماعات الواقع الافتراضي وجهاز المشي ٣٦٠ درجة، العصا، القفازات السلكية، أجهزة تتبع الحركة لمحاكاة تصرفات المستخدمين في البيئة الافتراضية، لقد تم توظيف تقنية الواقع الافتراضي على نطاق واسع لإنشاء ألعاب مثيرة مثل: (Second life & Half - Life Alyxgbatmen Arkham) **(Bale, [et. al], 2022:2).**

وتعد Oculus VR, Quest, Play Station من الأمثلة على سماعات الرأس الشائعة المستخدمة من قبل الأطفال. **(Unicef,2023:10)**

ويشير قاموس (وبيستر) العالمي إلى أن الواقع الافتراضي باعتباره الوجود في الجوهر أو التأثير ولكن ليس في الواقع؛ الواقع باعتباره حالة أو صفة يكون حقيقي، شيء موجود بشكل مستغل عند الأفكار المتعلقة به، وهكذا فإن الواقع الافتراضي هو مصطلح يناقض نفسه تناقض لفظي. كما عرف بأنه بيئة اصطناعية يتم اختيارها من خلال المنبهات الحسية مثل المشاهدات والأصوات التي يوفرها الحاسب الآلي أي أفعال الفرد تحدد جزئيًا ما يحدث في البيئة **(مصطفى، ٢٠٢٢: ١٠).**

- **مفهوم الواقع المعزز (Augmented Reality):**

هو عبارة عن تقنية تدمج العناصر الافتراضية في بيئة حقيقية يمكن للمستخدم التفاعل معها 3D في الوقت الفعلي وأهم خصائصه بأنه يجمع بين الواقعية والافتراضية والتفاعلية في الوقت الحقيقي. كما أن الواقع المعزز لا يدعي إنشاء عالم افتراضي على عكس الواقع الافتراضي، ويتم الوصول إلى الواقع المعزز بإستخدام معدات أكثر شيوعًا مثل الهواتف المحمولة ويقوم بتركيب صور مثل هذه الشخصيات أعلى الفيديو أو عارض الكاميرا وهو ما يمتلكه معظم المستهلكين بالفعل، مما يجعله أكثر قابلية للاستخدام للبيع بالتجزئة والألعاب والأفلام حيث يجمع الواقع المعزز بين العالم المادي والعناصر الافتراضية التي يتم انشاؤها بواسطة الحاسب الآلي، ثم يتم بعد ذلك إسقاط هذه العناصر على الأسطح المادية في الواقع ضمن مجال رؤية الأفراد، بقصد الجمع بين الاثنين لتعزيز بعضها البعض **(مصطفى، ٢٠٢٢: ١٥– ١٦)**.

فالواقع المعزز على عكس الواقع الافتراضي الذي يحاكي بيئة افتراضية، يعمل الواقع المعزز على تحسين كائنات العالم الحقيقي وإعادتها إلى الحياة من خلال الرسومات التي يتم إنشاؤها بواسطة الكمبيوتر وإنشاء تجربة تفاعلية الاستخدام هي الأكثر شيوعًا للواقع المعزز. **(Bale, (et. al,) 2022:2)**

لقد أصبح الواقع المعزز سائدًا في عام ٢٠١٦ مع ظهور لعبة (Poke' Mon, Go,13) وهي لعبة (AR) من إنتاج (Niantic)، ويمكن استخدام الواقع المعزز في العديد من السياقات في الألعاب والتسوق، حيث يمكنك تصور المنتج في منزلك قبل شرائه، والتعليم، حيث يمكن للطلاب والمعلمين تراكب المعلومات، المرئيات والمحتويات الأخرى، مثل تراكب الأحداث الماضية على المباني التاريخية.

(Unicef, 2023:10).

كما أتاحت لعبة البكيمون للمستخدمين السفر حول مدينتهم لالتقاط كائنات افتراضية تعرف باسم (Poke Mon) والتي تظهر فعليًا في بيئتهم المادية التي تمكن الأشخاص من تصور الأشياء الطبيعية التي تنبض بالحياة بطريقة ثلاثية الأبعاد من

خلال الشاشة يمكن مسح الكائنات وعرضها من خلال الهاتف الذكي أو حتى نظارات الواقع المعزز المصممة خصيصًا. تسمح هذه الأدوات للمستخدم بالتفاعل مع الكائن في العالم الحقيقي كما إنه لو أصبح واقعًا وبمجرد عرضه يتلقى المستخدم جميع المعلومات حول الكائن الذي يراه **(Bale, (et. al,) 2022:2)**.

- **مفهوم الواقع المختلط (Mixed Reality):**

هو ما يجمع بين العالم الحقيقي والعناصر الرقمية وفيه تتفاعل وتتحكم بالعناصر المادية والافتراضية بإستخدام تقنيات تولد الخيال والشعور ويسمح لك بالرؤية والتدخل في العالم الذي حولك حتى ولو كنت تتفاعل مع بيئة افتراضية باستخدام يديك بدون أن نخلع سماعات الأذن، وهو يزودك بإمكانية أن تملك رجل أو يد واحدة في العالم الحقيقي والأخرى في مكان وهمي وهو يتجاوز المفهوم المتعارف عليه بين الحقيقة والوهم، يوفر لك تجربة يمكن أن تغير الطريقة اليومية التي تلعب أو تعمل بها. حيث يعتبر الواقع المختلط ما هو إلا تطور هام للواقع المعزز وذلك على افتراض أن التقنية التي كانت وراء ظهوره عبارة عن بيئة هجينة يتم فيها إضافة عناصر أو أجسام افتراضية إلى البيئة المادية أي أنه يخلط بين الحقيقي والافتراضي، ويمكن للمستخدم أن يعيش في هذه البيئة الافتراضية ويغير مكان وحجم الأشياء ويتحكم بها. وفي حين تتشابه الفرضية الأساسية لكل من الواقع المعزز والواقع المختلط فإن الفرق الحاسم بينهما هو التقنية التحتية الضمنية، فالواقع المختلط حتى الآن يعتمد على سماعات الأذن، أما الواقع المعزز فهو مرئي من خلال شاشة مسطحة مثل الهاتف الذكي أو التابلت **(مصطفى، ٢٠٢٢: ٢٠)**.

ففي إعدادات الواقع المختلط، يمتزج المحتوى الرقمي في البيئة المادية؛ تتصرف الكائنات أو الشخصيات الافتراضية كما لو كانت حقيقية متفاعلة بالضوء والصوت والفضاء على سبيل المثال يمكن أن تظهر الأشياء المادية التي تحملها أيضًا في بيئة افتراضية، حيث يتم تصور أجهزة MR كأدوات من شأنها أن توفر قيمة لمختلف القطاعات بما في ذلك التعليم والتصنيع والصحة. وإلى جانب التقنيات الأساسية هناك حاجة إلى عناصر إضافية لتطوير النظام البيئي Metaverse، وكما يشير "ماثيوبول" إن

الإنترنت كما نعرفه اليوم يمتد إلى كل بلد، وهناك (٤٠) ألف شبكة، وملايين من التطبيقات، وأكثر من (١٠٠) مليون خادم، وما يقرب من (٢) مليار موقع ويب، وعشرات المليارات من الأجهزة... على الرغم من مرونة الإنترنت واسعة النطاق والقوية، لم يتم تصميمها للتجارب الحية والتفاعلية والتي تشمل عددًا كبيرًا من المشاركين، والخصوصية لضمان الثقة والبنية التحتية والأجهزة (من قوة الحوسبة الهائلة لعرض عوالم ثلاثية الأبعاد إلى أجهزة (XR) والمنصات لاستضافة المبدعين والمساحات ثلاثية الأبعاد) والمحتوى والتجارب (يمكن الوصول إليها عبر التطبيقات والعوالم الافتراضية) وتمثل كل طبقة من هذه الطبقات صناعات وقطاعات بأكملها، مما يشير إلى مدى تعقيد النظام البيئي في الميتافيرس **(Unicef, 2023: 11)**

جدول رقم (٢): الفرق بين الواقع الافتراضي – المعزز – المختلط

الواقع الافتراضي (VR)	الواقع المعزز (AR)	الواقع المختلط (MR)
تقنية تستخدم جهازًا يتم ارتداءه على الجسم مثل سماعة الواقع الافتراضي لوضع المستخدم داخل بيئة افتراضية تفاعلية.	تقنية تضيف محتوى رقميًا إلى المحتوى المرئي للمستخدم من خلال تراكب الكائنات الرقمية فوق كائنات حقيقية ولا تتفاعل هذه الأصول الرقمية مع بيئة المستخدم.	يجمع الواقع المختلط بين تجارب الواقع الافتراضي والواقع المعزز من خلال عرض البيئات الافتراضية والفعلية معًا والسماح للكائنات التي يتم إنشاؤها بواسطة الكمبيوتر التفاعل مع أشياء من الحياة الواقعية.

الجدول من إعداد الباحثة اعتمادًا على (Fredrisksson, 2023: 22)

ويستخدم مفهوم التقنيات الناشئة إجرائيًا في البحث الراهن للإشارة إلى:

- مجمل الابتكارات والتطورات التكنولوجية؛
- التي تتميز بالقدرة على أحداث تغيير ذي تأثير عميق في المجتمع؛
- مثل الذكاء الاصطناعي، الميتافيرس، إنترنت الأشياء والحوسبة السحابية وغيرهم؛
- الأمر الذي يتطلب إدراكًا شاملًا ليس فقط للفوائد الناجمة عنهم؛
- ولكن للتحديات والأثار السلبية والفرص الإجرامية التي قد توفرها مثل هذه التقنيات.

(٤) مفهوم الضحية في الإجرام الميتافيرسي:

الضحية مصطلح قديم يعود إلى ما قبل القرن الخامس عشر عندما كانت تتم الضحية لأجل الإلهة، يشار إليه باللاتينية (Victim) وفي أواخر القرن الخامس عشر

(١٤٩٥م) أصبح ذلك المصطلح يشمل الأشخاص الذين لحقهم الضرر سواء من النواحي الجنائية أو الاجتماعية أو النفسية **(مصطفى، ٢٠١٥: ٢٤٥)**.

لقد عرف الإعلان الصادر بشأن المبادئ الأساسية لتوفير العدالة لضحايا الجريمة وإساءة استعمال السلطة الصادر بموجب قرار الجمعية العامة للأمم المتحدة ٣٤/٤٠ والمؤرخ في ١٩٨٩/١١/٢٩ إنه يقصد بمصطلح الضحايا " الأشخاص الذين أصيبوا بضرر فرديًا أو جماعيًا بما في ذلك الضرر البدني أو العقلي أوالمعاناة النفسية أو الخسارة الاقتصادية أو الحرمان بدرجة كبيرة من التمتع بحقوقهم الأساسية عن طريق أفعال أو حالات إهمال يشكل انتهاكًا للقوانين الجنائية النافذة في الدولة الأعضاء بما فيها القوانين التي تحرم الإساءة الجنائية لاستعمال السلطة" **(الأمم المتحدة: ١٩٨٥)**.

ويشمل مصطلح الضحية حسب الاقتضاء العائلة المباشرة للضحية الأصلية أو معاليها المباشرين والأشخاص الذين أصيبوا بضرر من جراء التدخل لمساعدة الضحايا في محنتهم أو لمنع الإيذاء – تطبيق الأحكام الواردة هنا على الجميع دون التمييز من أي نوع كالتمييز بسبب العرق واللون والسن والجنس واللغة والدين والجنسية والرأي السياسي أو غيره والمعتقدات أو الممارسات الثقافية والملكية أو المركز الأسري والأصل العرقي أو الاجتماعي والعجز. وقد توسعت المحكمة الجنائية الدولية في تعريف ضحايا الجريمة بأنهم "من تم التعدي عليه في جريمة من جرائم الإبادة الجماعية أو الجرائم ضد الإنسانية أو جرائم الحرب أو جريمة من جرائم العدوان وضحايا الجرائم الخطرة وموضع الاهتمام الدولي" **(مصطفى، ٢٠١٥: ٢٤٦)**.

وتجدر الإشارة أن مصطلح الضحية يختلف عن المجني عليه، فإذا كان الأخير هو من تم التعدي عليه بشكل مباشر عن فعل يشكل جريمة معاقبًا عليها قانونًا، فالضحية قد يكون مجنيًا عليه في الجريمة، أو شخص لحقه ضرر ما، كضحايا العنف الأسري (المرأة والأطفال) وقد يكونون الورثة الذين لحقهم ضرر مباشر من جراء التعدي على مورثهم، ومن ثم يكون مصطلح الضحية أعم وأشمل نطاقًا من مصطلح المجني عليه، **ويتفرع عن ذلك النتائج الآتية: (مصطفى، ٢٠١٥: ٢٤٩)**.

- لا ينال من اعتبار الشخص ضحية من الجريمة أن تتوصل السلطات إلى مرتكب الفعل أو يظل مجهولًا وقد يكون قد صدر عليه حكم يقضي بمعاقبته عن الجريمة أو قضي ببراءته منها؛
- لا يقتصر مفهوم الضحية عن حد الشخص الذي وقع التعدي عليه بل يشمل أفراد أسرته ومن يعولهم وورثته، غير إنه يشترط في هؤلاء أن يكون قد أصابهم ضرر مباشر من جراء التعدي على الضحية؛
- لا يهم في اعتبار الشخص ضحية أن يتمتع بجنسية دولة معينة أو تكون له معتقدات معينة أو تتبع ديانة معينة، ومن ثم يعد ضحية كل من أصيب بضرر فردي أو جماعي؛
- يدخل في مفهوم الضحايا من تعرضوا للتعذيب السياسي.

ويمكن تفنيد الفئات الضحايا المجني عليهم فيما يلي:

- **المؤسسات المالية والجهات الحكومية:** ينجذب مرتكبي الجرائم السيرانية إلى القطاعات المالية لتنفيذ أفعالهم الإجرامية، فمن أكثر الأماكن استهدافًا؛ البنوك والمؤسسات المالية والبورصة، وذلك أن أي تعطيل في حركة البورصة يؤثر بدرجة كبيرة على حجم التعاملات المالية ليس فقط بين الأفراد بل قد يصل إلى التعاملات المالية والتجارية بين الدول.
- **الأشخاص الطبيعيون:** كثيرًا ما تعد شبكة الإنترنت المجال الخصب لارتكاب تلك الجرائم ضد الأشخاص الطبيعيين لاسيما ما يتعلق بالمساس بحق الخصوصية والبيانات الشخصية للأفراد، كما تعتبر جرائم الاتلاف المعلوماتي عن طريق الفيروسات من أكثر الجرائم التي يتعرض لها الأشخاص الطبيعيون عبر بريدهم الإلكتروني والذي يعتبر من أهم البوابات التي يقفز منها القراصنة إلى اجهزة الحواسب الخاصة بالأشخاص.
- **مقدمي الخدمات الوسيطة في شبكة الإنترنت:** وهم الأشخاص متعهدي توصيل المؤسسات والأشخاص إلى شبكة المعلومات الدولية الإنترنت، وقد يكون الأشخاص

والشركات الوسطاء ما بين الزبون والعميل وما بين شبكة الإنترنت هما ضحايا الجريمة المعلوماتية **(الزنط، ٢٠٢٢ :٢٥٨ – ٢٥٩)**.

ويستخدم مفهوم الضحية إجرائيًا في البحث الراهن للإشارة إلى:

- أي فرد أو جماعة أو كيان يتعرض لأنشطة غير قانونية أو ضارة؛
- ضمن البيئات الافتراضية؛
- مما قد يتسبب في أضرار نفسية أو مالية؛
- مثل تعرض الضحية للاختراق أو الاحتيال وفقدان الأصول الرقمية؛
- أو الإساءة النفسية والتعرض لمضايقات أو تهديدات؛
- أو الخسائر المالية أو الإضرار بالسمعة الشخصية.

(٥) مفهوم المجرم الميتافيرسي (الجناة المحتملين):

لقد تعددت المسميات التي أطلقت على هذه الطائفة من المجرمين بين قراصنة المعلوماتية، والهكر، والمجرم الإلكتروني، والمجرم المعلوماتي ومجرم الإنترنت، ومجرم التقنية. فالمجرم الإلكتروني هو المجرم الذي لديه القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الإلكتروني في ملحقاته ووسائل الاتصال الرقمية، وذلك بأداء فعل الامتناع عنه، مما يحدث اضطرابات في المجتمع الدولي والمحلي نتيجة لمخالفة الضبط الاجتماعي محليًا ودوليًا. أو هو مجرم سلك سبيل التقنية لارتكاب جرائمه والممثل في استخدامه لتقنية المعلومات.وتجدر الإشارة إلى أن هناك فرق بين مجرم الإنترنت ومجرم الحاسب الألي على الرغم من أن كل منهما يعتبران مجرما تقنيًا؛ فمجرم الإنترنت هو الهاكرز الذي يتخذ الشكل الخبيث له، في حين أن مجرم الحاسوب هو القرصان مرتكب جرائم العدوان على الملكية الأدبية والفكرية، مع تخصيص جزء لها تتعلق بمدى إمكانية التقنية في السيطرة على استخدام الحاسوب كما هو الشأن في اختراق كلمات المرور لملفات مشفرة مخزنة في الحاسوب، كل ذلك دون أن يكون الحاسوب مرتبطًا بالإنترنت يختلف هذا من جهة، ومن جهة أخرى فإن المجرم التقني عبر

الحاسوب لكونه مجرم لا يتمتع بمدراك علمية أو تخصصية ذات طابع أكاديمي إنما هو أبسط من ذلك بكثير إذ إنه يقترب إلى حد كبير من المجرم بالصفة. بالإضافة إلى أن سلوك ونشاط مجرم الإنترنت يرتبط بظاهرة الاختراق وهو يتمتع بمستوى مهاري خاص لا يمكن التوصل إليه من قبل جمهور العامة وعادة ما يتطلب تعليمًا إضافيًا مع التدريب **(بكوش& هروال، ٢٠٢١: ٧٦)**.

ويعود الفضل في تسمية الهكرة إلى كاتب الخيال العلمي الأمريكي (ويليام جيسون) عام ١٩٨٤ ويمكن القول إنه استدعى المرور بأربعة أجيال لكي يصل إلى مصطلح الإنترنت إلى ما هو عليه الآن من حيث الإجرام؛ فقد تشكل الجيل الأول لمصطلح الهاكر في فترة الستينيات من القرن العشرين ليتم إطلاقة على المبرمجين المبدعين من طلبة الحاسوب والاتصالات وبصفة خاصة طلاب معهد ماساشوستس للتكنولوجيا. ثم امتد ليطلق على مطوري علوم الحاسب وتقنية الاتصالات وقد مثل هؤلاء الجيل الثاني للهكرة في السبعينات. أما الجيل الثالث فقد ظهر في الثمانينات وأطلق هذا المصطلح على مخترقي الألعاب الإلكترونية وحقوق النسخ عبر خدمات شبكة الكمبيوتر، ويسمى هذا الجيل،جيل الحاسوب الشخصي. ثم تطور أخيرًا إلى ما هو عليه الآن ليستقر عند المجرمين والتافهين وهم العناصر البشرية للجيل الرابع **(بكوش& هروال، ٢٠٢١: ٧٧)**.

ويستخدم مفهوم المجرم الميتافيرسي في البحث الراهن للإشارة إلى:

- فرد أو مجموعة أفراد أو منظمات أو دول؛
- يستغلون بيئات الواقع الافتراضي المعززة، مثل العوالم الافتراضية؛
- وألعاب الفيديو متعددة اللاعبين، أو تطبيقات الواقع المعزز ؛
- ليقوموا بتنفيذ أفعال ضارة وغير قانونية؛
- ومن أمثلة السلوكيات الإجرامية لهؤلاء المجرمين؛
- التحايل والاحتيال في المعاملات الافتراضية مثل بيع أصول رقمية مزيفة؛
- القرصنة والدخول غير المصرح به إلى حسابات المستخدمين؛
- الاعتداءات الإلكترونية والتهديدات والمضايقات والتحرش؛

- وإنشاء وتوزيع محتوى غير قانوني أو مسيء ومروج للكراهية والعنف؛
- ضمن العوالم الافتراضية.

سادسًا: الأدبيات السابقة :

استراتيجية البحث:

(أ) قبل إجراء البحث تم تحديد مصطلحات البحث للوصول إلى أكبر عدد من الأبحاث والمقالات ذات الصلة وتمثلت المصطلحات التي تم البحث عنها في [الجرائم السيبرانية – الميتافيرس – الواقع المعزز – الواقع الافتراضي – الواقع الممتد – التقنيات الناشئة – الذكاء الاصطناعي – Blockchain] الأمر الذي من شأنه أن يوسع نطاق البحث، وتم البحث باللغة العربية واللغة الإنجليزية، وتم إجراء البحث على قواعد بيانات [GOOGLE-GOOGLE SCHOOLR]، بنك المعرفة المصري الذي يشمل على عدد من قواعد البيانات العربية والإنجليزية، وذلك لتحديد الأبحاث، الأطروحات، الكتب، والمجلات الأكاديمية، تقارير المنظمات الدولية والإقليمية والمحلية، وكافة المطبوعات العلمية حتى تتمكن الباحثة من الوصول إلى كافة أشكال الأدب ذات الصلة بالبحث الراهن.

(ب) لقد وجدت الباحثة عددًا كبيرًا من الأبحاث الأجنبية حول الميتافيرس سواء مشابه لعنوان البحث الراهن أو النص، ويعكس هذا الاتجاه اهتمام الباحثين المتزايد بالتكنولوجيا والتقنيات الناشئة والغرص والتهديدات المرتبطة بها.

(ج) ولأن البحث الراهن يركز على الجرائم والمخاطر المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة؛ قد قامت الباحثة بفلترة كل ما تم جمعه من الدراسات السابقة، وتم استبعاد الأوراق والدراسات والمقالات التي تحتوي على الكلمات الرئيسية، ولكنها ليست مُرتبطة مباشرة بإشكالية البحث الراهن.

(د) ثم تم الاحتفاظ فقط بالدراسات والأبحاث والمقالات ذات الصلة المباشرة بالبحث الراهن.

ويمكن الإشارة إلى الدراسات والبحوث ذات الصلة بالبحث الراهن على النحو التالي:

- **دراسة (دهشان، ٢٠٢٢) حول جرائم الذكاء الاصطناعي وآليات مكافحتها:**

تناولت الدراسة الدور الذي يلعبه الذكاء الاصطناعي في مكافحة والحد من الجرائم الجنائية بصفة عامة، فعلى الرغم من ظهور واستحداث جرائم جديدة مرتبطة بالذكاء الاصطناعي، فإنه في المقابل يمكن للحكومات تحقيق نتائج رائعة بشأن مكافحة الجرائم الجنائية جميعها عن طريق استخدام خوارزميات تلعب دورًا مزدوجًا؛ الأول منها إنها تستطيع تحديد معدل الجريمة المتوقع في منطقة معينة، وتحديد نطاق الميول الإجرامية للأشخاص من خلال معطيات معينة متعلقة بشخصيتهم وللبيئة المحيطة بهم، أما الثاني فيتمثل في لعب دور رئيس في عمليات جمع الاستدلالات والتحقيق والمكافحة. لقد توصلت الدراسة إلى أن هناك أشكال جديدة ستنتج عن تقنيات الذكاء الاصطناعي منها ما يتعارض مع القيم والتقاليد، والآخر يتعارض مع الدين، ويترتب على انتشار الذكاء الاصطناعي العديد من السلبيات والمشكلات التي تؤثر على المجتمع ككل مما يوجب على الدولة التدخل لمعالجتها.

- **دراسة (سعيد،٢٠٢٢) حول "المسئولية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي:**

أدى انتشار الذكاء الاصطناعي في كافة المجالات إلى تأثير واضح في حياة البشرية مما نتج عنه ظهور العديد من جرائم الذكاء الاصطناعي. لقد هدفت الدراسة إلى التطرق إلى قواعد المسئولية الجنائية والعقوبات على تطبيقات الذكاء الاصطناعي في حياتنا، وسلطت الضوء على تناول القانون الجنائي للمسئولية الجنائية لتلك التطبيقات من حيث القواعد القانونية المعترفة والعقوبات المناسبة. لقد توصلت الدراسة إلى تسارع معظم دول العالم في التسابق لإدخال كافة أنظمة الذكاء الاصطناعي في العديد من مجالات الحياة وباستخدام التقنيات الحديثة مما ترتب عليه ظهور الكثير من الجرائم الناتجة عن الاستغلال السيئ لتلك الأنظمة.

- **دراسة (Haber& Eldar, 2022) حول "التحول الإجرامي":**

أشارت الدراسة إلى الميتافيرس أو التحول الإجرامي بإعتباره تعطيلًا محتملًا للقانون الجنائي وإنفاذه على أرض الواقع. وهناك أسئلة حول ما يجب أن يشكل جريمة من

التحديات الجديدة لجهات إنفاذ القانون؛ لينظر إلى التحرش الجنسي كمثال اثناء السير في الشارع الافتراضي، حيث يلمس مستخدم آخر الصورة الرمزية الخاصة بالمستخدم بطريقة قد تشكل تحرشًا جنسيًا في العالم المادي، وعلى العكس لعب الفيديو أو استخدام المنصات السابقة إلى محاكاة العوالم الافتراضية، يمكن أن يكون Metaverse غامرًا مما يجعل مثل هذه الإجراءات تبدو حقيقًا للمستخدمين، فإن عواقبها تختلف بشكل كبير ويمكن أن تتطابق الشيء نفسه على الجرائم الجنائية الأخرى مثل السرقة والمطاردة والاغتصاب وحتى الاعتداء، والتي بصرف النظر عن الضرر الاقتصادي يمكن أن يؤدي إلى ضرر عقلي في حين أن الإنترنت يتيح أيضًا لارتكاب جرائم ضد الأفراد.

- **دراسة (Ortiz,2022) حول "مخاطر الميتافيرس، دراسة حالة VRCHAT."**:

تناولت الدراسة المخاطر الاجتماعية للميتافيرس وقد وجدت الأبحاث السابقة أن ألعاب الفيديو بما في ذلك الواقع الافتراضي (VR) يمكن أن يرتبط بتطبيع العنف وتمييز المرأة، علاوة على ذلك اشارت بعض الدراسات إلى أن منصات الألعاب تعمل أيضًا كأدوات للجماعات المتطرفة لتجنيد الأشخاص الضعفاء وتطرفهم ومع ذلك لم تتم دراسة هذه المخاطر بشكل أكبر في سياق الميتافيرس. لقد قامت الدراسة بتحليل الحالات ذات الصلة من منصات الألعاب المختلفة بما في ذلك "Horizon Worlds" علاوة على ذلك تمت دراسة لعبة "VR CHAT" نظرًا لتشابهها مع Metaverse من حيث التصميم والمميزات، تم إجراء تقييم لتجربة مستخدم "VR CHAT" من خلال تحليل المراجعات الأكثر شيوعًا على الرغم من عدم العثور على أي علامات للتطرف، إلا أن عددًا كبيرًا من هذه المراجعات عبرت عن مشاعر مثل الوحدة والاكتئاب مما يجعل الناس أكثر عرضة للتطرف، بالإضافة إلى ذلك تم العثور على ممارسات مثل التحرش عبر الإنترنت والانحراف الجنسي في اللعبة منذ عام ٢٠١٨م وحتى الآن. وتم إجراء مقابلة مع أحد أطباء النفس، وقد وجد أن مطوري ألعاب"VR" Chat لم يفعلوا ما يكفي لمعالجة سوء السلوك الجنسي بشكل فعال وحماية مستخدميه الأكثر عرضة للخطر، كشفت نتائج هذه الدراسة إلى أنه نظرًا لعدم وجود حوافز لدى مطوري الألعاب لتقييم منصاتهم بأنفسهم من أجل الصالح الاجتماعي وأن هناك حاجة إلى مزيد من التدخل من جميع أصحاب

المصلحة المعنيين وهذا يشمل صانعي السياسات وأولياء الأمور والأوصياء القانونيين والمعلمين.

- **دراسة (Bale, [et. al] 2022) "دراسة شاملة عن الميتافيرس وتأثيراته":**

أشارت الدراسة إلى أن الواقع الافتراضي (VR) والواقع المعزز (AR) أحدث ثورة في التكنولوجيا في العالم، كما انهم وضعوا الأساس للعديد من الابتكارات المستقبلية، وأنه يتم استخدام الواقع الافتراضي والمعزز على نطاق واسع لتحسين تجارب المستخدم في مختلف المجالات، وبمرور الوقت بدأت المزيد من الشركات في استخدام هذه التكنولوجيا المتطورة لتحسين منتجاتها وخدماتها، وفي الآونة الأخيرة لقد انفجر الاهتمام بالواقع الافتراضي والواقع المعزز مع ظهور Metaverse في وسائل الإعلام الرئيسية. لقد ركزت الدراسة على شرح مفهوم Metaverse وتاريخه والفوائد المرتبطة به من أجل فهم مخاوف الناس بشأن Metaverse وكيف يمكن أن يؤثر على البشر عقليًا وجسديًا ونفسيًا. لقد أجريت الدراسة الميدانية على مجموعة من المتخصصين في مجال الصحة مثل علماء النفس، والمعالجين، وأطباء الأعصاب، الأطباء في مجال الصحة العامة وغيرهم، للحصول على آرائهم حول Metaverse من أجل معرفة أفضل حول كيفية حدوث Metaverse وبعد التشاور مع المتخصصين في مجال الصحة، تم إجراء استطلاع عبر الإنترنت للحصول على فهم أفضل لآراء الناس حول Metaverse وكيف يعتقدون تأثيره على حياتهم. حصل الاستطلاع على أكثر من (٢٥٠) إجابة وكان معظم المستجيبين ينتمون إلى الفئة العمرية (٢٦– ١٥)، ولقد ساعدت النتائج في رسم صورة قوية للتأثيرات المختلفة التي يمكن أن تحدثها التحولات حقًا على الأشخاص، وأنهم يطورون شخصية مزدوجة أثناء انغماسهم في العالم الافتراضي ويؤثر بشدة على تصرفات الأشخاص وأن لدى المستهلكين العديد من المخاوف بشأن التأثيرات التي قد تحدثها الميتافيرس على حياتهم وقد تم التحقيق من صحة هذه المخاوف من قبل المتخصصين في مجال الصحة الذين قدموا فهمًا أوسع وأعمق لكيفية ارتباط هذه المخاوف وأهميتها بشكل كبير بالنسبة لصحة الناس وعافيتهم، فالاستخدام المكثف لـ Metaverse يمكن أن يضر العقل والجسم البشري.

- **دراسة (Henz, 2022) حول "التأثير المجتمعي للميتافيرس":**

ناقشت الدراسة فرص ومخاطر الميتافيرس بما في ذلك النظرة المستقبلية للتأثير المجتمعي المتوقع، نظرًا لأن الميتافيرس لم يظهر إلا في أجزاء أصغر حتى الآن، حيث هدفت الدراسة إلى مناقشة أكاديمية، وأكدت الدراسة إلي أن المفاهيم الفعلية مستوحاه على نطاق واسع من روايات الخيال العلمي الشهيرة. ولقد أشارت إنه حتى لو تم استخدام منصة Metaverse عالميًا يجب على المستخدمين الالتزام بالقوانين الموجودة في المنطقة الفعلية، وهذا أمر مهم، حيث تحدث الجرائم في الواقع الافتراضي على سبيل المثال أو السرقة أو إزالة الصور الرمزية أو اختطافها، إذا كان الجاني والضحية المحتملان من بلدان مختلفة قد يتم تطبيق القوانين بالإضافة إلى بعضها البعض، ويعتمد هذا على قوة الدولة في توسيع نطاقها القانوني دوليًا، وينظر إلى الصورة الرمزية على جزء فريد من المستخدم وأي نوع من العنف ضدها سيكون له تأثير ذي صلة على الشخص، بما في ذلك إذا تم ارتكابه أثناء وجود المستخدم خارج المنزل، حيث يجب أن تعد السلامة أمر مقصودة للإقامة داخل Metaverse ولكن أيضًا مع العواقب في العالم المادي، هناك أمرًا ضروريًا لجذب المستخدمين للبقاء. كما أشارت الدراسة أنه لم يتم أي شكل جديد من أشكال الاتصال الجماهيري محل الشكل السابق بشكل كامل، يمكن أن تعرض أن Metaverse لن يحل محل منصات الوسائط الاجتماعية الحالية ولكنه سيقلل من استخدامها، يعتمد الاختيار بين وسائل التواصل الاجتماعي و Metaverse على عوامل مختلفة مثل التكاليف والمحتوى والترويج من قبل المؤثرين المتصورين.

- **دراسة (Hinz ,2022) حول "المخاطر التي يشكلها Metaverse للأطفال المراهقون تحليل المحتوى الاستكشافي":**

تناولت هذه الدراسة أنواع المخاطر النفسية والفسيولوجية التي يمكن أن يشكلها استخدام Metaverse للأطفال والمراهقين من خلال إنشاء قاعدة معرفية مستمدة من الوضع الحالي للأدبيات والمقابلات مع الخبراء، حيث ركزت الدراسة في الإجابة على تساؤل رئيس: ما أنواع المحتوى أو السلوك غير المناسب للأطفال التي يمكن تحديدها في المساحات الاجتماعية أو مساحات الألعاب التي قد يواجهها الأطفال والمراهقين أثناء

اللعب؟ قامت الدراسة بالجمع بين المراجعة الأولية للأدبيات والمقابلات مع الخبراء، لتقديم رؤى حول كيفية المخاطر التي يواجهها الأطفال والمراهقين في البيئات الافتراضية، بعد ذلك تم تطوير إطار مفاهيمي لتوجيه تحديد وتصنيف أنواع مختلفة من المحتوى أو السلوك غير المناسب للأطفال الموجودين في مساحة التحول الاجتماعيVRCHAT وفي مساحة تحويل الألعاب. (Rec Room) بينت نتائج الدراسة أن هناك أنواع عديدة من المحتوى أو السلوك غير المناسب للأطفال وهي على سبيل المثال طبيعية، مهنية أو جنسية أو عنيفة، وتتراوح من التحرش اللفظي إلى الجسدي إلى أنواع التحرش البيئي. كما أثبتت النتائج أن Metaverse لا يوفر حاليًا بيئة آمنة للأطفال والمراهقين للمشاركة فيها، وأن انتشار المحتوى أو السلوك غير المناسب للأطفال واضح ويجب عدم تجاهله من قبل الآباء أو المطورين أو صانعي السياسات، لأنه قد تحدث اضرارًا نفسية أو فسيولوجية نتيجة دخول القاصرين إلى العوالم الافتراضية، ومن المحتمل أن تؤدي إلى عواقب طويلة المدى، وبالمقارنة مع وسائل التواصل الاجتماعي والألعاب عبر الإنترنت؛ هناك اتجاه واضح يمكن ملاحظته وهو أن الميتافيرس يعيد إنشاء مشكلات مماثلة تم فحصها بالفعل في تلك المساحات السابقة عبر الإنترنت، بالإضافة إلى حالة تفاقم بسبب عوامل الانغماس والتجسيد؛ فمن المتوقع حدوث تأثيرات أكثر خطورة للمضايقة والمحتوى أو السلوك غير المناسب من خلال تعرضهم لصدمات يمكن أن تؤثر بشكل عميق على حياتهم بأكملها. كما يتعرض القاصرون لخطر المعاناة من تغير في نمو الدماغ واضطراب عاطفي وجسدي دائم.

- **دراسة (سليمان & آخرون، ٢٠٢٣م) حول "الآثار النفسية والاجتماعية للميتافيرس وعلاقتها بالترابط المجتمعي":**

استهدفت الدراسة التعرف على الآثار النفسية والاجتماعية للميتافيرس على مستخدميه، والكشف عن آراء الخبراء فيما يتعلق بالآثار النفسية والاجتماعية للميتافيرس، إلى جانب تحديد مدى علاقة ارتباطية بين التعرض للميتافيرس والآثار النفسية والاجتماعية لاستخدامه، وذلك باستخدام أداة الاستبيان الإلكتروني وبالتطبيق على عينة قوامها (٢٠٠) مفردة من مستخدمي الميتافيرس و(٥٠) مفردة من الخبراء. توصلت الدراسة

إلى وجود علاقة ذات دلالة إحصائية بين مدى التعرض للميتافيرس والآثار النفسية لاستخدام الميتافيرس، كما توصلت الدراسة إلى أن دوافع التعرض للميتافيرس "لوصف مفهوم الاصدارات المستقبلية المفترضة للإنترنت، احتل الترتيب الأول بنسبة بلغت (٣٦%) ثم جاء بالترتيب الثاني تمكين "المستهلك تجربة واختيار المنتجات قبل الشراء، وجذب المستخدمين والوصول إلى جمهور أكبر" بنسبة بلغت (٣٢%) ثم يلي تلك بالترتيب الثالث "أداة تعليمية وترفيهية قوية من خلال تقديم المعلومات" بنسبة بلغت (٢٨%) ثم توالت باقي البدائل بنسب متتالية. لقد أوصت الدراسة بأن تقنية ميتافيرس التي يمهد لاستخدامها، ستخلق عالم افتراضي أكثر عزلة عن الواقع الحقيقي، رغم الرفاهيات التي ستوفرها في المقابل.

- **دراسة (Marshall & Tompsetl, 2023) حول "الميتافيرس- ليس هناك حدودًا جديدة للجريمة"**:

تم الإشارة في هذه الدراسة إلى أن النهج التفاعلي الغامر الذي يركز على الواجهة لتعريف Metaverse قد خلق تحديات خطيرة لأصحاب المصلحة في مجال الحماية العامة. قدمت الدراسة نهجًا بديلًا لتعريف Metaverse لأغراض الحماية العامة، وتركز الدراسة علي التفاعلات الرئيسية التي يفترض اصحاب المصلحة انها ستحدث في بيئات Metaverse المستقبلية.

ومن خلال القيام بذلك تم اقتراح ما يلي:

- سيكون الانتقال إلى الميتافيرس تدريجيًا وليس مفاجئًا؛
- إن مثل هذا التحول يجري بالفعل منذ عقود؛
- أن المخاطر الخطيرة المرتبطة بالحماية العامة منتشرة بالفعل على نطاق واسع؛
- التركيز على تكنولوجيا العرض المستقبلية قد يعنف أصحاب المصلحة في الحماية العامة في تحديد ذلك.

وفي النهاية أشارت الدراسة إلى أن الميتافيرس باعتبارها بيئة افتراضية غامرة، تتمتع بالقدرة على تسهيل الجريمة بنفس الطريقة التي تتمتع بها تقنيات الإنترنت الأخرى،

لأسباب ليس أقلها أنها مبنية على تلك التقنيات، التي لديها القدرة على توفير معلومات حول طبيعة الأعمال الإجرامية، على غرار المعلومات المستخرجة من الهواتف المحمولة والأجهزة اللوحية أو أجهزة الكمبيوتر الشخصية ولكنها ستكون مفيدة لتكوين برنامج الجهاز وقدرته على تسجيل مثل هذه المعلومات وقد تظهر فقط عرضًا محدودًا لتسجيل النشاط الذي تم تضمينه، وبالنظر إلى معظم الجرائم يتم التعرف عليها قبل الضحايا فإن هذا يؤدي إلى وضع تكون فيه الأجهزة التي سيتم فحصها هي في المقام الأول تلك الخاصة بالضحايا مما يؤدي إلى رؤية ضحايا متحيزين إلى حد ما للجرائم عبر الإنترنت.

- **دراسة (Stavola,J&Choi,K, 2023) حول "الضحية من قبل التزييف العميق في الميتافيرس، بناء إطار عملي للإدارة":**

قدمت الدراسة اقتراحًا للممتخصصين لاستخدامه في التخفيف من الجرائم الشخصية العميقة في الميتافيرس، وتوفر ايضًا الدعم للضحايا الذين يعانون من اضرار نفسية نتيجة لذلك، مع استمرار تطور التحول؛ ستزداد الحاجة إلى التخفيف والتدخل للتصدي الجرائم الإلكترونية مع وجود التزييف العميق باعتباره تهديدًا رئيسيًا. لهذا السبب تركز هذه الدراسة على مخاطر التزييف العميق في الميتافيرس وتوفر إطارًا للتدخل والوقاية. لقد تم اختيار خبراء الميتافيرس من كوريا الجنوبية من خلال طريقة أخذ عينات كرة الثلج للمشاركة في هذه الدراسة، يعزي التركيز الأساسي على الخبراء الكوريين الجنوبيين إلى الدعم الحكومي النشط للبلاد لمشاريع الميتافيرس عبر مجموعة من الصناعات، بالإضافة إلى التطوير الأخير لمنصات الميتافيرس العديدة كانت شهادات الخبراء هذه بمثابة الأساس لاطار هذه الدراسة حيث تم إنشاء حلول الوصاية القادرة على الأساليب القانونية والسياسية والتوعوية والتكنولوجية إلى جانب دعم الأدبيات السابقة، وقد وجد أن التزييف العميق يمثل تهديدًا متزايدًا لمستخدمي الميتافيرس وتحديدًا الأطفال المراهقين مما يستدعي ضرورة إقامة الإجراءات الجنائية وإنفاذ القانون ومواصلة تقديم العلاج النفسي للضحايا المتأثرين بهذه الجرائم. كما أشارت نتائج هذه الدراسة إلى أنه يمكن تطبيق نظرية الأنشطة الروتينية بنجاح لإنشاء إطار نظري، حيث يخدم كل مكون غرضًا عظيمًا لهذه الدراسة:

١- فهم المجرم المتحمس.

٢- فهم الهدف المناسب، ومزيد من مخاطر الإيذاء.

٣- الوصاية القادرة والتي كانت بمثابة مبدأ توجيهي لبنية إطار هذه الدراسة ساعد استخدام حراسة (RAT) القادرة في تطوير آليات مراقبة رسمية مناسبة لإدارة جرائم التزييف العميق في العالم الخارجي مثل تنفيذ القوانين الحياتية والملاحقة القضائية وآمن انفاذ القانون والمبادئ التوجيهية المجتمعية.

- **دراسة (Gomez – Quintero [et. al], 2024) حول" نطاق الجريمة التي يسهلها الميتافيرس":**

أشارت الدراسة إلى أن الميتافيرس هو تقارب ناشئ للتكنولوجيا مثل الواقع الافتراضي وblockchain الذي يُمكن المستخدمين من تجربة حقائق مختلطة/ موسعة لأغراض مشروعة مختلفة مثل الألعاب والسياحة والتصنيع والتعليم، ولسوء الحظ غالبًا ما يتم التغاضي عن الآثار المترتبة على الجريمة والأمن للتكنولوجيات الناشئة لتوقع الجرائم التي يسهلها التحول. قامت الدراسة بالإبلاغ عن نتائج دراسة تقنية المجموعة الأسمية (NGT) والتي تضمنت مراجعة حديثة النطاق الأدبيات الموجودة وتمارين الاستنباط مع مجموعتين من الخبراء (مجموعة من المملكة المتحدة وأوروبا) والأخرى تمثل إنفاذ القانون على المستوى الدولي مع مجموعة واسعة من الخبرات، تم تحديد مجموعة من (٣٠) تهديدًا بالجريمة في الأدبيات أو من قبل المشاركين. جاءت التقييمات لهذه الجوانب متسقة إلى حد كبير عبر العينتين مع تصنيف الجرائم الجنسية على سبيل المثال (مواد الاعتداء الجنسي على الأطفال) والجرائم المرتكبة ضد الأشخاص مثل جرائم الكراهية) على إنها تمثل أعلى المخاطر المستقبلية (أي كونها عالية الضرر والتردد العالي) وهو الأصعب في معالجتها. كما سلطت النتائج الضوء على فهم التهديدات الإجرامية الأكثر والأقل ضررًا المحتملة التي يمكن أن يسهلها الميتافيرس وبالتالي يساعد أصحاب المصلحة على تحديد أولويات الجرائم التي يجب التركيز عليها.

- **دراسة (Singh, 2024) حول "الجرائم الإلكترونية في الميتافيرس":**

أشارت الدراسة أن التطور السريع للتكنولوجيا أدى إلى ظهور مساحة افتراضية تسمى Metaverse حيث يتفاعل الناس ويتواصلون اجتماعيًا ويتواصلون مع بعضهم البعض وممارسة الأعمال في بيئة رقمية غامرة، في حين اصبحت العوالم الافتراضية جزءًا لا يتجزأ من حياتنا اليومية وأصبحت بيئة خصبة لجميع أنواع الجرائم الإلكترونية. هدفت الدراسة إلى استكشاف الجرائم الإلكترونية في العالم الافتراضي الذي هو عالمنا الرقمي، ودراسة القوى الاقتصادية والاجتماعية والسياسية التي تحرك العالم الافتراضي، حيث أن الأمور سيئة في هذه الفضاءات الرقمية. أن فهم الدافع وراء ارتكاب الجرائم الإلكترونية في العالم الافتراضي أمر بالغ الأهمية لتطوير استراتيجيات الوقاية والتخفيف، كما حاولت الدراسة فحص الإطار القانوني واللوائح الحالية لحل المشاكل الناجمة عن الجرائم الإلكترونية في العالم الافتراضي، وتقييم الحلول والممارسات الأفضل لزيادة الأمان في البيئة الافتراضية.

- **دراسة (Smaili &Raymand, 2024) حول "الميتافيرس سوق الاحتيال الجديد":**

تمثل الغرض من هذه الدراسة في دراسة مخاطر النظام البيئي، حيث تقدم هذه الدراسة لمحة عامة عن الميتافيرس وتطوره، وتناقش مخاطر الاحتيال المختلفة التي يشكلها على المنظمات، ونظرًا لمزايا الميتافيرس والاهتمام المتزايد الذي تجتذبه المنظمات فإن هذه الورقة تلقي الضوء على أهمية التخفيف من مخاطرها. واستنادًا إلى مراجعة منهجية للأدبيات المتعلقة بـ Metaverse وتحليل مثلث الاحتيال، ناقشت هذه الدراسة مخاطر الاحتيال المختلفة التي يشكلها الميتافيرس، وبشكل أكثر تحديدًا حللت هذه الدراسة ٢١ مقالًا عن الميتافيرس المنشورة بين عامي (٢٠٢١، ٢٠٢٢) وحاولت الإجابة عن أسئلة البحث التالية: ما المخاطر الكامنة في الميتافيرس أو ما مخاطر الاحتيال المرتبطة به؟ وما الفرص والضغوط التي يجلبها؟ وما هو المبرر الكامن وراء استخدامه؟ أجريت هذه الدراسة التحليل على مستويين؛ مستوى الفرد المستخدم، ومستوى المنظمة. وتلخص هذه الورقة نتائج المنشورات حول الميتافيرس في عامي (٢٠٢١– ٢٠٢٢) لإكتشاف تعريفاته المختلفة والفرص والمخاطر التي تمثلها. قدمت نتائج هذه الدراسة مناقشة ثاقبة

للمزايا والمخاطر التي يمكن أن يجلبها الميتافيرس نظرًا لأن التحليل يوضح أي منظمة يمكن أن تكون عرضة للمخاطر العكسية، فإن هذه الدراسة تزود المؤسسات باستراتيجيات الردع وكشف ومنع الاحتيال ومخاطر السمعة.

- **دراسة (Council of Europe and IEEE SA,2024) حول "الميتافيرس وتأثيرها على حقوق الإنسان وسيادة القانون والديمقراطية"**

هدف هذا التقرير الصادر عن مجلس أوروبا وجمعية معايير IEEE؛ وهي منظمة وضع معايير معترف بها عالميًا، إلى مساعدة الدول الأعضاء في مجلس أوروبا في فهم إمكانات الميتافيرس وتطبيقاته وما يرتبط به من المخاطر المتعلقة بحقوق الإنسان وسيادة القانون والديمقراطية، والنهج القائم على تطور التكنولوجيا، مع الاعتراف بعدم اليقين بشأن تطور المستقبل.واعتمد التقرير على ما يقرب من رؤى (٥٠ خبيرًا) والتي تشمل مختلف الجوانب الفنية والأخلاقية والقانونية والإدارية للمنظمة.

كشفت نتائج التقرير عن أن هناك نقص بشأن الطريقة التي سيتطور بها الميتافيرس بمرور الوقت، يعتمد التقييم الأولي حول تأثيره على مجموعة من المشكلات الحالية وغير المعروفة في التعبيرات الحالية للميتافيرس في العوالم الافتراضية والشبكات الاجتماعية ومنصات الألعاب وقد أشار التقرير إلى عدة نقاط مهمة للنظر فيها واتخاذ الإجراءات بشأنها ومنها:

- **إنه لا يوجد فهم مشترك حول الميتافيرس وتعقيده وتأثيره:**

يمكن أن يتم فهم أفضل لطبيعة وخصوصيات الميتافيرس من خلال رسم خريطة للنظام البيئي وأصحاب المصلحة والتقنيات المعنية والابتكارات المجاورة المحتملة والترابط والفجوات، مع إسناد المسئولية والمسائلة عبر مختلف المشاركين في النظام البيئي لخلق إطار شفاف وواضح، وإجراء تقييمات قصيرة ومتوسطة وطويلة الأجل لتأثير الميتافيرس من أجل تقييمات حقوق الإنسان والمخاطر التكنولوجية والأثر البيئي.

- **إن الميتافيرس هو عرضي في طبيعته ويمكن أن يغير نسيج المجتمع ذاته:**

إن المسئولية والقرارات المتعلقة بالقيم التي نريدها لمجتمعنا المستقبلي يجب أن تشمل

الجميع، هناك الحوار التشاركي والتشاور مع مختلف أصحاب المصلحة لتقييم القبول المجتمعي والمخاوف، من خلال إشراكهم في عملية التصميم والنشر والرقابة والحوكمة.

- **عدم ترك أحد حلف الركب – نحو تحول شامل ومسؤول:**

حيث يجب إعطاء الأولوية لفئات السكانية الضعيفة، بما في ذلك الاشخاص ذوي الإعاقة والأطفال والمسنين وجميع الفئات الأخرى المعرضة لخطر التمييز أو أن تكون أهدافًا للكراهية بناء على خصائصها الشخصية بما في ذلك النساء والأقليات، حيث تواجه فرصًا ومخاطرة فريدة في العالم الافتراضي، مما يتطلب استراتيجيات لضمان الشمولية والسلامة لهم داخل العالم الافتراضي.

- **إيلاء مزيد من الاهتمام لحماية الأطفال والشباب في الميتافيرس:**

إن تأثير التحول المتطور على النمو الجسدي والنفسي للأطفال يدعو إلى تحقيق التوازن بين التجارب الافتراضية والتفاعلات خارج الإنترنت، من أجل صحة جسدية وعقلية. للمساهمة في تجربة أكثر أمانًا ومسؤولية عبر الإنترنت للأطفال والكبار على حد سواء؛ يتم بذل الجهود التشريعية والتنظيمية عالميًا لمعالجة هذه الاعتبارات.

- **دراسة (Mclntosh,2024) حول "ما الذي يحتاجه صناع السياسات إلى معرفته حول التحرش في عالم الميتافيرس":**

أظهرت الدراسة إلى إنه على الرغم من أن الميتافيرس يتم وصفه غالبًا كتقنية "أفق المستقبل" فمن الواضح أن الإصدارات المبكرة من الميتافيرس موجودة بالفعل، وأن حالات المضايقة وسوء المعاملة تحدث مع عواقب وخيمة محتملة على المواطنين. لدى الحكومات فرصة للنظر بشكل عاجل في مدى ملائمة وفاعلية التشريعات القائمة، وتقييم ما إذا كانت الصكوك القانونية الجديدة، هناك حاجة لتعكس التجربة المميزة للبيئات المجسدة والغامرة والمتعددة للأشخاص، وقد يرغب صناع السياسات أيضًا في النظر في استراتيجيات المنع والإبلاغ والملاحقة القضائية، بالإضافة إلى مسائلة كل من الأفراد والمنصات/ مقدمي الخدمات فيما يتعلق بالسلوكيات المسيئة في بيئات الميتافيرس، يمكن لبرامج محو الأمية في الميتافيرس أن تزود أصحاب المصلحة والجمهور الأوسع بالمعلومات التي يحتاجونها للتصميم الجماعي والدعوة لمستقبل أكثر إيجابية لميتافيرس.

التحليل النقدي للأدبيات السابقة:

بعد عرض أهم الدراسات السابقة وثيقة الصلة بموضوع البحث الراهن، سوف تتناول الباحثة تلك الدراسات بالتحليل النقدي من عدة جوانب على النحو التالي:

(١) من حيث موثوقية الدراسات:

(أ) مصدرها:

تم تقييم موثوقية تلك الدراسات من حيث جهة إصدارها، وتبين أن معظمها دراسات أجنبية تنتمي إلى جامعات ومراكز أبحاث معترف بها، من قبل باحثين متخصصين في مجالات متعددة، جزء منها أبحاث فردية، وجزء منها أجراها مجموعة من الباحثين، وجزء آخر تقارير لمنظمات دولية ويعكس ذلك الاهتمام العالمي والإقليمي والمحلي بالظاهرة.

(ب) المنهجية وطريقة البحث:

- هناك حوالي ثماني دراسات من إجمالي الدراسات السابقة، قاموا بإجراء دراسات وثائقية، وتحليل التراث النظري السابق ومراجعة منهجية للأدبيات المتعلقة بالميتافيرس، والاعتماد على التقارير المختلفة المنشورة حول الميتافيرس.
- استخدمت حوالي ثلاث دراسات أساليب منهجية تجمع بين الأساليب الكمية والكيفية.
- اعتمدت أكثر من دراسة من الدراسات السابقة على أسلوب التحليل الإحصائي الكيفي حول ظاهرة الميتافيرس ومخاطرة، ومن أهم الأساليب التي استخدمتها تلك الدراسات المقابلات المتعمقة مع الخبراء.
- لقد استفاد البحث الراهن من تحليل منهجية الدراسات السابقة في تطوير منهجية البحث الراهن، واعتمد على إطار منهجي يجمع بين الأساليب الكمية والكيفية في التنبؤ بالجرائم والمخاطر التي قد يتم ارتكابها عبر الميتافيرس والتقنيات الناشئة.

(٢) المفاهيم والمصطلحات:

- لم يكن الميتافيرس شيء معروفًا بل كان خيالًا علميًا قبل عام ١٩٩٢، ومنذ ذلك العام

أصبح للميتافيرس معنى ودلالة وآثار مترتبة عليه، عندما قام "نيل ستينفسون" بالإشارة إلى الميتافيرس لأول مرة في رواية الخيال العلمي"Snow Crash".

- تم استخدم المفهوم للإشارة عالم افتراضي عبر الإنترنت، تمكن المستخدمين من تجربة واقع مختلف يجمع بين العالم الافتراضي والمادي كنوع من الواقع المختلط.
- من المفاهيم وثيقة الصلة بمفهوم الميتافيرس والتي أشارت إليها الدراسات السابقة: الواقع الافتراضي؛ الواقع المعزز ؛ الواقع المختلط؛ الواقع الممتد؛ التوائم الرقمية.
- لقد اعتمد البحث الراهن على مفهوم الميتافيرس ليشمل كل المزج بين العالم الافتراضي والمادي عبر سماعات الواقع الافتراضي ونظارات الواقع المعزز، وتطبيقات الهواتف الذكية وغيرها، لإنشاء بيئات افتراضية تحاكي البيئة الواقعية يمكن من خلالها التعلم واللعب والتجارة وارتكاب الجرائم أيضًا.

(٣) التوجه النظري:

- لم تحدد الغالبية العظمى من الدراسات التي تم الرجوع إليها في البحث توجهًا نظريًا تنطلق منه، وقد يرجع ذلك إلى عدم تخصص باحثي تلك الدراسات في تخصص علم الاجتماع، حيث هناك تنوع بين باحثين في مجال القانون، والهندسة، والاقتصاد والإعلام وعلم النفسي وغيرهم، الأمر الذي ترتب عليه عدم وجود إطار نظري لتلك الدراسات.
- اعتمدت حوالي ثلاث دراسات على توجه نظري انطلقت منه الدراسة، حيث تم الاستعانة بنظرية النشاط الرتيب أو الأنشطة الروتينية في تفسير جرائم الميتافيرس، واعتمدت أخرى على نظرية ثراء الوسيلة وهي نظرية إعلامية.
- لم تهتم معظم نتائج الدراسات السابقة بربط نتائجها في ضوء إطار نظري محدد أو ربط النتائج بنتائج الدراسات السابقة.
- ولتجنب تلك الثغرات قامت الباحثة بالاعتماد على توجه نظري محدد يتمثل في نظرية النشاط الرتيب أو الأنشطة الروتينية لتفسير تهديدات الجرائم المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة.

(٤) الفجوات البحثية:

(أ) التوجهات البحثية غير المكتشفة:

- أغفلت معظم الدراسات السابقة دراسة العوامل التي قد تدفع إلى ارتكاب الجرائم عبر الميتافيرس والتقنيات الناشئة، والتي قد تختلف حدة وأهمية تلك العوامل من مجتمع لأخر، فمن المهم دراسة تلك العوامل ومعرفة أليات مجابهة تلك الجرائم، ومن ثم فإن البحث الراهن اهتم بدراسة العوامل والدوافع التي تدفع إلى حدوث تلك الجرائم وبالأخص في المجتمعات العربية وتحديدًا مصر.
- أغفلت الدراسات السابقة دراسة المخاطر التي يشكلها الميتافيرس على الأطفال في الدول العربية، باعتبار الأطفال من أهم الفئات التي يشكل الميتافيرس خطرًا عليها، نتيجة عدم إدراكهم بخطورة تلك الجرائم، وكيفية تجنبها والتعامل معها عند حدوثها والتي من السهل أن يصبحوا ضحايا لها، ومن ثم قام البحث الراهن بدراسة أهم المخاطر التي قد تواجه الأطفال مستخدمي الميتافيرس.
- لم تقوم الدراسات السابقة بدراسة فئات الجناة الذين قد يرتكبوا الجرائم عبر الميتافيرس، وكذلك الضحايا المحتملين لتلك الجرائم، وبناء عليه قام البحث الراهن بتبيان فئات الجناة والضحايا للإجرام الميتافيرسي، الأمر الذي يساعد في صياغة استراتيجيات وسن التشريعات لضبط الجناة وحماية الأفراد قبل أن يصبحوا ضحايا، أو حماية حقوقهم كضحايا فعليين.
- أغفلت الدراسات السابقة دراسة الأليات والحلول المقترحة وأثر القانون والسياسات والتوعية في تقليل ومجابهة تهديدات جرائم الميتافيرس، وهو ما يحاول البحث الراهن أن يركز عليه.
- تجاهلت العديد من الدراسات السابقة استطلاع وجهة نظر مستخدمي الميتافيرس وبالأخص من الشباب حول تهديدات الجرائم المحتمل ارتكابها من قبل الميتافيرس بإعتبار الشباب هم الفئات الأكثر استخدامًا للإنترنت والميتافيرس حسب ما أشارت إليه الإحصائيات، ومن ثم يعد من الأهمية بمكان معرفة استجابتهم تجاه نلك الجرائم، وهو ما يحاول البحث الراهن أن يقوم به.

(ب) التركيز على قضايا معينة:

ركزت معظم الدراسات الأجنبية تحديدًا على الجرائم والمخاطر التي يسهلها الذكاء الاصطناعي والتقنيات الناشئة، وكذلك المزايا والفرص التي يوفرها الميتافيرس في مجالات التعليم والتجارة والعمل وغيرها.

ومن خلال عرض الدراسات السابقة وتحليلها، وتحديد ما بها من فجوات بحثية، يحاول البحث الراهن سد تلك الفجوات، والإفادة من تلك الدراسات في بناء إطار نظري ومنهجي منضبط وتحديد القضايا النظرية للبحث الراهن بوضوح، إلى جانب تبني التوجه النظري الذي يتماشى مع البحث الراهن، بالإضافة إلى ربط نتائج الدراسات السابقة مع نتائج البحث الراهن وتحديد أوجه الاتفاق ونقاط الاختلاف.

سابعاً: الرؤى النظرية للبحث:

- **نظرية النشاطات الرتيبة (الأنشطة الروتينية) وتفسير الإجرام الميتافيرسي:**

يحتوي علم الإجرام على نظريات متعددة تفتح وجهات نظر مختلفة حول معرفة لماذا وكيف تحدث الجرائم ؟ ولكن نظرية الأنشطة الرتيبة تختلف عن نظريات الجريمة الأخرى؟ لأنها تفسر وتقدم منظورًا جديدًا ومختلفًا للجريمة والمجرمين والضحايا فهي تركز على دراسة الجرائم والأنشطة التي يرتكبها المجرمون والضحايا قبل ارتكاب الجريمة والتي تؤدي في الواقع إلى حدوث الجريمة بحيث ظهرت هذه النظرية كمحاولة لإعطاء تفسير أكثر تفصيلًا لآلية الجرائم، ودراسة تقنية ارتكاب الجرائم، لذا فهي تقدم تفسيرًا مختلفًا للجريمة؛ لأنها لا تركز على أسباب الجريمة ولكن على الجريمة نفسها بما في ذلك الأنشطة التي يتم القيام بها عند ارتكاب الجرائم.

تعد نظرية النشاط الروتيني التي صاغها لأول مرة "لورانس كوهين وماركوس فيلسون" عام (١٩٧٩) ثم طورها فيلسون لاحقًا هي واحدة من أكثر البنى النظرية للاستشهاد بها وتأثيرًا في مجال علم الجريمة ـ الإجرام وعلى النقيض من نظريات الإجرام التي تتمحور حول شخصية المجرم والعوامل النفسية أو البيولوجية أو الاجتماعية التي

حفزت الفعل الإجرامي فإن تركيز النشاط الروتيني هو دراسة الجريمة كحدث وتسلط الضوء على علاقتها بالمكان والزمان والتأكيد على طبيعتها البيئية وانعكاساتها في صياغتها الأولية افترض كوهين وفيلسون أن التغيرات في بنية أنماط النشاط اليومية للناس في أعقاب الحرب العالمية الثانية يمكن أن تفسر ارتفاع معدلات الجريمة التي حدثت وفقًا للدراسات الرائدة في ذلك الوقت، وكانت فرضيتهم هي أن ما بعد الحداثة قد سهل التقارب في المكان والزمان بين المجرمين المحتملين بهدف ارتكاب جرائم ضد أهداف مناسبة في غياب الأوصياء القادرين، ومن هنا تم استقاء فكرتين بسيطين ظاهريًا لهما آثار مهمة:

أولًا: إن فرصة ارتكاب الجريمة قد يعتمد على تشكيلة من العناصر المتميزة، وإن لم تكن منفصلة للمعتدي أو المجرم؛

ثانيًا: يرتبط الأول بأن غياب أي من العنصرين الأولين (المعتدي والهدف) أو وجود العنصر الثالث (الحراس القادرين) سيكون كافيًا في حد ذاته لمنع وقوع حدث إجرامي محتمل **(Miro, 2014: 2)**.

ومن زاوية أخري فإن التحولات في المجتمع الحديث أعطت أهمية أكبر للأنشطة خارج المنزل، على سبيل المثال أدى التقدم التكنولوجي إلى ظهور واستهلاك الأجهزة الإلكترونية مثل أجهزة التلفزيون ومسجلات الفيديو وأجهزة الأستريو ذات القيم الأعلى والأوزان الأقل مما جعلها جذابة للغاية وسهلة الإزالة والتنقل، وأخيرًا فإن ظهور أجهزة الصرف الآلي، وزيادة المعاملات المصرفية والودائع والسحب جنبًا إلى جنب مع التغيرات في النشاط اليومي المرتبط بتداول الممتلكات أدى بشكل عام إلى زيادة حركة السلع الاستهلاكية وظهورها،بإختصارفإن العدد المتزايد من الأشياء المتاحة وزيادة عدد المنازل غير الخاضعة للحراسة وزيادة احتمالات الاتصال المباشر بين الأشخاص أو ممتلكاتهم والمجرمين؛ قد أدي إلى زيادة الأهداف المناسبة وانخفاض الأوصياء القادرين على حمايتها.**(Miro, 2014: 2)**

لقد اختبر كوهن وفيلسون تفسيراتهما للتغيرات في اتجاهات الجريمة من خلال التقييم التجريبي لافتراضاتهما الرئيسية وللتأكيد على أن تشتيت الأنشطة بعيدًا عن المنزل

والأسرة يمكن أن يزيد من احتمالية أن تصبح هدفًا مناسبًا وتقلل من وجود أولياء أمور قادرين، وللتأكد من أن مدى ملائمة الأهداف يؤثر على الاتصالات المكثفة، وأن الحياد الانفرادية بعيدًا عن البيئة الأسرية يمكن أن تزيد من معدلات الإيذاء. وعلى الرغم من أن العلاقة بين عناصر الحدث الإجرامي في المكان والزمان قد تم الاعتراف بها بالفعل من خلال نظريات سابقة مثل النظريات البيئية الأقدم " لشو ومكاي" وكذلك نظرية الضبط الاجتماعي " لهيرشي"، فإن "كوهين وفيلسون" لم يحددا الجانب الاجتماعي والبيئي لحدث الجريمة فحسب بل قاموا بالتركيز على أن الأنشطة الروتينية نموذجًا يتمتع بقوة تعبيرية كثيرة لشرح الطبيعة البيئية للجريمة وتوضح كيف يمكن للعناصر التي تبدو غير مرتبطة بالنشاط غير القانوني أن تشكله وتحدده أو غيابه، وهكذا على سبيل المثال فإن العديد من التطورات التكنولوجية لأغراض مشروعة، مثل السيارات أو الأجهزة الإلكترونية أو الهواتف يمكن أن تستخدمها الجناة في أنشطتهم غير المشروعة، وهذا يعني أن الأنشطة القانونية الروتينية تحدد أيضًا كيفية تنظيم الجريمة في المجتمع وكذلك مكان حدوثها بشكل متكرر مع ما يترتب على ذلك من عواقب وقائية مهمة **(Miro, 2014: 2)**.

ولكي تحدث جريمة على الأشخاص أو جريمة على الممتلكات فلا بد أن يكون هناك وفي الزمان والمكان نفسه دافع لدى الجاني (Perpetrator) وضحيته (Victim) وكذلك شيء ما متملك (Property)، إن حدوث الجريمة يمكن أن يكون سهلًا إذا كانت هناك ظروف وأشخاص آخرون في الموقف يشجع على حدوثها، أو منعها إذا كانت الضحية المحتملة أو شخص آخر حاضرًا يمكن أن يقوم بفعل أو حركة لمنع وقوعها ولقد أخذ "لورنس كوهين وماركوس فيلسون" هذه العناصر الأساسية للزمان والمكان والموضوعات والأشخاص ليطوروا نظرية في النشاطات الرتيبة لحدوث الجريمة ولقد قاموا بذلك عن طريق وضع هذه العناصر في ثلاث فئات من المتغيرات التي تزيد أو تنقص من احتمالية أن يكون الأشخاص من ضحايا جرائم الاتصال المباشر سواء كانت هذه الجرائم واقعة على الأشخاص أو الممتلكات. **(البداينة & الخريشة،٢٠١٣: ٦٣– ٦٤)**.

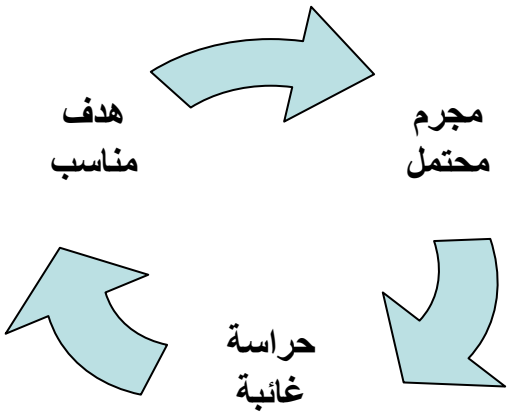
- **المتغيرات الرئيسة لنظرية الأنشطة الروتينية أو (النشاط الرتيب):**

تتمثل العناصر الأساسية الثلاث من المتغيرات التي حددها كوهين وفيلسون على النحو التالي:

أ – المجرم الذي لديه الدافع.

ب– الهدف المناسب؛ أي وجود هدف ذو قيمة يستحق ارتكاب الجريمة.

ج– غياب الحارس المؤهل للأشخاص أو الممتلكات.



شكل رقم (١) يوضح عوامل النشاط الإجرامي

والأطروحة (المقولة) الرئيسة في النظرية هي أن معدلات الضحايا الجريمة ستزداد عندما يكون هناك التقاء أو تقارب في الزمان والمكان لعناصر الحد الأدنى للاتصال المباشر لوقوع الجريمة، وهذا يعني ان احتمالية وقوع الجريمة ستزداد إذا تواجد شخص أو أكثر ولديهم الدافع لارتكاب الجريمة، وإذا تواجد الهدف المناسب أو الضحية المحتملة، وكذلك إذا عاب الحراس الرسميون وغير الرسميين والذين يمكن أن يتم ردع أو وقف المجرم المحتمل عن تنفيذ النشاط الإجرامي، إن الحضور أو الغياب النسبي لهذه المتغيرات متفاوت ومخاطر الوقوع ضحية للجريمة تتفاوت على نحو دراماتيكي بين هذه الحالات، المكان الذي يضع فيه الأفراد أنفسهم وممتلكاتهم.

لهذا اشتقت النظرية اسمها من حقيقة إن "كوهن وفيلسون" قد بدأوا بالافتراض القائل بأن اقتران وتزامن عناصر الجريمة هذه ترتبط بالنشاطات العادية والقانونية

والروتينية للضحايا المحتملين وللحراس. أن التنظيم المكاني والزماني للنشاطات الروتينية الشرعية يلعب دورًا مهمًا في تحديد موقع نمط، ومقدار، الأفعال غير الشرعية قانونيًا التي تحدث في المجتمع المحلي (Community) أو المجتمع العام (Society) **(البداينة& الخريشة، ٢٠١٣: ٦٤).**

ويمكن مناقشة تلك المقولات وتوظيفها في البحث الراهن على النحو التالي:

١- المجرمين أو الجناة المحتملين (الجاني الدافع):

قد يكون الجاني المحتمل أي شخص لديه دافع لارتكاب الجريمة ولديه القدرة على القيام بذلك، على الرغم من إنه من المرجح أن يكون شابًا ليس لديه وظيفة مستقرة، على الرغم من أن كوهن وفيلسون استخدما في صياغتهما الأولية مصطلح (الجاني الدافع) إلا أنه في الأعمال اللاحقة تجنبا مصطلح (الدافع) في الإشارة إلى الجاني لأن ما يعتبروه ذا صلة حقًا لم يكن التصرف أو الدافع لارتكاب الجريمة؛ بل العوامل المادية التي مكنت الشخص من التورط في الجريمة، وما ساهم به هذا النهج هو توضيح الحاجة إلى صرف الانتباه عن الجاني من أجل فهم الجريمة **(Miro, 2014: 2).**

وبتبنى نظرية الأنشطة الوتينية أو الرتيبة على البحث الراهن يمكن تحديد الجناة المحتملين عبر الميتافيرس والتقنيات الناشئة من خلال اتفاق الجميع تقريبًا على أن هناك (مجرمين متحمسين) يبحثون عن فرص مناسبة لارتكاب الجرائم وهو عنصر مطلوب في فهم جميع أنواع الجرائم بما في ذلك الجريمة السيرانية. على الرغم من أن طبيعة الفضاء الإلكتروني ذاتها تسمح لمرتكبي الجرائم بعدم الاقتراب جسديًا من الضحايا من أجل تعريض أجهزة كمبيوتر الضحايا للخطر، والأهم من ذلك المعلومات/ البيانات المخزنة عليها هناك خصائص مكانية في العالم الافتراضي يمكن تحديدها على إنها متطابقة جزئيًا مع الفضاء العادي لبدء الاختراق وحساب التوقيت والإيقاع المكاني والزماني لشن هجوم، على سبيل المثال، قد يبقى الجناة في الفضاء الإلكتروني في انتظار النقر على أدوات مفيرسة من قبل مستخدمي الإنترنت من أجل غزو جهاز المستخدم، تعد البرامج الضارة طريقة نموذجية لفتح الباب الخلفي لنظام المعلومات للمتسللين في هجوم

إلكتروني، بعد ظهور الهندسة الاجتماعية ولزيادة التعرض للضحايا المحتملين على أفضل وجه؛ سيحاول الجناة إبقاء ملفاتهم ومتداولة لأطول فترة ممكنة، في أي موقع إلكتروني مثل (مرفقات البريد الإلكتروني، مواقع التواصل الاجتماعي، صفحات الويب، الإعلانات عبر الإنترنت، غرف الدردشة والبوابات) وسوف يلعب الضحايا دورًا نشطًا في بدء البرامج الضارة المخفية وبهذا المعنى فإن احتمالية الوقوع ضحية تعتمد على الدرجة التي يكون بها سلوك الضحية عبر الإنترنت قريبًا تقريبًا من البرامج الضارة المبرمجة لمرتكب الجريمة، مثل فيروسات الكمبيوتر، الديدان، أحصنة طروادة، برامج الفدية وبرامج التجسس وغيرها من الرموز الضارة. وبالمثل لخداع الضحايا المحتملين غالبًا ما يتم تسهيل مواقع الويب الزائفة التي تحتوي على برامج ضارة مضمنة والتي يتعين عليها تغيير عناوين الإنترنت باستمرار وقبل اكتشافها وإغلاقها، عن طريق رسائل تحتوي على ارتباطات متشعبة لتقصير المسافة الافتراضية.**(Hsieh & Wang, 2018: 336)**

٢- الهدف المناسب:

هو شخص أو ممتلكات قد تتعرض للتهديد من قبل الجاني ويفضل "فيلسون" مصطلح الهدف على مصطلح الضحية، إذ يسلط الأول الضوء على أن غالبية الجرائم تهدف إلى الحصول على البضائع، وبالتالي قد يكون الضحية غائبًا عن مكان الجريمة **(Miro, 2014: 2).**

الهدف المناسب وجرائم الميتافيرس والتقنيات الناشئة:

في مجتمع اليوم الحديث يستخدم الأفراد شبكة الإنترنت السطحية كعامل أساسي في الحياة مما يعرض أنفسهم دون وعي لخطر الوقوع ضحية للجرائم الإلكترونية في حين أن المشاركة عبر الإنترنت على شبكة الإنترنت السطحية يمكن أن يكون لها العديد من الفوائد، إلا إنها تزيد من خطر الوقوع ضحية للجرائم الإلكترونية. حيث يشير "كوهن وفيلسون" إلى أن أسلوب حياة الفرد يجعل منه هدفًا مناسبًا بشكل أساسي والذي يتضمن الأنشطة المهنية والترفيهية مثل التفاعل الاجتماعي من خلال المشاركة عبر الإنترنت. **(Stavola,J & Choi,K 2023: 8).**

إن تقييم الأهداف هو عامل حاسم في الجرائم السيرانية، يمكن للمجرمين ارتكاب مجموعة واسعة من الجرائم الإلكترونية المختلفة بدءًا من اختراق أنظمة الكمبيوتر وإتلافها وسرقة البيانات الشخصية والتنظيمية والملكية الفكرية، ومطاردة ومضايقة مستخدمي الإنترنت والتدخل في الخدمات عبر الإنترنت للتجارة والبيع وتبادل الخدمات، ولكن هذه الجرائم (الأهداف) في الفضاء الإلكتروني هي معلوماتية بطبيعتها، بالنسبة للمجرمين تعد القيمة العالية وقابلية النقل من الخصائص المستهدفة المرغوبة، تلك الموجودة في الفضاء الإلكتروني تكاد تكون (عديمة الوزن) بعد اختيار الأفراد والمنظمات المناسبة في الفضاء الإلكتروني. حيث الأفراد والمنظمات الذين يتمتعون بمستويات أعلى من الضعف؛ أمرًا ضروريًا للحصول على احتمال أكبر معدلات النجاح فيما يتعلق بالمكافآت المربحة أو المكاسب المالية أو الأغراض الضارة الأخرى.**(Hsieh& Wang, 2018: 337)**

باختصار يزيد من التفاعل عبر الإنترنت من خطر وقوع المستخدمين ضحية للجرائم الإلكترونية وتحديدًا خمسة أنواع رئيسية (الهندسة الاجتماعية،الخداع، التحرش، عبر الإنترنت، جرائم الهوية، القرصنة،الحرمان من الخدمات والمعلومات).ويقترح فيلسون أن هناك أربعة مقاييس لكي تكون هدفًا مناسبًا للجريمة السيرانية قيمة الهدف المناسب، القصور الذاتي، الرؤية المادية، فضلًا عن إمكانية الوصول إلى الهدف.

(Stavola,J & choi,K, 2023: 6).

٣- غياب الحارس المؤهل:

العنصر الثالث والأخير الموصوف هو غياب الوصي القادر أي الشخص الذي يمكنه التدخل لوقف أو إعاقة الجريمة والوصي أو الحارس القادر على منع الجريمة هو الذي لا ترتكب الجريمة بحضوره والذي يزيد غيابة احتمال ارتكاب الجريمة، ويشمل هذا التعريف أي شخص يتحرك عبر منطقة ما يعمل كحارس للأشخاص أو الممتلكات.

لقد خضع الحارس المؤهل حاضرًا أو غائبًا إلى تحديثات عمليًا عن صياغته الأولية، وقد تمت مناقشة تعريفه وإعادة صياغته عند "فيلسون" وكذلك من قبل باحثين آخرين، على سبيل المثال عرف "هوليس بيل وآخرون" في مواجهة أولية لشخصية الحارس

في نظرية النشاط الروتيني بأنه "الوجود الجسدي أو الرمزي لفرد أو مجموعة من الأفراد، يتصرف سواء عن قصد أو غير قصد، لردع حدث إجرامي محتمل". وقد قام فيلسون بربط نظريته بنظرية هيرشهي عن الرقابة الاجتماعية، حيث يأخذ فيلسون العناصر الأربعة للحارس في نظرية هيرشي، (التعلق، الالتزام، المشاركة، والاعتقاد وذلك في التحقيق في فكرة أن شخصًا ما يمكن أن ينبئ مرتكب الجريمة عن طريق وجوده في مكان ما، أو أن الشخص يمكن أن يثبط مرتكب الجريمة المحتمل بسبب علاقته به، يتوافق فيلسون مع فكرة السيطرة الاجتماعية من حيث أن السيطرة عنصرًا حاسمًا في اتجاهات معدل الجريمة. **(Miro, 2014: 3)**.

ويمكن تعريف الوصاية على المستويين الفردي والبيئي ويمكن استخلاصها من نظرية الفرصة الجنائية متعددة السياقات للحصول على تعريفات محددة على كل مستوى.

على المستوى الفردي يتم تعريف الوصاية على أنها: "امتلاك صفات تتعلق بالروابط الاجتماعية والسيطرة على العلاقات الشخصية "حيث تشير الشخصية إلى الدرجة التي يمكن بها ملاحظة الأفراد والأشياء في مكان محدد ومنعهم من التعرض لأعمال إجرامية لأنهم قريبون ومعرضون لوكلاء السيطرة الرسمية ووكلاء السيطرة غير الرسمية.

أما الوصاية على المستوى البيئي "الدرجة الجماعية التي يمتلك بها الأفراد أو الأشياء في منطقة محلية محدودة صفات مرتبطة بالروابط الاجتماعية والسيطرة الاجتماعية. **(Argun & Daglar, 2016: 1180)**.

جادل كوهين وفيلسون بأن الافتقار إلى آليات الرقابة الاجتماعية والغياب من شأنه أن يؤدي إلى زيادة في اليقين والسرعة وقيمة المكافآت التي يتم الحصول عليها من أعمال النهب غير القانونية مما يؤدي إلى المزيد من جرائم النهب، وعلى نحو مماثل بجون وصاية قادرة في الفضاء الإلكتروني، سواء كان ذلك على المستوى الحكومي أو المستوى التنظيمي أو المستوى الفردي هناك احتمال متزايد لتحقيق مكاسب غير قانونية وميل إلى الإيذاء. وتتراوح الوصاية السيرانية على نطاق واسع من الأوصياء غير السميين (مثل مديري الشكات الداخليين ومستخدمي الكمبيوتر الخاصين والعامة الأخلاقيين) إلى

الأوصياء الرسميين مثل (جدران الحماية، برامج مكافحة الفيروسات، موظفي تكنولوجيا المعلومات، مراقب الخطورة والمشرفين) علاوة على ذلك فإن ما إذا كان الوصي على استعداد للإشراف والتدخل عند الضرورة، فضلًا عن قدرته على اكتشاف المجرمين المحتملين وهو أمر مهم عمليًا يعتبر كل هذه الجهود حاسمة لردع المجرمين المحتملين، ومراقبة منع التقارب بين المجرمين المتحمسين والأهداف المناسبة في الفضاء الإلكتروني. أن مستخدمي الإنترنت الذين كانوا أقل عرضة للاعتماد والسلب وكانت تدابير الوصاية الجسدية مثل استخدام نظام تصفية البريد الإلكتروني وتثبيت تصفح مكافحة الفيروسات واستخدام جهاز الكمبيوتر واحد فقط، أكثر عرضة للوقوع ضحية بمقدار(١.٣٢) مرة بالإضافة إلى ذلك فقد تتضمن السلوك الروتيني عالي المخاطر عبر الإنترنت أيضًا استخدام شبكات غير محمية من خلال الاتصال بأي شبكة Wi–Fi عامة مثل (المطار، مترو الإنفاق، والمقاهي، والحافلات، والمطاعم، والفنادق) بمعنى آخر غالبًا ما يعرض الأفراد أنفسهم لخطر أكبر للتعرض للاختراق دون أن يدركوا ذلك.

(Hsieh & Wong, 2018: 338).

بإختصار تسهم نظرية الأنشطة الروتينية بشكل كبير في تفسير الجرائم الإلكترونية المختلفة حيث إنه لا يمكن ارتكاب الجريمة إلا إذا اعتقد الجاني أن الهدف مناسب وأن الوصي القادر غائب ويمكن لأنشطة الجناة اليومية والعادية أن تضع الناس في موقف يجعلهم بسهولة ضحية للجريمة **(Argun& Daglar, 2013: 1190)**.

ويمكن تطبيق ذلك أيضًا على الميتافيرس على سبيل المثال (Roblox) وهي منصة ميتافيرس صاعدة تسمح باستخدام الألعاب التي أنشأها متخصصون آخرون، ويستهدف من بين مجموعات أخرى، مستخدمي الإنترنت من المراهقين الذين يتراوح أعمارهم بين (٨ و٤١ عامًا) والذين من المحتمل أن يصبحوا ضحايا للجرائم الإلكترونية من خلال التعامل مع هذه المنصة. ففي عام ٢٠٢١ تبين إنه من بين أكثر من (١٢) مليون لاعب على Roblox كان (٥٤%) من اللاعبين تحت سن (١٣ عامًا) وحوالي (٩٠%) من مطوري الألعاب كانوا فوق (١٨ عامًا)، بالإضافة إلى ذلك فإن التركيبة السكانية الأسرع نموًا في "Roblox" تكون بين الأفراد الذين تتراوح أعمارهم (١٧ و٤٢

عامًا)حيث لا يقل أكثر من (٥٠%) من المستخدمين عن (١٣ عامًا)، ومع ارتفاع عدد اللاعبين الشباب، فالأطفال معرضون بشكل كبير لخطر الوقوع ضحايا للجرائم الإلكترونية بسبب إمكانية وصول اللاعبين البالغين إليهم، حيث يتوقع مركز بيو للأبحاث أن مستخدمي Metaverse سيصبحون مدمنين وبالتالي يزيدون من الإيذاء لأنهم اقل وعيًا بالمخاطر.**(Stavola, J & Choi,K 2023:7)**

ثامنًا: القضايا النظرية التي يناقشها البحث :

١ـ الأحداث التاريخية التي أدت إلى ظهور الميتافيرس ومراحل تطوره:

شهد تطور الميتافيرس عدة مراحل مختلفة متتالية، يمكن الإشارة إليهما على النحو التالي: **(يحيى،٢٠٢٢: ٣٩ –٤٢) & (سليمان،٢٠٢٣: ٢٠٠) & (Wang, [et.al], 2022: 3)**.

المرحلة الأولى (التوائم الرقمية):

ظهرت بوادر التطبيق العمل الأول عام ١٩٩٣ حين أعلنت شركة ألعاب الفيديو العالمية سيغا SEGA ومقرها الرئيس طوكيو في اليابان نموذجًا أوليًا لنظارات الواقع المعزز، إلا أن تلك الشركة عانت إخفاقات تجارية كثيرة **(يحيى، ٢٠٢٢ :٣٩)**، وفي عام ١٩٩٥م تم إطلاق العوالم النشطة (Active World) بالاعتماد على رواية تحطم الثلج (Snow Crash) والتي من خلالها تم تمكين المستخدمين من زيارة عوالم الواقع الافتراضي واستكشاف البيئات والمباني والتي صنعها المستخدمون وإنشاء البيئات الخاصة بهم، حيث تتيح المرحلة الأولى عالم مرآة يتكون من توائم رقمية واسعة النطاق، عالية الدقة من البشر والاشياء في البيئات الافتراضية، وتهدف إلى تمثيل رقمي حيوي للواقع المادي. وفي هذه المرحلة تكون الأنشطة والخصائص الافتراضية مثل عاطفة المستخدم وحركاته بمثابة تقليد لنظرياتها المادية حيث يكون الواقع والواقعية مساحتين متوازيتين.

ويمثل التوأم الرقمي النسخ الرقمي للأشياء والأنظمة في العالم الحقيقي بدقة عالية، كما إنها تمكن النسخ المتطابق للكيانات المادية وكذلك التنبؤ بأجسادهم الافتراضية وتحسينها، وتحليل التدفقات في الوقت الحقيقي من البيانات الحسية والنماذج المادية

ومعلومات تاريخية. في التوأم الرقمي يتم إرجاع البيانات من البيانات المادية، يمكن استخدام الكيانات للتعلم الذاتي والتكيف الذاتي في الفضاء. علاوة على ذلك يمكن للتوأم الرقمي أن توفر نماذج رقمية دقيقة للكائنات دقة عالية في الميتافيرس من خلال محاكاة النظام للعمليات الفيزيائية ومساعدة تقنيات الذكاء الاصطناعي فهي مفيدة لإنشاء وعرض الميتافيرس على نطاق واسع. إلى جانب ذلك يتيح التوأم الرقمي الصيانة التنبؤية وإمكانية التتبع للسلامة الجسدية، وذلك بسبب الاتصال ثنائي الاتجاه بين الكيانات المادية ونظيراتها الافتراضية وبالتالي تحسين الكفاءة وتقليل المخاطر في العالم المادي.

المرحلة الثانية (المواطنين الرقميين):

تركز المرحلة الثانية بشكل أساسي على إنشاء المحتوى الأصلي، حيث يمكن للمواطنين الرقميين الذين تم تمثيلهم بالصور الرمزية إنتاج ابتكارات داخل العوالم الرقمية، وقد تكون هذه الإبداعات الرقمية موجودة في المساحات الافتراضية. في هذه المرحلة تصبح المحتويات التي تم إنشاؤها على نطاق واسع في العالم الافتراضي متساوية مع نظيراتها المادية ويكون للعالم الرقمي القدرة على تحويل وابتكار عملية الإنتاج في العالم المادي وبالتالي خلق المزيد من التعاطفات بين هذين العالمين.

ونلاحظ أنه في مطلع عام ٢٠٠٠ شهد العالم طفرة كبيرة نحو التوجه إلى العالم الرقمي الثلاثي الأبعاد، وظهرت افكار وابتكارات للمشاهدة الثلاثية الأبعاد.وعلى سبيل المثال أطلقت شركة ليندن لاب (Linden Lab) في كاليفورنيا عام ٢٠٠٣ منصة (سكند لايف) لتقدم واقًعا افتراضيًا ثلاثي الأبعاد مشابهًا للواقع الحقيقي، وحياة ثانية موازية للحياة البشرية التي نعيشها على كوكب الأرض، بلغ سكانها الملايين من جميع أنحاء العالم، ويمكنهم التعايش، التسوق، الترفيه، وشراء الأراضي الافتراضية والبناء عليها. وفي عام ٢٠٠٦ تم إنشاء منصة (Roblox) وهي منصة ألعاب يمكن للمستخدمين من خلالها اللعب وإنشاء الألعاب الخاصة بهم والتي يمكن مشاركتها مع آخرين، من جانب آخر طرحت في عام ٢٠١٤ نظارة جوجل كاردبو (Google Cardboard) الافتراضية المبسطة التي يمكنها تحويل الهاتف الذكي التقليدي منصة واقع افتراضي. وظهرت في

عام ٢٠١٥ منصة (Spatials debuts) للمبرمجين، لإنشاء عوالم افتراضية متكاملة، وطرحت منصات كثيرة لتكنولوجيا الواقع الافتراضي،أدوات مختلفة منها خوذة الواقع الافتراضي (بلايستيشن في آر) (Play Station VR) التي طورتها شركة سوني للترفيه التفاعلي (Entrainment Sony Interactive) وفي عام ٢٠١٧ انشأت شركة إيبك للألعاب (Epic games) نظامًا للألعاب يسمى "فورتنايت Fortnite " قائم على التفاعل الثلاثي الأبعاد. وفي عام ٢٠١٨م أنشأت شركة (Solivax) لعبة متعددة اللاعبين عبر الإنترنت متعدد الأكوان واطلقت عليها اسم نيوس في آر (Neos V R).

المرحلة الثالثة (السريالية):

توالت الابتكارات وصولًا إلى السنوات الأخيرة التي شهدت تفشي جائحة كوفيد ١٩ أواخر عام ٢٠١٩ وترسيخ قاعدة التباعد الاجتماعي في أغلبية البلدان مما سرع وتيرة البحث عند سبل التعايش في ظل طول أمد هذا التباعد وتحوله منهجًا ثابتًا وأسلوب حياة مستقبليًا للبشر، ومن ثم اعتمدت الشركات على التكنولوجيا والبرمجيات ومنصات التواصل الاجتماعي التي عرفها العالم طوال السنوات الماضية من أجل تطويرها والحفاظ على تدفق سير الحياة الإنسانية ولكن داخل بيئة رقمية، قد تُعد الوضع الطبيعي الجديد الذي ينبغي أن يعتاده البشر وتمثل النواة الأولى لتغيير جذري في الحضارة الإنسانية. ففي هذه المرحلة ينمو الميتافيرس إلى مرحلة النضج ويتحول إلى عالم سريالي مستمر ومستدام ذاتيًا يستوعب الواقع نفسه، سيتم تحقيق التكامل والتعايش المتبادل بين العوالم المادية والافتراضية، في هذه المرحلة، حيث يكون نطاق العالم الافتراضي أكبر من نطاق هذه المرحلة، ويمكن أن يوجد المزيد من المشاهد والحياة غير الموجودة في الواقع في العوالم الافتراضية.

ويمكننا الإشارة إلى أهم الأحداث التاريخية التي أدت إلى ظهور الميتافيرس في الجدول التالي:

جدول رقم (٣) الأحداث التاريخية لظهور الميتافيرس

العام	الحـــــــدث
١٩٨٩	قام "تيم بيرنرز"بإخترع العالم الويب الواسع (WWW)
١٩٩٢	قام كاتب الخيال" نيل ستيفنسون" بتقديم مفهوم الميتافيرس لوصف عالم افتراضي ثلاثي الأبعاد
٢٠٠٣	قام "فيليب روزديل" بتصميم أول عالم لافتراضي على الإنترنت مع فريقه LidenLap
٢٠٠٩	تم اختراع منصة للعملات المشفرة وسلسلة الكتل بتكوين
٢٠١٢	تم تقديم NFTS والرموز المميزة غير القابلة للاستبدال والتي تحدد بشكل فريد أي أصل رقمي عبر شبكة blocchain
٢٠١٤	فيسبوك تستحوذ على أجهزة الواقع الافتراضي ومنصة Oculus
٢٠١٥	التكرار الأول لـ Decentraland الافتراضية على الإنترنت
٢٠١٦	Pokemon Go أول لعبة تستخدم البيئة الافتراضية والواقع المعزز التي أحدثت ثورة في العالم
٢٠١٧	تم إطلاق لعبة Fortnite وهي لعبة متعددة اللاعبين ومركز اجتماعي
٢٠٢٠	جائحة كوفيد ١٩ تجتاح العالم وأجبرت الجميع على استكشاف المجال الافتراضي للتفاعل والتواصل
٢٠٢١	تكشف Microsoft عن إضافة Mesh لجعل التعاون ممتعًا وشخصيًا
٢٠٢١	يكشف "مارك زوكربيرج" أن الشركة الأم لفيسبوك تتبني الاسم Meta وتزيح الستار عن خطط Metaverse

الجدول السابق من إعداد الباحثة اعتمادًا على (Bale [et.al],2022:3)

٢- سمات الميتافيرس وخصائصه:

ستكون هناك حاجة إلى عدد لا يحصى من التقنيات لتمكين الميتافيرس ستعمل أجهزة الواقع الافتراضي (VR) والواقع المعزز (AR) بالفعل كأنواع من نقاط الوصول التي من خلالها يمكن للأفراد الوصول إلى الميتافيرس في المستقبل. ومن المتوقع أن تعمل الهواتف الذكية والهواتف الذكية المحمولة إلى جانب الأجهزة الناشئة الأخرى مثل الواقع المختلط (MR) أو أجهزة الدماغ والحاسوب (BCI) بمثابة نقطة دخول أيضًا، كما ستعمل التقنيات الأخرى مثل نظام تحديد المواقع العالمي (Gps) وإنترنت الأشياء على تسهيل الاستشعار الذكي لالتقاط البيانات حول الأفراد (الموقع، الحركات، القياسات الحيوية، وما إلى ذلك) واستخدامها كمدخلات للإجراءات في البيئات الافتراضية كما

ستسمح تقنيات الواقع الممتد (XR) بدمج الكيانات المادية والافتراضية في تجربة واحدة. كما ستزود تقنية (Metaverse Blockchain) بمعرفات فريدة وأليات مصادقة من شأنها أن تدعم المعاملات وملكية الأصول الرقمية. كما أن العملات المشفرة والرموز غير القابلة للاستبدال (Nfts) والتي تستخدمها منصات مثل Sandbox و Decentraland من تمكين المعاملات الاقتصادية في الميتافيرس. ستكون تكنولوجيا الشبكة والحوسبة مطلوبة لضمان استمرار نشاط متعدد المستخدمين واسع النطاق يسمح بتفاعلات سلسلة وغامرة في الوقت الحقيقي في الميتافيرس، بالإضافة إلى الحوسبة السحابي والحوسبة الطرفية، كما ستتيح تقنيات الذكاء الاصطناعي (مثل التعلم الآلي ومعالجة اللغات الطبيعية) تجارب غامرة من خلال تحسين كيفية تفاعل تمثيلات المستخدم الرقمي والكيانات الافتراضية.
(Gomes-Quintero[et.al,] 2023: 3)

ولا يفوتنا أن ننوه إلى أن أحد الباحثين قدم تصنيفًا لعشر سمات للميتافيرس وهي:

- متعدد المستخدمين؛
- متعدد الأغراض؛
- من إنشاء المستخدم؛
- مكاني؛
- لدى المستخدمين إحساس بالوجود في البيئة الافتراضية؛
- مستمر (على سبيل المثال، لا ينتهي عندما يقوم المستخدم بتسجيل الخروج أو تركه أو قد تنتهي الأصول الرقمية عند انتهاء اللعبة)؛
- متعدد المنصات (على سبيل المثال ستكون هناك منصات متعددة مترابطة)؛
- قابلية التشغيل البيني من عوالم افتراضية ثلاثية الأبعاد في الوقت الفعلي (على سبيل المثال، سيتمكن المستخدمون من التنقل بين المنصات)؛
- الملكية (الأصول الرقمية العملات المشفرة)؛
- الصور الرمزية (على سبيل المثال ستكون هناك تمثيلات رقمية بين المستخدمين).

(Gomes-Quintero[et.al,] 2023: 3)

بالإضافة إلى ميزة استمرارية البيانات، مثل الهوية والإجراءات والاتصالات والمدفوعات مما يضمن إنه عندما يعود المستخدم إلى الميتافيرس فإن كل ما فعله من قبل لا يزال موجودًا. **(Uncief, 2023: 9)**

ومن السمات الأخرى التزامن كما هو الحال في الاتصالات والتفاعلات والمعاملات المتزامنة، والتهجين المادي الافتراضي (بمعنى خليط بين العالمين المادي والافتراضي)، مفتوح (بمعنى أنه يمكن لأي شخص إنشاء محتوى)، لا مركزي، زمانية ومكانية مفرطة (بمعنى القدرة على التحول من مساحة افتراضية إلى أخرى بسلاسة) قابليته للتطوير (أي البقاء فعال على الرغم من العدد المتزايد من المستخدمين والتفاعلات والتعقيد) غير المتجانس (من حيث المنصات والأجهزة وأنواع البيانات وأوضاع الاتصال).

فالميتافيرس بإعتباره عالمًا افتراضيا متعدد الأراض سيقدم نطاقًا متنوعًا من التطبيقات وحالات الاستخدام، من المرجح أن تكون القطاعات الرئيسة هي (الألعاب، الترفيه، الضيافة، السياحة، العمل، التعليم، التدريب، تجارة التجزئة، الصحة والرفاهية) ويرتبط العديد من هذه التطبيقات بإنشاء التوائم الرقمية (DTS) أي رقمي **(Gomes-Quintero [et.al,] 2023: 3)**.

٣- الميتافيرس والتقنيات الناشئة وحالات الاستخدام والمخاطر:

يبقى التساؤل المطروح هل ستنجم فرص جديدة للنشاط الإجرامي من الميتافيرس سواء كميًا أو حتى نوعيًا ؟ يجب اعتبار الميتافيرس وتطبيقاته جزء من الجريمة السيريانية القائمة أو كجزء من الجريمة السيبرانية التي لا تزال بحاجة إلى التطوير. يمكن النظر إلى الميتافيرس على أنها مجتمعات صغيرة فردية يمكن أن يؤدي فيها السلوك المنحرف إلى تأثيرات معينة والتي يمكن ممارستها بالاضطراب والتهيج الناجم عن الإجرام في المجتمع الحقيقي. والسؤال هنا ما إذا كان السلوك المنحرف الذي يجب تعريفه على إنه إجرامي يمكن أن يؤدي إلى تأثيرات مماثلة في الميتافيرس كما تفعل الجريمة في المجتمع الحقيقي؟ إن النظر في العوالم الاجتماعية قد يساعد باستخلاص استنتاجات حول أسباب الجريمة وآثارها في المجتمع الافتراضي الحقيقي **(Law, 2011: 20)**.

وقد تؤدي التقنيات الأساسية المتاحة بالفعل للمستهلكين الوصول إليها والتعامل مع الميتافيرس إلى حدوث ما يلي: **(DAWES,2022:4)**

- **الأذى– الضحية، أو الأذى الاجتماعي:** يعتبر الضرر الجسدي أو العاطفي المرتبط بجريمة ما أو الخسارة المالية للفرد أو تقويض الثقة في المؤسسات العامة. حيث تتيح أجهزة الواقع الافتراضي والمعزز التي تمزج بين الشات المادية والافتراضية؛ تجربة عالم ما بعد الكون مثل استكشاف عوالم افتراضية متخيلة بحتة أو توائم رقمية لعوالم حقيقية، بطريقة غامرة أكثر لكثير مما يمكن تحقيقه من خلال الكمبيوتر اللوحة أو الكمبيوتر؛
- **التكرار:** العدد المحتمل للمرات التي قد تحدث فيها الجريمة خلال فترة زمنية ما؛
- **قابلية الإنجاز:** ما مدى سهولة ارتكاب جريمة مع الأخذ في الاعتبار الاستعداد المحتمل للتكنولوجيا الأجهزة التي يمكن ارتداؤها والتي تحاكي الإحساس الجسدي بما في ذلك اللمس والألم؟ يمكن شراؤها بالفعل من المتاجر الكبرى، وتوفر مستوى إضافي من الانغماس وتمكين المستخدمين من الشعور بالتفاعلات مع الآخرين؛
- **القدرة على الهزيمة:** ما مدى سهولة تطوير تطبيق التدابير اللازمة لمنع الجريمة أو اكتشافها أو جعلها غير مجزية .

جدول رقم (٤) ملخص للميتافيرس والتقنيات الناشئة التي شملها البحث وحالات الاستخدام ومخاطرها(التقنيات الحديثة المتعلقة بالبيانات والذكاء الاصطناعي، ٢٠٢٣: ٦٤-٦٥)

التقنية	حالات الاستخدام	مخاطر
الذكاء الاصطناعي	- إتمام المهام - تعزيز القدرات	- التحيز - الهجمات السيرانية - التزييف العميق - الأسلحة ذاتية العمل - البطالة
الميتافيرس	- الرعاية الصحية - التدريب والتأهيل - التجزئة	- الهيمنة التقنية - الاختراقات السيبرانية - التأثير التقني الواسع
سلسلة الكتل	- الخدمات المالية - سلسلة التوريد	- إمكانية الاختراق - خصوصية البيانات

التقنية	حالات الاستخدام	مخاطر
	- توثيق ملكية المنتجات الرقمية - قطاع التأمين	- التأثير البيئي
العملات الرقمية	- العملات الرقمية الوطنية - العملات المشفرة للشركات - الطرح الأولي للعملات	- إمكانية الاختراق - التعاملات المشبوهة -إمكانية الاحتيال والتلاعب - استنزاف الطاقة
إنترنت الأشياء	- إنترنت الأشياء الصناعي - إنترنت الأشياء الطبي - المدن الذكية - المنازل الذكية	- الأمن السيراني - حماية الخصوصية
الحوسبة الكمومية	- التشفير - التحسين لإيجاد الحلول المثلى - المحاكاة	- أمن الشبكات - إساءة الاستخدام
الحوسبة الطرفية	- النقل - الصحة - الطاقة - الخدمات المالية	- الأمان
المركبات ذاتية القيادة	- تنقلات الأفراد - المجال اللوجيستي - المجال العسكري	- مخاطر استخدام غير متوقعة - نقص الوظائف -انخفاض الأمان والخصوصية - زيادة مشاكل المرور

٤- مساحات الجريمة في الميتافيرس:

تعمل الجرائم السيبرانية عبر مجالات مختلفة يمكن تصنيفها إلى ثلاث مجالات محددة: افتراضية ومختلطة ومادية. في الفضاء الافتراضي ترتكب الجرائم بالكامل عبر الإنترنت؛ يشمل العالم المختلط الجرائم التي تنتقل بين العالمين المتصل بالإنترنت وغير المتصل بالإنترنت؛ ويشير الفضاء المادي إلى المواقع الجغرافية الملموسة المرتبطة بالأنشطة الإجرامية في الميتافيرس، يقدم كل مجال جريمة لها تحدياتها وتعقيداتها الخاصة، ويدل مصطلح فضاء الجريمة على البيئة التي تقع فيها هذه الجرائم،أما المناطق الجغرافية فتشير إلى المواقع الملموسة المرتبطة بالجريمة التي قد تتطابق أو لا تتطابق مع أماكن مرتكبي الجرائم أو الضحايا. إن التفاعل المعقد بين هذه الأمور يخلق شبكة من

التحديات الفضائية، والقوانين المتضاربة، والمخاوف المتعلقة بخصوصية البيانات والإنفاذ القانوني، وتؤدي هذة التعقيدات إلى تفاقم الصعوبات في القبض على الجناة وحماية الضحايا لاسيما عندما ينتشرون في مناطق جغرافية مختلفة. ويستضيف العالمان الميتافيرس والافتراضي مجموعة واسعة من الأنشطة بدءًا من التواصل الاجتماعي والألعاب والتجارة الافتراضية إلى سلوكيات غير قانونية أو ضارة مثل الجرائم التي يتم تسهيلها عبر الإنترنت أو الجرائم التي يتم تمكينها عبر الإنترنت بما في ذلك القرصنة وغسل الأموال، الاحتيال، المطاردة والمراقبة. حيث يشمل سوء السلوك الافتراضي في الميتافيرس الإجراءات التي تنتهك القواعد أو المعايير الأخلاقية أو الأطر القانونية والتي تتراوح من القواعد البسيطة وانتهاكات شروط الخدمة إلى الجرائم الخطيرة. يمكن أن تؤدي الطبيعة المجهولة للتفاعلات عبر الإنترنت في كثير الأحيان إلى سلوك عدواني، وتنمر عبر الإنترنت واضطراب نفسي، مما يعرض سلامة وشمولية الفضاء الافتراضي للخطر، تنتشر السرقة والاحتيال والقرصنة الافتراضية في الاقتصادات الافتراضية، مما يؤدي إلى خسائر مالية وتقويض الثقة، العنف الافتراضي (أي قيام لاعبي الألعاب الافتراضية بإثارة الآخرين ومضايقتهم عمدًا) والهجمات الافتراضية يمكن أن يضر بالأفراد ورفاهية المجتمع. يتضمن هذا التكرار التالي للجرائم في البيئة الرقمية السلوكيات المعروفة والطرق التي يحدث بها سوء السلوك والجريمة، مع التأثير المحتمل في العالم غير المتصل بالإنترنت ومنه قد يظهر بعض الأنواع الجديدة أو الأشكال المختلفة من البيئات الغامرة. يمكن لمثل هذه السلوكيات أن تطمس الخطوط الفاصلة بين العالمين المادي والرقمي، مما يجعل من الصعب تحديد الولاية القضائية ومحاسبة الجناة عن الجرائم المرتكبة في هذه البيئات الافتراضية. **(Council of Europe and EEEI ,2024:21)**

ويمكن الإشارة إلى مساحات الجريمة على النحو التالي:(Blake, 2024:68-69)

- **جرائم الإنترنت الكاملة:**

يتم ارتكاب الجرائم الإلكترونية عبر الإنترنت في الفضاء الرقمي. وهذا يعني أن النشاط الإجرامي بأكمله منذ البداية وحتى التنفيذ يحدث داخل حدود الإنترنت أو الشبكة

الرقمية مما يجعل من الصعب تتبعها وقابلة للتكيف بشكل فريد مع المشهد التكنولوجي سريع التطور. وغالبًا ما تستغل هذه الأنواع من الجرائم ميزة إخفاء الهوية التي توفرها الميتافيرس ويمكن أن يكون لها تأثيرات عالمية نظرًا لطبيعة الشبكات الرقمية التي لا حدود لها. أحد الأمثلة التوضيحية هو انتشار برامج الفدية، حيث يتم إنشاء تعليمات برمجية ضارة ونقلها عبر الإنترنت لتشفير ملفات الضحايا مع تسجيل طلبات الفدية عادة من خلال العملات المشفرة.

- **الجرائم الهجينة:**

بعض الجرائم ليست رقمية ولا مادية بحتة، بل تمتد إلى كلا العالمين، وتشمل عناصر التفاعل عبر الإنترنت وخارجه، تعكس هذه الجرائم الهجينة أو المتقاطعة الترابط بين حياتنا الرقمية والمادية. على سبيل المثال قد يستخدم المجرمون منصات افتراضية مثل الميتافيرس للعثور على الضحايا المحتملين والاتصال بهم، وبالتالي الانخراط في أنشطة غير قانونية عبر العالم المادي مثل السرقة أو الاعتداء أو أشكال أخرى من الضرر خارج الإنترنت. أحد الأمثلة التوضيحية هو عملية احتيال عبر الإنترنت حيث يتم التلاعب بالضحايا عن طريق إرسال الأموال أو تقديم معلومات شخصية عبر الإنترنت، والتي يستغلها مرتكب الجريمة بعد ذلك خارج الإنترنت لارتكاب السرقة أو الاحتيال.

تشبه هذه الجرائم جسرًا يربط بين أرضين منفصلتين حيث تؤدي البداية الرقمية إلى عواقب ملموسة في العالم الحقيقي، وتؤكد هذه الأنواع من الجرائم شبكة الاتصال المعقدة بين الأنشطة عبر الإنترنت والتداعيات خارج الإنترنت. مما يعزز الحاجة إلى تدابير قانونية وحماية شاملة ومنفصلة. وعلى العكس من ذلك تبدأ الجرائم الهجينة التي تبدأ فعليًا في العالم غير المتصل بالإنترنت وتبلغ ذروتها أو تمتد إلى المجال الرقمي. ومن الأمثلة على ذلك عملية السطو التقليدية حيث يتم استخدام المستندات المادية المسروقة، مثل بطاقات الائتمان أو الهوية الشخصية عبر الإنترنت لإجراء عمليات شراء غير مصرح بها أو إنشاء هويات رقمية احتيالية. تتطلب الطبيعة المزدوجة لهذه الجرائم اتباع نهج متعدد الأوجه للوقاية والتحقيق والملاحقة القضائية.

- **الجرائم العالمية المادية:**

لا يمكن ارتكاب الاعتداء الجسدي والقتل، باعتبارهما أعمال عنف جسدية مباشرة عبر الإنترنت، وتتطلب هذه الجرائم تفاعلًا ملموسًا وواقعيًا بين الجاني والضحية، ومع ذلك فإن الخط الفاصل بين العالمين المادي والافتراضي أصبح غير واضح بشكل متزايد، وقد تجد جرائم مثل هذه أصولها في الميتافيرس وفي البيئة الافتراضية الواسعة، يمكن لمرتكبي الجرائم الانخراط في اختيار الضحايا والتخطيط، وحتى التآمر مع الأخرين. لقد أضاف استخدام الميتافيرس لهذه الأنشطة الأولية بعدًا جديدًا للأنماط الإجرامية التقليدية، حيث تشابك المادي مع الافتراضي. إن العلاقة بين هذين العالمين تزيد من تعقيد طبيعة التحقيقات الجنائية، حيث يجب على جهات إنفاذ القانون أن تنتقل بين المسارات الرقمية التي خلقها المجرمون والأدلة الملموسة الموجودة في العالم المادي. كما أن الطبيعة الدولية لقضاء الجريمة تزيد من تعقيد التحقيقات الجنائية، قد تمتد الجرائم عبر مناطق جغرافية، مما يؤدي إلى نسج شبكة متعددة تتجاوز الحدود التقليدية، على سبيل المثال قد يستهدف مرتكب الجريمة الموجود في المملكة المتحدة ضحية في الصين، كل ذلك ضمن الحدود الافتراضية للميتافيرس المستضاف على خوادم في الولايات المتحدة، هذا السيناريو ليس نظريًا فحسب بل شائع بشكل متزايد في عصر الاتصال العالمي. تثير مثل هذه الجرائم الولية قضايا معقدة فيما يتعلق بالولاية القضائية والتي تنطوي على أنظمة قانونية متعددة.

٥- سيناريوهات تهديدات الجرائم المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة:

على الرغم من أن هناك الكثير من عدم اليقين بشأن الجرائم الفعلية التي يمكن أن يتم تمكينها بواسطة الميتافيرس إلا أن توقع التهديدات المحتملة الآن أمر مهم، حيث إن القيام بذلك يساعد أصحاب المصلحة مثل وكالات الشرطة والهيئات التنظيمية والحكومات ومقدمي الهجمات على الاستعداد لما قد يأتي ومعالجة مثل هذه التهديدات بشكل مثالي قبل ظهور حصاد جديد للجريمة.**(Gomez – Quintero, 2024:2)**

ويستضيف العالمان الميتافيرس والعالم الافتراضي مجموعة واسعة من الأنشطة بدءًا من التواصل الاجتماعي والألعاب وحتى التجارة الافتراضية، في نفس البيئات يمكن

أن تحدث سلوكيات غير قانونية وضارة بشكل عام مثل الجرائم التي يتم تسهيلها عبر الإنترنت أو الجرائم التي تنفذ عبر الإنترنت.

ويشمل سوء السلوك الافتراضي في الميتافيرس الإجراءات التي تنتهك القواعد أو المعايير الأخلاقية أو الأطر القانونية التي يتراوح من القواعد البسيطة وانتهاكات شروط الحرفة إلى الجرائم الخطيرة، يمكن أن تؤدي الطبيعة المجهولة للتفاعلات عبر الإنترنت في كثير من الأحيان إلى سلوك عدواني، وتنمر عبر الإنترنت واضطرابات نفسي، مما يعرض سلامة وشمولية الفضاء الإلكتروني للخطر، تنتشر السرقة والاحتيال والقرصنة الافتراضية في الاقتصاديات الافتراضية مما يؤدي إلى خسائر مالية وتقويض الثقة والعنف الافتراضي (أي قيام لاعبي الألعاب الافتراضية بإثارة الآخرين ومضايقاتهم عمدًا) والهجمات الافتراضية يمكن أن تضر بالأفراد ورفاهية المجتمع، يتضمن هذا التكرار التالي للجرائم في البيئة الرقمية السلوكيات المعروفة والطرق التي تحدث بها السلوك والجريمة، مع التأثير في العالم غير المتصل بالإنترنت ومنه، في حين قد يظهر بعض الأنواع الجديدة أو الأشكال المختلفة من الجريمة في البيئات الغامرة، يمكن لمثل هذه السلوكيات أن تطمس الخطوط الفاصلة بين العالمين المادي والرقمي، مما يجعل من الصعب تحديد الولاية القضائية ومحاسبة الجناة عن الجرائم المرتكبة في هذه البيئات الافتراضية. **(Coldncil of Europe, 2024: 21)**.

إن الطبيعة الغامرة وزيادة إخفاء الهوية لـ الميتافيرس تربط الناس بطرق جديدة ومثيرة بينما تفضل الأشخاص بشكل عكسي عن العالم الحقيقي وتأثير سلوكهم وأفعالهم ويؤدي هذا جنبًا إلى جنب مع الافتقار إلى التنظيم والرقابة إلى ديناميكية جديدة للضرر الإجرامي حيث يشعر الأفراد بأنهم أكثر قدرة على الانخراط في سلوك إجرامي أو غير أخلاقي بينما يحرمون في الوقت نفسه الضحايا الأقل قدرة على التماس الانصاف أو العدالة. لقد أنشأ الإنتربول مجموعة من الخبراء في الميتافيرس تعمل على تصنيف للجرائم في الميتافيرس والذي سيعمل على توفير اطار توجيهي للتنسيق والتعاون بين وكالات إنفاذ القانون في جميع انحاء العالم على الرغم من أن التصنيف لا يزال قيد التنفيذ، فقد شارك (ووكيونج يونج) من الإنتربول فئات واسعة من الجرائم في الميتافيرس وتشمل: **(Responsible, 2023: 5)**.

- الجرائم الواقعة على السلامة العامة (الإكراه).
- الجرائم الإلكترونية؛
- جرائم الملكية– جرائم الملكية الفكرية؛
- الجرائم المالية؛
- الجرائم ضد الأطفال (الاعتداء والعنف الجنسي؛
- الجرائم المتعلقة بالإرهاب؛
- الأفعال التي تهدف إلى إثارة الخوف أو الاضطراب العاطفي.

ويمكن مناقشة سيناريوهات تهديدات الجرائم المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة على النحو التالي:

جدول رقم (٥) سيناريوهات تهديدات الجرائم المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة

الأنماط	سيناريوهات التهديد والمخاوف الأمنية
الجرائم المالية	– **السرقة / الخداع السيراني:** **من المحتمل أن تكون هناك العديد من الفرص الجديدة للسرقة الإلكترونية والخداع الإلكتروني، في العوالم الاجتماعية الافتراضية. يصعب الحكم على السرقة المحتملة للأشياء الافتراضية من وجهة نظر قانونية وهي أيضًا نوع جديد من الجرائم لا يمكن تصوره إلا في عالم افتراضي اجتماعي (Cornelius & Herman, 2011: 2023)** – **الاحتيال المالي:** **سيتم جذب المجرمين والجماعات الإجرامية إلى هذا العالم بسبب الحجم الهائل للمعاملات التجارية الإلكترونية التي ستحدث في هذه العوالم، سيكون هناك الكثير ممن يحاولون استغلال المستخدمين وسرقة أموالهم والاستيلاء على أصولهم الرقمية. (Huq (et. al), 2022: 9).** – **هجمات البلوكتشين:** **قد يقدم الميتافيرس اقتصادًا رقميًا جديدًا غير متجانس يتضمن Bitcoin وEthereum و Pay pal والتحويلات الإلكترونية وما إلى ذلك، سوف يعمل هذا الاقتصاد في الميتافيرس حيث سيتم التحكم في أسعار الصرف من خلال السوق الحرة وسوف يصبح هدفًا رئيسًا للمجرمين ذوي الخبرة المالية الذين يحاولون التلاعب بالسوق واستغلاله .(Huq (et. al), 2022: 9)** – **سرقة الهوية لتحقيق مكاسب مالية:** **تعني زيادة اعتماد ووظائف تكنولوجيا الميتافيرس أن الهويات الرقمية والوصول إليها سوف تصبح أكثر قيمة، نظرًا لأن التمثيل الافتراضي للمستخدمين في الميتافيرس سيصبح أكثر واقعية ودائم، ومن ثم فإنه هذا يوفر فرصًا لنسخ مظهر المستخدم بشكل مقنع (ما يسمى بالتزييف العميق).ومع وجود طرق أكثر تقدمًا للتفاعل مع النظام باستخدام أجهزة استشعار مختلفة وتتبع العين، وتتبع الوجه واللمس على سبيل المثال ستكون هناك معلومات بيومترية أكثر تفصيلًا حول المستخدمين الفرديين، ستسمح هذه المعلومات للمجرمين بانتحال شخصية شخص ما، وسرقة هويته بشكل أكثر إقناعًا، علاوة على ذلك يمكن استخدام هذه المعلومات للتلاعب بالمستخدمين بطريقة أكثر دقة بكثير ولكنها أكثر فعالية بكثير مما هو ممكن في الوقت الحاضر على الإنترنت. (Europol, 2022: 13)**

الأنماط	سيناريوهات التهديد والمخاوف الأمنية
	– التزييف: يمكن للجهات الفاعلة الخبيثة إنشاء سلع رقمية مزيفة (بما في ذلك NFTS) تتظاهر بأنها منتجات مشروعة من علامات تجارية على سبيل المثال حقائب Guuci الرقمية المزيفة. (DAWES, 2024: 5)
NFTS	الرمز الغير القابل للاستبدال (NFTS) هو وحدة فريدة من البيانات التي يتم تخزينها في Block Cain ويمكن بيعها وتداولها، يمكن أن تتضمن بيانات NFTS تجزيئيات أو روابط الملفات الرقمية من النصوص والصور ومقاطع الفيديو والصوت، كما توفر NFTS شهادات عامة على صحة أو إثبات ملكية البيانات، على الرغم من عدم وجود أساس قانوني لهذا النوع من الملكية. ونلاحظ أن هناك قضايا تتعلق بالنزاهة، ومن ثم تنظم NFTS ملكية الأصول ولكنها لا توفر مساحة تخزين الأصول، قد يؤدي هذا إلى فدية أو هجمات إجرامية أخرى، إذ تم تشفير ملكات بيانات NFTS في ملف عند هجموه برامج الفدية، سيظل المستخدم محتفظًا بالملكية ولكن يمكن منعه من الوصول إلى الأصول إذ لم يدفعوا الفدية. في حين إنه من الممكن من حيث المبدأ استخدام NFTS للتحقق من ملكية الأصول الرقمية إلا أن الكثير من الأشياء لا يزال من الممكن أن تستمر خطأ على سبيل المثال، يتم التحقق من ملكية NFTS باستخدام blockchain بحيث تكون عرضة لهجمات اختطاف blockchain يمكن أن تكون NFTS التي تعتمد على سلاسل الكتل الأصغر عرضه لهجوم Sybil حيث يكتسب المهاجم السيطرة على أكثر من(٥٠%) من المعاملات وبالتالي يمكن التعامل مع التحقق من ملكية NFTS. (Huq, 2022: 7)
الجرائم الجنسية	– المواد الإباحية الفحش عبر الإنترنت: تقدم Social Metaverse طرقًا جديدة لتوزيع الصور الإباحية، في عام ٢٠٠٧م واجهت Second life مشاكل لأن المستخدمين صمموا صورًا رمزية لذلك يشبهون الأطفال ويتم عزمهم في صور إباحية وكان من السهل أيضًا شراء صورًا إباحية حقيقية وهمية للأطفال عن طريق البريد الإلكتروني من مستخدمي Second Life ودفع ثمنها باستخدام Linden Dollars، ويستغل بعض الأعضاء فرص النشاط التجاري التي توفرها شركة Linden lab لنشر الصور الإباحية للأطفال ويمكن النظر إلى هذا على الأقل كامتداد كمي لإمكانيات الإنترنت ويمكن القول أن العوالم الافتراضية الاجتماعية على وجه الخصوص تقدم طرقًا جديدة لتوزيع المواد الإباحية وخاصة فيما يتعلق بالعرض الوهمي للمواد الإباحية المتعلقة، ومع ذلك فهي ليست قناة توزيع جديدة نوعيًا .(Cornelius & Herman, 2011: 24) – الاستمالة للطفل: أثناء مراقبة السلوك في Metaverse تحدث أشكال جديدة من المضايقات؛ قد يمثل Metaverse للمكان المثالي للاستمالة الجنسية عبر الإنترنت، وقد يوفر لمرتكبي الجرائم الجنسية مع الأطفال فرصًا للتعامل مع الأطفال (أي من خلال الألعاب) وتعميق تفاعلهم مع الأطفال أو تصعيد السلوك دون الإضرار إلى مغادرة هذه البيئة. في الوقت الحالي يقوم المجرمين بإقناع الأطفال في إحدى الألعاب عبر الإنترنت أو وسائل التواصل الاجتماعي أو غرف الدردشة بتقديم تفاصيل شخصية، وفي عالم Metaverse قد يتمكن الجناة من تنفيذ عملية الاستمالة بأكملها دون مثل العوائق، سيكون من الصعب جدًا على الأطفال التمييز بين البالغين والأطفال الآخرين لأنه سيكون من الصعب معرفة من يتحدثون معهم خاصة بالنسبة للأطفال، كما ستوفر هذه الظروف بيئة تمكينيه خطيرة لجهود الاستمالة وأي شكل من أشكال الاستغلال الجنسي للأطفال (Europol, 2022:18) – مواد الاعتداء الجنسي على الأطفال:

الأنماط	سيناريوهات التهديد والمخاوف الأمنية
	يمكن تقديم مواد الاعتداء الجنسي على الأطفال في الميتافيرس، حيث يمكن استخدام أجهزة Teledildonics والمعدات واستخدام البدلات اللمسية وغيرها من المعدات الغامرة لجعل التجربة أكثر واقعية، كما قد يؤدي البث الشامل المدفوع لمواد الاعتداء الجنسي على الأطفال إلى إشراك الجناة والضحايا في اماكن بعيدة يمكن أن تتفاقم الأضرار، كما يمكن إنشاء مساحات مشفرة متعددة المستخدمين بحيث يتمكن العديد من المستخدمين من تجربتها معًا. – التحرش: في الإعدادات الافتراضية يمكن أن تقترب صور رمزية أخرى من المستخدمين لمضايقتهم، يمكن حتى مطاردتهم عبر منصات الميتافيرس المختلفة. – جرائم الصور الجنسية غير الرضائية: يمكن للجهات الفاعلة الضارة استغلال المواد الشخصية والحساسة التي يشاركها المستخدمون في أفعال جنسية غير رضائية في الواقع الافتراضي، وقد يتضمن ذلك استخدام التزييف العميق. (DAWES, 2024: 4). – الاتجار الافتراضي: يمكن استغلال الصور الرمزية للمستخدمين الضعفاء جنسيًا بشكل متكرر في إعدادات افتراضية دون الحاجة إلى عبور الحدود أو الاختفاء. (DAWES, 2024: 4).
الإرهاب	يمكن أن تؤثر التحولات أيضًا على الأمن الدولي بالمعنى التقليدي، أثار الباحثون في المركز الوطني لمكافحة الإرهاب والابتكار والتكنولوجيا والتعليم التابع لجامعة بنراسكا؛ مخاوف بشأن قدرة المتحولين على مساعدة الجماعات الإرهابية في حملات التجنيد، ويؤكدون أن التجنيد والمشاركة عبر الإنترنت هما من السمات المميزة للجماعات الإرهابية (Rickli & Mantellass, 2022: 8). حيث سيحاول الإرهابيون دائمًا استغلال الخيارات التكنولوجية الجديدة لتسجيل أنشطتهم وفي حالة الميتافيرس قد يؤدي ذلك إلى فرص جديدة للمنظمات الإرهابية في المقام الأول للدعاية والتجنيد والتدريب. ومع وجود المزيد من التكنولوجيا الغامرة والبيانات المولدة ذات الصلة تحت تصرفهم، سيصبح من الأسهل على الإرهابيين اختيار واستهداف الأشخاص الضعفاء، وتصميم رسائلهم بما يتناسب مع تحيزاتهم وهذا سيمكنهم من استهداف دعايتهم وتجنيد الأشخاص بشكل أكثر فعالية. كما يمكن لأعضاء مثل هذه الأماكن أن يعيشوا حياتهم الافتراضية وفقًا لقواعد قد تتعارض مع القوانين والقيم الأساسية للمجتمع الذي يعيشون فيه في العالم المادي، بل إن هذه العوالم الافتراضية قد تسمح لهم بفرض قواعدهم المتطرفة على أي شخص يدخل إلى "دولتهم" وهذا من شأن أن يخلق عالمًا موازيًا حقًا لهؤلاء الناس ليعيشوا فيه ينفذوا سيناريوهات تعوض القبول العام لسادة القانون، علاوة على ذلك فإن مثل هذه الأماكن من شأنها أن توفر بيئة مثالية لتجنيد الأشخاص للقيام بالأنشطة الإرهابية في عوالم افتراضية أخرى بل وحتى في العالم المادي. (EUROPOL, 2022: 19)
التطرف	يمكن أن يصبح الميتافيرس أداة قوية للجماعات المتطرفة لتوسيع صفوفها من خلال تكثيف جوانب الإنترنت التي تسهل التطرف من خلال إمكانية تمكين علاقات شخصية افتراضية أكثر واقعية من شأنها أن تقلل من أهمية عنصر التطرف "غير المتصل بالإنترنت"، علاوة على ذلك يمكن للمرء أن يفترض أن العمليات يمكن أن تسهل على الجماعات الإرهابية إجراء استطلاع وتنسيق الهجمات لا سيما من خلال تكرار أهداف رقمية والتدرب على الهجمات مسبقًا. (Rickli & Mantellassi, 2022: 8).
جرائم الملكية	– هجمات البنية التحتية: سيكون الميتافيرس بيئة تفاعلية للويب المكاني؛ الويب المكاني عبارة عن بيئة للحوسبة الموجودة في الفضاء ثلاثي الأبعاد – توأمة بين الواقع الحقيقي والافتراضي عبر المليارات من

الأنماط	سيناريوهات التهديد والمخاوف الأمنية
	الأجهزة المتصلة وتمكن الوصول إليها من خلال واجهات (VR – AR – MR –XR) هذا التكامل بين الإنترنت الأشياء والإنترنت العوالم يمكن أن تؤدي إلى تهديدات سيرانية مادية. وسوف تحدث التفاعلات بين الكيان والمستخدم عبر الميتافيرس على سبيل المثال يمكن للبنية التحتية للمدينة الذكية أن تفعل ذلك التواصل مع المستخدمين الذين يرتدون مزارات الواقع المعزز التي تدعم تقنية الميتافيرس وهذا يمكن أن يؤدي إلى طرق تهديد جديدة مثيرة الاهتمام على سبيل المثال (هجمات رجل في الوسط (MitM) والوصول غير القانوني إلى البنية التحتية لـ ICS/SCADA والوصول غير المصرح به إلى التوائم الرقمية وما إلى ذلك وطرق جديدة لاستغلال القوى السيرانية المادية. كما ستحتوي مرافق البنية التحتية الحيوية (CI) على معدات مادية متصلة بالتوائم الرقمية، سيتم الوصول إلى المساحات عبر الميتافيرس يؤدي هذا إلى تحسين العمليات ويتيح العمل عن بعد، ولكن من المحتمل أيضًا أن تتعرض CI للهجمات الالكترونية الخارجية عبر الميتافيرس (Huq, 2022: 11) – السطو المادي السيراني يمكن استغلال الواقع الافتراضي والواقع المعزز ومواد الاستشعار الذكية الأخرى من قبل المستخدمين الضارين للحصول على معلومات مثل(الموقع والوصول والأشياء الثمينة)حول الممتلكات ومحاولة السطو على المواقع الفعلية. – التعدي على ممتلكات الغير يمكن للمجرمين التعدي على الممتلكات الافتراضية أو الأحداث الافتراضية في الميتافيرس دون إذن.
جرائم ضد الأشخاص	– الهجمات المادية السيرانية يمكن إساءة استخدام الواقع الافتراضي والواقع المعزز والبدلات اللمسية وغيرها من الأجهزة القابلة للارتداء من قبل جهات ضارة لتسبب أضرارًا للمستخدمين على سبيل المثال التلاعب محدود النشاط البدني المحددة في الجهاز. – التحريض على إيذاء النفس يمكن أن يجتمع العديد من المستخدمين معًا في بيئة افتراضية، ويمكن جعل الصور الرمزية المصممة بواسطة الذكاء الاصطناعي أكثر تعاطفًا من أجل تحريض المستخدمين الضعفاء على إيذاء أنفسهم. – استغلال المستخدمين المدمنين لأغراض الابتزاز أو الإكراه أو التحريض: يمكن أن يقع الأفراد الضعفاء فريسة للمغرضين والمنظمات الإجرامية لاستغلالهم ماليًا أو تحريضهم على ارتكاب الجرائم. – عمالة الأطفال العبودية الحديثة لتطوير محتوى الميتافيرس وسيخلق الطلب على السلع والأصول والخدمات الرقمية حوافز لتعويض المنافسين، ربما عن طريق استخدام عمالة الأطفال والعبودية الحديثة. – انتحال صفة يمكن للمجرمين التظاهر بأنهم سلطات إنفاذ القانون في الميتافيرس لمجموعة متنوعة من الأغراض، بما في ذلك الحصول على معلومات استخباراتية. (DAWES, 2024: 5) – الاستخدام غير المصرح به يمكن للجهات الفاعلة الخبيثة استخدام مساحات افتراضية مفصلة تشبه مواقع العالم الحقيقي مثل التوائم الرقمية للتخطيط والتدريب على ارتكاب الجريمة في العالم المادي. – الحرمان من الخدمات الأساسية يمكن للجهات الفاعلة الخبيثة منع الوصول إلى العديد من المستخدمين إلى الخدمات الأساسية التي يتم توفيرها في الميتافيرس مثل الرعاية الصحية والتعليم (DAWES, 2024:5)

الأنماط	سيناريوهات التهديد والمخاوف الأمنية
Dark verse	يشبه Dark verse الويب المظلم، إلا أنه موجود داخل الميتافيرس في بعض النواحي، وهو أكثر خطورة من الويب المظلم بسبب الوجود المادي الزائف للمستخدمين، إنه يحاكي المادية السيرانية عبر الإنترنت في المنتديات الإجرامية على شبكة الإنترنت المظلمة، الكون المظلم يعيش داخل الكون العميق وهو غير مفهرس مثل الويب العميق. لقد تم إنشاء dark verse لتسهل أنشطة غير قانونية أو إجرامية فقط بل يمكن استخدام الفضاء لحرية التعبير ضد الحكومات القمعية. كما يمكن أن تكون مساحة للأسواق السريعة في الميتافيرس؛ حيث يتم استخدام الأسواق للأنشطة غير القانونية أو الإجرامية وربما يحتاج المستخدمون إلى رموز المصادقة للوصول حيث إذا كانت الحالات إنفاذ القانون (LEA) على علم بهذه المساحات فلن تتمكن من التسلل إليها بدون رموز المصادقة هذا يعني أن مخبأ الميتافيرس يمكن أن يكون موجودًا على مرأى من الجميع ويكون غير قابل للوصول إلى LEA لأن LEA ليس لديها طريقة مراقبة المواد الإباحية المتعلقة بالأطفال أو الاعتداء الجنسي في Dark verse سوف تنمو هذه الأنواع من الجرائم تدريجيًا سوف تواجه LEA صعوبة في تعقب المجرمين. (Huq , 2022: 8).
تهديدات الواقع الافتراضي المعزز / المختلط	سيكون الميتافير موجودًا كعالم VRوعالم MR ستحدث تفاعلات المستخدم داخل الوضع ثلاثي الأبعاد أو مع كائنات ثلاثية الأبعاد معززة في العالم الحقيقي. ومن المتوقع أن تكون هناك مساحات تشبه VR Metaverse تتصل في غضون عامين إلى ثلاثة أعوام، بينما تتصل مساحات Metaverse AR/MRIبعد أربع أو خمس سنوات على الأقل يمكن للمستخدمين إنشاء هوية وحياة جديدة في Metaverse وما هي الآثار المترتبة على هذه الازدواجية في العالم الحقيقي؟ يمكن للمجرمين التظاهر بأنهم LEA في الميتافيرس لجمع المعلومات سيستخدم الأفراد السيئون عالمًا افتراضيًا للتخطيط والتدريب على جرائم العالم الحقيقي. سيحاول المجرمون منع الصور الرمزية للمستخدم من الوصول إلى الخدمات التي دفعوا مقابلها. أحد الأمثلة على ذلك هو منعهم من الوصول أو الخروج من مساحة افتراضية؛ حيث ستقوم الجهات الخبيثة من منع المستخدم حتى الوصول إلى الخدمات التي دفعوا مقابلها. ستقوم الشركات بإنشاء نسخ رقمية متماثلة لمتاجرها الحقيقية في الميتافيرس سوف ينسخ المجرمون هذه المتاجر الرقمية في مساحة مختلفة لخداع المتسوقين. ويمكن للمجرمين إنشاء مساحات الميتافيرس لنشر الأخبار المزيفة ويمكن تحويلها إلى مصائد جذب للواقع الافتراضي لأجهزة الاستخبارات. كما يمكن للمجرمين إنشاء مساحة وهمية من أجل جمع المعلومات الاستخبارية من المجموعات المستهدفة. (Huq, 2022: 12 – 13)
هجمات تكنولوجيا المعلومات التقليدية	مثل هجمات تكنولوجيا المعلومات التقليدية التي توفرها شركة Trend Micro وشركات الأمن الأخرى؛ نظرًا لأن عوالم Metaverse ستعمل على أجهزة تكنولوجيا المعلومات العادية فهي عرضة لهجمات تكنولوجيا المعلومات هذه من المرجح جدًا أن تستمر سيناريوهات تهديد تكنولوجيا المعلومات الحالية في الحدوث في Metaverse.يمثل الحرمان من الخدمة الموزعة (DDOS) للابتزاز مشكلة كبيرة في الميتافيرس وهي مكلفة للغاية عند تشغيليها، لذلك ستدفع المؤسسات مقابل إيقاف هجمات DDOS وتدفع أيضًا مقابل الغاية منها. يمكن للجهات الفاعلة السيئة تشفير الخوادم التي تخزن بيانات المستخدم أو الشركة واحتجازها كرهينة للحصول على فدية فبمجرد نشر واجهات برمجة التطبيقات لتطبيقات الميتافيرس ستحاول الجهات الفاعلة السيئة إرسال برامج ضارة وتعليمات برمجية أو التصيد للأشخاص من خلال استغلال واجهة برمجة التطبيقات.(Huq, 2022: 14)
معلومات خاطئة ومضللة	لقد أدى الويب الحالي إلى ظهور رؤى غير مسبوقة في القدرة على استهداف مجموعات سكانية محددة التأثير على سلوكهم سواء كان ذلك لتحقيق مكاسب تجارية أو سياسية الكمية الكبيرة والمتزايدة بشكل كبير من البيانات التي يمكن للأجهزة الجديدة جمعها من حسابات

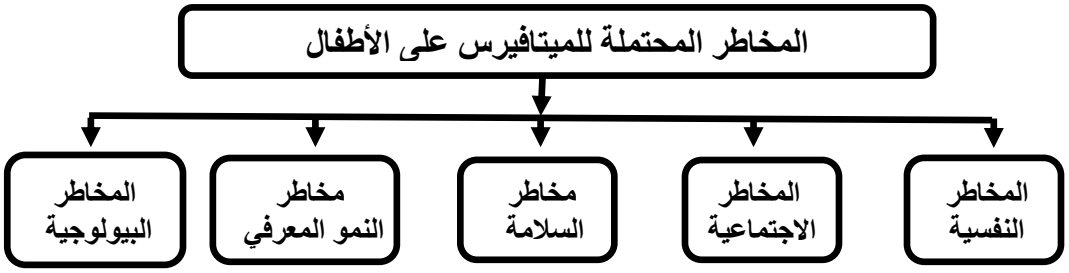
الأنماط	سيناريوهات التهديد والمخاوف الأمنية
	المستخدمين، سيكون للبيئة المباشرة ومن المستخدمين أنفسهم القدرة على تأثير بشكل كبير بكثير على سلوك الناس، وبما أن هذا قد يؤدي إلى زعزعة استقرار المجتمعات التي تكلف سلطات إنفاذ القانون بحمايتها وقد يستخدم مجرمون نفوذهم لاستهداف ضحاياهم. **لقد ساعدت شبكة الإنترنت القديمة على جمع كميات هائلة من البيانات حول التفضيلات والسلوك الفردي من خلال جمع البيانات المتاحة على وسائل التواصل الاجتماعي، ومتابعة ما يفعله الأشخاص عبر الإنترنت وتحويلها إلى مسار رقمي، يمكن استخدام هذا المسار للتلاعب بالأشخاص وتحديد هويتهم وتعقبهم عبر الإنترنت، فالتفاعلات الأكثر غامرة التي تتيحها التقنيات المزيفة بـ الميتافيرس ستخلق مسارًا رقميا أكثر بكثير.وسيتم جمع كميات غير مسبوقة من البيانات التي تسمح برؤى أكبر بكثير وقوة تنبؤيه للسلوك، وقد تسمح بتحديد هوية الأفراد بناء على تعرف هذه التفاعلات. مع الأخذ في الاعتبار إنه لا تسمح الرؤى حول تفضيلات الأشخاص وسلوكهم باستهداف أكبر دقة للمعلومات فحسب؛ بل قد تسمح أيضًا بتخصيص المحتوى وفقًا لهذه الرؤى، ن خلال استخدام هذه الأفكار لتعظيم فرص استقبال الهدف المقصود لرسالة معينة، من خلال الاستفادة من التجربة الغامرة كما يمكن أن تزداد القوة التي تمارس على سلوك المستخدم. وفي الوقت نفسه قد يصبح من المستحيل إزالة المعلومات الخاطئة نظرًا لأن انتشارها أصبح لا مركزيًا بشكل متزايد مع اعتماد تقنية Web3 على نطاق واسع. (Europol, 2022: 20)**

٦- سيناريوهات المخاطر المحتملة للإجرام الميتافيرس على الأطفال:

أظهرت الأبحاث مدى وصول الأشخاص الأصغر سنًا إلى الإنترنت، فطبقًا لدراسة بحثية أجرتها هيئة (Of Com) التنظيمية والمعنية بقطاع الاتصالات في المملكة المتحدة، أن جميع الأطفال الذين تتراوح أعمارهم بين (١٣و١٧) عامًا تقريبًا بنسبة (٩٧%) كانوا مستخدمين للإنترنت في عام ٢٠٢٢م، وفيما قد تحقق زيادة نسبة الوصول إلى الإنترنت واستخدامه بعض الفوائد، فإنه يُعرض الأطفال لمجموعة كبيرة من المخاطر ومنها الاستغلال والاعتداء الجنسي، كما تعني زيادة عدد الأطفال، على الإنترنت زيادة عدد الأهداف المحتملة للمعتدين وغيرها من العوامل المسببة للضرر **(تقييم التهديد العالمي،٢٠٢٢: ١٠)**.

ولابد من التأكيد على أن الألعاب عبر الإنترنت تعد وسيلة شائعة وهدفًا لمشتهى الأطفال وغيرهم من الأشخاص أحاب الاعتداءات الجنسية، وإذا اقترن التكرار الأكثر واقعية للتفاعلات في العالم الحقيقي بسهولة اللقاء في المساحات الافتراضية، فإن استمالة الأطفال وإقامة العلاقات المفترسة يمكن أن يحدث بشكل أسهل وأسرع.

(Rickli &Montellassi, 2022: 8).



شكل رقم (٢) يوضح المخاطر المحتملة للميتافيرس على الأطفال

ويمكن تناول ومناقشة أهم المخاطر المرتبطة بالميتافيرس والتقنيات الناشئة على الأطفال على النحو التالي:

- **المخاطر النفسية – المرض السيراني:**

من أبرز المخاطر التي تم تحديدها هو تطور الإدمان على هذه المساحات الافتراضية. فقد تم تعريف الإدمان على إنه عملية اضطراب انتكاس مزمن يصور بالإكراه البحث عن مادة أو سلوك واستخدامه، يشمل فقدان السيطرة في الحد من سلوكيات معينة أو تناول الدواء ويرتبط في الغالب بظهور مشاعر سلبية (مثل القلق).**(Hinz, 2022: 2)**

وتشير الأدلة الحديثة أن ضعف إمكانية استخدام HMDS الحديثة قد يكون ضارًا بالصحة العقلية. حيث قارنت إحدى الدراسات تجربة المشاركين الذين أمضوا أسبوع عمل مدته (٤٠ ساعة) في الواقع الافتراضي، وأخرى في بيئة مكتبية تقليدية وباستخدام تطبيق الواقع الافتراضي القياسي المتوفر؛ أظهرت الدراسة زيادة نسبة (٣٥%) في عبء العمل المتصور عند تنفيذ العمل في بيئة عامرة. وقد أبلغ المشاركون عن شعور بالإحباط بنسبة (٤٢%) والقلق بنسبة (١٩%) وإجهاد العين بنسبة (٤٨%) مع انسحاب اثنين منهم من الدراسة في اليوم الأول بسبب الصداع النفسي والغثيان والقلق، ومن النتائج المهمة الأخرى هي الطبيعة المتراكمة للتأثيرات السلبية على مدار الأسبوع، خاصة فيما يتعلق بعبء العمل والغثيان **(Berastegui, 2024: 5)** بالإضافة إلى الدوخة والارتباك الذي يحتمل أن يحدث بسبب الصراع بين المحفزات البصرية والجهاز الدهليزي، بالإضافة إلي أمراض الحركة الأخرى مثل دوار السيارة أو دوار البحر. ومن الجدير بالذكر أن التأثيرات

التي ترتبط خطورتها بمدة اللعب تكون مؤقتة، ويعاني منها الأطفال بدرجة أقل أو بعد فترات تعرض أطول من البالغين.**(Hinz, 2022:4)**

- **المخاطر الاجتماعية:**

ما زالت قصة الاستغلال والاعتداء الجنسي على الأطفال عبر الإنترنت قضية مركبة ومتعددة الأوجه، ومن عام ٢٠٢١ بدأت توجيهات جديدة للإضرار في الظهور، في حين أن الإضرار التي كانت موجودة مسبقًا ما زالت لم يتغلب عليها، وتشكل الصور ومقاطع الفيديو النسبة الأكبر في هذا النوع من الاعتداء، وفي عام ٢٠٢٢ بلغت نسبة الوقائع التي تنطوي على مواد يشتبه في كونها مواد اعتداء جنسي على الأطفال أكثر من (٩٩.٥%) من البلاغات التي تلقاها المركز الوطني للأطفال المفقودين والمستغلين ومن بين (٨٨.٣) مليون ملفًا قدمتها الشركات المقدمة للخدمات الإلكترونية في العام نفسه كان هناك(٤٩.٤ مليون صورة و٣٧.٧ مليون مقطع فيديو) **(تقييم التهديد العالمي، ٢٠٢٣: ٢٠)**

- **مخاطر السلامة:**

تحجب أجهزة الواقع الافتراضي HMDS رؤية العالم الحقيقي، مما يؤدي إلى تفاقم خطر الإصابات الذاتية أثناء الاستخدام، قد تكون هذه الإصابات ناجمة عن الاصطدام بإنشاء هذا العالم الحقيقي أو التعثر. في نظام الواقع الافتراضي فإن التطورات الأخيرة في أجهزة HMDS قللت بشكل كبير من خطر الاصطدام اثناء الانغماس في بيئة الواقع الافتراضي مثل HMDS المستقلة (أي بدون أسلاك أو كابلات متصلة) أو استخدام الحدود الافتراضية لمسائلة المستخدم على البقاء داخل المنطقة الخالية. لقد تم العثور على أن التأثيرات قصيرة المدى بعد استخدام الواقع الافتراضي تشمل انخفاض عمق الإدراك، وانخفاض وقت رد الفعل، وصعوبة التركيز يمكن أن يؤدي هذا الضعف في الأداء الإدراكي بدون أي إصابات مستدامة تنطوي على سبيل المثال على مخاطر الانزلاق أو التعثر أو السقوط. في الواقع هناك بعض الأدلة التي تشير إلى التأثير السلبي للواقع الافتراضي على التوازن بعد الاستخدام لفترة طويلة، بالإضافة إلى عدد من دراسات الحالة التي توضح إنه حتى السقوط منخفض التأثير يمكن أن يسبب إصابات كبيرة. على

سبيل المثال أبلغ (وارنر ويتو) عن حالة سقوط منخفض التأثير مرتبط بالواقع الافتراضي مما أدى إلى إصابة الحبل الشوكي وإصابة العصب تحت اللسان وتشريح الشريان الفقري، وإصابة الدماغ المؤلمة، هناك أيضًا خطر محتمل بحدوث عواقب وخيمة إذا شارك الفرد في نشاط مثل القادة أو أداء المهام التي تتطلب التنسيق الدقيقي بين اليد والعين مباشرة بعد الانغماس في بيئة افتراضية، أخيرًا قد تؤدي الإشارات الصوتية المقنعة في العديد من البيئات الغامرة إلى قطع التحفيز الصوتي، بشكل فعال عن العالم الحقيقي مما يطرح المزيد من مشكلات السلامة بالمستخدمين. **(Berastegui, 2024: 4)**.

- **المخاطر البيولوجية:**

تؤدي HMDS المعرضة للاستخدام المستمر بمستويات عالية إلى الملوثات البكتيرية، أي ما يعادل أو يتجاوز تلك الموجود على لوحات مفاتيح الكمبيوتر بسبب تصميمها، تساهم HMDS إلى جانب الحرارة المتولدة عن الجهاز، انها تصبح أرضًا خصبة لتكاثر البكتريا المختلفة، تم اكتشاف مجموعة متنوعة من الملوثات البكتيرية المختلفة. لقد ثبت أن التعقيم باستخدام (٧٠%) من الايثانول هو وسيلة فعالة لتقليل خطر التلويث والعدوى من سماعات الواقع الافتراضي. **(Berastegui, 2024: 4)**

- **مخاطر النمو المعرفية:**

يمكن أن تشكل التقنيات المرتبطة بـ Metaverse و XR مخاطر على النمو المعرفي والاجتماعي للأطفال، ففي دراسة أجريت حول كيفية استجابة البالغين والأطفال لتجارب الواقع الافتراضي تمكن البالغون من استخدام قشرة الفص الجبهي لتنظيم ما كانت أدمغتهم تعالجه أثناء محاكاة وهمية، ولم يفعل الأطفال المشاركون في الدراسة (متوسط أعمارهم ثماني سنوات) وذلك بنفس القدر ونتيجة لذلك لم يتمكنوا دائمًا من التميز بين العالم الافتراضي والعالم الحقيقي. ويشير "توماس بومفارتنر" إلى أن قشرة الفص الجبهي لدى الأطفال بعيدة كل البعد عن التطور الكامل في هذا العمر. وعندما تصبح البيئات أكثر واقعية وغامرة؛ قد يكون من الصعب على الأطفال فهم الخط الفاصل بين العالم الافتراضي والعالم الحقيقي، مما يؤثر على فهم الأطفال للواقع. ونلاحظ أن دمج سماعات

الرأس XR مع واجهات الدماغ والحاسوب (BCIS) مثل أجهزة استشعار مخطط كهربية الدماغ (EEG) يمكن أن "يسمح لمطوري التطبيقات ومصمم الألعاب بإنشاء "ألعاب مخصصة " لتستجيب بشكل مختلف بناء على ما إذا كان المستخدم متحمسًا أو سعيدًا أو حزينًا". فقد حذر الخبراء من أن الميتافيرس يمكن أن يعزز رؤية ممزقة للواقع مما يؤدي إلى غرف صدى أو حقائق موازية. يمكن أن يرى مستخدمان في نفس البيئة الافتراضية إعلانات أو رسائل أو أنشطة سياسية مختلفة دون معرفة ذلك، مما يزيد من صعوبة تحديد المعلومات الخاطئة. **(UNICEF, 2019: 19)**

- **المخاطر المالية:**

إن للعوالم الافتراضية اقتصادات وتحديات مرتبطة بها، قبل وقت طويل من دخول مفهوم "ما وراء الكون" إلى الخطاب العالمي، تتعلق إحدى المجموعات من المشاكل بحوكمة هذه الاقتصادات:إما أن تحدد الشركات الخاصة أسعار الصرف أو توريد العملات بشكل مباشر، أو تحدد الأسعار والعرض للعناصر داخل اللعبة أو في العالم، مما يجعلها بنوك مركزية أو سندات خزانة بحكم الأمر الواقع، مع عدم وجود مساءلة حقيقية وتتعلق المجموعة الثانية من المشاكل بالمنطقة الرمادية بين الأسواق والأنشطة الاقتصادية غير المتصلة بالإنترنت شديدة التنظيم (بما في ذلك أسواق العمل والافتراض، والإقراض، توفير الخدمات المالية) ونظيراتها في العالم الافتراضي، على سبيل المثال، تقع العملات المشفرة على نطاق واسع من المعاملة التنظيمية في بلدان مختلفة وفي البيئات غير المنظمة بشكل كاف.

ومن أشكال الاعتداء والأضرار والمخاطر الأخرى للأطفال عبر الميتافيرس والتقنيات الناشئة:

- **الإكراه وإنتاج مواد الاعتداء الجنسي على الأطفال:**

شهدت حالات الابتزاز الجنسي المدفوع أسباب مالية وإكراه الأطفال زيادة في العام الماضي، ففي عام ٢٠٢٢ تلقى المرز الوطني للأطفال المفقودين والمستغلين١٠ آلاف بلاغ مقارنة بـ ١٣٩ بلاغًا في عام ٢٠٢١ حيث أن الأطفال هم الفئة المعرضة للمخاطر

على وجه الخصوص ففي استطلاع للرأي شمل أكثر من ١٥٠٠ من الضحايا الناجين، كان أكثر من (٤٦%) من الأطفال. وتجدر الإشارة إلى أن الابتزاز الجنسي والإكراه المدفوعين بأسباب مالية يسببان صدمات شديدة للضحايا وأدى إلى إقدام عدد من الأطفال على الانتحار. حيث يعمد الجناة إلى خداع الأطفال وابتزازهم لإنتاج محتوى جنسي "منشئ ذاتيًا" ومشاركتهم معهم بغرض تحقيق أرباح مالية والكثير من المبتزين ينتحلون صفة فتيات صغيرات عبر الإنترنت وفي الأغلب يتواصلون مع الفتيات الذين يتراوح أعمارهم ما بين (١٥ –١٧ عامًا) عبر شبكات التواصل الاجتماعي مقترحين عليهم تبادل صور ذات طابع جنسي صريح. فقد كشف تحليل المركز الكندي لحماية الطفل (C3P) شمل ٦٥٠٠ منشورًا عامًا لناجين – ضحايا للابتزاز الجنسي في عام ٢٠٢٢ عن استخدام العديد من المبتزين استراتيجيات مشابهة وفور إرسال ذات الطابع الجنسي الصريح يهدد المبتز بإرسال الصور إلى أصدقاء الطفل وأسرته ويواصل ابتزازه للحصول على أموال، ويضفي المبتزون مصداقية على التهديدات عن طريق إرسال لقطات شاشة لحسابات جهات الاتصال لدى الطفل على شبكات التواصل الاجتماعي. حيث أن هناك العديد من المخططات تنظمها عصابات إجرامية من خارج البلاد يقال أن منشئها بلدان مثل نيجيريا وكوت ديفوار والفلبين وتستهدف الأطفال الأكثر ثراء.

(تقييم التهديد العالمي، ٢٠٢٣ : ٢٠).

كما وجد تحليل الجناة المشاركين في الابتزاز الجنسي السيبراني أن مرتكبي جرائم الابتزاز الجنسي المدفوع بأسباب مالية يختلفون عن مرتكبي جرائم الابتزاز الجنسي السيبراني ذوي الدوافع غير المالية، فقد يستخدم النوعان الجنس لإغراء الضحايا– الناجين والإيقاع بهم إلى أن مطالب الفئة الأولى تكون مالية تمامًا ولا يبدو عليهم أنهم يسعون إلى مزيد من المواد ذات الطابع الجنسي الصريح ولا إلى اتصال بدني بالأطفال، أما الجناة الآخرون فقد يلجأون أيضًا إلى انتحال الشخصيات إلا أن جرائم الابتزاز الجنسي المالي تتطور سريعًا وغالبًا ما تنطوي على زيادة في المطالب مما يؤدي إلى شعور بالإلحاح **(تقييم التهديد العالمي، ٢٠٢٣: ٢٠).**

- **الـذكاء الاصـطناعي التوليـدي ومـواد الاعتـداء الجنسـي علـى الأطفـال المنشـأة بواسطة الكمبيوتر:**

شـهد استخدام العامـة لتقنيـات الـذكاء الاصـطناعي زيـادة مذهلـة ويقصـد بالـذكاء الاصـطناعي التوليـدي؛ خوارزميـات الـذكاء الاصـطناعي التـي تولـد مخرجـات جديـدة بنـاء علـى البيانـات التـي دربـت عليهـا. وبخـلاف أنظمـة الـذكاء الاصـطناعي التقليديـة المصـممة للتعرف على الأنماط وتقديم تنبؤات، فإن الذكاء الاصطناعي التوليدي ينشئ محتوى جديدًا في شكل صور ونصوص وأصوات وما إلى ذلك. ويستعمل Chat GPT وهو روبوت دردشة متاح للاستخدام مجانًا يعمل بالذكاء الاصطناعي التوليدي باستخدام معالجة اللغة الطبيعية (NLP) لبناء حوار يشبه الحوار البشري، ما يقدر بمليار زائر شهريًا. منذ مطلع عام ٢٠٢٢ تشهد حالات المعتدين الذين يستخدمون الذكاء الاصطناعي التوليدي لإنشاء مواد اعتداء جنسي على الأطفال واستغلال الأطفال تزايدًا مستمرًا. وقد وجدت مؤسسة "Thorn" أنه بينما يعد أقل من (١%) من ملفات الاعتداء الجنسي على الأطفال التي تمت مشاركتها في العينة التي تمثل مجتمعات الجناة هي صور اعتداء جنسي على الأطفال واقعية منشأة بواسطة الكمبيوتر، فإن حجم هذه المواد يتزايد زيادة مطردة منذ اغسطس ٢٠٢٢. وفي مدة خمسة أسابيع من عام ٢٠٢٣ فحصت مؤسسة مراقبة الإنترنت ٢٩ بلاغًا لروابط (URL) تحتوي على صور يشتبه في كونها اعتداء جنسي على الأطفال، وشملت صفحات الويب التي ازيلت مواد من الفئة (أ) والفئة (ب) لفتيان وفتيات، ظهر فيها أطفال يتراوح أعمارهم بين (١٣ و١٦ عامًا) **(تقييم التهديد العالمي، ٢٠٢٣: ٢١)**.

- **استمالة الأطفال وإكراههم لإنتاج مواد جنسية " المنشأة ذاتيًا":**

أشارت الأبحاث إلى أن معدلات انتشار الاستمالة عبر الإنترنت يتراوح بين (٩% و١٤%) وتظهر بيانات البلاغات الواردة من الجمعية الوطنية لمنع القسوة ضد الأطفال (NSPCC) أيضًا ارتفاعًا في جرائم الاستمالة عبر الإنترنت بنسبة (٨٠%) خلال السنوات الأربع الأخيرة، وتبين أغلب الدراسات إلى زيادة الاستمالة عبر الإنترنت

بين الفتيات إلا أن تلك الفوارق بين الجنسين أقل وضوحًا بين الأطفال الذين تقل أعمارهم عن(١٣ عامًا). بالإضافة إلى ذلك يحدد العديد من المعتدين الذين يحاولون استمالة الأطفال أهدافهم على شبكات التواصل الاجتماعي وفي غرف الدردشة ومنصات الألعاب وغير ذلك من المنصات التي تسمح بالتواصل المباشر بين المستخدمين، وينتقل المعتدون بالمحادثات إلى أحد تطبيقات المراسلة الخاصة أو بيئة تعمل بتقنية التشفير بين الطرفين لانخفاض احتمالية اكتشافها وهو أسلوب يعرف باسم "الاستدراج إلى خارج المنصات "وفي الدراسة المشتركة بين التحالف وبين "Economist Impact" التي شملت ٢٠٠٠ مراهقًا في عمر (١٨ عامًا) على مستوى أربعة بلدان أوروبية، كان (٥٤%) من المشاركين الذين وصلتهم مواد ذات طابع جنسي صريح قد استلموا بعضها على الأقل عبر إحدى خدمات مشاركة الفيديو الخاصة، (٤٦%) استلموها عبر إحدى خدمات المراسلات الخاصة. حيث يفترض في الاستمالة على الأغلب أنها نشاط مطول يبين فيه المعتدي ثقة بينه وبين الطفل على مدار أيام وأسابيع بل وشهور، فالمحادثات على منصات الألعاب الاجتماعية يمكن أن تتحول سريعًا إلى موقف عالي الخطورة.

ولا يفوتنا أن ننوه إلى أن هناك أربعة أصناف للمستميلين استنادًا إلى بناء العلاقات والحديث عن الأمور الجنسية وأساليب الإخفاء: المستميل الباحث عن علاقة حميمة، والمستميل المخلص صاحب السلوك الجنسي القهري، والمستميل الاجتماعي، والمستميل الاجتماعي الانتهازي. حيث تشكل الاستمالة خطرًا ملحوظًا في بيئات الألعاب متعددة اللاعبين على الإنترنت وذلك لأن الميزات البيئية التي تتسم بها بيئة الألعاب الأمر الذي يؤدي إلى زيادة كبيرة في الاحتمالات الكلية لتعرض الطفل للاستغلال، ويقدم تقرير الألعاب وعلم الميتافيرس Gaming and Metaverse الصادر عن مؤسسة Bracket عام ٢٠٢٢ نظرة أوسع للمخاطر على مستوى منصات الألعاب الاجتماعية وعالم ميتافيرس، مستخدمًا في تصنيفها إطار "مخاطر المحتوى والاتصال والسلوك" **(تقييم التهديد العالمي، ٢٠٢٣: ٢٣)**.

- **البث المباشر لأفعال الاعتداء الجنسي على الأطفال:**

من الصعب التأكد من مواد الاعتداء الجنسي على الأطفال التي يتم بثها مباشرًا وذلك لعدد من الأسباب المتداخلة، فأولًا: لا يعتبر البث المباشر لأفعال الاعتداء الجنسي على الأطفال محرمًا باستمرار. ثانيًا: إنه في البلدان التي يعتبر فيها البث المباشر فعلًا جنائيًا فإنه غالبًا ما يكون صعب التحقيق فيه ورفعه للقضاء، إذ بمجرد انتهاء البث المباشر لن تكون هناك سوى أدلة قليلة ما لم تكن مسجلًا. وثالثًا: لا تراقب معظم منصات البث المباشر الخاص، ففي اغسطس ٢٠٢٢ أصدر مسئول السلامة الإلكترونية الإسترالي أول مجموعة من أخطارات الشفافية الإلزامية إلى شركات ,Microsoft Skype,omegle, Whats App, Apple Meta, Snap حيث أن هناك أربع منهم تقدم خدمات البث المباشر أو المكالمات/ مؤثرات الفيديو، وقد كشفت الاستجابات عن أن ثلاثًا من الأربعة لا تستخدم حاليًا أدوات لاكتشاف أعمال الاعتداء أو الاستغلال الجنسي للأطفال التي يتم بثها بثًا مباشرًا، يمكن أيضًا الإكراه على البث المباشر لفعل الاعتداء من جانب المعتدين عبر الإنترنت. ففي دراسة جرت من أكتوبر ٢٠٢٠ إلى أغسطس ٢٠٢٢ على إحدى منصات البث المباشر الشهيرة، اكتشف (١٩٧٦) مستخدمًا كانوا بشكل أساسي قد فهرسوا وشاهدوا مواد البث المباشر للأطفال وحاولوا التلاعب بالأطفال كبيع صور جنسية وقد تعرض أكثر من ٢٧٠ ألف طفل للاستهداف من فئات هذه الحالات. لقد أظهرت الإعلانات الترويحية لأعمال الاعتداء الذي يتم بثه مباشرًا على شبكة الإنترنت السطحية كثيرًا، وغالبًا ما ترفع صور الأطفال في منشورات مخيفة للمستخدم كلمات مفتاحية مشفرة على إحدى صفحات شبكات التواصل الاجتماعي العامة للوصول إلى عدد أكبر من المشترين ومع ذلك فعادة ما يحدث البث المباشر لأنشطة الاعتداء في البيئات الآمنة التي تمنع كلمات المرور أو تقنيات التشفير الوصول المفتوح للجميع، وقد توصل تحليل شمولي لـ١٩ دراسة متعلقة بالبحث المباشر للاعتداء على الأطفال في الفلبين أن الضرر عادة ما كان يحدث في بيئة آمنة تنطوي على اتصال مشفر بين طرفين أو أكثر. **(تقييم التهديد العالمي، ٢٠٢٣: ٢٥– ٢٦)**

٧- المخاطر المحتملة للميتافيرس والتي قد تواجه الدول العربية:

إن تقنية الميتافيرس وافرة بالاستغلال وسوء الاستخدام من بعض المهاجمين، كما هو الحال مع جميع التقنيات الجديدة، ويتطلب تحديد المخاطر التي تواجهها اعتماد تقنية الميتافيرس الاعتراف بأن نشر هذا النظام الافتراضي على نطاق واسع يتضمن استخدام تقنيات متنوعة لتحقيق هدف موحد يعود بالفائدة التجارية، ومع ذلك تتطور هذه التقنيات بحقوقها الخاصة، وهو ما يجعل الآثار والمستخدمات السلبية لتقنية الميتافيرس مجموعة من التهديدات والتحديات متعددة الجوانب والتطور. لذلك يجب على الدول العربية بذل الجهود لتشكيل تقنية الميتافيرس كنظام افتراضي متماسك ولا حدود له، ولا يكون ذلك من خلال تطبيق الدروس التنظيمية من الإنترنت التقليدي (ويب ٢.٠) والأنظمة والأطر التنظيمية الحالية فقط، بل أيضًا من خلال فهم أن بعض التحديات والتهديدات التي تواجهها تقنية الميتافيرس جديدة حتى إن كانت تندرج تحت فئات معروفة، ولا تتيح معالجة هذه التحديات بشكل منفصل للدول العربية فرصة لا تضاهي تنفيذ اعتماد تقنية الميتافيرس وتنظيمها فقط، إنما تتيح أيضًا ربط تقنياته المكونة والناشئة كجزء من حركة أوسع نحو تأمين اهتمام إقليمي متزايد في التحول الرقمي والمبدأ التوجيهي للدول العربية هو أن تقنية الميتافيرس هو تحدٍ أمني مشترك وعابر للحدود يجب التصدي له بشكل مشترك ومفيد للجميع **(سليمان وأخرون، ٢٠٢٣: ٤٥)**.

ويمكن أن نحدد سبعة مجالات رئيسة للمخاطر التي تواجه الدول العربية:

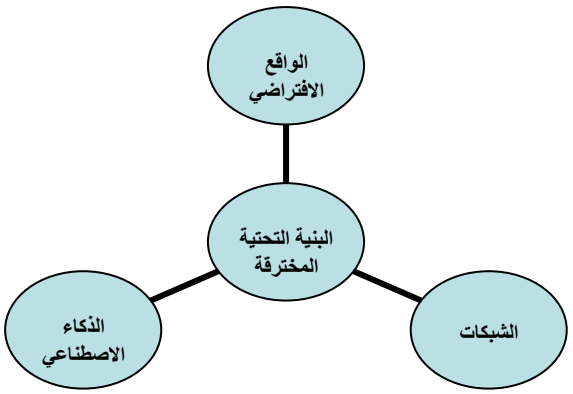
- البنية التحتية المخترقة؛
- التلاعب بالهوية؛
- محاذير الخصوصية؛
- الاختراقات؛
- نشر المعلومات المضللة والزائفة؛
- مخاطر على السيادة والثقافة؛
- التعبئة الاجتماعية والسياسية؛

وتتضمن المجالات هذه انتهاكات محددة لتقنية الميتافيرس بما في ذلك الهجمات على البنية التحتية الحيوية وتنسيق الجهود السيبرانية، وسرقة الملكية الفكرية وغسل الأموال، نشر الدعاية وجهود الجماعات المتطرفة في التجنيد والتحديات التي تواجه الاستقرار الاجتماعي وغيرها.

ويمكن مناقشة تلك المخاطر على النحو التالي (سليمان وأخرون،٢٠٢٣: ٤٧-٧٦):

أ- البنية التحتية المخترقة:

تلك الخصائص نفسها التي تشكل تقنية الميتافيرس، وتوفر تقنية الميتافيرس إمكاناتها المحتملة يمكن أن تتعرض للاختراق، إما عبر نقاط ضعف في النظام أو كأدوات للأذى وعند فهم المجالات التي يمكن فيها استخدام تقنية الميتافيرس سلبيًا يجب أن يؤخذ في الاعتبار فساد الخصائص الحرجة والبنية التحتية لتقنية الميتافيرس.



شكل رقم (٣) مناطق البنية التحتية المخترقة

ب- التلاعب بالهوية:

تطرح تقنية الميتافيرس تحديات جديدة فيما يتعلق باستخدام الهويات الرقمية وسوء استخدامها، ونظرًا لأنه عالم افتراضي انغماسي، فإن مفهوم الهوية الرقمية يتجاوز مجرد اسم مستخدم وملف تعريف، فقد تشمل الهوية الرقمية شخصيات رمزية قابلة للتخصيص بالكامل وتاريخ شخصي وإنجازات وأصول افتراضية مملوكة، ويثير هذا المستوى الفريد من

التخصيص العديد من المحاذير، إذ يمكن سرقة هويتك الرقمية أو استنساخها أو إساءة استخدامها، وهو ما يؤدي إلى شكل من أشكال سرقة الهوية التي تكون النظم الحالية والتي غير مجهزة بشكل جيد للتعامل معها ويمكن للمحتالين استغلال الهوايات الرقمية وإنشاء نسخ مزيفة مطابقة تقريبًا للشخصيات الافتراضية المعروفة لخداع الأخرين، وعلى غرار عمليات التصيد الاحتيالي في الويب (٢.٠) الحالي ويمكن أن تؤدي القدرة على التنكر كأشخاص أخرين إلى أشكال جديدة من التنمر والتحرش أو المعاملات الاحتيالية. ويمثل اتجاه حديث بين المهاجمين السيرانيين في نشر تقنية التزييف العميق في المساحات الإلكترونية، ويمثل استخدام تقنية التزييف العميق بشكل ضار مصدر قلق آخر في تقنية الميتافيرس، حيث تطور مفهوم الهوية ونتيجة لتقنية التزييف العميق التي يقمها الذكاء الاصطناعي، يمكن إنتاج محتوى فيديو أو صوت مركب بشكل واقعي يصور شخصًا يفعل أو يقول شيئًا لم يفعله في الواقع.

ج – محاذير الخصوصية:

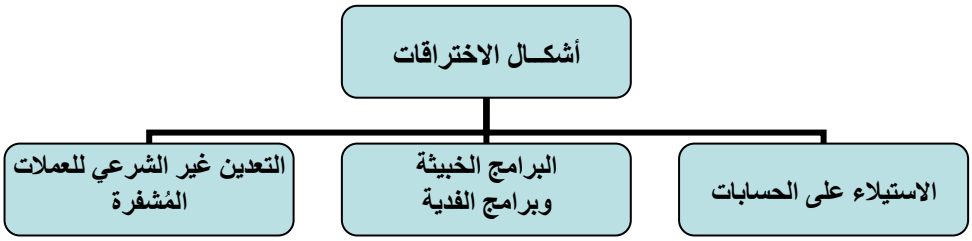
مع اكتساب الجهات الخبيثة مزيدًا من المعرفة ومحاولتهم مهاجمتها وقاعدة مستخدميها يجب أن تظل حماية خصوصية مستخدمي تقنية الميتافيرس في المقام الأول، خاصة مع التشغيل المتبادل القائم على فكرة التوافق والتكامل، حيث أن التعرض لأي نوع من أنواع الخصوصية في العالم الرقمي سيؤثر في العالم الحقيقي والعكس بالعكس. وعلى الرغم من أن تقنية الميتافيرس هي سلاحه جديدة، فإن سرية البيانات وسلامتها وتوافرها (ثالوث سي أي أية) ضرورة غير قابلة للتغيير ومطلقة للجميع. يجب على الدول العربية أن تتابع مدخلات المستخدمين وتبادلهم المعلومات في تقنية الميتافيرس، وفقًا لقواعد الخصوصية والحماية، وتكون البيانات هي النطاق الجديد ودورها المركزي يستدعي حمايتها بأي ثمن. ولقد استخدمت بعض الجهات الإنترنت لفترات طويلة لسرقة المعلومات الشخصية الخاصة بحكومات بعض الدول وبعض المواطنين، كما سرقوا خطط الأسلحة والوثائق الخاصة بالسفن والطائرات وكتائب تحمية وطبيعة الإنترنت المظلمة تسمح أيضًا بالإنكار المعقول وتصعيد التوترات بين الحكومات، فضلًا عن الأشخاص، ومن المتوقع

أن يزداد توافر البيانات في تقنية الميتافيرس فقط، وهو ما يعني وجوب وضع عمليات لحكاية البيانات الحاسمة والمؤسسات من البداية.

وتتمثل محاذير الخصوصية في (خصوصية بيانات المستهلك، تخزين البيانات، خصوصية البيانات المؤسسية**)**

د- الاختراقات:

رافقت أعمال القراصنة تلك التقنية في مهدها محاولة بلا انقطاع اختراق المصادقة واستغلالها ومراقبة الجهات بهدف الاستفادة من الشبكات وسرقة البيانات وترك بصمتهم الخاصة في العالم الافتراضي، وتهدف هذه العمليات التي يقومون بها إلى الربح المالي، أو سرقة الموارد الرقمية ونشرها في بلادهم، أو نشر رسائل سياسية من خلال أعمال القرصنة وتشكل تقنية الميتافيرس باعتبارها المحطة التالية للتكرار الافتراضي للعالم الواقعي مطمعًا للقراصنة المسيرين بدوافع مختلفة، وتكون منصات الميتافيرس ومستخدموها عرضة للقرصنة، وهو ما يدعو مسئولي الأمن إلى أخذ ذلك بعين الاعتبار.



شكل رقم (٤) يوضح أشكال الاختراقات

هـ- التضليل ونشر المعلومات المغلوطة:

الميتافيرس عرضة لخطر انتشار المعلومات المغلوطة كما في شبكة الإنترنت في وقتنا الحاضر، ويقصد بالمعلومات المغلوطة إنشاء ومشاركة المعلومات الكاذبة عمدًا بقصد الخداع أو التضليل، وقد تكون حملات المعلومات المضللة أكثر فاعلية بسبب الطبيعة الغامرة للبيئة الافتراضية. كما يمكن تقديم الروايات الكاذبة بطرق أكثر جاذبية وإقناعًا باستخدام مجموعة متنوعة من أشكال وسائل الإعلام والعناصر التفاعلية. وعلاوة

على ذلك قد تؤدي ميزات الميتافيرس الاجتماعية والتفاعلية إلى توسيع مدى انتشار المعلومات المضللة. كما يمكن للجهات الفاعلة الخبيثة استغلال تقنية التزييف العميق في الميتافيرس لخلق سيناريوهات كاذبة، وفي ذات الوقت واقعية للغاية أو انتحال شخصية من العالم الحقيقي مُعقدًا بذلك مشكلة المعلومات المضللة ويمكن إقران هذه التقنية مع نماذج اللغة الكبيرة (وهي نماذج حاسوبية تستخدم تقنيات الذكاء الاصطناعي والتعلم العميق لفهم وإنتاج اللغة الطبيعية) وأنظمة الذكاء الاصطناعي المولدة الأخرى المتاحة لتعزيز واقعية السيناريوهات والروايات الكاذبة.

و- مخاطر على السيادة والثقافة:

يمكن أن يؤدي الميتافيرس، بوصفه ساحة افتراضية خالية من الحدود يمكن الوصول إليها من أي مكان، إلى تقويض سيادة الدول وثقافتها، وبالنظر إلى تركيز سلطة بعض شركاء وسائل التواصل الاجتماعي على النظام الرقمي الناشئ الذي تهيمن الشركات الخاصة عليه بشكل متزايد على حساب الدول، فمن المحتمل أن يأخذ الميتافيرس هذه الخطوة إلى الأمام، وبإمكانه فك مركزية المساحة الافتراضية الغامرة مع الحفاظ على أهمية العالم الرقمي الاجتماعية والاقتصادية والسياسية في الوقت نفسه، وتيسير للفكرة أو الاعتقاد الذي يبدأ افتراضيًا، الانتشار بسهولة في العالم المادي، حيث يكتسب زخمًا بين المؤمنين به الذين يعملون على تحقيقه في العالم المادي. وقد تنبأت وسائط الإعلام الرقمية بتلك التهديدات وخاصة منصات التواصل الاجتماعي، وتنبأ بها كذلك الانخفاض المتزامن في الأنماط الاجتماعية، التي تؤخذ من المسلمات في العديد من المجتمعات الغربية، وهو ما يؤدي إلى انقطاع مجتمعي، وقد يعزز الميتافيرس هذا الاتجاه ويوسعه من خلال أبعاد الأفراد عن بلدانهم ومجتمعاتهم، ونظرًا للاندماج بين المعدات المنزلية التي تعمل بتقنية الحوسبة السحابية مع إمكانية الوصول إلى مجموعة من العملات المُشفرة مع نقل البيانات الشخصية عالميًا من خلال التقنية اللامركزية المتأصلة؛ قد يرى الأفراد أن دولهم وثقافتهم غير ضرورية أو هامشية، على الرغم من تحصين الدول لهؤلاء الأفراد من أجل ضمان وصولهم المستقر إلى العالم الافتراضي. وسيكون الميتافيرس بيئة خصبة

للتعاون وتوليد الأفكار للأشخاص المنبوذين من أقرانهم أو مجتمعاتهم أو بلدانهم، وأدى الإنترنت إلى ظهور العديد من الفئات الجديدة في المجتمع، وهذه الفئات تزدهر الأن وتحفز كلا منها الأخرى، مثل جماعات العزوبية غير الطوعية (الإنسيلز) أصحاب نظرية المؤامرة، والمتداولين في الأسواق المالية الذين منحوا أنفسهم ألقابًا معينة. ومن الممكن لمثل هذه المجموعات أن تكتسب تأييدًا كبيرًا لأفكارهم عبر الإنترنت، وأن تستخدم جماهير مشتركة مع مجموعات مشتركة لتشكيل تهديد حقيقي لشعب آخر، أو للقضاء على ثقافة معينة، أو لتنفيذ أمور قد تكون أسوأ من ذلك وهذا المنظور يمتد ليشمل الجماعات الهامشية، كالجماعات الدينية المتطرفة داخل منطقة الشرق الأوسط وخارجها، وتلك الجماعات ترمي إلى إضفاء الطابع المؤسسي على الآراء التي تتمتع بتأييد شعبي والتي تسعى لتقويض النظام المؤسسي، ولما كان من الصعب لمجموعة متطرف، أن تنشئ حزبًا سياسيًا في العالم الحقيقي، فمن الممكن أن العالم الافتراضي ملاذًا لها، وهو الأمر الذي يشكل بديلًا سيئًا من شأنه أن يقوض أو يضعف مؤسسات العالم الحقيقي تدريجيًا.

٨- العوامل والدوافع المؤدية إلي حدوث الإجرام الميتافيرسي:

تواجه أي "مؤسسة أمنية" تهدف لخدمة المجتمع وتهيئة مقومات تحقيق نهضته، تحديات جمة أهمها مجموعة من "الجرائم" والتي في حقيقتها ثغرات نتيجة الاختلالات المستجدة نتيجة المتغيرات البيئية الاجتماعية والاقتصادية والتكنولوجية وغيرها، والتي قد يستغلها ضعاف النفوس من المجرمين ليهددوا حالة الأمن والسلم والنظام العام داخل المجتمع، ويقوضوا حركة تقدمه ونمائه، مستفيدين في ذلك من التقدم العملي والتكنولوجي المتاح لهم في كل مرحلة من مراحل التطور البشري، ليجعلوا منها وسيلة لخرق وانتهاك وتهديد أمن وخصوصيات الأخرين، بسلب حقوقهم وتدمير ممتلكاتهم، أو بإخضاعهم تحت مزلة نشر الشائعات عنهم أو فضح أعمالهم لابتزازهم.

ويعد الدافع هو العامل المحرك للإرادة التي توجه السلوك الإجرامي، وتتنوع الدوافع وتتباين تبعًا لطبيعة ودرجة خبرته في مجال المعلوماتية والهدف من وراء ارتكاب الجريمة **(الزنط،٢٠٢٢: ٢٤٣-٢٥٤)**.

ويمكن تعريف العامل الإجرامي بأنه "الحالة أو الواقعة التي ترتبط بالجريمة برابط السببية أيًا كانت هذه الرابطة، فقد تتفاوت القوة والضعف حسب نوع العامل ومدى مساهمته في وقوع الجريمة". قد تكون هذه العوامل فردية داخلية أو عوامل خارجية، ويرى جانب من العلماء أن هناك عدد من العوامل التي تؤدي إلى ارتكاب الجرائم الافتراضية منها ما يقع على مستوى كوني، ومنها ما يقع على مستوى مجتمعي، ومنها ما يقع على مستوى فردي أو شخصي، كما أن هذه العوامل تتفاوت وفق نوعها ونوع المستهدف، ونوع الجاني ومستوى تنفيذه، هذا بالإضافة إلى أن العوامل الدافعة للسلوك الإجرامي الميتافيرسي تتجح مع ذات العوامل التي من الممكن أن تدفع لارتكاب الجريمة الافتراضية ومن أهمها الدوافع المادية فبعض الجرائم الافتراضية تحقق قدرًا كبيرًا من الربح كجرائم السرقة والاحتيال الإلكتروني وتزوير وتقليد بطاقات الائتمان وغيرها، بالإضافة إلى عامل الرغبة في تعلم كل ما يتعلق بالتكنولوجيا الحديثة والشبكات الإلكترونية حتى لو أدى إلى ارتكاب الجريمة، وكذلك الدوافع الذهنية والتي تتمثل في المتعة والتحدي والرغبة في فهم النظام المعلوماتي وإثبات الذات من خلال تحدي النظام والتفوق على تعقيد وسائل التقنية وايضًا الدوافع الموضوعية حيث قد يتأثر المجرم المعلوماتي والميتافيرسي ببعض المواقف قد تكون دافعة له على اقتراف الجريمة الافتراضية السعي إلى مجرد المتعة والتسلية وكسب المال **(إبراهيم،٢٠٢٣م: ٣٢-٣٣)**.

حيث يُعد الدافع هو العامل المحرك للإرادة التي توجه السلوك الإجرامي، وتتنوع الدوافع وتتباين تبعًا لطبيعة ودرجة خبرته في مجال المعلوماتية، والهدف من وراء ارتكاب الجريمة، وثمة ثلاث بواعث تحرك المجرم السيبراني تتمثل في:

- **الباعث الأول:** هو الرغبة في تحقيق الربح وكسب المال؛
- **الباعث الثاني:** فهو المتعة والتسلية، بدافع التحدي والرغبة في إثبات الخبرة والمستوى التقني الذي يتمتع به؛
- **الباعث الثالث:** في الرغبة في الإضرار بهذه الأنظمة بدوافع الانتقام.

وفي كل الأحوال فقد ذهب الفقه القانوني إلى إرجاع مصدر هذه الدوافع إجمالًا نوعين هما: دوافع شخصية وأخرى خارجية، ومع ذلك فيمكن تصنيف دوافع ارتكاب الجرائم السيرانية على النحو التالي **(الزنط، ٢٠٢٢ :٢٥٥)**:

- **دوافع مادية:** من العوامل الرئيسة لارتكاب الجرائم السيرانية نظرًا للسرعة في ارتكابها وسهولة التخفي وإمكانية إزالة الآثار والدلائل على ارتكابها وتمثل في تحقيق (الكسب المادي– الرغبة في تحقيق الثراء السريع السهل).
- **الرغبة في التعلم:** قد يكون إقدام المجرم المعلوماتي على ارتكاب جريمته بدافع الرغبة إظهار تفوقه على وسائل التكنولوجيا الحديثة وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية وإنما ينطلق من دافع التحدي وإثبات المقدرة.
- **دوافع المتعة والتحدي وإثبات الذات:** وتحقيق الانتصار على تقنية الأنظمة المعلوماتية دون أن يكون لهم نوتيا آثمة، وإنما بدوافع الشغف والرغبة في تحدي وقهر النظام والتفوق على تعقيد وسائل التقنية.
- **دافع الانتقام:** ويُعد من أخطر الدوافع التي تدفع شخص يملك معلومات كبيرة عن المؤسسة أو شركة يعمل بها تجعله يقدم على ارتكاب جريمته، وغالبًا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية.
- **دافع سياسي:** يركز هذا الدافع على الوقائع التي تجتذب اهتمام وسائل الإعلام من أجل إثارة الفتن ونشر الشائعات وبلبة الرأي العام.
- **دافع الإرهاب:** ويعتمد على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية من أجل تخويف وترويع الأخرين وإلحاق الضرر بهم.

٩- العوامل التي تساهم في التنبؤ بالضحايا المحتملين للإجرام الميتافيرسي :

هناك العديد من العوامل التي تساهم في التنبؤ بالضحايا المحتملين عبر الإجرام الميتافيرسي يمكن الإشارة إليها على النحو التالي:

جدول رقم (٦) العوامل التي تساهم في التنبؤ بالضحايا المحتملين للإجرام الميتافيرسي

العوامل	التفسير
توفر المعلومات الشخصية عبر الإنترنت	تلعب سهولة الوصول إلى المعلومات الشخصية دورًا حيويًا في جعل الأفراد أهدافًا محتملة. على سبيل المثال أولئك الذين يشاركون بنشاط ويبالغون في المشاركة في الميتافيرس قد يعرضون أنفسهم لمجرمي الإنترنت عن غير قصد يمكن استغلال هذه المعلومات مثل التفاصيل الشخصية والتوصيلات في هجمات ذات طابع شخصي للغاية مثل التصيد الاحتيالي أو حتى تؤدي إلى سرقة الهوية.
العادات الرقمية	تساهم العادات الرقمية في احتمالية الوقوع ضحية السلوكيات التي قد تبدو غير مهمة مثل استخدام كلمة مرور ضعيفة أو يمكن تخمينها بسهولة أو تبديل ملفات من مصادر لم يتحقق منها. يمكن أن تزيد هذه المخاطر بشكل كبير إن غياب التدابير الأمنية القوية مثل المصدقة متعددة العوامل يجعل الأفراد أكثر عرضة للهجمات.
المعرفة الرقمية	أن المعرفة الرقمية أي القدرة على التفاعل مع التكنولوجيا بأمان وفعالية هي عامل حاسم في تحديد نقاط الضعف الأفراد الذين يعتقدون غلى الوعي بأفضل الممارسات الأمن السيراني أو الأنشطة المختلفة عبر الإنترنت هم أكثر عرضة للوقوع فريسة للجرائم الإلكترونية. حيث تؤكد العلاقة بين الوقت الذي تقضيه في الميتافيرس واحتمالية الوقوع ضحية على أهمية محو الأمية الرقمية من التهديدات المحتملة.
العوامل الديموغرافية	بعض الأشخاص أكثر عرضة للخطر، على سبيل المثال قد يفتقر الأفراد الأصغر سنًا أو الأكبر سنًا إلى الوعي بالخبرة اللازمة للتعرف على التهديدات السيرانية وقدرتها. في حين الذين يعملون في مهن رفيعة المستوى أو حساسة قد يتم استهدافهم على وجه التحديد للحصول على معلومات قيمة أو الوصول إليها.

- **الجدول من إعداد الباحثة اعتمادًا على (Blake, 2024: 72).**

١٠- الجناة المحتملين للإجرام الميتافيرسي وسماتهم:

تتجلى مظاهر الخطورة في الجريمة السيرانية، أن مرتكبيها يتسمون بالذكاء والدراية في التفاعل مع أجهزة الحاسب الآلي وشبكات المعلومات ومعطياتها ويتوافر لديهم قدرات ومهارات ومعارف تمكنهم من التعامل معها بصورة احترافية **(الزنط،٢٠٢٢: ٢٤٧-٢٤٨)**. يمكن تحليل مرتكبي الجرائم عبر الإنترنت المحتملين من خلال أبعاد مختلفة بما في ذلك تصور عدم الكشف عن هويتهم، إن التنبؤ بعدم الكشف عن هويته عبر الإنترنت والذي يتم إنشاؤها من خلال أسماء مستعارة والشبكات الافتراضية الخاصة، وغيرها من التقنيات لإخفاء الهوية الحقيقية، من الممكن أن يقلل من الموانع ويعزز الانفصال عن الواقع، قد ينجذب الأشخاص الذين قد لا يفكرون أبدًا في الانخراط في جرائم تقليدية إلى السلوك الإجرامي عبر الإنترنت بسبب الاعتقاد بأن مثل هذه الأفعال لا يمكن تعقبها أو أنها موجودة خلف شخصية رقمية، مما يقلل من المساءلة. كما قد تكون تأثيرات الجرائم

السيرانية أكثر تجريدًا أو بعدًا مقارنة بالتأثيرات المباشرة والمرتبة للجرائم الجسدية مما يخلق انفصالًا بين الأفعال عواقبها في العالم الحقيقي. كما أن التنبؤ باحتمالية تورط فرد ما في جريمة إلكترونية أمر معقد يمكن للعوامل الاجتماعية والديموغرافية المختلفة، مثل العمر والجنس والتعليم والمهنة. كما تلعب السمات الشخصية أيضًا دورًا في التنبؤ بسلوك المجرمين الإلكترونيين سمات مثل المستويات العالية من الفضول، يفضل عادة الكشف عن هويته والرغبة في الإثارة أو التحدي وانخفاض مستويات التعاون أو المشاركة الأخلاقية قد تكون مؤشرًا، قد تكون النرجسية والصفات المعادية للمجتمع شائعًا أيضًا بين مجرمي الإنترنت. بالإضافة إلى ذلك قد يشير التاريخ الإجرامي السابق خاصة فيما يتعلق بالجرائم المسندة إلى التكنولوجيا إلى ميل أكبر لأنشطة الجرائم الإلكترونية المستقبلية يمكن للسلوك الماضي في كثير من الأحيان التنبؤ بالسلوك المستقبلي، خاصة إذا كان يتضمن أنشطة إجرامية متكررة وقهرية ومع ذلك قد يشمل سياق الجريمة السيرانية أيضًا مرتكبي الجرائم لأول مرة والذين يتمتعون بالكفاءة التكنولوجية دون أن يكون لهم سجل إجرامي سابقً. **(Blake , 2024: 31)**

تقول نظرية آيسنك عن الإجرام إن المرض العقلي تحديدًا الذهان يؤدي إلى سلوك إجرامي مما يشير إلى أن العوامل النفسية لها أهمية مركزية فيما يتعلق بكل من أسباب الجريمة والسيطرة عليها وترتبط العوامل النفسية للإجرام بالعوامل الوراثية للفرد، فالتركيبة التي تتحد مع عوامل النزعة الإجرامية لزيادة احتمال ارتكابهم للجريمة تشير هذه القرابة على نطاق واسع أن المجرمين والمرضى النفسيين يظهرون أنماطًا سلوكيًا من خلال الاضطرابات الشخصية التي يتم تحديدها من خلال الطيف الوراثي البيولوجي ويحتمل من الصعب على الفرد مقاومة الانخراط في أعمال الانحراف مما يؤدي إلى سلوك سيكوباتي وإجرامي. وفيما يتعلق بنظرية أيسنك حول الإجرام فإن المجرم المتحمس الذي يعيش مع مرض عقلي غالبًا ما يكون مدفوعًا بحاجته النفسية للانخراط في السلوك الإجرامي خاصة مع الجرائم الإلكترونية والتي يمكن أن تشمل الجرائم التي يسهلها التزييف العميق. **(Stavola,J& choi,K, 2023: 6)**.

جدول رقم (٧) سمات المجرم الميتافيرسي

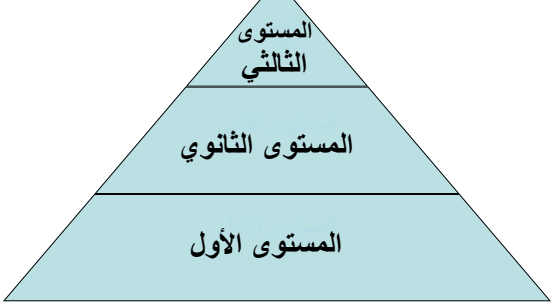
السمات	التفسير
الاجتماعية، الديموغرافية	مثل العمر والجنس والتعليم المهني إن المراهقون ذوو المهارات التكنولوجية المقدمة أكثر عرضة للمشاركة في الجرائم السيرانية يفوق عدد الجناة الذكور عدد الإناث.
السمات الشخصية	مثل المستويات العالية من الفضول وتفضيل عدم الكشف عن هويته والرغبة في الإثارة أو التحدي وانخفاض مستويات التعاون أو المشاركة الأخلاقية، النرجسية، الصفات المعادية للمجتمع.
السمات النفسية	إن المجرمين والمرضى النفسيين يظهرون انماطًا سلوكية من خلال اضطرابات الشخصية كما أن مرتكب الجريمة السيرانية ينحدر عادة من عائلة مرضية حيث يوجد تاريخ من الأمراض العقلية الوراثية في أسلافهم. تشير النتائج إلى أن ما يقرب من(٢٥%) من سكان العالم يعانون من اضطرابات نفسية أو عصبية ويمكن تمثيل عدد كبير من المستخدمين الرقميين في هذه المجموعة من المرجح أن يكون الأفراد الذين يعيشون مع اضطرابات الشخصية المعادية للمجتمع مرتكب الجرائم بسبب خداعهم وتلاعبهم وضعف التوافق الاجتماعي والاندفاع والعدوانية مما قد يساعد في انماط السلوك العنيفة وغير العنيفة مثل التنمر عبر الإنترنت، التحرش عبر الإنترنت، العنف عبر الإنترنت والمطاردة. أن الجناة الذين يقفون وراء هذه الجرائم هم الأفراد الذين يقفون خلف الصورة الرمزية حيث يسلط الضوء على أن عنف صورة رمزية تجاه أخرى في Metaverse يمكن أن يسبب ضررًا نفسيًا للفرد.
مجرم متخصص	له قدرة فائقة على التخطيط والتنظيم، ولديه المهارة التقنية ويشغل مداركه ومهاراته في اختراق الشبكات واختراق كلمات المرور.
مجرم عائد الإجرام	يتصف المجرم المعلوماتي أنه عائد للجريمة دائمًا ولديه القدرة على تبرير جرائمه، فهو يوظف مهاراته في كيفية عمل الحواسب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشكات في الدخول غير المصرح به مرات ومرات. بالإضافة إلى ذلك يشير التاريخ الإجرامي السابق خاص فيما يتعلق بالجرائم المسندة إلى التكنولوجيا إلى ميل أكبر لأنشطة الجرائم الإلكترونية المستقبلية يمكن للسلوك الماضي في كثير من الأحداث التنبؤ بالسلوك المستقبلي خاصة غذا كان يتضمن أنشطة إجرامية متكررة وقهرية، ومع ذلك قد يشمل لسياق الجريمة. ومع ذلك قد يشمل سباق الجريمة السيرانية أيضًا مرتكب الجرائم لأول مرة والذين يتمتعون بالكفاءة التكنولوجية دون أن يكون لديهم سجل إجرامي سابق.
مجرم محترف	لديه من القدرات والمهارات التقنية ما يؤهله لأن يوظفهما في الاختراق والسرقة والنصب والاعتداء على حقوق الملكية الفكرية وغيرها ومستوى المهارة لديه تحدد الأسلوب الذي يرتكب به الجرائم ودرجة خطورته، بحيث إذا كان الشخص مرتكب الجريمة المعلوماتية على قدر ضئيل من مستوى المهارة نجد أن الجرائم التي قد يرتكبها لا تعد الاتلاف المعلومات أو نسخ البيانات والبرامج والعكس صحيح.
مجرم ذكي يتمتع بالمهارة والذكاء	فهو يمتلك من المعارف والمهارات ما يؤهله لأن يقوم بتعديل وتطوير الأنظمة الأمنية الخاصة به، حتى لا تستطيع أجهزة الشرطة ملاحقته وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب. فالإجرام المعلوماتي هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى استخدام القوة والعنف.
التعليم والمعرفة والقدرة	ينتمي مرتكبو هذه الجرائم عادة إلى الطبقة المتعلمة ومعظمهم يكونوا من أصحاب التخصصات ومستخدمي شبكة الإنترنت، كما تتطلب الجريمة المعلوماتية عادة شخصين على الأقل أحدهما متخصص في الحاسبات الآلية يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من

السمات	التفسير
التقنية الهائلة	المحيط ذاته أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب، وفي أحيانًا أخرى يمكن تجنيد المجرم المعلوماتي القادر على اختراق نظم المعلومات ضمن عصابات الجريمة المنظمة عن طريق شبكة الإنترنت.
الحرص الشديد	عادة ما يلجأ المجرم المعلوماتي إلى التمهيد لارتكاب جريمة بالتعرف على المحيط الذي تدور فيه وكذا الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها، ويساعده في ذلك درجة المهارة التي يتمتع بها.
الخوف والتخفي	يتخفى مرتكب هذه النوعية من الجرائم عبر دروب الإنترنت بحيث يمكن أن يختفوا تحت قناع فني يظهرهم من دولة إلى أخرى، وهو يخشى من افتضاح أمره خاصة لصغار السن وهم الذين يتراوح أعمارهم عادة بين (١٨ – ٤٦) بمتوسط ٢٥ عام وتوضح دراسة أجراها معهد Stand Ford Research أن محترف الجرائم المعلوماتية من الجيل الحديث هم غالبًا من الشباب الذين يتراوح أعمارهم (٢٥ إلى ٤٥ عامًا)، وتبين الإحصاءات في هذا المجال ما يلي: - ٥٢% من أفعال الغش المعلوماتي أو الجرائم المعلوماتية يرتكبها الشخص التقني. - ٨٠% من هذه الأفعال يرتكبها مبرمجون. - ٧١% يرتكبها المستخدم الذي لديه افكار خاصة بنظم المعلومات الذي يتواجد فيه نظم المعلومات. - ١١% من هذه الأفعال يرتكبها فني التشغيل.

الجدول من إعداد الباحثة اعتمادًا على: (الزنط، ٢٠٢٢م: ٢٤٦– ٢٤٨)
(Blake 2024: 74) & (Stavola,J& choi,K ,2023: 6)

١١- أليات التصدي والوقاية من جرائم الميتافيرس والتقنيات الناشئة:

يعد هرم الوقاية الذي اعتمد في مجال الصحة العامة أن الوقاية الفعالة تتطلب تطوير التدخلات على المستوى الأول والثانوي والثالثي، وتستهدف هذه التدخلات الأشخاص المُعرضين لخطر ارتكاب الاعتداء أو الوقوع ضحايا له، وأولئك الذين سبق أن تعرضوا للاعتداء أو ارتكبوا الاعتداءات **(تقييم التهديد العالمي، ٢٠٢٣: ٤٥)**



شكل رقم (٥) يوضح هـــرم الوقاية

ويركز المستوى الثالثي: التعامل مع الأفراد الذين اقترفوا جريمة ويتضمن التدخل لوقف المزيد من الجرائم. ترتبط الوقاية عمومًا بهيئات العدالة الجنائية وبخاصة المحاكم والسجون وبرامج إعادة التأهيل بعد الجريمة.

أما المستوى الثانوي: فإنه يشارك في الكشف المُبكر عن الجناة المحتملين ويسعى للتدخل لمنع الأعمال الإجرامية. تُوجه الوقاية نحو الأفراد المُعرضين لخطر ارتكاب الجريمة، ويمكن أن تشمل برامج للمساعدة في معالجة السلوكيات الضارة ولضمان فهم الأفراد للعواقب المحتملة للاعتداء.

أما المستوى الأول فإنه يحدد الظروف البيئية المادية والاجتماعية التي توفر الفرص لارتكاب الأعمال الإجرامية أو تثيرها، ويهدف التدخل إلى تغيير تلك الظروف حتى لا تحدث الجرائم **(تقييم التهديد العالمي، ٢٠٢٣: ٤٥)** .

ومن بين الفرص الأكثر قابلية للتنفيذ على الفور للجهات الحكومية التي تتعامل مع هذا الموضوع، هي برامج التدريب وإعطاء أصحاب المصلحة خبرة مباشرة في منصات Metaverse المجسدة، وتوفير نظرة ثاقبة للمسار الحالي ووتيرة التكنولوجيا، والطريقة التي ترتبط بها إمكانيات هذه الوسيلة بقضايا إساءة الاستخدام والتحرش. وقد ترغب الحكومات في إعطاء الاولوية لمحو الأمية الرقمية لدى الهيئات مثل المشرعين والشرطة والسلطة القضائية حملات محو الأمية العامة التي قد تكون ذات قيمة في دعم المواطنين لفهم حقوقهم، وتمكينهم من اتخاذ قرارات مستنيرة ومتمكنة بشأن مشاركتهم مع الميتافيرس.**(Mclntosh,2024:5)**.

ووفقًا لنظرية الأنشطة الروتينية فإن بناء الفرصة الإجرامية ومعادلة الجريمة يمكن تلخيصها في (الجاني، الهدف، وغياب الوصي) والتفاعل بينهم عبر المكان والزمان، ومن ثم فإن مواجهة الجرائم عبر الميتافيرس وإعداد برامج للحماية والوقاية تتطلب الانتباه لتلك العوامل التي تشكل مثلث الجريمة. كما أن الدرجة التي يكون فيها شخص ما هدفًا مناسبًا لمجرم متحمس تسمح إلى حد كبير بالإيذاء ومن ثم فإن تأثير الحراسة القادرة أمر مهم ويعد أهم عامل لتقليل الجريمة. **(علي، ٢٠٢٢: ١٢٥)**

تاسعًا: الإطار المنهجي للبحث:

(١) أساليب الدراسة:

جمع البحث الراهن بين الأسلوب الكمي والكيفي للوصول إلى نتائج صادقة حول قضية البحث الراهن، والتوصل إلى السيناريو الأقرب حدوثة، إلى جانب تحقيق التكامل المنهجي والشمولية في جمع البيانات المتعمقة ومعالجتها حول استشراف الجرائم والمخاطر المرتبطة بالميتافيرس والتقنيات الناشئة، إلى جانب التنبؤ بفئات الجناة والضحايا لهذه الجرائم.

- **الأسلوب الكمي:**

تم تصميم دليل المقياس الذي تم تطبيقه على عينة من الخبراء، وعينة من الشباب مستخدمي الميتافيرس والتقنيات الناشئة، لإجراء المقارنات حول استجابات كلًا منهما حول تهديدات الجرائم المرتبطة بالميتافيرس والتقنيات الناشئة.

ومن أهم المبررات المنهجية لاختيار عينة الخبراء:

- أنها من أفضل الطرق لاستنباط أراء أشخاص ذوي خبرة كبيرة في أحد الظواهر والمستجدات التي تشغل العالم بأكمله؛
- أن الخبراء مختلف التخصصات قادرون على استشراف الوضع المستقبلي المتعلق بالميتافيرس والتقنيات الناشئة؛
- سعت الباحثة لإضفاء مصداقية عند اختيار عينة أخرى.

ومن أهم المبررات المنهجية لاختيار عينة من الشباب مستخدمي الميتافيرس والتقنيات الناشئة:

- أن الشباب من الجنسين في الفئة العمرية (١٨- ٣٥) بينهم اختلاف في الخصائص الديموغرافية، البيئات السكنية والمستويات المعيشية، وكلها خصائص تضفي دلالة في استجابتهم حول إشكالية البحث الراهن؛
- أظهرت أحدث الإحصائيات أن عدد مستخدمي الإنترنت في مصر بلغ (٨٠.٧٥) مليون مستخدم، أي ما يعادل (٤١.٤%) من أجمالي السكان وذلك في بداية عام ٢٠٢٣، حيث بلغ معدل انتشار الإنترنت في مصر (٧٢.٢%)؛

- لقد بلغ عدد مستخدمي وسائل التواصل الاجتماعي في مصر (٤٦.٢٥) مليون في يناير ٢٠٢٣، وهو ما يعادل (٤١.٤%) من إجمالي السكان، وفي الوقت نفسه تشير البيانات المنشورة إلى وجود (٤٢.١٠) مليون مستخدم تبلغ أعمارهم ١٨ عامًا فأكثر يستخدمون وسائل التواصل الاجتماعي في بداية عام ٢٠٢٣، وهو ما يعادل (٦٠.٩%) من السكان الذين تبلغ أعمارهم ١٨ عام فأكثر في ذلك الوقت؛
- وفي ذلك الوقت حسب ما أشارت إليه الإحصائيات كان (٦٠.٩%) من مستخدمي وسائل التواصل الاجتماعي في مصر من الذكور،في حين جاءت نسبة (٣٩.١%) من الإناث.**(Datareportal, 2025)**

ومن ثم فإن اختيار عينة من الشباب المستخدمين للميتافيرس والذين يمثلون الفئة الأكبر في استخدام الإنترنت ووسائل التواصل الاجتماعي سوف يضفي على نتائج البحث أهمية وفهم أعمق لمضامينها.

- **الأسلوب الكيفي:**

لقد أعتمد البحث الراهن عليه لتوفير بعض البينات والنتائج الكيفية التي تساعد في تفسير النتائج الكمية وفهم دلالاتها. من خلال عقد (٤١) مقابلة مع مجموعات من النخب في مختلف المهن (اكاديميون- مهندسون متخصصون في الأمن السيبراني- رجال إنفاذ القانون- مستشارون) وممن لهم صلة وثيقة بقضايا الميتافيرس والتقنيات الناشئة.

(٢) أدوات جمع البيانات:

اعتمد البحث الراهن على دليل المقياس الإلكتروني لعينة من الخبراء والشباب مستخدمي الميتافيرس، لتصنيف سيناريوهات تهديد الجرائم المرتبط بالميتافيرس، ودليل المقابلة الفردية لعينة من الخبراء فقط.

وقد تضمن دليل المقياس المحاور التالية:

ـ البيانات الأساسية.

ـ سيناريوهات تهديد الجرائم عبر الميتافيرس والتقنيات الناشئة.

لقد تم تحديد (٤٢) سيناريو لتهديدات الجرائم المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة، وقد تم تجميع هذه السيناريوهات في (٥) فئات عالية المستوى، وقد تضمن كل سيناريو مجموعة من الجرائم الفرعية، ولقد تم التوصل إليها من خلال البحث في الأدبيات السابقة وتقارير المنظمات الدولية والإقليمية والمحلية المختلفة، وذلك على النحو التالي:

الفئة الأول: الجرائم المالية؛

الفئة الثانية: الجرائم الجنسية؛

الفئة الثالثة: الجرائم ضد الأشخاص؛

الفئة الرابعة: جرائم الممتلكات؛

الفئة الخامسة: جرائم أخرى.

- رصد العوامل الدافعة إلى ارتكاب الجرائم عبر الميتافيرس والتقنيات الناشئة.

واشتملت على ثلاث عوامل رئيسة تضمن كل عامل مجموعة من العوامل الفرعية، وقد تمثلت في: (العوامل العالمية – العوامل المجتمعية – العوامل الفردية).

- تبيان أليات والحلول المقترحة لمواجهة الجرائم والمخاطر المُرتبطة بالميتافيرس والتقنيات الناشئة.

واشتملت على أربع أليات رئيسة تضمن كل جانب مجموعة من الجوانب الفرعية، وهي على النحو التالي: (الحلول القانونية – حلول السياسات – الحلول التقنية– الحلول التوعوية)

كما تتضمن دليل المقابلة المحاور التالية:

- رصد واقع المجال الافتراضي ومنصات التواصل الاجتماعي في التحريض على إساءة الاستخدام والتحرش.
- تبيان مدى الخصوصية بشأن الميتافيرس والتقنيات الناشئة.
- رصد فئات الضحايا المحتملين لتهديدات جرائم الميتافيرس والتقنيات الناشئة.
- رصد فئات الجناة المحتملين لارتكاب الجرائم عبر الميتافيرس والتقنيات الناشئة.

(٣) عينة البحث:

اعتمد البحث الراهن على أسلوب المعاينة بدلًا من الحصر، وذلك بسبب كبر حجم مجتمع البحث، ومحدودية الوقت والجهد والتكلفة المتاحة لإعداد البحث، ونظرًا لكبر حجم مجتمع البحث، فقد تم اختيار العينة العشوائية البسيطة.

وتمثلت عينة البحث في:

- عدد (٤١) من النخب في مختلف المهن (أكاديميون- مهندسون ومتخصصون في الأمن السيبراني- رجال إنفاذ القانون- مستشارون) وممن لهم صلة وثيقة بقضايا الميتافيرس والتقنيات الناشئة.
- إلى جانب مجموعة من الشباب مستخدمي الميتافيرس والتقنيات الناشئة، بلغ عددهم (٤٠٤).

(٤) الصدق والثبات لأداة البحث:

(أ) صدق الأداة:

يقصد بصدق الأداة، أن نقيس أسئلة الأداة ما وضعت لقياسه، وقد قامة الباحثة بالتأكد من صدق الأداة، بطريقتين وهما صدق المحكمين وصدق المقياس.

صدق المحكمين الصدق الظاهري

ويعني الصدق الظاهري صدق المقياس المستخدم ودقتة في قياس المتغير النظري أو المفهوم المراد قياسه، وللتحقق من صدق المقياس المستخدم في البحث قامت الباحثة بعرض المقياس على مجموعة من المحكمين تألفت من (١٠) متخصصين في علم الاجتماع والإحصاء وقد استجابت الباحثة الأراء المحكمين وقامت بإجراء ما يلزم من حذف وتعديل في ضوء المقترحات المقدمة، وفي ضوء أراء السادة المحكمين قامت الباحثة بحساب الدرجة المقدرة والوزن النسبي، حيث تم اختيار العبارات التي حصلت على نسبة (٨٠%) فأكثر من مجموع آراء المحكمين، وبذلك خرج دليل المقياس في صورته النهائية.

(ب) صدق المقياس

الاتساق الداخلي (Internal Validity)

يقصد بصدق الاتساق الداخلي الوصول إلى اتفاق متوازن في النتائج بين الباحثين عند استخدامهم لنفس الأسس والأساليب مدى اتساق كل فقرة من فقرات المقياس مع المجال الذي تنتمي إليه هذه الفقرة. وقد تم توزيع عينة استطلاعية حجمها (٣٠) دليل مقياس لاختبار الصدق والثبات للمقياس، حيث تم جمع هذه المقاييس وإخضاعها للتحليل الإحصائي وتم إدخال هذه المقاييس ضمن التحليل النهائي التي تم توزيعها على عينة البحث، وقد قامت الباحثة بحساب الاتساق الداخلي للمقياس وذلك من خلال حساب معاملات الارتباط بين كل فقرة من فقرات مجالات المقياس والدرجة الكلية للمجال نفسه.

جدول رقم (٨): جدول يوضح صدق الاتساق الداخلي للهدف الأول " الكشف عن الجرائم المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة " وبين المقياس بعبارته المختلفة في (الخبراء – المستخدمين) والهدف الأول ككل

العبارات	الخبراء ن= ٤١	المستخدمين ن= ٤٠٤	إجمالي الاستجابات ن= ٤٤٥
العبارات	الجرائم المالية		
١	.٤٠٩**	.٧٧٢**	.٧٧٣**
٢	.٨٨٦**	.٨١٠**	.٨٢٩**
٣	.٩٣٥**	.٩١١**	.٩١٩**
٤	.٨٣٠**	.٨٧١**	.٨٨٠**
٥	.٩٤١**	.٨٧٤**	.٨٨٧**
٦	.٧٥٧**	.٨١٨**	.٨٢٥**
٧	.٨٣٦**	.٩١٦**	.٩١٧**
٨	.٨٠٣**	.٨٦٠**	.٨٦٧**
٩	.٨٤١**	.٨٩٨**	.٩٠٤**
الجرائم الجنسية			
١	.٨٢٠**	.٨٨٣**	.٨٩٠**
٢	.٧٥٦**	.٨٦٠**	.٨٦٧**
٣	.٨٩٤**	.٨٦٩**	.٨٨١**
٤	.٧٨٥**	.٨٩٤**	.٨٩٥**
٥	.٩٤١**	.٩٣٩**	.٩٤٤**
٦	.٧٤٧**	.٨٦٨**	.٨٧٢**
٧	.٩٠٣**	.٨٩٣**	.٩٠٣**
٨	.٨٢٤**	.٨٨٤**	.٨٩٢**
الجرائم ضد الأشخاص			

العبارات	الخبراء	المستخدمين	إجمالي الاستجابات
	ن= ٤١	ن= ٤٠٤	ن= ٤٤٥
١	.٧٨٣**	.٨٧٧**	.٨٨٣**
٢	.٨٢٨**	.٨٦٣**	.٨٧٣**
٣	.٧٦١**	.٨٤٧**	.٨٥٦**
٤	.٧٥٩**	.٨٧٧**	.٨٨٠**
٥	.٧٦٥**	.٨٥٠**	.٨٥٤**
٦	.٩٠٧**	.٩١٨**	.٩٢٤**
٧	.٨٥٧**	.٧٩٨**	.٨١٢**
٨	.٨٧٣**	.٨٨٢**	.٨٩١**
٩	.٨٣٨**	.٨٧٠**	.٨٧٩**
١٠	.٨٩٧**	.٩١٧**	.٩٢٣**
١١	.٧٦٢**	.٨٧٩**	.٨٨٤**
١٢	.٦٧٣**	.٧٧١**	.٧٨١**
١٣	.٧٨٣**	.٩٠٤**	.٩٠٥**
جرائم الممتلكات			
١	.٧٣٦**	.٨٥٤**	.٨٦٢**
٢	.٨٥٣**	.٨٧٦**	.٨٨٦**
٣	.٦٩٦**	.٨٣٢**	.٨٣٩**
جرائم أخري			
١	.٩٣٥**	.٩١٥**	.٩٢٢**
٢	.٨٣٧**	.٨٨٤**	.٨٩١**
٣	.٨٢١**	.٨٤٨**	.٨٥٩**
٤	.٨٦٣**	.٨٢٧**	.٨٤٥**
٥	.٧٤٦**	.٨٨٠**	.٨٧٩**
٦	.٩٣٥**	.٩١١**	.٩١٩**
٧	.٨٥٠**	.٧٤٨**	.٧٦٨**
٨	.٧١٩**	.٨٤١**	.٨٤٥**
٩	.٦٠٨**	.٦٥٩**	.٦٦٩**
الجرائم المالية ككل	.٩٦٣**	.٩٦٨**	.٩٧٠**
الجرائم الجنسية ككل	.٩٤٢**	.٩٧٢**	.٩٧٣**
الجرائم ضد الأشخاص ككل	.٩٧٥**	.٩٨٢**	.٩٨٣**
جرائم الممتلكات ككل	.٩٠٧**	.٩٣٤**	.٩٣٩**
جرائم أخري ككل	.٩٦٧**	.٩٦٧**	.٩٧٠**

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات البحث الميداني.
ن=٤٤٥ مفردة

يتضح من نتائج الجدول رقم (٨) وجود ارتباط بين جميع متغيرات الهدف الاول، ويتضح من ذلك أن الجرائم ضد الأشخاص ذات قيمة ترابط عالية بقيمة إجمالية (٠.٩٨٣) وأخيرا جرائم الممتلكات بقيمة (٠.٩٣٩) وهو ذات ترابط أقل الجرائم بالنسبة للبعد الأول ولكن له تاثير معنوي.

ويتبن من خلال القيم السابقة تقارب قيم الترابط بالنسبة لمجموعة عينة البحث (الخبراء – المستخدمين) ومن خلال ذلك يظهر تقارب وجهات النظر بين الخبراء والمستخدمين في الكشف عن الجرائم المحتمل ارتكابها عبر التقنيات الناشئة.

جدول رقم (٩): جدول يوضح صدق الاتساق الداخلي للهدف الثانى " المخاطر الكامنة التي من المحتمل أن يتعرض لها الأطفال عبر الميتافيرس والتقنيات الناشئة " بعباراته المختلفة في (الخبراء – المستخدمين) والهدف الثاني ككل

المخاطر الكامنة التي من المحتمل أن يتعرض لها الأطفال عبر التقنيات الناشئة	الخبراء	المستخدمين	إجمالي الاستجابات
العبارات	ن= ٤١	ن= ٤٠٤	ن= ٤٤٥
١	.٧٤٠**	.٩١٥**	.٩١٦**
٢	.٧٥٨**	.٨٩٠**	.٨٩٣**
٣	.٧٣٣**	.٩٠٢**	.٩٠٤**
٤	.٦٩٨**	.٨٦٢**	.٨٦٤**
٥	.٦٦٥**	.٨٢٧**	.٨٣١**
٦	.٧٠٢**	.٨٠١**	.٨٠٦**
٧	.٦٢٠**	.٨٩١**	.٨٩١**
٨	.٧١٢**	.٩٠٢**	.٩٠٣**

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات البحث الميداني.
ن=٤٤٥ مفردة

وتكشف نتائج الجدول رقم (٩) وجود ارتباط بين جميع متغيرات الهدف الأول، ويتضح من ذلك أن "مخاطر المحتوي وتعني المخاطر التي يتعرض فيها الطفل لمحتوي غير لائق أو قانوني" ذات قيمة ترابط عالية بقيمة إجمالية (٠.٩١٦) وأخيرًا المخاطر البيولوجية بقيمة (٠.٨٠٦) وهو ذات ترابط أقل الجرائم بالنسبة للبعد الأول ولكن له تاثير معنوى.

جدول (١٠): جدول يوضح صدق الاتساق الداخلي للبعد الثالث " رصد العوامل الدافعة إلى حدوث الجرائم عبر التقنيات الناشئة" بعبارته المختلفة في (الخبراء ـ المستخدمين) والهدف الثالث ككل

رصد العوامل الدافعة إلي حدوث الجرائم عبر الميتافيرس والتقنيات الناشئة	الخبراء	المستخدمين	إجمالي الاستجابات
العبارات	ن= ٣٩	ن= ٤٠٤	ن= ٤٤٣
	العوامل العالمية		
١	.١١٣	.٤٤١**	.٤٦٢**
٢	.٣٩٨*	.٥٠٠**	.٥٢٦**
٣	-.٠٢١	.٤٠١**	.٤١٩**
٤	-.٠١٦	.٢٥٤**	.٢٨٣**

رصد العوامل الدافعة إلي حدوث الجرائم عبر الميتافيرس والتقنيات الناشئة	الخبراء ن= ٣٩	المستخدمين ن= ٤٠٤	إجمالي الاستجابات ن= ٤٤٣
العوامل المجتمعية			
١	.٥٣٣**	.٧٦٧**	.٧٦٦**
٢	.٤٩٧**	.٧٥٩**	.٧٦٩**
٣	.٣٠٣	-.٢٤٠**	-.١٧٢**
٤	.٥٩٤**	.٨٠٨**	.٨٠٤**
٥	.٦٦٩**	.٧٧٧**	.٧٨٥**
٦	.٧٩٧**	.٨١٥**	.٨٢٤**
٧	.٦٨٣**	.٧٧٧**	.٧٨٤**
العوامل الفردية			
١	.٥٦٢**	.٦٩٧**	.٧٠٩**
٢	.٥٨٤**	.٧٩٧**	.٨٠٤**
٣	.٦٦٤**	.٧٦٨**	.٧٧٤**
٤	.٧٣٨**	.٧٧٧**	.٧٨٤**
٥	.٧٣٨**	.٨٠٨**	.٨١٠**
٦	.٦٦١**	.٤٦٩**	.٤٩٦**
٧	.٥٢٩**	.٢٠٣**	.٢٣٣**
٨	.٦٦٦**	.٨١٢**	.٨١٩**
العوامل العالمية ككل	.٢٩٣	.٥٤٨**	.٥٧٥**
العوامل المجتمعية ككل	.٨٨٦**	.٩٣٣**	.٩٣٧**
العوامل الفردية ككل	.٩١٢**	.٩٤٦**	.٩٤٨**

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات البحث الميداني.
ن=٤٤٥ مفردة

وتظهر نتائج الجدول (١٠) وجود ارتباط بين جميع متغيرات الهدف الثالث، ويتضح من ذلك أن العوامل الفردية ذات قيمة ترابط عالية بقيمة أجمالية (٠.٩٤٨) ثم يليه العوامل المجتمعية بقيمة إجمالية (٠.٩٣٧) وأخيرًا العوامل العالمية بقيمة (٠.٥٧٥) وهو ذات ترابط أقل العوامل ترابطا بالنسبة للبعد الثالث ولكن له تاثير معنوى .

ويتضح من خلال القيم السابقة تقارب قيم الترابط بالنسبة لمجموعة عينة البحث (الخبراء – المستخدمين) و من خلال ذلك يظهر تقارب وجهات النظر بين الخبراء والمستخدمين في رصد العوامل الدافعة إلي حدوث الجرائم عبر التقنيات الناشئة.

جدول (١١): جدول يوضح صدق الاتساق الداخلي للبعد الرابع " رصد أليات وحلول مواجهة جرائم ومخاطر الميتافيرس والتقنيات الناشئة" بعبارته المختلفة في (الخبراء – المستخدمين) والهدف الرابع ككل.

أليات وحلول مواجهة جرائم ومخاطر الميتافيرس و التقنيات الناشئة	الخبراء	المستخدمين	إجمالي الاستجابات
	ن= ٤١	ن= ٤٠٤	ن= ٤٤٥
العبارات	الحلول القانونية		
١	٦٧٨.**	٧٢٩.**	٧٢٩.**
٢	٩٣٩.**	٦٧٣.**	٦٨١.**
٣	٩٣٩.**	٧٨١.**	٧٨٥.**
٤	٩٣٩.**	٧١٤.**	٧١٩.**
حلول السياسات			
١	٧٤٩.**	٦٥٦.**	٦٦٣.**
٢	٠.١٨٤	٦٥٦.**	٦٤٦.**
٣	٨٦٥.**	٦٣٥.**	٦٤٧.**
٤	٠.٢٦٦	٧٠٦.**	٧٠٤.**
٥	٩٣٩.**	٧٢٠.**	٧٢٩.**
الحلول التقنية			
١	٦٧٨.**	٦٥٦.**	٦٥٩.**
٢	٠.٢٦٦	٦٧٧.**	٦٧٥.**
٣	٩٣٩.**	٧٤٣.**	٧٤٨.**
الحلول التوعوية			
١	٨٧٥.**	٧١٤.**	٧١٨.**
٢	٩٦٩.**	٧٦٧.**	٧٧٢.**
٣	٩٣٩.**	٧٠٦.**	٧١٥.**
٤	٩٣٩.**	٦٩٢.**	٦٩٧.**
٥	٩٣٩.**	٦٢٣.**	٦٣١.**
الحلول القانونية ككل	٩١٨.**	٨٩٦.**	٨٩٨.**
حلول السياسات ككل	٨٨٩.**	٨٨٩.**	٨٩٢.**
الحلول التقنية ككل	٨٩٨.**	٨٤٠.**	٨٤٢.**
الحلول التوعوية ككل	٩٧١.**	٨٩٥.**	٨٩٧.**

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات البحث الميداني.
ن=٤٤٥ مفردة

يتضح من نتائج الجدول (١١) وجود ارتباط بين جميع متغيرات الهدف الرابع، ويتضح من ذلك أن الحلول القانونية و الحلول التوعوية ذات قيمة ترابط عالية بقيمة أجمالية (٠.٨٩٨) و(٠.٨٩٧) بالتوالي ثم حلول السياسات بقيمة إجمالية (٠.٨٩٢) وأخيرا الحلول التقنية بقيمة (٠.٨٤٢) وهو ذات ترابط أقل العوامل ترابطا بالنسبة للبعد الرابع ولكن له تاثير معنوي.

ويتضح من خلال القيم السابقة تقارب قيم الترابط بالنسبة لمجموعة عينة البحث (الخبراء – المستخدمين) ومن خلال ذلك يظهر تقارب وجهات النظر بين الخبراء و المستخدمين في رصد أليات مواجهة مخاطر وجرائم التقنيات الناشئة ويتضح أن أهم حل هو استخدام الحلول القانونية.

جدول (١٢): جدول يوضح الصدق البنائي للمقياس ككل مع الأهداف المختلفة محل الدراسة في (الخبراء – المستخدمين)

أهداف المقياس ككل	الخبراء	المستخدمين	إجمالي الاستجابات
	ن= ٤١	ن= ٤٠٤	ن= ٤٤٥
الهدف الأول: الكشف عن الجرائم المحتمل ارتكابها عبر التقنيات الناشئة	**٠.٨٥٦	**٠.٩٠٤	**٠.٩١١
الهدف الثاني: أهم المخاطر الكامنة التي من المحتمل أن يتعرض لها الأطفال عبر التقنيات الناشئة	**٠.٨٨٨	**٠.٩٢١	**٠.٩٢٥
الهدف الثالث: رصد العوامل الدافعة إلي حدوث الجرائم عبر التقنيات الناشئة	**٠.٨١٣	**٠.٨٥٠	**٠.٨٦٤
الهدف الرابع: رصد أليات مواجهة مخاطر وجرائم التقنيات الناشئة	**٠.٤٢٩	**٠.٢٤٨	**٠.٢٨٣

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات البحث الميداني.
ن=٤٤٥ مفردة

يتضح من نتائج الجدول (١٢) وجود ارتباط ثنائي بين جميع متغيرات الدراسة، حيث أن قيمة معامل الارتباط الأقل من (٠.٣) تعبر عن درجة ارتباط ضعيف، وأن قيمة معامل الارتباط من (٠.٣ إلى أقل من ٠.٧) تعبر عن درجة ارتباط متوسطة، بينما تعبر قيمة معامل الارتباط الأكبر من أو يساوي (٠.٧) عن درجة ارتباط قوية، ويتضح ذلك الهدف الثاني ذات قيمة ترابط عالية بقيمة أجمالية (٠.٩٢٥) وثم يليه الهدف الأول بقيمة (٠.٩١١) وثالثًا الهدف الثالث (٠.٨٦٤) وأخيرًا الهدف الرابع بقيمة (٠.٢٨٣) وهو ذات ترابط ضعيف ولكن له تاثير معنوي عالي. وبناء على ماسبق فإن الصدق البنائى يشير إلى قدرة أداة البحث على قياس صدق عبارات المقياس لضمان موثوقية ودقة البحث حيث يساعد على التأكد من أدواتهم وتعكس بدقة المفهوم الذي يسعى إليه الباحث من خلال دراسته، مما يعزز من الثقة فى النتائج والاستنتاجات.

ثبات وصدق المقياس "Reliability":

يقصد بثبات المقياس أن تعطي أسئلة المقياس نفس النتيجة لو تم إعادة توزيعه أكثر من مرة تحت نفس الظروف والشروط، أو بعبارة أخرى أن ثبات المقياس يعني الاستقرار في نتائجه، وعدم تغييرها بشكل كبير فيما لو تم إعادة توزيعها على أفراد العينة عدة مرات خلال فترات زمنية معينة.

- معامل الفا كرونباخ لقياس ثبات المقياس

استخدمت الباحثة طريقة ألفا كرونباخ لقياس ثبات المقياس ، وكانت النتائج كما هي مبينة في الجداول التالية:

جدول (١٣): يوضح درجة الثبات باستخدام معامل الفا كرونباخ بين الهدف الأول وعباراته وبين المقياس وعباراته المختلفة والخاصة بـ "أنماط الجرائم والمخاطر المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة"

الهدف الأول: الجرائم المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة:	عدد العبارات	درجة الثبات معامل الفا كرونباخ		
		الخبراء	المستخدمين	الاستجابات ككل
الجرائم المالية	٩	٠.٩٤٠	٠.٩٦٦	٠.٩٦٨
الجرائم الجنسية	٨	٠.٩٥٧	٠.٩٧١	٠.٩٧٣
الجرائم ضد الأشخاص	١٣	٠.٩٥٩	٠.٩٧٦	٠.٩٧٨
جرائم الممتلكات	٣	٠.٧٨٤	٠.٩٠٢	٠.٩٠٧
جرائم أخري	٩	٠.٩٣٩	٠.٩٥٨	٠.٩٦١
الهدف الأول ككل	٤٢	٠.٩٨٦	٠.٩٩٢	٠.٩٩٢

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات البحث الميداني.
ن=٤٤٥ مفردة

يتضح من الجدول (١٣) أنه تم حساب ثبات المقياس باستخدام معامل ألفا كرونباخ لعينة المجتمع ويتضح من بيانات الجدول أن جميع معاملات الثبات للمقياس المستخدم لقياس متغيرات البحث مرتفعة ونسبها عالية ومقبولة باعتبار أن نسب معامل الثبات مرتفعة ومقبولة وقد سجلت البيانات معاملات ثبات مرتفعة لجميع متغيرات البحث كما أن معاملات الثبات للقائمة ككل مرتفعة (٠.٩٨٥) ، (٠.٩٧٧) الخبراء و(٠.٩٨٤) للمستخدمين على التوالي، وتدل هذه النتائج على ثبات واعتمادية أداة القياس وصلاحيتها من الناحية الإحصائية لجمع بيانات البحث الميداني.

جدول (١٤): يوضح درجة الثبات باستخدام معامل الفا كرونباخ بين الهدف الثاني وعباراته وبين المقياس وعباراته المختلفة والخاصة بـ "أنماط الجرائم والمخاطر المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة"

الهدف الثاني: المخاطر الكامنة التي من المحتمل أن يتعرض لها الأطفال عبر الميتافيرس والتقنيات الناشئة ككل	عدد العبارات	درجة الثبات معامل الفا كرونباخ		
		الخبراء	المستخدمين	الاستجابات ككل
	٨	٠.٨٥١	٠.٩٥٦	٠.٩٥٧

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات البحث الميداني.
ن=٤٤٥ مفردة

يتضح من الجدول (١٤) أنه تم حساب ثبات المقياس باستخدام معامل ألفا كرونباخ لعينة المجتمع ويتضح من بيانات الجدول أن جميع معاملات الثبات للمقياس المستخدم لقياس متغيرات البحث مرتفعة ونسبها عالية ومقبولة باعتبار أن نسب معامل الثبات مرتفعة ومقبولة وقد سجلت البيانات معاملات ثبات مرتفعة لجميع متغيرات البح كما أن معاملات الثبات للقائمة ككل مرتفعة (٠.٩٨٥) ، (٠.٩٧٧) للخبراء و (٠.٩٨٤) للمستخدمين على التوالي، وتدل هذه النتائج على ثبات واعتمادية أداة القياس وصلاحيتها من الناحية الإحصائية لجمع بيانات البحث الميداني.

جدول (١٥): يوضح درجة الثبات باستخدام معامل الفا كرونباخ بين الهدف الثالث وعباراته وبين المقياس وعباراته المختلفة والخاصة بـ "أنماط الجرائم والمخاطر المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة"

الهدف الثالث: رصد العوامل الدافعة إلي حدوث الجرائم عبر الميتافيرس والتقنيات الناشئة:	عدد العبارات	درجة الثبات معامل الفا كرونباخ		
		الخبراء	المستخدمين	الاستجابات ككل
العوامل العالمية	٤	٠.١١٢	٠.٧٢١	٠.٧٣٠
العوامل المجتمعية	٧	٠.٧٤١	٠.٨١١	٠.٨٢٣
العوامل الفردية	٨	٠.٨٤٦	٠.٨٦٧	٠.٨٧٦
الهدف الثالث ككل	١٩	٠.٨٥٠	٠.٩٠٧	٠.٩١٤

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات البحث الميداني.
ن=٤٤٥ مفرد

يتضح من الجدول (١٥) أنه تم حساب ثبات المقياس باستخدام معامل ألفا كرونباخ لعينة المجتمع ويتضح من بيانات الجدول أن جميع معاملات الثبات للمقياس المستخدم لقياس متغيرات البحث مرتفعة ونسبها عالية ومقبولة باعتبار أن نسب معامل

الثبات مرتفعة ومقبولة وقد سجلت البيانات معاملات ثبات مرتفعة لجميع متغيرات البحث كما أن معاملات الثبات للقائمة ككل مرتفعة (٠.٩٨٥)، (٠.٩٧٧) الخبراء و(٠.٩٨٤) للمستخدمين على التوالي، وتدل هذه النتائج على ثبات واعتمادية أداة القياس وصلاحيتها من الناحية الإحصائية لجمع بيانات البحث الميداني.

جدول (١٦): يوضح درجة الثبات باستخدام معامل الفا كرونباخ بين الهدف الرابع وعباراته وبين المقياس وعباراته المختلفة والخاصة بـ "أنماط الجرائم والمخاطر المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة"

الهدف الرابع : الأليات والحلول لمواجهة جرائم ومخاطر الميتافيرس والتقنيات الناشئة:	عدد العبارات	درجة الثبات معامل الفا كرونباخ		
		الخبراء	المستخدمين	الاستجابات ككل
الحلول القانونية	٤	٠.٩٤٠	٠.٨٢١	٠.٨٢٥
حلول السياسات	٥	٠.٧٠٩	٠.٨١١	٠.٨١٢
الحلول التقنية	٣	٠.٤٦٨	٠.٧٦٤	٠.٧٦٦
الحلول التوعوية	٥	٠.٩٤٧	٠.٨٣٧	٠.٨٤٣
الهدف الرابع ككل	١٧	٠.٩٤١	٠.٩٣٢	٠.٩٣٣
المقياس ككل	٨٦	٠.٩٧٧	٠.٩٨٤	٠.٩٨٥

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات البحث الميداني.
ن=٤٤٥ مفردة

يتضح من الجدول (١٦) أنه تم حساب ثبات المقياس باستخدام معامل ألفا كرونباخ لعينة المجتمع ويتضح من بيانات الجدول أن جميع معاملات الثبات للمقياس للمستخدم لقياس متغيرات البحث مرتفعة ونسبها عالية ومقبولة باعتبار أن نسب معامل الثبات مرتفعة ومقبولة وقد سجلت البيانات معاملات ثبات مرتفعة لجميع متغيرات البحث كما أن معاملات الثبات للقائمة ككل مرتفعة (٠.٩٨٥)، (٠.٩٧٧) للخبراء و(٠.٩٨٤) للمستخدمين على التوالي، وتدل هذه النتائج على ثبات واعتمادية أداة القياس وصلاحيتها من الناحية الإحصائية لجمع بيانات البحث الميداني.

(٥) المعالجات والأساليب الإحصائية:

لقد تم وصف المتغيرات الفئوية بالعدد والنسبة المئوية (N %)، بينما تم وصف المتغيرات المستمرة بالمتوسط والانحراف المعياري (Mean, SD)، ولقد تم استخدام

اختبار مربع كاي للمقارنة بين المتغيرات الفئوية، حيث تم المقارنة بين المتغيرات المستمرة باختبار (T) والعينات المستقلة. تم اعتبار (P ثنائي الذيل < ٠.٠٥) ذا دلالة إحصائية. كما تم استخدام ارتباط سبيرمان لإظهار الارتباط بين المتغيرات. ثم تم إجراء جميع التحليلات باستخدام برنامج. IBM SPSS 26.

(٦) الخصائص الديموجرافية والاجتماعية لعينة البحث:

١- عينة الخبراء:

جدول (١٧) الخصائص الديموجرافية والاجتماعية لعينة الخبراء ن= (٤١)

المتغير	التكرار	النسبة
النوع	ك	%
ذكر	٣٢	٧٨%
أنثي	٩	٢٢%
الوظيفة	ك	%
أستاذ جامعي	٢٧	٦٥.٨
مهندسون متخصصون أمن سيبراني	٩	٢٢
رجال إنفاذ القانون	٣	٧.٣
مستشارون	٢	٤.٩
سنوات الخبرة	ك	%
خبرة أقل من ٢٠ سنة	١٣	٣١.٧
خبرة أكبر أو تساوى ٢٠سنة	٢٨	٦٨.٣

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية

٢- الخصائص الديموجرافية والاجتماعية لعينة الشباب مستخدمي الميتافيرس:

جدول (١٨) الخصائص الديموجرافية والاجتماعية لعينة المستخدمين من الشباب ن= (٤٠٤)

المتغير	التكرار	النسبة المئوية
النوع	ك	%
انثي	٨٩	٢٢.٠
ذكر	٣١٥	٧٨.٠
السن		
المدى	١٧ ـ ٢٧ سنة	
المتوسط ± الانحراف المعياري	١٩.٣٧±١.٤٧	
الموطن الأصلي		
حضر	٢٣٤	٥٧.٩
ريف	١٧٠	٤٢.١

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية.

عاشرًا: نتائج أهداف البحث الميداني ومناقشتها:

١- نتائج التحليل الكمي لأهداف البحث:

- نتائج الهدف الأول: رصد سيناريوهات تهديدات الجرائم المحتمل إرتكابها عبر الميتافيرس والتقنيات الناشئة من وجهة نظر الخبراء والمستخدمين من الشباب:

(أ) نتائج المقارنات بين استجابات عينة الخبراء واستجابات عينة المستخدمين من الشباب حول سيناريوهات تهديدات الجرائم المحتمل إرتكابها عبر الميتافيرس والتقنيات الناشئة.

جدول (١٩) يوضح المقارنة بين (الخبراء - المستخدمين) وترتيب أكثر الجرائم تأثيرًا

الهدف الأول: سيناريوهات تهديد الجرائم المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة:	الخبراء			المستخدمين		
	المتوسط	الانحراف المعياري	الترتيب	المتوسط	الانحراف المعياري	الترتيب
الجرائم المالية						
١- هجمات البلوكتشين لسرقة العملات الرقمية من المستخدمين.	٢.٦٧	٠.٦٦	٦	١.٨٦	٠.٩٢	٣ مكرر
٢- غسل الاموال باستخدام العملات المُشفرة وتسهيل التحويلات المالية الإجرامية	٢.٨٢	٠.٥٦	٢ مكرر	١.٨٤	٠.٩٣	٥ مكرر
٣- سرقة الهوية الرقمية عن طريق سرقة المعلومات المالية للمستخدمين لتحقيق مكاسب مالية	٢.٨٢	٠.٥٦	٢ مكرر	١.٨٨	٠.٩٥	٢
٤- عمليات احتيال الاستثمار واختلاس أصول الأخرين	٢.٦٩	٠.٦١	٥ مكرر	١.٨	٠.٩٢	٧
٥- التزييف من خلال إنشاء وبيع منتجات وسلع رقمية مزيفة وغير مشروعة	٢.٨٥	٠.٥٤	١	١.٨٥	٠.٩٥	٤
٦- التلاعب بالسوق	٢.٥٩	٠.٧٥	٧	١.٨٤	٠.٩	٥ مكرر
٧- الخداع الإلكتروني	٢.٧٤	٠.٦٤	٣	١.٩٢	٠.٩٥	١
٨- انتهاك حقوق الملكية من خلال استخدام الصور الرمزية والمواد المصورة وغيرها والمتاح عبر الميتافيرس	٢.٦٩	٠.٦٦	٥ مكرر	١.٨٦	٠.٩٥	٣ مكرر
٩- الوسيط المحتال، عن طريق التظاهر بأنهم وسطاء للأصول الرقمية التي تنقلها بين منصات الميتافيرس بغرض سرقة المالكين والاحتيال عليهم	٢.٧٢	٠.٦	٤	١.٨٢	٠.٩٣	٦
الجرائم الجنسية						
١- استمالة الأطفال والمراهقين عبر الصور الرمزية لإجبارهم على الاشتراك في أنشطة جنسية	٢.٦٩	٠.٦٦	٥	١.٧٧	٠.٩٢	٥
٢- الإعتداء الجنسي على الأطفال عبر الصور الرمزية	٢.٦٢	٠.٧١	٧	١.٧	٠.٨٩	٧
٣- جرائم الصور الجنسية من خلال إشراك المستخدمين في أفعال جنسيةعبر الواقع الافتراضي	٢.٧٤	٠.٥٩	٣	١.٧٨	٠.٩٢	٤
٤- التحرش وإساءة معاملة الأطفال عبر الصور الافتراضية والرمزية ومطاردتهم عبر منصات الميتافيرس المختلفة	٢.٥٩	٠.٧٢	٨	١.٧٩	٠.٩٣	٣ مكرر

الهدف الأول: سيناريوهات تهديد الجرائم المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة:	الخبراء			المستخدمين		
	المتوسط	الانحراف المعياري	الترتيب	المتوسط	الانحراف المعياري	الترتيب
٥- التشهير والابتزاز من خلال استغلال المعلومات الخاصة والصور الرمزية، وتسجيل التفاعلات والمحادثات وتهديدهم بنشر المعلومات الشخصية للمستخدمين من أجل ابتزازهم	٢.٨٥	٠.٥٤	١	١.٨٨	٠.٩٦	٢
٦- التنمر الإلكتروني	٢.٧٢	٠.٦٥	٤	١.٨٩	٠.٩٥	١
٧- المواد الإباحية، حيث قامت ميتافيرس بفتح طرقًا جديدة لتوزيع الصور الإباحية	٢.٧٧	٠.٥٨	٢	١.٧٩	٠.٩٤	٣ مكرر
٨- الإتجار الافتراضي بالأشخاص من أجل الاستغلال الجنسي.	٢.٦٧	٠.٦٦	٦	١.٧٤	٠.٩١	٦
الجرائم ضد الأشخاص						
١- التحريض على إيذاء النفس.	٢.٦٩	٠.٦٦	٥	١.٧٥	٠.٩٢	٩ مكرر
٢- التحريض على الإدمان.	٢.٦٧	٠.٦٢	٦	١.٧٥	٠.٩١	٩ مكرر
٣- التحريض على ارتكاب الجرائم من قبل المنظمات الإجرامية.	٢.٥٦	٠.٦٤	٩	١.٧	٠.٨٩	١١
٤- المطاردة، جيت يمكن لشخص ملاحقة المستخدمين عبر منصات الميتافيرس المختلفة،ويمكن للمجرمين استخدام الصور الرمزية لتجنب اكتشافهم.	٢.٥٩	٠.٦٤	٨ مكرر	١.٨	٠.٩١	٧
٥- التطرف، يمكن استخدام الذكاء الاصطناعي ليكون الوسيلة لتطرف المستخدمين الضعفاء والمراهقين	٢.٥٩	٠.٧٢	٨ مكرر	١.٨٣	٠.٩٢	٥
٦- الإساءة ضد الأشخاص في مناصب السلطة	٢.٧٩	٠.٥٧	٢	١.٨٥	٠.٩٤	٤
٧- إنشاء حسابات مُزيفة.	٢.٧٤	٠.٥٩	٣ مكرر	٢.٠١	٠.٩	١
٨- التجسس الافتراضي.	٢.٧٤	٠.٥٩	٣ مكرر	١.٨٨	٠.٩٢	٣
٩- العنف السيبراني، حيث يوفر الميتافيرس فرصًا لبناء هويات افتراضية لارتكاب الجرائم.	٢.٥٩	٠.٦٨	٨ مكرر	١.٧٢	٠.٨٩	١٠
١٠- انتهاك الخصوصية	٢.٨٢	٠.٥٦	١	١.٨٩	٠.٩٥	٢
١١- إثارة الخوف والإثارة الخوف والاضطراب الانفعالي.	٢.٧٢	٠.٦٥	٤	١.٨١	٠.٩١	٦
١٢- عمالة الأطفال والعبودية المستحدثة	٢.٣٨	٠.٧٨	١٠	١.٦١	٠.٨٣	١٢
١٣- استغلال المدمنين لأغراض الابتزاز أو الإكراه أو التحريض على ارتكاب جرائم.	٢.٦٢	٠.٦٧	٧	١.٧٨	٠.٩٢	٨
جرائم الممتلكات						
١- السطو المادي عن طريق استغلال الواقع الافتراضي والواقع المعزز ومواد الاستشعار الذكية ومحاولة السطو على الممتلكات والأشياء الثمينة.	٢.٦٢	٠.٦٧	٢	١.٦٩	٠.٨٧	٢
٢- هجمات البنية التحتية السيبرانية من قبل المجرمين والجهات الفاعلة المنظمة.	٢.٦٩	٠.٦١	١	١.٧٦	٠.٩	١
٣- التعدي على ممتلكات الغير في الميتافيرس	٢.٥٤	٠.٦٨	٣	١.٦٧	٠.٨٧	٣

الهدف الأول: سيناريوهات تهديد الجرائم المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة:	الخبراء			المستخدمين		
	المتوسط	الانحراف المعياري	الترتيب	المتوسط	الانحراف المعياري	الترتيب
جرائم أخرى						
١- انتحال صفة شخصية	٢.٨٢	٠.٥٦	١ مكرر	١.٨٨	٠.٩٥	٣
٢- التأمرعن طريق استغلال العالم الافتراضي عبر التوائم الرقمية لارتكاب جرائم في العالم المادي.	٢.٦٤	٠.٦٧	٤	١.٧٧	٠.٩١	٥ مكرر
٣- الإرهاب ن يكون الميتافيرس فرصًا جديدة للمنظمات الإرهابية للدعاية والتجنيد والإرهاب.	٢.٦٧	٠.٦٦	٣ مكرر	١.٧٧	٠.٩١	٥ مكرر
٤- حدوث الاستقطاب المجتمعي من الجهات المعادية	٢.٧٤	٠.٥٩	٢	١.٧٤	٠.٨٧	٦
٥- السلوك العنيف	٢.٦٢	٠.٧١	٥	١.٨٩	٠.٩١	٢
٦- نشر المعلومات الخاطئة والمضللة بهدف زعزعة استقرار المجتمعات.	٢.٨٢	٠.٥٦	١ مكرر	١.٨٧	٠.٩٥	٤
٧- التاثير في العالم المادي عبر الأدوات المختلفة.	٢.٦٧	٠.٦٦	٣ مكرر	١.٩٣	٠.٨٩	١
٨- إنتحال صفة رجال إنفاذ القانون	٢.٥٤	٠.٦٨	٦	١.٧٧	٠.٨٩	٥ مكرر
٩- حرمان المستخدمين من الخدمات الأساسية كالصحة والتعليم.	٢.١٨	٠.٨٥	٧	١.٥٩	٠.٨٤	٧

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية
ن=٤٤٥ مفردة أكبر قيمة للمتوسط هي ٣ و أقل قيمة هي ١

ومن قراءة الجدول السابق يمكن الإشارة إلى:

- **الجرائم المالية:** تبين من وجهة نظر الخبراء أن تهديد الجريمة رقم (٤) وهى (عمليات احتيال الاستثمار واختلاس أصول الأخرين) أقوى تأثيرًا في الجرائم المالية طبقًا لإجماع أراء الخبراء بمتوسط (٢.٨٥)، بينما من وجهة نظر المستخدمين جاء تهديد الجريمة رقم (٧) وهي (الخداع الإلكتروني) أقوى تأثيرًا في الجرائم المالية طبقا لإجماع أراء المستخدمين بمتوسط (١.٩٢).
- **الجرائم الجنسية:** اتضح من وجهة نظر الخبراء أن تهديد الجريمة رقم (٥) وهى (التشهير والابتزاز من خلال استغلال المعلومات الخاصة والصور الرمزية، وتسجيل التفاعلات والمحادثات وتهديدهم بنشر المعلومات الشخصية للمستخدمين من أجل ابتزازهم) أقوى تأثيرًا في الجرائم الجنسية طبقًا لإجماع أراء الخبراء بمتوسط (٢.٨٥)، بينما من وجهة نظر المستخدمين أن تهديد الجريمة رقم (٦) وهي (التنمر الإلكتروني) أقوى تأثيرًا في الجرائم الجنسية طبقًا لإجماع أراء المستخدمين بمتوسط (١.٨٩).

- **الجرائم ضد الاشخاص:** كشفت وجهة نظر الخبراء أن تهديد الجريمة رقم (١٠) وهي (انتهاك الخصوصية) أقوى تأثيرًا في الجرائم ضد الأشخاص طبقًا لإجماع أراء الخبراء بمتوسط (٢.٨٢)، بينما من وجهة نظر المستخدمين جاء تهديد الجريمة رقم (٧) وهي (إنشاء حسابات مُزيفة) أقوى تأثيرًا في الجرائم ضد الاشخاص طبقا لإجماع أراء المستخدمين بمتوسط (١.٨٥).
- **جرائم الممتلكات:** أظهرت وجهة نظر الخبراء أن تهديد الجريمة رقم (٢) وهي (هجمات البنية التحتية السيبرانية من قبل المجرمين والجهات الفاعلة المنظمة) أقوى تأثيرًا في جرائم الممتلكات طبقًا لإجماع أراء الخبراء بمتوسط (٢.٦٩) وكان هذا أيضًا بإجماع أراء المستخدمين على نفس تهديد الجريمة بمتوسط (١.٧٦).
- **جرائم أخرى:** بينت من وجهة نظر الخبراء أن تهديد الجرائم رقم (١و ٦) وهما (انتحال صفة شخصية، نشر المعلومات الخاطئة والمضللة بهدف زعزعة استقرار المجتمعات) أقوى تأثيرًا في الجرائم الأخرى طبقًا لإجماع أراء الخبراء بمتوسط (٢.٨٢) بينما من وجهة نظر المستخدمين جاء تهديد الجريمة رقم (٧) وهي (التأثير في العالم المادي عبر الأدوات المختلفة) أقوى تأثيرًا في الجرائم الأخرى طبقًا لإجماع أراء المستخدمين بمتوسط (١.٩٣).

جدول (٢٠) يوضح المقارنة بين (الخبراء – المستخدمين) وترتيب أكثر الجرائم تأثيراً

الهدف الأول: سيناريوهات تهديد الجرائم المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة	الخبراء			م	المستخدمين			الترتيب	ت
	المتوسط	الانحراف المعياري	المدى		المتوسط	الانحراف المعياري	المدى		
الجرائم المالية	٢.٧٣	٠.٥١	١-٣	١	١.٨٥	٠.٨٣	١-٣	١	٦.٤٩٨
الجرائم الجنسية	٢.٧١	٠.٥٦	١-٣	٢	١.٧٩	٠.٨٥	١-٣	٣	٦.٥٨٩
الجرائم ضد الأشخاص	٢.٦٥	٠.٥٣	١-٣	٣	١.٨٠	٠.٨٠	١-٣	٢ مكرر	٦.٥٥٣
جرائم الممتلكات	٢.٦٢	٠.٥٥	١-٣	٥	١.٧١	٠.٨٠	١-٣	٤	٦.٩١٢
جرائم أخرى	٢.٦٣	٠.٥٥	١-٣	٤	١.٨٠	٠.٧٨	١-٣	٢ مكرر	٦.٤٩٤
البعد الأول ككل	٢.٦٧	٠.٥١	١-٣		١.٨٠	٠.٧٩	١-٣		٦.٧٦٦

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية
ن= ٤٤٥ مفردة

يتضح من الجدول (٢٠) إنه بإجماع أراء الخبراء والمستخدمين تبين أن الجرائم المالية هي أقوى الجرائم المحتمل ارتكابها عبر التقنيات الناشئة بمتوسط (٢.٧٣) للخبراء و(١.٨٥) للمستخدمين.

(ب) نتائج الفروق بين الأوزان النسبية (الخبراء – المستخدمين) حول سيناريوهات تهديدات الجرائم المحتمل إرتكابها عبر الميتافيرس والتقنيات الناشئة.

جدول (٢١) الفروق بين الأوزان النسبية (الخبراء – المستخدمين)

الهدف الأول: سيناريوهات تهديد الجرائم المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة	خبراء ن= ٤١		المستخدمين ن= ٤٠٤		إجمالي الاستجابات ن= ٤٤٥		ز	الدلالة
	ق	ت	ق	ت	ق	ت		
الجرائم المالية								
١- هجمات البلوكتشين لسرقة العملات الرقمية من المستخدمين	٠.٨٨٩	٦	٠.٦٢١	٣	٠.٦٤٥	٤	-٥.١٣٧	**
٢- غسل الاموال باستخدام العملات المُشفرة وتسهيل التحويلات المالية الإجرامية	٠.٩٤	٢مكرر	٠.٦١٥	٦	٠.٦٤٣	٥	-٦.١٢٣	**
٣- سرقة الهوية الرقمية عن طريق سرقة المعلومات المالية للمستخدمين لتحقيق مكاسب مالية	٠.٩٤	٢مكرر	٠.٦٢٥	٢	٠.٦٥٣	٢	-٥.٨٣٩	**
٤- عمليات احتيال الاستثمار واختلاس أصول الأخرين	٠.٨٩٧	٥مكرر	٠.٦٠١	٩	٠.٦٢٧	٩	-٥.٧١٦	**
٥- التزييف من خلال إنشاء وبيع منتجات وسلع رقمية مزيفة وغير مشروعة	٠.٩٤٩	١	٠.٦١٨	٥	٠.٦٤٧	٣	-٦.١٢٥	**
٦- التلاعب بالسوق	٠.٨٦٣	٧	٠.٦١٤	٧	٠.٦٣٦	٧	-٤.٨٤١	**
٧- الخداع الإلكتروني	٠.٩١٥	٣	٠.٦٣٩	١	٠.٦٦٣	١	-٥.١٤٣	**
٨- إنتهاك حقوق الملكية من خلال استخدام الصور الرمزية والمواد المصورة وغيرها والمتاح عبر الميتافيرس	٠.٨٩٧	٥ مكرر	٠.٦١٩	٤	٠.٦٤٣	٦	-٥.٢٢٦	**
٩- الوسيط المحتال، عن طريق التظاهر بأنهم وسطاء للأصول الرقمية التي تنقلها بين منصات الميتافيرس بغرض سرقة المالكين والاحتيال عليهم	٠.٩٠٦	٤	٠.٦٠٨	٨	٠.٦٣٤	٨	-٥.٦٨٣	**
الجرائم الجنسية								
١- استمالة الأطفال والمراهقين عبر الصور الرمزية لإجبارهم على الاشتراك في أنشطة جنسية	٠.٨٩٧	٥	٠.٥٩٢	٥	٠.٦١٩	٦	-٥.٨٣٨	**
٢- الإعتداء الجنسي على الأطفال عبر الصور الرمزية	٠.٨٧٢	٧	٠.٥٦٧	٧	٠.٥٩٤	٨	-٥.٩٣١	**

الهدف الأول: سيناريوهات تهديد الجرائم المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة	خبراء ن= ٤١		المستخدمين ن= ٤٠٤		إجمالي الاستجابات ن= ٤٤٥		ز	الدلالة
	ق	ت	ق	ت	ق	ت		
٣- جرائم الصور الجنسية من خلال إشراك المستخدمين في أفعال جنسية عبر الواقع الافتراضي	٠.٩١٥	٣	٠.٥٩٥	٤	٠.٦٢٣	٤	٦.٠٨٢-	**
٤- التحرش وإساءة معاملة الأطفال عبر الصور الافتراضية والرمزية ومطاردتهم عبر منصات الميتافيرس المختلفة	٠.٨٦٣	٨	٠.٥٩٧	٣مكرر	٠.٦٢	٥	٥.١٠٨-	**
٥- التشهير والابتزاز من خلال استغلال المعلومات الخاصة والصور الرمزية، وتسجيل التفاعلات والمحادثات وتهديدهم بنشر المعلومات الشخصية للمستخدمين من أجل ابتزازهم	٠.٩٤٩	١	٠.٦٢٥	٢	٠.٦٥٤	١	٥.٩٧١-	**
٦- التنمر الإلكتروني	٠.٩٠٦	٤	٠.٦٢٩	١	٠.٦٥٣	٢	٥.١٦٦-	**
٧- المواد الإباحية، حيث قامت ميتافيرس بفتح طرقًا جديدة لتوزيع الصور الإباحية	٠.٩٢٣	٢	٠.٥٩٧	٣مكرر	٠.٦٢٥	٣	٦.١٠٣-	**
٨- الإتجار الافتراضي بالأشخاص من أجل الاستغلال الجنسي	٠.٨٨٩	٦	٠.٥٨١	٦	٠.٦٠٨	٧	٥.٩٤١-	**
الجرائم ضد الأشخاص								
١- التحريض على إيذاء النفس	٠.٨٩٧	٥	٠.٥٨٣	٩	٠.٦١١	٨	٥.٩٩٣-	**
٢- التحريض على الإدمان	٠.٨٨٩	٦	٠.٥٨٢	١٠	٠.٦٠٩	٩	٥.٩٩٣-	**
٣- التحريض على ارتكاب الجرائم من قبل المنظمات الإجرامية	٠.٨٥٥	١٠	٠.٥٦٧	١٢	٠.٥٩٢	١١	٥.٨٥٧-	**
٤- المطاردة حيث يمكن لشخص ملاحقة المستخدمين عبر منصات الميتافيرس المختلفة ويمكن للمجرمين استخدام الصور الرمزية لتجنب اكتشافهم	٠.٨٦٣	٨ مكرر	٠.٥٩٩	٧	٠.٦٢٢	٦	٥.٢٣٣-	**
٥- التطرف، يمكن استخدام الذكاء الاصطناعي ليكون الوسيلة لتطرف المستخدمين الضعفاء والمراهقين	٠.٨٦٣	٨مكرر	٠.٦٠٩	٥	٠.٦٣١	٥مكرر	٤.٩١٢-	**
٦- الإساءة ضد الأشخاص	٠.٩٣٢	٢	٠.٦١٦	٤	٠.٦٤٣	٤	٥.٩٠٥-	**
٧- إنشاء حسابات مُزيفة	٠.٩١٥	٣مكرر	٠.٦٧	١	٠.٦٩١	١	٤.٨٨٩-	**
٨- التجسس الافتراضي	٠.٩١٥	٣مكرر	٠.٦٢٥	٣	٠.٦٥١	٣	٥.٥٧٩-	**
٩- العنف السيبراني، حيث يوفر الميتافيرس فرصًا لبناء هويات افتراضية لارتكاب الجرائم	٠.٨٦٣	٩	٠.٥٧٢	١١	٠.٥٩٧	١٠	٥.٧٨٥-	**
١٠- إنتهاك الخصوصية	٠.٩٤	١	٠.٦٣	٢	٠.٦٥٧	٢	٥.٧٩٧-	**
١١- إثارة الخوف والإثارة الخوف والاضطراب الانفعالي	٠.٩٠٦	٤	٠.٦٠٥	٦	٠.٦٣١	٥مكرر	٥.٧٧٦-	**
١٢- عمالة الأطفال والعبودية المستحدثة	٠.٧٩٥	١١	٠.٥٣٥	١٣	٠.٥٥٨	١٢	٥.٤٧٦-	**

الهدف الأول: سيناريوهات تهديد الجرائم المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة	خبراء ن= ٤١		المستخدمين ن= ٤٠٤		إجمالي الاستجابات ن= ٤٤٥		ز	الدلالة
	ق	ت	ق	ت	ق	ت		
١٣- استغلال المدمنين لأغراض الابتزاز أو الإكراه أو التحريض على ارتكاب جرائم	٠.٨٧٢	٧	٠.٥٩٢	٨	٠.٦١٧	٧	٥.٣٩٨-	**
جرائم الممتلكات								
١- السطو المادي عن طريق استغلال الواقع الافتراضي والواقع المعزز ومواد الاستشعار الذكية ومحاولة السطو على الممتلكات والأشياء الثمينة	٠.٨٧٢	٢	٠.٥٦٣	٢	٠.٥٩	٢	٦.١٦٩-	**
٢- هجمات البنية التحتية السيبرانية من قبل المجرمين والجهات الفاعلة المنظمة	٠.٨٩٧	١	٠.٥٨٦	١	٠.٦١٣	١	٦.٠٧٩-	**
٣- التعدي على ممتلكات الغير في الميتافيرس	٠.٨٤٦	٣	٠.٥٥٧	٣	٠.٥٨٢	٣	٥.٩٠٦-	**
جرائم أخرى								
١- إنتحال صفة شخصية	٠.٩٤	١ مكرر	٠.٦٢٥	٣	٠.٦٥٣	١	٥.٨٥٢-	**
٢- التأمرعن طريق استغلال العالم الافتراضي عبر التوائم الرقمية لارتكاب جرائم في العالم المادي	٠.٨٨	٤	٠.٥٨٩	٥	٠.٦١٥	٢	٥.٦٥٩-	**
٣- الإرهاب ن يكون الميتافيرس فرصًا جديدة للمنظمات الإرهابية للدعاية والتجنيد والإرهاب	٠.٨٨٩	٣ مكرر	٠.٥٩١	٨	٠.٦١٧	٥	٥.٧٣٧-	**
٤- حدوث الاستقطاب المجتمعي من الجهات المعادية	٠.٩١٥	٢	٠.٥٧٩	٢	٠.٦٠٩	٤	٦.٥٥٨-	**
٥- السلوك العنيف	٠.٨٧٢	٥	٠.٦٣	٤	٠.٦٥١	٧	٤.٧٢٥-	**
٦- نشر المعلومات الخاطئة والمضللة بهدف زعزعة استقرار المجتمعات	٠.٩٤	١ مكرر	٠.٦٢٣	٧	٠.٦٥١	٣مكرر	٥.٨٧٨-	**
٧- التاثير في العالم المادي عبر الأدوات المختلفة	٠.٨٨٩	٣ مكرر	٠.٦٤٤	١	٠.٦٦٦	٣مكرر	٤.٨٦٧-	**
٨- إنتحال صفة رجال إنفاذ القانون	٠.٨٤٦	٦	٠.٥٩	٦	٠.٦١٢	٦	٥.١٥٢-	**
٩- حرمان المستخدمين من الخدمات الأساسية كالصحة والتعليم	٠.٧٢٦	٧	٠.٥٣١	٩	٠.٥٤٨	٨	٤.٢٤٣-	**

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية ن=٤٤٥ مفردة
ق:- الوزن النسبي، ت:- الترتيب، مستوى الدلالة وتشير (-) على عدم وجود دلالة إحصائية و(**) على وجود فروق مرتفعة ذات دلالة إحصائية و(*) على وجود فروق ذات دلالة إحصائية، ز: دلالة الفروق بين كلا من الخبراء والمستخدمين من الشباب.

تكشف نتائج الجدول (٢١) عند مستوى دلالة (٠.٠٥) لجميع عبارات المقياس دلالات سيناريوهات الجرائم والمخاطر المرتبطة بالميتافيرس والتقنيات الناشئة وبذلك توجد بعض فروق دالة إحصائيًا بين استجابات أفراد عينة البحث للجدول السابق طبقًا للآتي:

- **(الجرائم المالية):**

يتضح من قيمة الوزن النسبي لسيناريوهات تهديد الجرائم المالية أن أعلى وزن نسبي في عينة الخبراء جاءت لصالح تهديد الجريمة رقم (٥) (التزييف من خلال إنشاء وبيع منتجات وسلع رقمية مزيفة وغير مشروعة) بنسبة (٩٤.٩%) من الدرجة العظمى لأنماط تهديد الجرائم المالية، بينما في عينة المستخدمين من الشباب لصالح الجريمة رقم (٧) (الخداع الإلكتروني) بنسبة (٦٣.٩%) من الدرجة العظمى لأنماط تهديد الجرائم المالية، في حين جاء تهديد الجريمة الأقل وزن نسبي في الخبراء هي رقم (٦) (التلاعب بالسوق) بنسبة (٨٦.٣%) من الدرجة العظمى لأنماط تهديد الجرائم المالية، بينما جاءت عند المستخدمين من الشباب جاءت لصالح الجريمة رقم (٤) (عمليات احتيال الاستثمار واختلاس أصول الأخرين) بنسبة (٦٠.١%) من الدرجة العظمى لأنماط تهديد الجرائم المالية.

- **(الجرائم الجنسية):**

يتضح من قيمة الوزن النسبي لسيناريوهات تهديد الجرائم الجنسية أن أعلى وزن نسبي في الخبراء؛ جاء لصالح تهديد الجريمة رقم (٥) (التشهير والابتزاز من خلال استغلال المعلومات الخاصة والصور الرمزية، وتسجيل التفاعلات والمحادثات وتهديدهم بنشر المعلومات الشخصية للمستخدمين من أجل ابتزازهم) بنسبة (٩٤.٩%) من الدرجة العظمى لأنماط الجرائم الجنسية، بينما جاءت عند المستخدمين من الشباب جاءت لصالح تهديد الجريمة رقم (٦) (التنمر الإلكتروني) بنسبة (٦٢.٩%) من الدرجة العظمى لأنماط تهديد الجرائم الجنسية، في حين تهديد الجريمة الأقل وزن نسبي في الخبراء لصالح تهديد الجريمة رقم (٤(التحرش وإساءة معاملة الأطفال عبر الصور الافتراضية والرمزية ومطاردته عبر منصات الميتافيرس المختلفة) بنسبة (٨٦.٣%) من الدرجة العظمى

لأنماط تهديد الجرائم الجنسية، بينما جاءت عند المستخدمين من الشباب لصالح تهديد الجريمة رقم (٢) (الاعتداء الجنسي على الأطفال عبر الصور الرمزية) بنسبة (٥٦.٧%) من الدرجة العظمى لأنماط تهديد الجرائم الجنسية.

- **(الجرائم ضد الأشخاص):**

يتضح من قيمة الوزن النسبي لسيناريوهات تهديد الجرائم ضد الأشخاص أن أعلى وزن نسبي في الخبراء جاء لصالح تهديد الجريمة رقم (١٠) (انتهاك الخصوصية) بنسبة (٩٤%) من الدرجة العظمى لأنماط تهديد الجرائم ضد الأشخاص بينما جاءت عند المستخدمين من الشباب لصالح تهديد الجريمة رقم (٧) (إنشاء حسابات مُزيفة) بنسبة (٦٧%) من الدرجة العظمى لأنماط تهديد الجرائم ضد الأشخاص، في حين جاء تهديد الجريمة الأقل وزن نسبي جاء لصالح تهديد الجريمة رقم (١٢) (عمالة الأطفال والعبودية المستحدثة)عند الخبراء بنسبة (٧٩.٥%) وعند المستخدمين من الشباب بنسبة (٥٣.٥%) من الدرجة العظمى لأنماط تهديد الجرائم ضد الأشخاص.

- **(الجرائم ضد الممتلكات):**

يتضح من قيمة الوزن النسبي لسيناريوهات تهديد الجرائم ضد الممتلكات أن أعلى وزن نسبي جاء لصالح تهديد الجريمة رقم (٢) (هجمات البنية التحتية السيبرانية من قبل المجرمين والجهات الفاعلة المنظمة) عند الخبراء بنسبة (٨٩.٧%) المستخدمين من الشباب بنسبة (٦١.٣%) من الدرجة العظمى لأنماط تهديد الجرائم ضد الممتلكات، في حين العبارة الأقل وزن نسبي لصالح تهديد الجريمة رقم (٣) (التعدي على ممتلكات الغير في الميتافيرس) بنسبة (٨٤.٦%) عند الخبراء، وعند المستخدمين من الشباب بنسبة (٥٥.٧%) من الدرجة العظمى لأنماط تهديد الجرائم ضد الممتلكات.

- **(الجرائم الأخرى):**

يتضح من قيمة الوزن النسبي لسيناريوهات تهديد الجرائم الأخرى، أن أعلى وزن نسبي في الخبراء جاء لصالح تهديد الجريمة رقم (١ و٦) بنسبة (٩٤%) (انتحال صفة شخصية، نشر المعلومات الخاطئة والمضللة بهدف زعزعة استقرار المجتمعات) من

الدرجة العظمى لأنماط تهديدات الجرائم الأخرى، بينما جاء عند المستخدمين من الشباب لصالح تهديد الجريمة رقم (٧) (التأثير في العالم المادي عبر الأدوات المختلفة) بنسبة (٦٤.٤%) من الدرجة العظمى لأنماط تهديدات الجرائم الأخرى، في حين جاء تهديد الجريمة الأقل وزن نسبي في الخبراء لصالح تهديد الجريمة رقم (٨) (انتحال صفة رجال القانون) بنسبة (٨٤.٦%) من الدرجة العظمى لأنماط تهديدات الجرائم الأخرى، بينما جاء عند المستخدمين من الشباب لصالح تهديد الجريمة رقم (٩) (حرمان المستخدمين من الخدمات الأساسية كالتعليم والصحة) بنسبة (٥٣.١%) من الدرجة العظمى لأنماط تهديدات الجرائم الأخرى.

- **التعقيب على النتائج في ضوء الدراسات السابقة والتوجه النظري**:

تتفق النتائج السابقة مع ما كشفت عنه نتائج أحدى التقارير أن الميتافيرس والعالم الافتراضي يشمل مجموعة واسعة من الأنشطة بدءًا من التواصل الاجتماعي وحتى التجارة الافتراضية. في نفس البيئات يمكن أن تحدث سلوكيات غير قانونية وضارة بشكل عام مثل الجرائم التي يتم تسهيلها عبر الإنترنت بما في ذلك القرصنة وغسل الأصول الافتراضية والاحتيال والمطاردة والمراقبة، كما يشمل سوء السلوك الافتراضي في الميتافيرس الإجراءات التي تنتهك القواعد والمعايير الأخلاقية والأطر القانونية والتي تتراوح من القواعد البسيطة وانتهاكات وشروط الخدمة إلى الجرائم الخطيرة، يمكن أن تؤدي الطبيعة المجهولة للتفاعلات عبر الإنترنت في كثير من الأحيان إلى سلوك عدواني وتنمر عبر الإنترنت واضطراب نفسي، مما يعرض سلامة وشمولية الفضاء الافتراضي للخطر، حيث تنتشر السرقة والاحتيال والقرصنة الافتراضية مما يؤدي إلى خسائر مالية وتقويض الثقة، إلى جانب العنف الافتراضي والهجمات الافتراضية إلى يمكن أن تضر بالأفراد ورفاهية المجتمع.(**Council of Europe and IEEE SA,2024:18**)

كما كشفت نتائج إحدى الدراسات أن التفاعل عبر الإنترنت يزيد من خطر وقوع المستخدمين ضحية للجرائم الإلكترونية، وتحديدًا خمسة أنواع رئيسة: الهندسة الاجتماعية، الخداع، التحرش عبر الإنترنت، الجرائم المتعلقة بالهوية، القرصنة والحرمان من الخدمات والمعلومات. (**Stavola,J&Choi,K,2023: 6**)

كما بينت نتائج أحدى الدراسات أن هناك خمس مشكلات أمنية في الميتافيرس تتمثل في: عنصر Nfts حيث يتم استخدامه في تنظيم ملكية وأصول المنتجات الرقمية، وبالتالي سيكونوا عرضة للتصيد الاحتيالي والفدية والتهديدات الأخرى، ومن المرجح أن تزدهر الأنشطة غير القانونية أو الإجرامية في الميتافيرس لأنه سيكون من الصعب تتبعها ومراقبتها، حيث ستواجه LEA صعوبة في التسلسل إلى هذه المساحات، كما سيتم استخدام العقارات باهظة الثمن والرموز غير القابل للاستبدال لغسل الأموال.

(Huq[et.al,]2022:21).

كما تتفق النتائج مع نتائج دراسة **(Smailia, & Raymond, 2022:194)** حيث أوضحت أن الميتافيرس يجلب مخاطر تتعلق بالتشريعات والملكية والسيطرة والاحتيال وتهديدات الخصوصية والأخلاق والمسائلة وقضايا الأمن الكامنة في أي معاملة في بيئة ميتافيرس، وينبغي أن نؤخذ في الاعتبار انتهاك الأخلاق. كما أشارت الدراسة إلى أن هناك خمسة أنواع من المخاطر المتعلقة بالميتافيرس والتي يمكن أن تؤثر على الرفاهية الجسدية والصحة والسلامة وعلم النفس والأخلاق وخصوصية البيانات. كما بينت الدراسة أن مخاطر الميتافيرس تؤثر على الأفراد والمنظمات والمجتمعات، فمن المخاطر المتعلقة بالأفراد تتمثل في خصوصية البيانات المالية والجسدية والنفسية والاحتيال وخصوصية بيانات المسمعة ولمعلومات الخاطئة والمعلومات المضللة، كما أن على المؤسسات تأخذ في الاعتبار العديد من المخاطر مثل المتعلق بالمعاملات الفكرية والملكية والسمعة والخصوصية، وما إلى ذلك. كما يمكن أن يجلب Metaverse العديد من مخاطر الاحتيال الأخرى مثل التلاعب بالسوق والانتهاكات والهجمات السيبرانية وانتهاكات الخصوصية وغسل الأموال والتجسس على الشركات وسرقة الهوية. يتكون الميتافيرس من العديد من العناصر منها blockchain والعملات المشفرة، وNfts والتي يشكلا جزءًا مهمًا من الميتافيرس، حيث وجد المحتالون العديد من الأغراض، ونظرًا لعدم وجود تدابير تنظيمية يتمتع المحتالون بحرية الاحتيال على الشركات والأفراد، حيث يستخدم المحتالون تقنية البلوكتشين في عمليات احتيال مختلفة مثل سرقة الهوية وغسل الأموال، كما يمكن للمستخدمين في الميتافيرس شراء NFT لاستخدامه على منصات مختلفة، لقد كشف عن

العديد من عمليات الاحتيال التي تشمل التصيد الاحتيالي للوصول إلى بيانات حساب NFT المختلفة للضحايا لتنفيذ هجمات على الحساب وغسل الأموال باستخدام عدة حسابات والتلاعب وهجمات السمعة من خلال حسابات مُزيفة (روبوتات) تهدف إلى الإضرار بسمعة المنظمة بالإضافة إلى غياب اللوائح المنظمة بـ NFT والعملات المشفرة، فالمشكلة تنشأ من غياب الرقابة؛ بمعنى عدم وجود قواعد لحماية المستخدمين في العقود التجارية والملكية والمعاملات وما إلى ذلك.

كما تتفق النتائج السابقة ما أشارت إليه نتائج دراسة **(Bale,[et.al],2022:9)** أن الميتافيرس أرض خصبة للإساءة والتحرش، فقد أرتفع معدل الجريمة في مجال الإنترنت إلى حد إنه تم الشعور بالحاجة إلى قسم جديد تمامًا للجريمة، وأي تقنية تهدف إلى جمع الناس معًا لابد أن تتعرض للإساءة والمضايقة ويمكن أن يكون الميتافيرس مشروعًا جديدًا لمجرمي الإنترنت لمضايقة الأفراد وإساءة معاملتهم، ومالم يتم اتخاذ تدابير صارمة للحد من الجرائم الإلكترونية يمكن أن يكون الميتافيرس قاتل للأفراد وقد يتسبب في حالات ضعف الصحة العقلية لدى الأشخاص أو يؤدي إلى تفاقمها.

ووفقًا لنظرية النشاط الروتيني فإن الجريمة من المرجح أن تحدث عندما يواجه الجاني هدفًا مناسبًا في ظل غياب الوصاية القادرة ولا يقتصر الوصاية على الشرطة بل يشمل أي شخص يمكنه التصرف لردع الجناة أو حماية هدف محتمل، يمكن لأولئك الذين لديهم السلطة القانونية لممارسة السيطرة على مكان ما أن يلعبوا دورًا مهمًا من خلال تصميم المساحات لجعله أكثر أمانًا، ومن خلال توفير أفراد آخرين على توفير الوصاية اللازمة، حيث ستوثر التغيرات في أي من الظروف البيئة الموصوفة على احتمالية وقوع الجريمة، كما ستؤثر التغيرات في استراتيجيات إدارة المكان.

حيث أن النظريات والاستراتيجيات والتنظيم والتنفيذ أقل تطورًا مما هي عليه في الفضاءات المادية، يشمل ذلك أن الفضاءات على الإنترنت ليست محدودة بالولاية القضائية. حيث أن وقوع الجريمة في مكان معين يعتمد على تصورات الجاني للمخاطرة والجهد والمكافأة المرتبطة بالجريمة، وقد يعطل الكون الموضوعي كل هذه الأمور الثلاثة. **(Gomez–Quintero, [et.al], 2024:4)**

- **نتائج الهدف الثاني: رصد سيناريوهات تهديدات المخاطر التي قد يتعرض لها الأطفال عبر الميتافيرس والتقنيات الناشئة:**

(أ) نتائج المقارنة بين استجابات عينة كلًا من (الخبراء – المستخدمين) حول سيناريوهات تهديدات المخاطر التي قد يتعرض لها الأطفال عبر الميتافيرس والتقنيات الناشئة:

جدول (٢٢) يوضح المقارنة بين (الخبراء – المستخدمين) وترتيب أكثر المخاطر تأثيرًا

الهدف الثاني: تهديد ات المخاطر المرتبطة بالأطفال عبر الميتافيرس والتقنيات الناشئة:	الخبراء			المستخدمين		
	المتوسط	الانحراف المعياري	الترتيب	المتوسط	الانحراف المعياري	الترتيب
١- مخاطر المحتوي وتعني المخاطر التي يتعرض فيها الطفل لمحتوي غير لائق أو غير قانوني	٢.٨٥	٠.٤٩	١ مكرر	٢.٠٣	٠.٩٧	٢
٢- مخاطر الاتصال والتي تحدث عندما يتعامل الطفل مع أطفال أخرين ويرغبون في إشراكه في سلوكيات خطيرة	٢.٧٧	٠.٥٨	٣	١.٩٤	٠.٩٤	٥ مكرر
٣- مخاطر السلوك عندما يساهم السلوك في محتوى أو اتصال خطير على الطفل	٢.٧٩	٠.٥٧	٢ مكرر	١.٩٤	٠.٩٤	٥ مكرر
٤- المخاطر المادية والتي تتمثل في التأثيرات المحتملة الميتافيرس على الصحة الجسدية والتغيرات الفسيولوجية (مثل الصداع، الغثيان والدوخة نتيجة استخدام سماعات الواقع الافتراضي على السمع والتعرض للضوء الأزرق على النظام البصري) .	٢.٦٧	٠.٥٨	٤	١.٩٨	٠.٩١	٤
٥- مخاطر السلامة، والتي تتمثل في التأثيرات المحتملة لأجهزة الواقع الافتراضي على حدوث خطر الإصابات الذاتية أثناء الاستخدام مثل الانزلاق أو التعثر أو السقوط وضعف الأداء الحركي)	٢.٦٢	٠.٥٩	٥	١.٩٢	٠.٨٩	٦
٦- المخاطر البيولوجية	٢.٥١	٠.٦٨	٦	١.٨٢	٠.٨٥	٧
٧- المخاطر النفسية (الإحباط، القلق، الاكتئاب)	٢.٨٥	٠.٤٩	١ مكرر	٢.٠٧	٠.٩٢	١
٨- المخاطر الاجتماعية التنمر عبر الإنترنت الذي يتفاقم بسبب التأثيرات اللمسية)	٢.٧٩	٠.٤٧	٢ مكرر	٢.٠١	٠.٩٦	٣

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية

ن=٤٤٥ مفردة أكبر قيمة للمتوسط هي ٣ وأقل قيمة هي ١

أظهرت نتائج الجدول رقم (٢٢) وجهة نظر الخبراء أن تهديد المخاطر رقم (١ و٧) وهما (مخاطر المحتوى وتعني المخاطر التي يتعرض فيها الطفل لمحتوى غير لائق أو غير قانوني، والمخاطر النفسية (الإحباط، القلق، الاكتئاب) أقوى تأثيرًا في المخاطر التي من المحتمل أن يتعرض لها الأطفال طبقا لإجماع أراء الخبراء بمتوسط (٢.٨٥)، بينما من وجهة نظر المستخدمين أن تهديد المخاطر رقم (٧) وهي المخاطر النفسية (الإحباط، القلق، الاكتئاب) أقوى تأثيرًا طبقًا لإجماع أراء المستخدمين بمتوسط (٢.٠٧).

جدول رقم (٢٣) يوضح المقارنة بين (الخبراء – المستخدمين)

الهدف الثاني تهديدات المخاطر الكامنة التي من المحتمل أن يتعرض لها الأطفال عبر الميتافيرس والتقنيات الناشئة ككل	الخبراء			المستخدمين			ت
	المتوسط	الانحراف المعياري	المدى	المتوسط	الانحراف المعياري	المدى	
	٢.٧٣	٠.٣٩	٣-١	١.٩٦	٠.٨١	٣-١	٥.٨٧٠

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية
ن= ٤٤٥ مفردة

أظهرت نتائج الجدول السابق (٢٣) نتائج المقارنة بين استجابات الخبراء واللمستخدمين من الشباب حول تهديدات المخاطر الكامنة التي من المحتمل أن يتعرض لها الأطفال عبر الميتافيرس والتقنيات الناشئة، وجاءت نتائج الخبراء بمتوسط حسابي نسبته (٢.٧٣) وإنحراف معياري بلغ (٠.٣٩)، بينما جاء المتوسط الحسابي عند المستخدمين للميتافيرس بنسبة (١.٩٦) وإنحراف معياري (٠.٨١) ، وبلغت قيمة ت (٥.٨٧٠).

(ب) نتائج الفروق بين الاوزان النسبية (الخبراء– المستخدمين) حول سيناريوهات تهديدات المخاطر التي قد يتعرض لها الأطفال عبر الميتافيرس والتقنيات الناشئة:

جدول (٢٤) الفروق بين الاوزان النسبية (الخبراء – المستخدمين)

الهدف الثاني: المخاطر الكامنة التي من المحتمل أن يتعرض لها الأطفال عبر الميتافيرس والتقنيات الناشئة	الخبراء ن= ٤١		المستخدمين ن= ٤٠٤		إجمالي الاستجابات ن= ٤٤٥		ز	الدلالة
	ق	ت	ق	ت	ق	ت		
١. مخاطر المحتوى وتعني المخاطر التي يتعرض فيها الطفل لمحتوى غير لائق أو غير قانوني	٠.٩٤٩	١	٠.٦٧٦	٢	٠.٧	٢	٥.٠٧٧-	**
٢. مخاطر الاتصال والتي تحدث عندما يتعامل الطفل مع أطفال أخرين ويرغبون في إشراكه في سلوكيات خطيرة	٠.٩٢٣	٢	٠.٦٤٧	٥	٠.٦٧١	٥	٥.٢٣٧-	**
٣. مخاطر السلوك عندما يساهم السلوك في محتوى أو اتصال خطير على الطفل	٠.٩٣٢	٤	٠.٦٤٥	٦	٠.٦٧	٦	٥.٤٥٣-	**
٤. المخاطر المادية والتي تتمثل في التأثيرات المحتملة الميتافيرس على الصحة الجسدية والتغيرات الفسيولوجية (مثل الصداع، الغثيان والدوخة نتيجة استخدام سماعات الواقع الافتراضي على السمع والتعرض للضوء الأزرق على النظام البصري)	٠.٨٨٩	٥	٠.٦٥٨	٤	٠.٦٧٩	٤	٤.٥٢١-	**
٥. مخاطر السلامة، والتي تتمثل في التأثيرات المحتملة لأجهزة الواقع الافتراضي على حدوث خطر الإصابات الذاتية أثناء الاستخدام مثل الانزلاق أو التعثر أو السقوط وضعف الأداء الحركي)	٠.٨٧٢	٦	٠.٦٤	٧	٠.٦٦١	٧	٤.٦٦٤-	**
٦. المخاطر البيولوجية	٠.٨٣٨	٣	٠.٦٠٦	٨	٠.٦٢٧	٨	٤.٨٣٤-	**
٧. المخاطر النفسية (الإحباط، القلق، الاكتئاب)	٠.٩٤٩	١ مكرر	٠.٦٩١	١	٠.٧١٤	١	٥.٠٥٩-	**
٨. المخاطر الاجتماعية (التنمر عبر الإنترنت الذي يتفاقم بسبب التأثيرات اللمسية)	٠.٩٣٢	٢ مكرر	٠.٦٧٢	٣	٠.٦٩٥	٣	٤.٨٥٣-	**

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات البحث الميداني

ن=٤٤٥ مفردة

ق:- الوزن النسبي، ت:- الترتيب مستوى الدلالة، تشير (-) على عدم وجود دلالة إحصائية و(**) على وجود فروق مرتفعة ذات دلالة إحصائية و(*) على وجود فروق ذات دلالة إحصائية، ز: دلالة الفروق بين كلًا من الخبراء والمستخدمين من الشباب.

يتضح من الجدول (٢٤) عند مستوى دلالة (٠.٠٥) لجميع عبارات المقياس، وبذلك توجد بعض فروق دالة إحصائيًا بين استجابات أفراد عينة البحث للجدول السابق طبقا للآتي:

تبين من قيمة الوزن النسبي لسيناريوهات تهديد المخاطر على الأطفال أن أعلى وزن نسبي في الخبراء جاء لصالح المخاطر رقم (١ و٧) "مخاطر المحتوى وهي المخاطر التي يتعرض فيها الطفل لمحتوى غير لائق أو غير قانوني، المخاطر النفسية (الإحباط، القلق، الاكتئاب) بنسبة (٩٤.٩%) من الدرجة العظمى للمخاطر، بينما جاءت عند المستخدمين من الشباب لصالح المخاطر رقم (٧) "المخاطر النفسية (الإحباط، القلق، الاكتئاب) بنسبة (٦٩.١%) من الدرجة العظمى للمخاطر، في حين جاءت تهديد المخاطر الأقل وزن نسبي في الخبراء لصالح تهديد المخاطر رقم (٥) "مخاطر السلامة، والتي تتمثل في التأثيرات المحتملة لأجهزة الواقع الافتراضي على حدوث خطر الإصابات الذاتية أثناء الاستخدام مثل الانزلاق أو التعثر أو السقوط وضعف الأداء الحركي" بنسبة (٨٧.٢%) من الدرجة العظمى لتهديد المخاطر، بينما جاءت عند المستخدمين من الشباب لصالح تهديد المخاطر رقم (٦) "المخاطر البيولوجية" بنسبة (٦٠%) من الدرجة العظمى لتهديد المخاطر ضد الأطفال.

- **التعقيب على النتائج في ضوء الدراسات السابقة:**

تتماشى النتائج مع ما أشارت إليه إحدى التقارير أن الانتشار المتزايد للميتافيرس يثير مخاوف بشان تأثيره على الصحة البدنية للأطفال، يمكن أن يؤثر التفاعل المفرط مع البيئات الافتراضية مثل الميتافيرس سلبًا على النمو البدني للأطفال، مما يؤدي إلى تلف البصر والأرق ودوار الحركة ومشاكل صحية مرتبطة بالسلوك الخامل، كما يؤدي إلى العزلة والتفاعلات المحدودة وصعوبة تطوير مهارات التعامل مع الأخرين والتي قد تستمر حتى مرحلة البلوغ، بالإضافة إلى مخاطر الصحة العقلية والإدمان وزيادة خطر الانتحار والاكتئاب والقلق. **(Council of Europe and EEEI,2024:19)**

كما تتفق النتائج مع ما أشارت إليه أحد التقارير إلى أن هناك مخاوف من أن البيئات الافتراضية قد تؤدي إلى التحرش الجنسي والإساءة، حيث كشف باحثون مركز مكافحة الكراهية الرقمية الذين قضوا ١٢ ساعة في إحدى المنصات الاجتماعية الشهيرة للواقع الافتراضي، ووجدوا أن المستخدمين بما في ذلك الأطفال يتعرضون لسلوك مسيء، وشمل ذلك تعرض الُقصر لمحتوى جنسي مصور؛ التنمر والتحرش الجنسي وإساءة معاملة المستخدمين الأخرين، بما في ذلك القاصرين، ويتم إعداد القُصر لتكرار الإهانات العنصرية والمتطرفة، والسعي نحو تضخيم مثل تلك الحوادث. فالتقنيات الغامرة يمكن أن نزيد من تأثير التفاعلات السلبية مثل (التسلط عبر الإنترنت، استمالة الأطفال للإعتداء الجنسي عبر الإنترنت، والإساءة القائمة على الصور) وتؤدي إلى ارتفاع في الاعتداءات والإساءات عبر الإنترنت. فقد قالت النساء اللاتي تعرضن للتحرش الجنسي الافتراضي إنهن اعتقدن وشعرن أن الاعتداء حقيقي. ووفقًا لتقرير صادر عن اليونيسف أكتشف خبراء الأمن السيبراني ارتفاعًا في الهجمات السيبرانية المتطورة التي تتلاعب بالأطفال من أجل سرقة بيانات اعتماد هويتهم وملفات تعريف القياسات الحيوية الخاصة بهم، مع ما يترتب عليه من آثار أمنية مدى الحياة، ويشير التقرير إلى أن مثل هذه التهديدات أصبحت منشرة على منصات مثل (Facebook, Snapchat, Tictok, Margatsni) ولكنها سوف تتضخم في المستقبل. بالإضافة إلى أن التقنيات الغامرة المرتبطة بالميتافيرس والواقع الممتد تشكل مخاطر على النمو المعرفي والاجتماعي للأطفال، وفي دراسة أجريت حول كيفية استجابة البالغين والأطفال لتجارب الواقع الافتراضي، تمكن البالغون من استخدام قشرة الفص الجبهي لتنظيم ما كانت أدمغتهم تعالجه أثناء محاكاة وهمية، ولم يفعل الأطفال المشاركون في الدراسة (متوسط أعمارهم ثماني سنوات) بنفس القدر ولم يتمكنوا من التمييز بين العالم الافتراضي والعالم الحقيقي. **(Unicef,2023:18)**

كما أشارت الأدبيات السابقة **(Huq[et.al,] 2022:21)** إلى أنه في الميتافيرس سوف تبحث الجهات الفاعلة الإجرامية عن الفئات الضعيفة من الأشخاص الذين لديهم حساسة تجاه موضوعات معينة ومن ثم إسقاط الروايات المستهدفة للتأثير عليهم.

وتتفق تلك النتائج مع نتائج إحدى التقارير الأخرى التي بينت أن هناك مشكلة من قبل الجهات الفاعلة الخبيثة التي تتطلع إلى الاستفادة من التكنولوجيا الجديدة في CSAM، حيث هناك حالات موثقة لأطفال تعرضوا للإيذاء مباشرة في الميتافيرس عبر منصات ميتا هورايزون وولدزميتافيرس، حيث تجتذب الأطفال الذين تقل أعمارهم عن ١٨ عامًا، حيث لاحظت كوريا الجنوبية أن هناك بالفعل عددًا من الأفعال الإجرامية القائمة على الميتافيرس والمتعلقة بالأطفال؛ فقد كشفت الشرطة الوطنية في أبريل ٢٠٢١ أن شخصًا بالغًا حث قاصرًا على إرسال صور فاضحة مقابل عناصر داخل اللعبة في الميتافيرس، حيث تم استخدام الصور للإباحية الافتراضية والممارسات غير الأخلاقية، وقالت الشرطة أن المحتوى استغلالي، وهناك حالة أخري لفتاة تبلغ من العمر ١٤ عامًا تم إجبارها على خلع ملابس الصور الرمزية الخاصة بها في الميتافيرس، ثم طُلب منها أن تؤدي الصور الرمزية الخاصة بها أفعالًا جنسية.

(Elliptic Metavrse Report, 2022: 42).

كما تتفق النتائج السابقة مع العديد من نتائج الدراسات السابقة ومنها ما أشارت إليه دراسة **(العلوي & التوزاني،٢٠٢٣ :٢٦٦)** أن الأطفال هي الفئة العمرية الأكثر تأثرًا من هذه التقنيات الحديثة وذلك راجع لكونها الأكثر استعمالا لتطبيقات وتقنيات العوالم الافتراضية الميتافيرس، ذلك أنهم فئة سهلة المنال ويسيرة الجذب لمختلف الألعاب والتطبيقات التي تتوفر عليها عوالم الميتافيرس، مما يجعلهم أكثر عرضة للمخاطر والأضرار الناتجة عن سوء استعمال هذه التطبيقات أو نتيجة الإفراط فيها. ولعل من بين أضرار العالم الافتراضي المحتملة على الأطفال أنها ستكون السبب لا محالة في عزلة الطفل وجعلة انطوائيًا، بالإضافة إلى أنها ستضع طفلًا ومراهقًا أنانيًا لا يفكر سوى في إشباع حاجاته مع طفل صغير غير مميز في عالم افتراضي مشترك، بالإضافة إلى إنها قد تكون السبب والباعث من وراء تعرض الأطفال لظاهرة الانتحار وذلك جراء تعرض شريحة الأطفال والمراهقين لمضامين الثورة المعلوماتية السلبية.

كما أظهرت نتائج إحدى التقارير الدولية أن آثار الاستخدام المتزايد للواقع الافتراضي من قبل الأطفال والمراهقين مخاوف بشأن تعرضهم لمحتوى غير لائق أو

مضايقة أو تسلط بالإضافة إلى المخاطر المحتملة للتفاعل مع الجناة؛ حيث تعد الاستمالة والتحرش الجنسي من المخاطر التي يواجهها الأطفال في البيئات الافتراضية، والتي لها أثار ضارة على كرامتهم وحالتهم النفسية ورفاههم.

(Council of Europe and IEEE SA, 2024:18).

- **نتائج الهدف الثالث: رصد العوامل الدافعة إلى حدوث الجرائم عبر الميتافيرس والتقنيات الناشئة:**

(أ) نتائج المقارنات بين استجابات عينة كلًا من (الخبراء – المستخدمين) حول العوامل الدافعة إلى ارتكاب الجرائم عبر الميتافيرس والتقنيات الناشئة:

جدول (٢٥) يوضح المقارنة بين (الخبراء – المستخدمين) وترتيب أكثر العوامل تأثيرًا

الهدف الثالث: رصد العوامل الدافعة إلى حدوث الجرائم عبر الميتافيرس والتقنيات الناشئة	الخبراء			المستخدمين		
	المتوسط	الانحراف المعياري	الترتيب	المتوسط	الانحراف المعياري	الترتيب
العوامل العالمية						
١- التحول للمجتمع الرقمي	٢.٨٥	٠.٤٣	٣	٢.٣٢	٠.٧٩	٣
٢- إنكشاف البنية الإلكترونية التحتية للمجتمعات	٢.٧٧	٠.٤٨	٤	٢.٢٠	٠.٨٠	٤
٣- تزايد الوصولية للإنترنت والترابط العالمي	٢.٩٢	٠.٣٥	٢	٢.٥٠	٠.٧٣	٢
٤- التطور التكنولوجي السريع	٢.٩٧	٠.١٦	١	٢.٦١	٠.٦٨	١
٥- العوامل المجتمعية						
٦- ضعف الرقابة التقنية	٢.٧٢	٠.٦٥	٢ مكرر	٢.١٢	٠.٩٠	٣
٧- السرعة في تنفيذ الجرائم	٢.٨٢	٠.٥١	١ مكرر	٢.٠٣	٠.٩١	٥ مكرر
٨- إنخفاض تكلفة الإنترنت	٢.٤٤	٠.٨٥	٥	٢.١٣	٠.٨٩	٢
٩- إرتفاع معدلات البطالة	٢.٦٧	٠.٦٢	٤	٢.٠٩	٠.٩٤	٤
١٠- غياب التشريعات وبطء تعديل التشريعات الحالية تزامنًا مع التطور التكنولوجي	٢.٦٩	٠.٦١	٣	١.٩٩	٠.٩٠	٦
١١- الضغوط المجتمعية	٢.٨٢	٠.٥١	١ مكرر	٢.١٥	٠.٨٧	١
١٢- ضعف تطبيق قوانين مكافحة الجرائم السيبرانية	٢.٧٢	٠.٦٠	٢ مكرر	٢.٠٣	٠.٩٢	٥ مكرر
العوامل الفردية						
١. سهولة الوصول للضحايا والمستهدفين	٢.٧٩	٠.٥٢	٣	٢.١٤	٠.٨٨	٣
٢. الرغبة في الكسب غير المشروع	٢.٨٢	٠.٥١	٢	٢.٠٦	٠.٩٣	٦
٣. صعوبة متابعة الجناة والقبض عليهم وتقديمهم للعدالة	٢.٦٢	٠.٦٧	٧	١.٩٥	٠.٩٠	٨
٤. الضغوط الشخصية	٢.٧٢	٠.٥٦	٦ مكرر	٢.١٢	٠.٨٧	٥
٥. المشكلات النفسية	٢.٧٢	٠.٥٦	٦ مكرر	٢.١٣	٠.٩١	٤
٦. الربح والثراء السريع	٢.٩٢	٠.٢٧	١	٢.٤٨	٠.٧٣	٢

الهدف الثالث: رصد العوامل الدافعة إلى حدوث الجرائم عبر الميتافيرس والتقنيات الناشئة	الخبراء			المستخدمين		
	المتوسط	الانحراف المعياري	الترتيب	المتوسط	الانحراف المعياري	الترتيب
٧. المتعة والتحدي وإثبات الذات	٢.٧٧	٠.٤٨	٤	٢.٥٢	٠.٧٢	١
٨. سهولة ارتكاب الجريمة وضعف الوصول للجناة	٢.٧٤	٠.٥٩	٥	١.٩٧	٠.٩٢	٧

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية

ن=٤٤٣ مفردة أكبر قيمة للمتوسط هي ٣ و أقل قيمة هي ١

من قراءة الجدول السابق يمكن الإشارة إلى ما يلي:

- **العوامل العالمية:** أظهرت وجهة نظر الخبراء أن العامل رقم (٤) وهو (التطور التكنولوجي السريع) أقوى تأثيرًا **في** العوامل العالمية طبقًا لإجماع أراء الخبراء بمتوسط (٢.٩٧) وكان هذا أيضًا بإجماع أراء المستخدمين من الشباب على نفس العامل بمتوسط (٢.٦١).

- **العوامل المجتمعية:** بينت وجهة نظر الخبراء أن العوامل رقم (٢ و٦) وهما (السرعة في تنفيذ الجرائم، الضغوط المجتمعية) أقوى تأثيرًا في **العوامل** المجتمعية طبقًا لإجماع أراء الخبراء بمتوسط (٢.٨٢)، بينما من وجهة نظر المستخدمين أن العامل رقم (٦) وهو (الضغوط المجتمعية) أقوى تأثيرًا في العوامل المجتمعية طبقًا لإجماع أراء المستخدمين بمتوسط (٢.١٥).

- **العوامل الفردية:** كشفت وجهة نظر الخبراء أن العامل رقم (٦) وهو (الربح والثراء السريع) أقوى تأثيرًا في العوامل الفردية طبقًا لإجماع أراء الخبراء بمتوسط (٢.٩٢) بينما من وجهة نظر المستخدمين أن العامل رقم (٧) وهو (المتعة والتحدي وإثبات الذات) أقوى تأثيرًا في العوامل الفردية طبقًا لإجماع أراء المستخدمين بمتوسط (٢.٥٢).

جدول (٢٦) يوضح المقارنة بين (الخبراء – المستخدمين) وترتيب أكثر العوامل تأثيرًا

الهدف الثالث: رصد العوامل الدافعة إلى حدوث الجرائم عبر الميتافيرس والتقنيات الناشئة:	الخبراء				المستخدمين				ت
	المتوسط	الانحراف المعياري	المدى	الترتيب	المتوسط	الانحراف المعياري	المدى	الترتيب	
العوامل العالمية	٢.٨٨	٠.٢٠	٣-٢.٣	١	٢.٤١	٠.٥٥	٣-١	١	٥.٢٧٢
العوامل المجتمعية	٢.٧٠	٠.٣٩	٣-١.٣	٣	٢.٠٨	٠.٦٢	٣-١	٣	٦.١٢٦
العوامل الفردية	٢.٧٦	٠.٣٧	٣-١.٣	٢	٢.١٧	٠.٦٢	٣-١	٢	٥.٨٥٥
البعد الثالث ككل	٢.٧٦	٠.٢٨	٣-١.٦		٢.١٩	٠.٥٢	٣-١		٦.٧٧٧

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية

أظهرت نتائج الجدول (٢٦) إنه بإجماع أراء الخبراء والمستخدمين أن العوامل العالمية هي أقوى العوامل الدافعة الى حدوث الجرائم عبر الميتافيرس والتقنيات الناشئة بمتوسط (٢.٨٨) للخبراء و بمتوسط (٢.٤١) للمستخدمين.

(ب) نتائج الفروق بين الأوزان النسبية بين عينة كلًا من الخبراء والمستخدمين من الشباب حول العوامل الدافعة إلى ارتكاب الجرائم عبر الميتافيرس والتقنيات الناشئة:

جدول رقم (٢٧) الفروق بين الأوزان النسبية (الخبراء– المستخدمين)

الهدف الثالث: رصد العوامل الدافعة إلى حدوث الجرائم عبر الميتافيرس والتقنيات الناشئة	خبراء ن= ٤١		المستخدمين ن= ٤٠٤		إجمالي الاستجابات ن= ٤٤٥		ز	الدلالة
	ق	ت	ق	ت	ق	ت		
العوامل العالمية								
١. التحول للمجتمع الرقمي	٠.٩٤٩	٣	٠.٧٧٣	٣	٠.٧٨٩	٣	٤.١٥٣-	**
٢. إنكشاف البنية الإلكترونية التحتية للمجتمعات	٠.٩٢٣	٤	٠.٧٣٣	٤	٠.٧٥	٤	٤.٣٦٢-	**
٣. تزايد الوصولية للإنترنت والترابط العالمي	٠.٩٧٤	٢	٠.٨٣٣	٢	٠.٨٤٥	٢	٣.٨١٥-	**
٤. التطور التكنولوجي السريع	٠.٩٨٣	١	٠.٨٧	١	٠.٨٨	١	٣.٤٦٤-	**
العوامل المجتمعية								
١. ضعف الرقابة التقنية	٠.٩٠٦	٢مكرر	٠.٧٠٦	٣	٠.٧٢٤	٢	٤.٠٤٢-	**
٢. السرعة في تنفيذ الجرائم	٠.٩٤	١مكرر	٠.٦٧٧	٦	٠.٧	٥	٥.٢٢٧-	**
٣. إنخفاض تكلفة الإنترنت	٠.٨١٢	٥	٠.٧٠٩	٢	٠.٧١٨	٣	٢.١٣٤-	*
٤. إرتفاع معدلات البطالة	٠.٨٨٩	٤	٠.٦٩٦	٤	٠.٧١٣	٤	٣.٦٦٦-	**
٥. غياب التشريعات وبطء تعديل التشريعات الحالية تزامنًا مع التطور التكنولوجي.	٠.٨٩٧	٣	٠.٦٦٤	٧	٠.٦٨٥	٧	٤.٦٥٤-	**

الهدف الثالث: رصد العوامل الدافعة إلى حدوث الجرائم عبر الميتافيرس والتقنيات الناشئة	خبراء ن= ٤١		المستخدمين ن= ٤٠٤		إجمالي الاستجابات ن= ٤٤٥		ز	الدلالة
	ق	ت	ق	ت	ق	ت		
٦. الضغوط المجتمعية	٠.٩٤	١مكرر	٠.٧١٥	١	٠.٧٣٥	١	٤.٧٤٦-	**
٧. ضعف تطبيق قوانين مكافحة الجرائم السيبرانية	٠.٩٠٦	٢مكرر	٠.٦٧٨	٥	٠.٦٩٨	٦	٤.٤٧٦-	**
العوامل الفردية								
١. سهولة الوصول للضحايا والمستهدفين	٠.٩٣٢	٣	٠.٧١٥	٣	٠.٧٣٤	٣	٤.٥١٦-	**
٢. الرغبة في الكسب غير المشروع	٠.٩٤	٢	٠.٦٨٧	٦	٠.٧١	٦	٤.٩٠٧-	**
٣. صعوبة متابعة الجناة والقبض عليهم وتقديمهم للعدالة	٠.٨٧٢	٧	٠.٦٤٩	٨	٠.٦٦٨	٨	٤.٤٢٧-	**
٤. الضغوط الشخصية	٠.٩٠٦	٦مكرر	٠.٧٠٥	٥	٠.٧٢٣	٥	٤.١٦-	**
٥. المشكلات النفسية	٠.٩٠٦	٦مكرر	٠.٧١١	٤	٠.٧٢٨	٤	٣.٨٤١-	**
٦. الربح والثراء السريع	٠.٩٤٩	١	٠.٨٢٨	٢	٠.٨٤	٢	٣.٨١٤-	**
٧. المتعة والتحدي وإثبات الذات	٠.٩٢٣	٤	٠.٨٤١	١	٠.٨٤٨	١	١.٩٥٦-	-
٨. سهولة ارتكاب الجريمة وضعف الوصول للجناة	٠.٩١٥	٥	٠.٦٥٧	٧	٠.٦٧٩	٧	٥.٠٣٦-	**

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات البحث الميداني

ن=٤٤٥ مفردة، ق:- الوزن النسبي، ت:- الترتيب، مستوى الدلالة وتشير(-) على عدم وجود دلالة إحصائية و(**) على وجود فروق مرتفعة ذات دلالة إحصائية و(*) على وجود فروق ذات دلالة إحصائية، ز: دلالة الفروق بين كلًا من الخبراء والمستخدمين من الشباب.

يتضح من الجدول رقم (١٨) عند مستوى دلالة (٠.٠٥) لجميع عبارات المقياس وجود بعض الفروق دالة إحصائيا بين استجابات أفراد عينة البحث للجدول السابق طبقا للآتي:

- **(العوامل العالمية):**

يتضح من قيمة الوزن النسبي لعباراته أن أعلى وزن نسبي جاء لصالح العامل رقم (٤) (التطور التكنولوجي السريع) بنسبة (٩٨.٣%) عند الخبراء، وبنسبة (٨٧%) عند المستخدمين من الشباب، في حين جاء العامل الأقل وزن نسبي لصالح العامل رقم (٢) "انكشاف البنية الإلكترونية التحتية للمجتمعات) عند الخبراء بنسبة (٩٢.٣%) وعند المستخدمين من الشباب بنسبة (٧٣.٣%) من الدرجة العظمى للعوامل العالمية.

- **(العوامل المجتمعية):**

يتضح من قيمة الوزن النسبي لعباراته أن أعلى وزن نسبي في الخبراء لصالح

العوامل رقم (٢ و٦) وهما (السرعة في تنفيذ الجرائم، الضغوط المجتمعية) بنسبة (٩٤%) من الدرجة العظمى للعوامل المجتمعية، بينما جاء عند المستخدمين من الشباب لصالح العبارة رقم (٦) (الضغوط المجتمعية) بنسبة (٧١.٥%) من الدرجة العظمى للعوامل المجتمعية، في حين جاء العامل الأقل وزن نسبي في الخبراء لصالح العامل رقم (٣) (انخفاض تكلفة الإنترنت) بنسبة (٨١.٢%)، بينما جاء عند المستخدمين من الشباب لصالح العامل رقم (٥) (غياب التشريعات وبطء تعديل التشريعات تزامنًا مع التطور التكنولوجي) بنسبة (٦٦.٤%) من الدرجة العظمى للعوامل المجتمعية.

- **(العوامل الفردية):**

يتضح من قيمة الوزن النسبي لعباراته أن أعلى وزن نسبي في الخبراء لصالح العامل رقم (٦) (الربح والثراء والسريع) بنسبة (٩٤.٩%) من الدرجة العظمى للعوامل الفردية بينما جاء عند المستخدمين من الشباب لصالح العامل رقم (٧) (المتعة والتحدي وإثبات الذات) بنسبة (٨٤.١%) من الدرجة العظمى للعوامل الفردية، في حين جاء العامل الأقل وزن نسبي لصالح العامل رقم (٣) (صعوبة متابعة الجناة والقبض عليهم وتقديمهم للعدالة) بنسبة (٨٧.٢%) عند الخبراء، وبنسبة (٦٤.٩%) عند المستخدمين من الشباب.

التعقيب على النتائج في ضوء الدراسات السابقة والتوجه النظري للبحث:

في مجتمع اليوم الحديث نلاحظ أن الأفراد يقوموا باستخدام شبكة الإنترنت كعامل أساسي في الحياة، مما يعرضهم لخطر الوقوع ضحية للجرائم الإلكترونية، في حين أن شبكة الإنترنت يمكن أن يكون لها للعديد من الفوائد، إلا إنها تزيد من خطر الوقوع ضحية للجرائم الإلكترونية، ويشير كوهين وفيلسون إلى أن أسلوب حياة الفرد يجعل منه هدفًا مناسبًا بشكل أساسي، والذي يتضمن الأنشطة المهنية والترفيهية مثل التفاعل الاجتماعي من خلال المشاركة عبر الإنترنت. ومن منظور نظرية الأنشطة الروتينية السيبرانية فإن الجريمة من المرجح أن تحدث عندما تتلاقى ثلاثة عوامل هي الجاني المتحفز، والهدف المناسب، وغياب الحراسة، ومن ثم عدم وجود واحد من هذه العوامل كافي لمنع حدوث

ناجح لإكمال الاتصال المباشر، ويعطي اهتمام إلى التقارب في الزمان والمكان، وأن هذا التلاقي يمكن أن يؤدي إلى زيادة كبيرة في معدلات الجريمة من دون أي تغيير في الحالة الظرفية التي تحفز المجرمين. المبدأ الأساسي هو أن التغيرات الهيكلية في النشاط الروتيني تؤثر على التقارب في العناصر الثلاثة من الناحية النظرية وبالتالي تؤثر على معدل الجريمة فمن العناصر الرئيسة في العالم الافتراضي والمؤثرة في الجرائم الإلكترونية والسيبرانية حيث الجاني المتحفز (قد يكون) والمستهدف المناسب (استهداف المال أو الهوية) ولكن الحراسة القادرة (برامج الحماية). **(البداينة، ٢٠١٤ : ١٣)**، كما أن السلوك المحفوف بالمخاطر يزيد من خطر وقوع الفرد ضحية للجرائم الإلكترونية، حيث أن الافتقاد إلى تدابير الأمن السسيبراني، يجعل الأفراد عرضة لضحايا العنف عبر الإنترنت بين الأشخاص مثل المضايقات وانتحال الشخصية.**(Stavola,J&Choi,K,2023: 6)**

- **نتائج الهدف الرابع: رصد الأليات والحلول المقترحة لمواجهة الجرائم والمخاطر المرتبطة بالميتافيرس والتقنيات الناشئة:**

(١) نتائج المقارنات بين استجابات كلًا من الخبراء والمستخدمين من الشباب حول الحلول المقترحة لمواجهة الجرائم والمخاطر المرتبطة بالميتافيرس والتقنيات الناشئة:

جدول (٢٨) يوضح المقارنة بين (الخبراء – المستخدمين) وترتيب أكثر الحلول تأثيرًا

الهدف الرابع: رصد الحلول والأليات المقترحة لمواجهة مخاطر وجرائم الميتافيرس والتقنيات الناشئة:	خبراء			المستخدمين		
	المتوسط	الانحراف المعياري	الترتيب	المتوسط	الانحراف المعياري	الترتيب
الأليات والحلول القانونية						
١- إنشاء أليات رقابية لمراقبة الالتزام بالقواعد ومعاقبة أولئك الذين يخالفون القانون	٢.٩٥	٠.٢٢	٢	٢.٨٣	٠.٤٨	١
٢- سن التشريعات والقوانين اللازمة لمواجهة الجرائم عبر الميتافيرس.	٢.٩٧	٠.١٦	١ مكرر	٢.٧٦	٠.٥٣	٣
٣- تزويد الضباط والأجهزة المعنية بخطورة الجرائم الإلكترونية، وبالتقنيات الحديثة للتعرف على الجناة	٢.٩٧	٠.١٦	١ مكرر	٢.٨١	٠.٤٩	٢ مكرر
٤- إتخاذ التدابير الأمنية لضمان حماية المستخدمين من الهجمات الإلكترونية	٢.٩٧	٠.١٦	١ مكرر	٢.٨١	٠.٤٩	٢ مكرر

الهدف الرابع: رصد الحلول والأليات المقترحة لمواجهة مخاطر وجرائم الميتافيرس والتقنيات الناشئة:	خبراء			المستخدمين		
	المتوسط	الانحراف المعياري	الترتيب	المتوسط	الانحراف المعياري	الترتيب
أليات وحلول السياسات						
١- تعميق التعاون مع صناع السياسات وقادة المجتمع المدني والمنظمات من أجل صياغة وإنفاذ قوانين ولوائح سيبرانية قوية، وإشراك الدولة لأصحاب المصلحة في صنع السياسات	٢.٩٢	٠.٢٧	٣	٢.٧٢	٠.٥٨	٣
٢- إيجاد المبادئ التوجيهية والمجتمعية لضبط والتحكم في طرق التواصل بين الأفراد على الميتافيرس	٢.٩٠	٠.٣٨	٤	٢.٦٩	٠.٦٢	٤
٣- العمل على إتباع أساليب مصادقة الواقع الافتراضي، والمصادقة متعددة المستويات	٢.٨٧	٠.٤١	٥	٢.٦٠	٠.٦٧	٥
٤- ضرورة الفهم الشامل من قبل المعنيين بمكافحة هذه الجرائم المُستحدثة بمكونات وتهديدات المجتمع الافتراضي	٢.٩٧	٠.١٦	١	٢.٧٦	٠.٥٦	١
٥- أن تقوم الحكومات بسن وتنفيذ التشريعات التي تعكس دورها في تنظيم السلامة الرقمية المجتمعية	٢.٩٥	٠.٣٢	٢	٢.٧٥	٠.٥٦	٢
الأليات والحلول التقنية						
١- إيجاد الوسائل التكنولوجية التي تهدف إلى منع الهجمات السيبرانية والجرائم عبر الميتافيرس	٢.٩٥	٠.٢٢	٢.٠٠	٢.٨١	٠.٥١	١
٢- توفير أجهزة وتقنيات مراقبة الجريمة عبر الإنترنت لتحسين التنبؤ بالجرائم واكتشافها	٢.٩٧	٠.١٦	١ مكرر	٢.٧٥	٠.٥٥	٣
٣- إنشاء وتطوير أنظمة الكشف عن الجرائم والتهديدات وأليات الاستجابة لها في الفضاء السيبراني	٢.٩٧	٠.١٦	١ مكرر	٢.٧٦	٠.٥٥	٢
الحلول التوعوية						
١- نشر الوعي الفردي والمجتمعي بمخاطر الجرائم عبر الميتافيرس	٢.٩٢	٠.٣٥	٣ مكرر	٢.٨١	٠.٥٢	٢
٢- توفير الرعاية النفسية لأولئك الذين تضرروا من الجرائم عبر الميتافيرس	٢.٩٢	٠.٣٥	٣ مكرر	٢.٨٠	٠.٥١	٣
٣- دمج الجوانب التوعوية والأخلاقية والعملية للسلوك عبر الإنترنت ضمن المناهج التعليمية وفي القطاعات المدنية المختلفة في الدولة	٢.٩٥	٠.٣٢	٢	٢.٧٨	٠.٥٣	٤
٤- إرساء الأسس لبناء بيئة رقمية أكثر أمانًا وبناء مواطن رقمي أكثر مسئولية ووعي	٢.٩٧	٠.١٦	١ مكرر	٢.٨٢	٠.٥٠	١
٥- غرس القيم التي لا تشجع على الانخراط في أنشطة غير قانونية عبر الإنترنت	٢.٩٧	٠.١٦	١ مكرر	٢.٧٤	٠.٦٠	٥

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية

ن=٤٤٥ مفردة أكبر قيمة للمتوسط هي ٣ وأقل قيمة هي ١

من قراءة الجدول (٢٨) يمكن الإشارة إلى:

- **الحلول القانونية:** بينت وجهة نظر الخبراء أن الحلول رقم (٢ و٣ و٤) وهما (إيجاد المبادئ التوجيهية والمجتمعية لضبط والتحكم في طرق التواصل بين الأفراد على الميتافيرس، العمل على إتباع أساليب مصادقة الواقع الافتراضي، والمصادقة متعددة المستويات، ضرورة الفهم الشامل من قبل المعنيين بمكافحة هذه الجرائم المُستحدثة بمكونات وتهديدات المجتمع الافتراضي) هما أقوى تأثيرًا في الحلول القانونية طبقًا لإجماع أراء الخبراء بمتوسط (٢.٩٧) بينما من وجهة نظر المستخدمين جاء الحل رقم (١) وهو (تعميق التعاون مع صناع السياسات وقادة المجتمع المدني والمنظمات من أجل صياغة وإنفاذ قوانين ولوائح سيبرانية قوية، وإشراك الدولة لأصحاب المصلحة في صنع السياسات) من أقوى الحلول القانونية تأثيرًا طبقًا لإجماع أراء المستخدمين بمتوسط (٢.٨٣).

- **حلول السياسات:** كشفت وجهة نظر الخبراء أن الحل رقم (٤) وهو (ضرورة الفهم الشامل من قبل المعنيين بمكافحة هذه الجرائم المُستحدثة بمكونات وتهديدات المجتمع الافتراضي) هو أقوى تأثيرًا في حلول السياسات طبقًا لإجماع أراء الخبراء والمستخدمين بمتوسط (٢.٩٧) طبقًا لوجهة نظر الخبراء، ومتوسط (٢.٧٦) من وجهة نظر المستخدمين.

- **الحلول التقنية:** أظهرت وجهة نظر الخبراء أن الحلول رقم (٢ و٣) (توفير أجهزة وتقنيات مراقبة الجريمة عبر الإنترنت لتحسين التنبؤ بالجرائم واكتشافها، إنشاء وتطوير أنظمة الكشف عن الجرائم والتهديدات وأليات الاستجابة لها في الفضاء السيبراني) هما الأقوى تأثيرًا في الحلول التقنية طبقا لإجماع أراء الخبراء بمتوسط (٢.٩٧) بينما من وجهة نظر المستخدمين جاء العامل رقم (١) وهو (إيجاد الوسائل التكنولوجية التي تهدف إلى منع الهجمات السيبرانية والجرائم عبر الميتافيرس) هو الأقوى تأثيرًا في الحلول التقنية طبقًا لإجماع أراء المستخدمين بمتوسط (٢.٨٣).

- **الحلول التوعوية:** كشفت وجهة نظر الخبراء أن الحلول رقم (٤ و٥) وهما (إرساء الأسس لبناء بيئة رقمية أكثر أمانًا وبناء مواطن رقمي أكثر مسئولية ووعي، غرس القيم التي لا تشجع على الانخراط في أنشطة غير قانونية عبر الإنترنت) هما الأقوى تأثيرًا في الحلول التوعوية طبقًا لإجماع أراء الخبراء بمتوسط (٢.٩٧) بينما من وجهة نظر المستخدمين جاء الحل رقم (٤) هو (إرساء الأسس لبناء بيئة رقمية أكثر أمانًا وبناء مواطن رقمي أكثر مسئولية ووعي) الأقوى تأثيرًا في الحلول التوعوية طبقًا لإجماع أراء المستخدمين بمتوسط (٢.٨٢).

جدول (٢٩) يوضح المقارنة بين (الخبراء – المستخدمين) وترتيب أكثر الأليات والحلول تأثيرًا

الهدف الرابع: رصد الأليات والحلول المقترحة لمواجهة مخاطر وجرائم الميتافيرس والتقنيات الناشئة:	الخبراء				المستخدمين				ت	المعنوية
	المتوسط	الإنحراف المعيارى	المدى	ترتيب	المتوسط	الإنحراف المعيارى	المدى	ترتيب		
الحلول القانونية	٢.٩٧	٠.١٦	٣-٢	١ مكرر	٢.٨٠	٠.٤٠	٣-١	١	٢.٥٧٣	٠.٠١٠
حلول السياسات	٢.٩٢	٠.٢٢	٣-٢	٣	٢.٧٠	٠.٤٥	٣-١	٤	٢.٩٩٨	٠.٠٠٣
الحلول التقنية	٢.٩٧	٠.١٣	٣-٢.٣	١ مكرر	٢.٧٧	٠.٤٤	٣-١	٣	٢.٦٩١	٠.٠٠٧
الحلول التوعوية	٢.٩٥	٠.٢٦	٣-١.٤	٢	٢.٧٩	٠.٤٢	٣-١	٢	٢.٣٤٨	٠.٠١٩
البعد الرابع ككل	٢.٩٥	٠.١٩	٣-١.٩		٢.٧٦	٠.٣٨	٣-١		٣.٠١٢	٠.٠٠٣

المصدر: من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية
ن = ٤٤٥

من قراءة الجدول (٢٩) تبين أن الحلول القانونية والتقنية هي أقوى الحلول لمواجهة جرائم ومخاطر الميتافيرس والتقنيات الناشئة بمتوسط (٢.٩٧) من وجهة نظر الخبراء وأن الحلول القانونية هي أقوى الحلول لمواجهة جرائم ومخاطر الميتافيرس والتقنيات الناشئة بمتوسط (٢.٨٠) من وجهة نظر المستخدمين من الشباب.

(٢) نتائج الفروق بين الأوزان النسبية بين استجابات عينة كلًا من الخبراء والمستخدمين من الشباب حول الحلول والأليات المقترحة لمواجهة جرائم ومخاطر الميتافيرس والتقنيات الناشئة:

جدول (٣٠) الفروق بين الأوزان النسبية (الخبراء – المستخدمين)

الهدف الرابع: رصد الأليات والحلول المقترحة لمواجهة جرائم ومخاطر الميتافيرس والتقنيات الناشئة	خبراء ن= ٤١		المستخدمين ن= ٤٠٤		إجمالي الاستجابات ن= ٤٤٥		ز	الدلالة
	ق	ت	ق	ت	ق	ت		
الحلول القانونية								
١- إنشاء أليات رقابية لمراقبة الالتزام بالقواعد ومعاقبة أولئك الذين يخالفون القانون	٠.٩٨٣	٢	٠.٩٤٢	١	٠.٩٤٦	١	١.٤٤٩-	-
٢- سن التشريعات والقوانين اللازمة لمواجهة الجرائم عبر الميتافيرس	٠.٩٩١	١مكرر	٠.٩١٩	٤	٠.٩٢٦	٤	٢.٦٤-	*
٣- تزويد الضباط والأجهزة المعنية بخطورة الجرائم الإلكترونية، وبالتقنيات الحديثة للتعرف على الجناة	٠.٩٩١	١مكرر	٠.٩٣٦	٣	٠.٩٤١	٣	٢.١٩٣-	*
٤- إتخاذ التدابير الأمنية لضمان حماية المستخدمين من الهجمات الإلكترونية.	٠.٩٩١	١مكرر	٠.٩٣٨	٢	٠.٩٤٣	٢	٢.٠٥٥-	*
حلول السياسات								
١- تعميق التعاون مع صناع السياسات وقادة المجتمع المدني والمنظمات من أجل صياغة وصنع وإنفاذ قوانين ولوائح سيبرانية قوية، وإشراك الدولة لأصحاب المصلحة في صنع السياسات.	٠.٩٧٤	٣	٠.٩٠٧	٣	٠.٩١٣	٣	٢.١١٢-	*
٢- إيجاد المبادئ التوجيهية والمجتمعية لضبط والتحكم في طرق التواصل بين الأفراد على الميتافيرس	٠.٩٦٦	٤	٠.٨٩٦	٤	٠.٩٠٢	٤	٢.١٨٣-	*
٣- العمل على إتباع أساليب مصادقة الواقع الافتراضي، والمصادقة متعددة المستويات.	٠.٩٥٧	٥	٠.٨٦٦	٥	٠.٨٧٤	٥	٢.٥٨٩-	*
٤- ضرورة الفهم الشامل من قبل المعنيين بمكافحة هذه الجرائم المُستحدثة بمكونات وتهديدات المجتمع الافتراضي	٠.٩٩١	١	٠.٩١٩	١	٠.٩٢٦	١	٢.٤٩٢-	*
٥- أن تقوم الحكومات يسن وتنفيذ التشريعات التي تعكس دورها في تنظيم السلامة الرقمية المجتمعية	٠.٩٨٣	٢	٠.٩١٨	٢	٠.٩٢٤	٢	٢.٤١٩-	*
الحلول التقنية								
١- إيجاد الوسائل التكنولوجية التي تهدف إلى منع الهجمات السيبرانية والجرائم عبر الميتافيرس.	٠.٩٨٣	٢	٠.٩٣٦	١	٠.٩٤١	١	١.٥٥٦-	-

الهدف الرابع: رصد الأليات والحلول المقترحة لمواجهة جرائم ومخاطر الميتافيرس والتقنيات الناشئة	خبراء ن= ٤١		المستخدمين ن= ٤٠٤		إجمالي الاستجابات ن= ٤٤٥		ز	الدلالة
	ق	ت	ق	ت	ق	ت		
٢- توفير أجهزة وتقنيات مراقبة الجريمة عبر الإنترنت لتحسين التنبؤ بالجرائم واكتشافها.	٠.٩٩١	١مكرر	٠.٩١٨	٣	٠.٩٢٥	٣	٢.٥٦٧-	*
٣- إنشاء وتطوير أنظمة الكشف عن الجرائم والتهديدات وأليات الاستجابة لها في الفضاء السيبراني.	٠.٩٩١	١مكرر	٠.٩١٩	٢	٠.٩٢٦	٢	٢.٥١٧-	*
الحلول التوعوية								
١- نشر الوعي الفردي والمجتمعي بمخاطر الجرائم عبر الميتافيرس.	٠.٩٧٤	٣مكرر	٠.٩٣٦	٢	٠.٩٣٩	٢	١.٤٩٦-	-
٢- توفير الرعاية النفسية لأولئك الذين تضرروا من الجرائم عبر الميتافيرس	٠.٩٧٤	٣مكرر	٠.٩٣٣	٣	٠.٩٣٧	٣	١.٦٧٣-	-
٣- دمج الجوانب التوعوية والأخلاقية والعملية للسلوك عبر الإنترنت ضمن المناهج التعليمية، وفي القطاعات المدنية المختلفة في الدولة .	٠.٩٨٣	٢	٠.٩٢٧	٤	٠.٩٣٢	٤	٢.٢٣٧-	*
٤- إرساء الأسس لبناء بيئة رقمية أكثر أمانًا وبناء مواطن رقمي أكثر مسئولية ووعي.	٠.٩٩١	١مكرر	٠.٩٤	١	٠.٩٤٤	١	١.٩١٣-	-
٥- غرس القيم التي لا تشجع على الانخراط في أنشطة غير قانونية عبر الإنترنت	٠.٩٩١	١مكرر	٠.٩١٣	٥	٠.٩٢	٥	٢.٤٤٩-	*

ق:- الوزن النسبي، ت:- الترتيب، مستوى الدلالة وتشير(-) على عدم وجود دلالة إحصائية و(**) على وجود فروق مرتفعة ذات دلالة إحصائية و(*) على وجود فروق ذات دلالة إحصائية، ز: دلالة الفروق بين كلا من الخبراء والمستخدمين من الشباب.

يتضح من الجدول (٣٠) إنه عند مستوى دلالة (٠.٠٥) لجميع عبارات المقياس وجود بعض فروق دالة إحصائيًا بين استجابات أفراد عينة البحث للجدول السابق طبقًا للآتي:

- **(الحلول القانونية):**

يتضح من قيمة الوزن النسبي لعباراته أن أعلى وزن نسبي في الخبراء جاء لصالح الأليات رقم (٢ و٣ و٤) (سن التشريعات والقوانين اللازمة لمواجهة الجرائم عبر

الميتافيرس، تزويد الضباط والأجهزة المعنية بخطورة الجرائم الإلكترونية، وبالتقنيات الحديثة للتعرف على الجناة، اتخاذ التدابير الأمنية لضمان حماية المستخدمين من الهجمات الإلكترونية) بنسبة (٩٩.١%) من الدرجة العظمى للأليات القانونية بينما جاء عند المستخدمين من الشباب لصالح المتغير رقم (١) (إنشاء أليات رقابية لمراقبة الالتزام بالقواعد ومعاقبة أولئك الذين يخالفون القانون) بنسبة (٩٤.٢%) من الدرجة العظمى للأليات القانونية، في حين جاء المتغير الأقل وزن نسبي عند الخبراء لصالح العبارة رقم (١) (إنشاء أليات رقابية لمراقبة الالتزام بالقواعد ومعاقبة أولئك الذين يخالفون القانون) بنسبة (٩٨.٣%)، بينما جاء عند عينة المستخدمين من الشباب لصالح المتغير رقم (٢) (سن التشريعات والقوانين اللازمة لمواجهة الجرائم عير الميتافيرس)، بنسبة (٩١.٩%) من الدرجة العظمى للحلول القانونية.

وتجدر الإشارة إلى أن الجرائم الإلكترونية بين الأشخاص في الميتافيرس تستوجب إيجاد عقوبات قانونية على المجرمين الذين يرتكبون هذه الجرائم، لقد اشارت الأدبيات السابقة إنه ردًا على النشاط الإجرامي المحتمل في المطاردة والاعتداء الجنسي والسلوك المسيء والمواد الإباحية عن الأطفال والاختطاف وانتهاكات قانون الملكية الفكرية والاحتيال المالي، يجب استخدام إجراءات راسخة وناجحة في العالم المادي، ومع ذلك أوضحت نتائج دراسة خطورة الجرائم الإلكترونية بين الأشخاص مقارنة بالجرائم الجسدية أن ما يقرب من ثلثي الأشخاص اعتبروا أن هذه الجرائم لها نفس القدر من الخطورة، في المقابل أجاب (١١.١%) من المشاركين بأنهم يعتقدون أن المضايقات عبر الإنترنت جريمة أقل خطورة، وفي دراسة إضافية أجريت من قبل بعض الباحثين، تمت مقابلة ضباط الشرطة حو وجهة نظرهم حول خطورة التنمر عبر الإنترنت؛ أظهرت النتائج أن هؤلاء الضباط أقروا بأن التنمر عبر الإنترنت هو حادث شخصي غير إجرامي، وهذا ما يؤكد الحاجة إلى التدريب على إنفاذ القانون لتثقيف هؤلاء الضباط حول خطورة الجرائم الإلكترونية بين الأشخاص على شبكة الإنترنت وفي الميتافيرس.

(Stavola, J&Choi, K,2023: 8).

- **(حلول السياسات):**

يتضح من قيمة الوزن النسبي لعباراته أن أعلى وزن نسبي في الخبراء لصالح المتغير رقم (٤) (ضرورة الفهم الشامل من قبل المعنيين بمكافحة هذه الجرائم المُستحدثة بمكونات وتهديدات المجتمع الافتراضي) عند الخبراء بنسبة (٩٩.١%) من الدرجة وعند المستخدمين من الشباب بنسبة (٩١.٩%) من الدرجة العظمى لحلول السياسات، في حين جاءت العبارة الأقل وزن نسبي لصالح المتغير رقم (٣) (العمل على إتباع أساليب مصادقة الواقع الافتراضي، والمصادقة متعددة المستويات) بنسبة (٩٥.٧ %) عند الخبراء، وبنسبة (٨٦.٦%) عند المستخدمين من الشباب، وذلك من الدرجة العظمى لحلول السياسات.

وتتماشى النتائج مع ما أشار إليه مؤتمر سياسات الواقع الافتراضي لعام ٢٠٢١ قد سلط الضوء على أهمية تعزيز السلامة لمستخدمي الواقع الافتراضي، حيث يمكن التلاعب بواقعهم، مما يثير مخاوف بشأن الأذى الجسدي والعقلي والعاطفي للمستخدمين، ومن أهم التوصيات التي خرج بها المؤتمر هي إجراءات السياسة المستقبلية، واقتراح التعاون بين صناع السياسات وقادة المجتمع المدني ومستخدمي الميتافيرس. أن حلول السياسات مثل أليات التحكم الاجتماعي الرسمية وغير الرسمية لها نفس القدر من الأهمية، وتتمثل أليات مكافحة الجريمة غير الرسمية التي يمكن تنفيذها في الواقع الافتراضي من قبل المجتمع في المبادئ التوجيهية المجتمعية والتنظيمات الذاتية، بالإضافة إلى أن هناك حاجة إلى ضوابط رسمية صارمة ومفصلة مثل التنظيم القانوني وتوفير مزيد من الأمن من خلال مراقبة الشرطة والملاحقة الجنائية ومراكز الحماية عبر الإنترنت، ويقترح أحد الباحثين إنه لدمج الضوابط الرسمية وغير الرسمية علب منصة افتراضية ضرورة إنشاء مبادئ توجيهية مجتمعية بسيطة ولوائح قانونية، ودمج القوانين الجنائية التقليدية التي تنطبق على معايير الحياة الواقعية وكذلك الفضاء الإلكتروني، ومطالبة دوريات إنفاذ القانون بالفهم الشامل لمكونات وتهديدات المجتمع الافتراضي مثل الميتافيرس.**(Stavola,J&Choi,K,2023: 9)**

- **(الحلول التقنية):**

يتضح من قيمة الوزن النسبي لعباراته أن أعلى وزن نسبي في الخبراء لصالح العبارة رقم (٢ و٣) (توفير أجهزة وتقنيات مراقبة الجريمة عبر الإنترنت لتحسين التنبؤ بالجرائم واكتشافها، إنشاء وتطوير أنظمة الكشف عن الجرائم والتهديدات وأليات الاستجابة لها في الفضاء السيبراني) بنسبة (٩٩.١%) من الدرجة العظمى للحلول التقنية، بينما جاء عند المستخدمين من الشباب لصالح العبارة رقم (١) (إيجاد الوسائل التكنولوجية التي تهدف إلى منع الهجمات السيبرانية والجرائم عبر الميتافيرس) بنسبة (٩٣.٦%) من الدرجة العظمى للحلول التقنية، في حين جاء المتغير الأقل وزن نسبي في الخبراء لصالح العبارة رقم (١) (إيجاد الوسائل التكنولوجية التي تهدف إلى منع الهجمات السيبرانية والجرائم عبر الميتافيرس) بنسبة (٩٨.٣%) من الدرجة العظمى للحلول التقنية، بينما جاء عند المستخدمين من الشباب لصالح العبارة رقم (٣) (إنشاء وتطوير أنظمة الكشف عن الجرائم والتهديدات وأليات الاستجابة لها في الفضاء السيبراني) بنسبة (٩١.٩%) من الدرجة العظمى للحلول التقنية.

لقد أظهرت نتائج الدراسات السابقة إلى أن التحول يزيد من بشكل كبير من مخاطر تقنية التزييف العميق المتقدمة، مما يزيد من الفرص المتاحة للمستخدمين لتمثيل مستخدمين أخرين بشكل غير مشروع من خلال إنشاء التزييف العميق، حيث تساعد تقنيات الكشف عن التزييف العميق تحديد ما إذا كان مصدر الوسائط أصليًا أم اصطناعيًا، كما ستحدد تقنية الكشف نمط الفحص للصور التي تم التلاعب بها من خلال مقارنة انعكاس القرنية من نمط الفحص، ومن المتوقع أن تكون هذه التقنية بمثابة نهج مُرض لاكتشاف وسائط التزييف العميق في الميتافيرس، وكما يمكن استخدامها أيضًا لكشف الاستخدام غير المصرح به للنماذج الاصطناعية، بالإضافة إلى ذلك ينبغي اتخاذ التدابير الأمنية في الميتافيرس لضمان حماية المستخدمين من الهجمات الإلكترونية بين الأشخاص، فالميتافيرس منصة تم تطويرها مؤخرًا وبالتالي لم يتم استكشاف مجالات تقنيات الأمن السيبراني للجرائم الإلكترونية بين الأشخاص في الواقع الافتراضي،

ولهذا السبب من الضروري البدء في إطار التخفيف الذي يمكن تطبيقه في الميتافيرس. **(Stavola,J&Choi,K,2023:9-10)**

- **(حلول التوعوية):**

يتضح من قيمة الوزن النسبي لعباراته أن أعلى وزن نسبي في الخبراء لصالح العبارة رقم (٤ و٥) (إرساء الأسس لبناء بيئة رقمية أكثر أمانًا وبناء مواطن رقمي أكثر مسئولية ووعي، غرس القيم التي لا تشجع على الانخراط في أنشطة غير قانونية عبر الإنترنت) بنسبة (٩٩.١%) من الدرجة العظمى للحلول التوعوية بينما جاء عند المستخدمين من الشباب لصالح العبارة رقم (٤) (إرساء الأسس لبناء بيئة رقمية أكثر أمانًا وبناء مواطن رقمي أكثر مسئولية ووعي" بنسبة (٩٤%) من الدرجة العظمى للحلول التوعوية، في حين جاء ت العبارة الأقل وزن نسبي في الخبراء لصالح رقم (١ و٢) (نشر الوعي الفردي والمجتمعي بمخاطر الجرائم عبر الميتافيرس، توفير الرعاية النفسية لأولئك الذين تضرروا من الجرائم عبر الميتافيرس) بنسبة (٩٧.٤%) من الدرجة العظمى لحلول التوعوية، بينما جاء عند المستخدمين من الشباب لصالح العبارة رقم (٥) (غرس القيم التي لا تشجع على الانخراط في أنشطة غير قانونية عبر الإنترنت) بنسبة (٩١.٣%) من الدرجة العظمى للحلول التوعوية.

على الرغم من أن الميتافيرس يوفر مجموعة من الفرص الجديدة ونقاط الانطلاق للابتكار، إلا إنها بالفعل مساحة يتم استكشافها واستغلالها من قبل الجهات الفاعلة السيئة، ولذلك يجب على الأفراد والمؤسسات ضمان إنهم يتمتعون بالحماية الكفاية عند التعامل بشكل مباشر وغير مباشر– مع الأصول المرتبطة بالميتافيرس ، ولأن تهديدات الجرائم المالية جاءت في المرتبة الأولى في الجرائم المرتبطة بالميتافيرس، فقد أشارت نتائج إحدى التقارير إلى أليات الحماية التي يجب إتباعها للتخفيف منها وهي:

الفحص: من أجل الحماية من غسل الأموال ومخاطر التداول والعقوبات، فمن الأهمية فحص أي معاملات متعلقة بالميتافيرس بحثًا عن اتصالات غير مشروعة، لأنه

سوف يساعد في تحديد أي تعرض مباشر وغير مباشر، والتأكد من إمكانية اتخاذ أي خطوات تخفيفية، ويشمل هذا إجراء المزيد من التحقيقات أو منع عمليات السحب أو تنبيه الجهات ذات الصلة، ويمكن أن ساعد أدوات مثل Lenz، Elliptic، Navigator على إدارة مخاطر الجرائم المالية المتعلقة بمعاملات الأصول المشفرة والمحافظ الإلكترونية.

إجراءات العناية الواجبة: قبل إضافة دعم لمشروع ميتافيرس والأصول ذات الصلة، لابد من التأكد من إجراء المتابعة على المشروع والفريق الذي يقف وراءه. يمكن أن يساعد هذا في التأكد من أنه ليس هناك احتيال أو لديه أي مخاطر واضحة لاستغلال التعليمات البرمجية والتي تؤدي لاحقًا إلى خسارة أموال المستخدمين الذي يمتلكون تداول الأصول ذات الصلة في الميتافيرس.

استخدام أفضل التقنيات والابتكارات: سيسعى المجرمون إلى استخدام الابتكارات الجديدة لتجرتها للبقاء في صدارة تطبيق القانون، على هذا النحو من المهم على الأفراد والشركات في مجال العملات المشفرة استخدام أفضل التطبيقات للقبض على الأنشطة غير المشروعة. **(Ellitpic Metaverse Report, 2022:42)**

ثانيًا: التحليل الكيفي لنتائج المقابلات الفردية المتعمقة:

يساعد الاعتماد على البيانات والنتائج الكيفية في تفسير المعطيات الكمية، والوصول إلى فهم أكثر عمقًا لدلالاتها ومضامينها، تكتسب الأساليب الكيفية – أو النوعية أهمية كبرى خاصة في مجال دراسات الظواهر المستجدة والجرائم المستحدثة التي يعاني منها المجتمع. ويحاول البحث الراهن مناقشة نتائج المقابلات الفردية التي أجريت مع (٤١) حالة من الخبراء والنخب (أكاديميين– رجال إنفاذ القانون– مهندسون ومتخصصون في الأمن السيبراني– مستشارون) من أجل تعميق الفهم بنتائج الدراسة الكمية واستشراف الجرائم المُحتمل ارتكابها عبر الميتافيرس التقنيات الناشئة، وفئات الجناة والضحايا المحتملين لهذه الجرائم.

(١) مدى الشعور بالقلق بشأن خصوصية البيانات والمعلومات مع ظهور الميتافيرس والتقنيات الناشئة:

كشفت نتائج المقابلات عن إجماع الخبراء وشعورهم بالقلق والخوف وعدم الأمان بشأن خصوصية البيانات والمعلومات عبر الميتافيرس والتقنيات الناشئة. حيث ذكر بعض الخبراء: "**نعم، أشعر بالقلق بشأن بياناتي وخصوصيتي مع التقنيات الناشئة على الإنترنت، بالأخص مع زيادة التطور التكنولوجي، حيث أصبحت هناك مخاوف بشأن جمع البيانات وتخزينها واستخدامها بطريقة غير آمنة. وأتساءل دائمًا عما إذا كانت بياناتي آمنة أم أنها يمكن أن تُستغل لتحقيق مكاسب شخصية أو مالية لشركات أو أفراد آخرين، لذا أفضل أن أكون حذرًا في التعامل مع بياناتي الشخصية وأن أكون على دراية كاملة بالسياسات التي تتبعها الشركات والتطبيقات التي أستخدمها**". أشار خبيرًا آخر "**من المهم أن أتحكم قدر الإمكان في المعلومات التي أشاركها وأن أختار الخدمات التي تحترم خصوصيتي**" كما أشار أحد الخبراء إلى محاولة اختراق بياناته بالفعل حيث ذكر "**نعم وسبق أن تم اختراق بياناتي**" وأكد أحد الخبراء "**أشعر بقلق بالغ الخطورة وأتخذ إجراءات عدم الانسياق وراء المواقع ومنع إعطاء بيانات شخصية إلا في اضيق الحدود**" وأشار أخرون إلى أن هناك قلق ولكن يجب الحذر واتخاذ إجراءات التأمين اللازمة لذلك.

ويمكن القول إنه مع تزايد قلق مستخدمي الإنترنت في جميع أنحاء العالم بشأن بياناتهم الشخصية وخصوصيتهم، تواجه الشركات التي تعمل في الميتافيرس تحديًا أخر يتمثل في بناء الثقة بين المستخدمين، ويمثل هذا تحديًا كبيرًا لأنه عامل مهم يضع وسائل التواصل الاجتماعي في قائمة الوسائل المسيئة للعديد من الأشخاص في جميع أنحاء العالم. وعلى الرغم من أن الشركات تهتم بسلامة بيانات المستخدمين، فقد كانت هناك حالات كثيرة تم اختراقها؛ لقد تم اختراق بيانات المستخدم في العديد من المناسبات المختلفة عن قصد أو عن طريق الصدفة حتى أن بعض الشركات تستخدم هذه البيانات لتحقيق أرباح لنفسها **(Bale[et.al,],2022:9)**.

كما تتفق تلك النتائج مع ما أشارت إليه نتائج دراسة **(Huq[et.al,]2022:21)** حيث أكدت إنه في الميتافيرس ستكون الخصوصية مصدر قلق رئيس من مشغلي الفضاء نتيجة الوصول غير المسبوق إلى إجراءات المستخدم وستكون سيادة البيانات قضية رئيسة. كما أشارت نتائج إحدى الدراسات أن تقنية الميتافيرس لها تأثيرات خطيرة وتداعيات وخيمة على بيانات الأشخاص والمستخدمين لها ناهيك عن الانتهاكات الجسيمة لحياتهم الشخصية، أن تقنية الميتافيرس تساهم في ظهور نمط جديد من الإجرام، تجسد في انتشار الجرائم الإلكترونية المرتبطة بنظم وبيانات المؤسسات الرقمية في العالم الافتراضي والتي تعتر من أكبر السلبيات التي خلقتها الثورة المعلوماتية لكون هذه الجرائم تشمل اعتداءاتها على قيمًا جوهرية تخص جميع معلومات الأفراد ومختلف صورهم وكافة جزيئات حياتهم الخاصة. **(العلوي & التوزاني،٢٠٢٣: ٢٦٩- ٢٧٣)**

(٢) مدى الاعتقاد بأن المجال الافتراضي بما في ذلك منصات التواصل الاجتماعي والتقنيات الناشئة تؤدي إلى إساءة الاستخدام والتحرش:

إزاء هذا الموقف تبلورت استجابات حالات البحث من النخب في موقفين أساسيين، **<u>الأول</u>** يؤكد على أن وسائل التواصل الاجتماعي والميتافيرس والتقنيات الناشئة تؤدي إلى ممارسة سلوك التحرش حيث ذكر أحد الخبراء " **نعم، يؤدي المجال الافتراضي، بما في ذلك منصات التواصل الاجتماعي، إلى إساءة الاستخدام والتحرش. وذلك للأسباب التالية: (١) منصات التواصل الاجتماعي توفر مساحات للتفاعل الغير مراقب بشكل كبير، مما يسمح للأفراد بالتعبير عن آرائهم ومشاعرهم دون عقبات. هذا الوضع يمكن أن يؤدي إلى ظهور سلوكيات عدوانية أو سلوكيات كلها تحرش بالأخرين، (٢) قد يختبئ الناس وراء أسماء مستعارة أو شخصيات مزيفة، مما يسمح لهم بالتحرش دون أن يواجهوا عواقب مباشرة. (٣) يمكن الوصول بسهولة إلى الأشخاص عبر الإنترنت، مما يسهل على المتنمرين التواصل مع ضحاياهم بشكل متكرر، (٤) الأطفال والمراهقين الذين يستخدمون منصات التواصل الاجتماعي قد يكونون أكثر عرضة للتحرش وإساءة الاستخدام بسبب عدم نضجهم وقدرتهم المحدودة على التعامل مع المواقف الصعبة."**

وأشار عدد من الحالات: **"نعم فالمجال الافتراضي ومواقع التواصل الاجتماعي يؤديان إلى التحرش الجنسي"**، وذكر خبيرًا آخر: **"نعم أعتقد ذلك في ظل عدم مراقبة الوالدين لنشاط الاطفال على تلك المواقع"**، وأكد خبيرًا آخر: **"نعم وبدرجة عالية في غياب الرقابة الأسرية والمجتمعية "** وذكر آخرون **نعم، تعزز فرص الإساءة والتحرش"، "بالتأكيد إذا استخدم استخدام سيء"**، وأكد البعض **"أحيانا تستخدم في التحرش وإساءة الاستخدام ونشر المحتويات غير الهادفة والضارة".**

أما الفريق الثاني فقد ذهب إلى احتمالية تأثير وسائل التواصل الاجتماعي والميتافيرس والتقنيات الناشئة في ممارسة سلوك التحرش وإساءة الاستخدام. حيث ذكر مجموعة من الخبراء أن **إمكانية قيام وسائل التواصل الاجتماعي والميتافيرس والتقنيات الناشئة على التحريض على العنف من عدمه مرتبط "بالقيم والأخلاق والأسرة" وكذلك "وفق الاستخدام"**، بينما ذكر أخرون إلى أنه **"ليس بالضرورة" أن تؤدي مثل هذه التقنيات إلى إساءة الاستخدام والتحرش.**

ويمكن القول إن التحرش على الإنترنت يعد بالفعل قضية كبيرة، حيث تعرضت ما يصل إلى (٥٨%) من الفتيات في استطلاع دولي أجرته منظمة "Plan International" في عام ٢٠٢٠ للتحرش عبر الإنترنت. كما بدأ المجرمون بالفعل في بيع بصمات الأصابع الرقمية على شبكة الويب المظلمة، والتي تحاكي خصائص جهاز المستخدم وسلوكه، وهذا يسمح لمستخدم الخدمة باستخدام مكون إضافي للمتصفح لتقليد بصمة إصبع الضحية الرقمية لأغراض خداع أنظمة المصادقة. **(Singh,2022:94)**

كما كشفت نتائج دراسة أخرى أن وجود المضايقات والإساءة داخل منصات الميتافيرس خطرًا كبيرًا ومثبتًا بشكل جيد لاسيما في البيئات المفتوحة والمتعددة الأشخاص، حيث يتفاعل المستخدمون مع الغرباء، فقد كان خطرًا واضحًا منذ عدة سنوات، ويبدو إنه لا يزال في تزايد، تشير الأدلة إلى أن حالات التحرش تميل إلى الزيادة في البيئات الافتراضية الخالية من الاستضافة المُدارة أو الغرض الواضح، مع احتمال استهداف

المستخدمين من الإناث والأشخاص من الأقليات. ففي عام ٢٠١٨م وجدت إحدى باحثات الواقع الافتراضي "جيسيكا أوتلاو" أن (٤٩%) من مستخدمي الواقع الافتراضي من الإناث أبلغن عن تعرضهن للتحرش الجنسي أو الاعتداء في المساحات الاجتماعية الافتراضية منذ ذلك الحين، ومع تزايد الاعتماد العام لنظارات الواقع الافتراضي، تصاعد المشكلة واجتذبت قدرًا كبيرًا من اهتمام وسائل الإعلام. في السنوات القليلة الماضية، تم الإبلاغ عن العديد من التقارير عن التحرش الجنسي أو الاعتداء داخل الميتافيرس **(Cristea,2023:4)**.

فقد كشفت إحدى الدراسات التي قامت بسؤال المستجيبين عما إذا كان الميتافيرس سيؤدي إلى تفاقم مشكلة الإساءة والمضايقة؟ فقد أظهرت النتائج أن (٤١.٤%) من الأشخاص شعروا أن هذا قد يكون احتمالًا ويؤدي إلى تفاقم الجرائم عبر الإنترنت مقابل نفي (٢٢.٣%) من الأشخاص الذين أجابوا على هذا الاستطلاع.

(Bale[et.al,],2022:8)

ولابد من التأكيد على أن في السنوات الأخيرة تم توثيق حالات المضايقة والإساءة داخل منصات (Proto Metaverse) التي يشار إليها أحيانًا باسم منصات الواقع الافتراضي بشكل جيد في وسائل الإعلام، وتشير الأدلة إلى أن حالات التحرش تميل إلى الزيادة في البيئات الافتراضية الخالية من الاستضافة المُدارة أو الغرض الواضح، مع احتمال استهداف المستخدمين من الإناث والأشخاص من الأقليات، فقد أشارت دراسة استقصائية شملت أكثر من ٦٠٠ مستخدم في عام ٢٠١٨م إلى أن (٤٩%) من مستخدمي الواقع الافتراضي الإناث أبلغن عن تعرضهن للتحرش الجنسي أو الاعتداء في المساحات الاجتماعية الافتراضية، منذ ذلك الحين، ومع تزايد التبني العام لنظارات الواقع الافتراضي، يبدو أن المشكلة أستمرت وتصاعدت في عام ٢٠٢١م، كما تم الإبلاغ عن العديد من التقارير عن التحرش الجنسي والاعتداء الجنسي داخل الميتافيرس في وسائل الإعلام. **(Mclntosh,2024:2)**

ولابد من الإشارة إنه في عام ٢٠٢٢م أدعت نيناجين باتيل إنها تعرضت للاغتصاب الجماعي تقريبًا في "HorizonVenues" وهي منصة واقع افتراضي مشابهة "VRCHAT" المملوكة لشركة Meta، ووفقًا للضحية تبين أن (٣-٤) صور رمزية ذكورية قاموا باغتصاب صورتي الرمزية، بينما كنت أحاول الهروب صرخوا، وعلى الرغم من أن "HorizonVenues" تتمتع بميزة المنطقة الأمنه على غرار "VR CHAT" والتي تتكون من فقاعات واقية يمكن للمستخدمين تنشيطها في أي وقت حتى لا يتمكن أي شخص من لمسهم أو التحدث معهم بأي شكل من الأشكال؛ إلا أن باتيل أدعت أنها تجمدت ولأن كل شيء حدث بسرعة كبيرة، لم يكم لديها الوقت للتفكير في تفعيل المنطقة الأمنة. ووفقًا لباتيل تم تصميم الواقع الافتراضي بشكل أساسي ليتناسب مع العقل والجسم، مما يمحو الحدود بين العالم الرقمي والواقع، لذلك زعمت أن استجابتها الفسيولوجية والنفسية كانت إلى حد ما كما لو أنها حدثت في الحياة الواقعية. **(Ortiz,2023:58)**

(٣) فئات الضحايا المحتملين لجرائم الميتافيرس والتقنيات الناشئة:

ما فئات الضحايا المُحتملين للجرائم المرتبطة بالميتافيرس والتقنيات الناشئة، إزاء هذا التساؤل خرجت المقابلات لتشير إلى أن الضحايا يندرجون تحت عدة فئات هم "**(١) جميع المستخدمين الغير ملمين بمخاطر التكنولوجيا**"، **(٢) غير المتعلمين،(٣) كبار السن، (٤) الأطفال والمراهقين**".

وأشار عدد من الخبراء إلى أن فئات الضحايا تتمثل في "**(١) الأفراد العاديين مثل مستخدمي الإنترنت الذين قد يتعرضون للاحتيال أو سرقة الهوية أو انتهاك الخصوصية، (٢) الشركات، المؤسسات الحكومية حيث قد تتعرض الشركات أو المؤسسات الحكومية لهجمات إلكترونية أو سرقة بيانات أو اختراق أنظمتها، (٣) الأطفال الصغار والمراهقين، قد يكون الأطفال والمراهقين أكثر عرضة للجرائم الإلكترونية مثل الاستغلال الجنسي أو التنمر الإلكتروني**".

وجاءت فئة أخرى من الخبراء وأشارت إلى أن من أهم ضحايا جرائم الميتافيرس والتقنيات الناشئة "**هما الأطفال والمراهقين والنساء بشكل خاص معرضون ومستهدفون**

لجرائم الميتافيرس لقلة الوعي بمخاطرها حيث ذكر عدد من الخبراء أن "الأشخاص ذوي الخبرات الضعيفة بمجال تكنولوجيا المعلومات وتشمل فئات كثيرة الأطفال وكبار السن"، "الأطفال خاصة في سن المرهقة ومحدودي الدخل وقليلي الخبرة المعلوماتية والجهل بأساليب الاحتيال وطرقها"، "الأطفال والمراهقين وكل المدللين بشكل عام بحاجة للتوعية المستمرة بكل الاليات الممكنة".

" الأطفال؛ النساء؛ المستهلك الإلكتروني؛ المستخدم الأقل خبرة بمجال التكنولوجيا"، "الشباب والأطفال وكبار السن وذوي الهمم، الفئات المستبعدة اجتماعيًا من ذوي الدخول المنخفضة والتعليم المحدود والمتعطلين عن العمل والمفتقرين للثقافة العامة. في الحالة المصرية نحن نتكلم عن حوالي (٧٠- ٨٠) بالمائة من مستخدمي الإنترنت"، "المدمنين".

"الضحايا المحتملون يشملون الأفراد العاديين الغير مثقفين، خاصة الأطفال وكبار السن، والشركات التي قد تتعرض للاختراق، بالإضافة إلى الحكومات والمؤسسات التي تواجه هجمات إلكترونية."، الضعاف، ضعاف النفس، ضعاف الشخصية، ضعاف الحيلة ضعاف، ضعاف الوعي وهلم جرًا"، "الكبار في السن الذين لم يواكبوا التطورات التكنولوجية أو الأشخاص الذين ليس لديهم علم بالأخطار".

وأشار عددًا من الخبراء إلى أن جميع فئات المجتمع معرضون لأن يكونوا ضحايا الجرائم المرتبطة بالميتافيرس والتقنيات الناشئة بالإضافة إلى فئة الغير واعيين بتلك المخاطر وليس لديهم خبرة بها وغير قادرين على حماية أنفسهم "الغير فاهمين ليها او الجدد" "الغير الواعين بمخاطر الإنترنت"، "الغير واعيين بتلك المخاطر"، "الغير واعون بالخبرة في عالم الكمبيوتر"، "الغير قادرين بحماية انفسهم"، الغير قادرين على حماية أنفسهم من هذه الجرائم أو أنهم لا يعرفون كيف يحمون أنفسهم ف يجب بإقامة وعي بين هؤلاء الضحايا وتعليمهم كيفية حماية انفسهم"، "الغير متعلمين"، "الغير واعين بخطورة الجرائم التقنية" "غير الملمين بالأمن السيبراني".

وتتماشى النتائج مع ما أشارت إليه نتائج إحدى الأدبيات السابقة حيث من المتوقع أن يشمل ضحايا الجرائم الإلكترونية في الميتافيرس الجيل الأصغر (على وجه التحديد المراهقين الذين تتراوح أعمارهم ما بين ١٠ و٢٠ عامًا، وكبار السن والنساء، حيث تعد النساء أهدافًا أساسية لدوافع الجرائم الجنسية بين الأشخاص، على الرغم من أن الرجال يتعرضون للإيذاء أيضاً، كما أشارت النتائج إلى إجماع الخبراء حول كون الأطفال والمراهقين هما الضحايا الأساسيون للجرائم الشخصية مثل الاستمالة والمطاردة والتحرش عبر الإنترنت، حيث أن الأطفال غير الخاضعين للإشراف سيكونوا ضحايا الجرائم الإلكترونية. كما وجدت الأبحاث السابقة أن ما يقرب من (٦١%) من الأفراد الذين تتراوح أعمارهم بين ١٠ و٨١ عامًا يتعرضون للإيذاء عبر الإنترنت خاصة بالتزييف العميق. **(Stavola&Choi,2023:13)**

كما أظهرت نتائج إحدى الدراسات أن سهولة الوصول إلى المعلومات الشخصية تلعب دورًا في جعل الأفراد أهدافًا محتملة، على سبيل المثال أولئك الذين يشاركون بنشاط ويبالغون في المشاركة في الميتافيرس قد يعرضوا أنفسهم لمجرمي الإنترنت دون قصد، يمكن استغلال هذه المعلومات مثل التفاصيل الشخصية والتفضيلات في هجمات ذات طابع شخصي للغاية مثل التصيد الاحتيالي أو سرقة الهوية. علاوة على ذلك قد تكون مجموعات ديموغرافية محددة أكثر عرضة للخطر، مثل الأفراد الأصغر سنًا أو الأكبر سنًا قد يفتقروا إلى الوعي أو الخبرة اللازمة للتعرف على التهديدات السيبرانية ودرئها. في حين أولئك الذين يعملون في مهن رفيعة المستوى أو حساسة قد يتم استهدافهم على وجه التحديد للحصول على معلومات قيمة أو الوصول إليها. حيث تتشكل صورة الضحايا المحتملين للجرائم في الميتافيرس من خلال مجموعة من الصفات الشخصية والسلوكيات ومستويات التطور الرقمي.**(Blake,2024:72)**

ووفقًا لنظرية النشاط الروتيني فإن اختيارات الضحايا لسلوكيات معينة، وقرارات معينة كالسكن في مكان معين أو ممارسة الرياضة في زمن معين، أو السير في طرق معينة، أو ارتداء زي معين، إلى آخر هذه الاختيارات هي التي تمكن الأشخاص ذوي

الدافعية الإجرامية من تحديد أهدافهم، أو بمعنى آخر هي التي تخلق المواقف المهيئة لارتكاب الفعل الإجرامي، ويساعد ذلك على عدم وجود ضبط كافٍ أو أليات كافية لمنع حدوث الجريمة وهكذا تجتمع العناصر الثلاثة لحدوث الموقف الإجرامي **(زايد، ٢٠١٧: ١٩٠)** كما يمكن تفسير زيادة عدد ضحايا الجرائم الإلكترونية من خلال التغيرات في أنشطة الناس الروتينية في الحياة اليومية، فمع ظهور شبكة الإنترنت تغيرت طريقة الناس التي يتواصلون فيها أو يتفاعلون مع الأخرين في العلاقات الشخصية والترفيه...إلخ. إن التغيرات في أنشطة الناس الروتينية مثل استخدام النت وشبكات التفاعل الاجتماعي مثل الفيس بوك والإيميل، والمواقع وغيرها قد خلق فرصًا للجناة المتحفزين مع وجود أهداف قيمة وسهلة في الحيز الفضائي، مع غياب الحراسة. **(البداينة، ٢٠١٤: ١٢-١٣)**.

(٤) فئات الجناة المُحتملين لارتكاب الجرائم عبر الميتافيرس والتقنيات الناشئة ودوافعهم لارتكاب الجرائم:

هناك قضية مهمة وتساؤل محدد مفاده من هم الجناة المُحتملين لارتكاب الجرائم عبر الميتافيرس والتقنيات الناشئة "وفي هذا الإطار انقسمت أراء الخبراء إلى ثلاث اتجاهات؛ **الاتجاه الأول أشار إلى أن الجناة والمجرمين المحتمل قيامهم بارتكاب الجرائم عبر التقنيات الناشئة والميتافيرس يتمثلون في عدة فئات مختلفة، حيث أشار عدد من الحالات إلى أن "الجناة المحتملون لارتكاب الجرائم عبر التقنيات الناشئة يتنوعون بشكل كبير، ويشملون:**

١- **الأفراد أو الجماعات يستخدمون الإنترنت لتنفيذ جرائم مثل الاختراق، الاحتيال، والتجسس الإلكتروني.**

٢- **الإرهابيون الذين يستغلون التقنيات الحديثة للتخطيط والتنفيذ والترويج لأعمالهم، مثل استخدام الشبكات الاجتماعية لنشر الفكر المتطرف أو تجنيد الأفراد.**

٣- **الأفراد العاديون يمكن أن يتركبوا جرائم بسيطة عبر الإنترنت مثل التنمر الإلكتروني أو نشر معلومات مضللة.**

٤- الهواة أو المخترقون وهم أفراد لديهم مهارات تقنية ويدفعهم الفضول أو الرغبة في إثبات الذات.

٥- المجرمون المنظمون الذين يستغلون التقنيات الجديدة لتسهيل أنشطتهم غير القانونية، مثل غسل الأموال أو الاتجار غير المشروع".

وأشار أخرون إلى أن فئات المجرمين تتمثل في "**(١) المستخدمين ذوي الميول الإجرامية، العصابات التي تسعى للنصب والابتزاز، (٢) الدول والجماعات المعادية،(٣) المنظمات- الدول- الجناة هما "أشخاص لديهم ميول عدوانية"، "مخترقين من دول أخرى"، "الأعداء في الداخل والخارج لتحقيق أهداف الغزو الثقافي والسيطرة والحروب النفسية في إطار حروب الجيل الرابع"، "الجناة في أي مكان في العالم وخاصة المحترفين والمبدعين منهم".**

وجاء **الاتجاه الثاني** وذهب إلى أن فئات الجناة الذين من المحتمل ارتكابهم للجرائم عبر الميتافيرس والتقنيات الناشئة تتمثل في "**الجناة في أي مكان في العالم وخاصة المحترفين والمبدعين منهم "الهاكرز"، "ومن يمتلكون الوعي والدراية بهذه التقنيات"، حيث أشار عدد من الخبراء إلى أن الجناة هم "الذين يملكون الدراية والخبرة بالتقنيات الحديثة وعندهم دافع للجريمة"، "من يستطيع إتقان التكنولوجيا الحديثة والتعامل على شبكات الإنترنت" "الأفراد المدربين"، "الذين يديرون هذه التقنيات"، "خبراء التقنيات الناشئة "والمتطفلين وأصحاب الرغبة في الثراء السريع"، "أي حد لديه القدرة على اختراق بيناتي يحتمل إن يكون مجرم الكتروني"، "محتالين يعلمون جيدا استخدام التكنولوجيا" بالإضافة إلى "الخارجون على القانون، اللصوص، الإرهابيون، المتحرشون"، "فئات مختلفة من المجتمع اكثرهم من معتادي الإجرام أو راغبي الثراء السريع وحب الشهرة والظهور وبعض المرضى النفسيين".**

وجاء **الاتجاه الثالث** وأشار إلى عدم وضوح وتحديد دقيق للجناة الذين من المحتمل قيامهم بارتكاب الجرائم عبر الميتافيرس والتقنيات الناشئة، **حيث ذكر بعض**

الخبراء إلى أن أي شخص ممن الممكن أن يرتكب الجرائم عبر الميتافيرس "ينسحب ذلك على الذكور بنسبة أعلى من الإناث ولكنهما لديهما الرغبة في ذلك، ويرجع ذلك للكسب السريع غير المشروع"، "بعض الشباب"، "الشباب"، "فئات مختلفة باختلاف نوعية الجرائم.

وفي نفس الصدد أكدت أحدى الدراسات إن التنبؤ باحتمالية تورط فرد ما في جريمة إلكترونية أمر معقد. قد يكون المراهقون ذوو المهارات التكنولوجية المتقدمة أكثر عرضًا للمشاركة في الجرائم السيبرانية، ويفوق عدد الجناة الذكور عدد الإناث وهذا هو الحال في جميع معدلات الجريمة. كما أن الأفراد في المجالات المتعلقة بتكنولوجيا المعلومات مسلحون بالمهارات اللازمة لتنفيذ الجرائم السيبرانية. **(Blake,2024:71)**

وتتماشى النتائج مع ما أشارت إليه نتائج إحدى الدراسات أن هؤلاء المجرمين المتحمسين من المرجح أن يكونوا في العشرينات من العمر، وأن هناك مخاوف بشأن زيادة معدلات الجريمة، حيث أن زيادة الفرص المتاحة للمجرمين المتحمسين لارتكاب الجرائم ستؤدي إلى تطور الميتافيرس، كما أن الدافع من وراء هذه الجرائم سيكون الدوافع الجنسية والمكاسب المالية، بل أن المكسب المالي هو الدافع الأساسي لهؤلاء المجرمين السيبرانيين الذين يرتكبون جرائم مالية عميقة بين الاشخاص، من المتوقع أن يصبح ابتزاز الأموال إلى جانب الجرائم المالية الأخرى سائدًا في الميتافيرس. **(Stavola&Choi,2023: 12)**

ووفقًا لنظرية النشاط الروتيني فإن الجاني المحتمل لارتكاب الجرائم عبر الميتافيرس والتقنيات الناشئة لديه الهدف المناسب والديه الدافع ولديه القدرة على ارتكاب الجرائم، ويقوم باستغلال غياب الحراسة أو الأوصياء وضعف الضوابط الفعالة، وبالتالي يعد وجود الجاني من أهم دوافع ارتكاب الفعل الإجرامي، كما أنهم يقوموا باستغلال كافة جوانب الضعف في البيئة لدى الضحايا والبيئة، وتوظيف كل التقنيات والتطورات التكنولوجية من أجل تحقيق هدفهم وتنفيذ أنشطتهم غير المشروعة.

حادي عشر: نتائج البحث وتوصياته:

(١) النتائج العامة للبحث:

في ضوء التحليلات السابقة يمكن الوقوف على أبرز نتائج البحث:

- حول سيناريوهات تهديدات الجرائم المحتمل ارتكابها عبر الميتافيرس والتقنيات الناشئة من وجهة نظر الخبراء والمستخدمين، أظهرت نتائج البحث إنه بإجماع أراء الخبراء والمستخدمين؛ تبين أن الجرائم المالية هي أقوى الجرائم المحتمل ارتكابها عبر التقنيات الناشئة بمتوسط (٢.٧٣) للخبراء وبمتوسط (١.٨٥) للمستخدمين، يليها الجرائم الجنسية في الترتيب الثاني عند الخبراء بمتوسط (٢.٧١)، وفي الترتيب الثالث عند المستخدمين بمتوسط (١.٧٩)، والجرائم ضد الأشخاص في الترتيب الثالث عند الخبراء بمتوسط (٢.٦٥) وفي الترتيب الثاني عند المستخدمين بمتوسط (١.٨٠)، وجاءت الجرائم الأخرى في الترتيب الرابع عند الخبراء بمتوسط (٢.٦٣)، وفي الترتيب الثاني مكرر عند المستخدمين بمتوسط (١.٨٠)، وجاءت جرائم الممتلكات في الترتيب الخامس عند الخبراء بمتوسط (٢.٦٢) وفي الترتيب الرابع عند المستخدمين بمتوسط (١.٨٠).
- حول سيناريوهات تهديدات المخاطر التي قد يتعرض لها الأطفال عبر الميتافيرس والتقنيات الناشئة، أظهرت نتائج البحث أن تهديدات مخاطر المحتوى (وتعني المخاطر التي يتعرض فيها الطفل لمحتوى غير لائق أو غير قانوني، والمخاطر النفسية (الإحباط، القلق، الاكتئاب) أقوى تأثيرًا في المخاطر التي من المحتمل أن يتعرض لها الأطفال طبقًا لإجماع أراء الخبراء بمتوسط (٢.٨٥)، بينما من وجهة نظر المستخدمين، تبين أن تهديدات المخاطر النفسية (الإحباط، القلق، الاكتئاب) أقوى تأثيرا طبقًا لإجماع أراء المستخدمين بمتوسط (٢.٠٧).
- وحول العوامل الدافعة إلى حدوث الجرائم عبر الميتافيرس والتقنيات الناشئة، أظهرت نتائج البحث أنه بإجماع أراء الخبراء والمستخدمين تبين أن العوامل العالمية هي أقوى

العوامل الدافعة الى حدوث الجرائم عبر الميتافيرس والتقنيات الناشئة بمتوسط (٢.٨٨) للخبراء، وبمتوسط (٢.٤١) للمستخدمين، يليها العوامل الفردية بمتوسط (٢.٧٦) عند الخبراء، وبمتوسط (٢.١٧) عند المستخدمين، وأخيرًا جاءت العوامل المجتمعية بمتوسط (٢.٧٠) عند الخبراء، وبمتوسط (٢.٠٨) عند المستخدمين.

- وحول الحلول المقترحة لمواجهة الجرائم والمخاطر المرتبطة بالميتافيرس والتقنيات الناشئة، أظهرت نتائج البحث أن الحلول القانونية والتقنية هي أقوى الحلول لمواجهة جرائم ومخاطر الميتافيرس والتقنيات الناشئة بمتوسط (٢.٩٧) من وجهة نظر الخبراء، وأن الحلول القانونية هي أقوى الحلول لمواجهة جرائم ومخاطر الميتافيرس والتقنيات الناشئة بمتوسط (٢.٨٠) من وجهة نظر المستخدمين من الشباب.

(٢) توصيات البحث:

مع ظهور الميتافيرس والتقنيات الناشئة التي تواكبه، أصبح من الضروري التعامل مع الجرائم المرتبطة بهذه البيئة الافتراضية. يتطلب هذا الأمر استراتيجيات جديدة لمواجهة التحديات القانونية والأمنية، تهدف التوصيات التالية إلى المساعدة في تضييق الفجوات المعرفية والتنظيمية والسياسية التي تنشأ مع الميتافيرس للوصول إلى التأثير الإيجابي وتقليل التحديات والتهديدات إلى أقصى حد ممكن، وهذا يتطلب جهودًا موحدة ومنسقة من جانب أصحاب المصلحة من الشركات الخاصة والحكومات وأولياء الأمور والمستثمرين والباحثين، حيث يكون لكل منهم دورة الخاص الذي يؤديه.

وترى الباحثة إنه من خلال نظرية الأنشطة الروتينية التي تبناها البحث الراهن والتي أشارت إلى أن مثلث الفعل الإجرامي يكمن في وجود (جاني محتمل– هدف مناسب – غياب الحراسة) فإنه يمكن التصدي للجرائم عبر الميتافيرس والتقنيات الناشئة من خلال السيطرة على الجاني المحتمل والقضاء على الأهداف التي تهيء ارتكاب الفعل الإجرامي وذلك من خلال تعزيز الحراسة والتي تعد أحد أهم أليات مواجهة الجرائم ويمكن تحقيقها عن طريق:

- **تطوير إطار قانوني شامل:**

يجب على الحكومات وضع قوانين واضحة تشمل جميع الجوانب المتعلقة بالجرائم الإلكترونية لتناسب بيئات الميتافيرس. ينبغي أن يتضمن ذلك تحديث القوانين لحماية المستخدمين من الجرائم الرقمية مثل الاحتيال، والإيذاء والاعتداءات وخرق الخصوصية. كما ينبغي أن يجب أن تكون هذه القوانين مرنة لتتمكن من التكيف مع التغيرات السريعة في التكنولوجيا، كما يجب أن تشمل هذه التشريعات أيضًا تفاصيل حول الحماية القانونية للضحايا، كما يجب أن تكون هناك توضيحات حول مسؤولية المنصات والشركات المعنية عن الأفعال التي تحدث داخل الميتافيرس.

- **تعزيز التعاون الدولي:**

نظرًا لأن الميتافيرس يتجاوز الحدود الوطنية، فإن التعاون الدولي هو عنصر أساسي في مكافحة الجرائم المرتبطة به. يجب تشجيع الدول على تبادل المعلومات وتعزيز التنسيق بين وكالات إنفاذ القانون على المستوى الدولي لمواجهة التهديدات العابرة للحدود نظرًا للطبيعة العالمية للميتافيرس، كما يجب تبادل المعلومات والتجارب بين الدول حول كيفية التعامل مع الجرائم الافتراضية، بالإضافة إلى تطوير آليات قانونية مشتركة لمقاضاة الجناة.

- **إنشاء وحدات شرطة متخصصة:**

من المهم إنشاء وحدات شرطة متخصصة في الجرائم الإلكترونية مع التركيز على الميتافيرس. هذه الوحدات ستكون مسؤولة عن التحقيق في الجرائم المتعلقة بالتقنيات الناشئة وتقديم الدعم للمستخدمين الذين قد يكونون ضحايا لهذه الجرائم. بالإضافة إلى ذلك، يمكن لهذه الوحدات تقديم التعليم والتدريب للمستخدمين حول كيفية التعامل مع التهديدات.

- **تدريب جهات الإنفاذ:**

يجب على الجهات المسؤولة عن إنفاذ القانون تلقي التدريب المناسب للتعامل مع

الجرائم المرتبطة بالتقنيات الجديدة. يتعين على المحققين والقضاة فهم كيفية عمل الميتافيرس والتقنيات المستخدمة فيه لتطبيق القانون بشكل فعال.

- **إنشاء منصات للإبلاغ عن الجرائم:**

يجب توفير طرق سهلة وآمنة للمستخدمين للإبلاغ عن أي نشاط مشبوه أو جريمة حدثت داخل الميتافيرس. يمكن أن تشمل هذه المنصات دعمًا فنيًا وقانونيًا للمستخدمين، مما يعزز ثقتهم في استخدام هذه البيئات الافتراضية.

- **دعم ضحايا الجرائم الإلكترونية:**

من المهم توفير الدعم النفسي والقانوني والمادي لضحايا الجرائم المرتبطة بالميتافيرس حيث يجب على الحكومات ومنظمات المجتمع المدني العمل معًا لتأسيس خدمات مؤهلة تقدم الدعم والاستشارة للضحايا، بالإضافة إلى ضمان أن يكون لديهم إمكانية الوصول إلى العدالة. كما يجب أن تتوفر موارد مثل الخطوط الساخنة، والمراكز القانونية، وبرامج الدعم النفسية لمساعدة الضحايا في التعافي من تجاربهم.

- **تطوير تكنولوجيات حماية وأمان:**

تطوير تقنيات الأمان؛ تعتبر التقنيات المستخدمة في الميتافيرس مسؤولة عن حماية المستخدمين. يجب الاستثمار في تطوير أدوات أمان فعالة تشمل تقنيات التعرف على الوجه، وبيانات المستخدم، وأنظمة المراقبة، طرق التحقق من الهوية، وتشفير البيانات، وأنظمة الكشف عن الاحتيال، كما يتوجب إنشاء بروتوكولات موثوقة لتأمين المعاملات الافتراضية وحماية الهوية. كما يمكن أن تشمل هذه التقنيات يضمن ذلك حماية المستخدمين من المخاطر وخلق بيئة آمنة للتفاعل.

- **دعم تقنيات الأمان السيبراني:**

ينبغي الاستثمار في تقنيات الأمان السيبراني لحماية المستخدمين من الهجمات والاختراقات. يمكن استخدام تقنيات متقدمة مثل الذكاء الاصطناعي والتعلم الآلي لتحليل

الأنماط المشبوهة والتنبؤ بالجرائم قبل وقوعها. كما يجب تعزيز الأمان في تصميم منصات الميتافيرس لتكون أكثر أمانًا.

- **رفع مستوى الوعي والتثقيف:**

تُعَدُّ التوعية من أهم الوسائل للتصدي للجرائم المرتبطة بالميتافيرس. ينبغي تنظيم حملات توعية تهدف إلى تعليم المستخدمين حول المخاطر المحتملة وكيفية التصرف في حال تعرضهم لجرائم معينة. يجب أن تضم هذه الحملات محتوى يسهل الوصول إليه ويعكس تجارب حقيقية لتعزيز الفهم والوعي. كما يجب أن تركز حملات التوعية العامة على أهمية الحذر في استخدام الميتافيرس. يجب أن تشمل هذه الحملات معلومات حول كيفية التعرف على المحتالين، وطرق حماية الخصوصية، وكيفية الإبلاغ عن الجرائم. ولأن التعليم والتوعية ضروريين لتمكين الأفراد من اتخاذ قرارات آمنة، كما ينبغي تخصيص موارد لتوعية المستخدمين حول المخاطر المرتبطة باستخدام الميتافيرس. يتطلب الأمر ورش عمل وحملات إعلامية تركز على كيفية حماية أنفسهم ومعلوماتهم الشخصية. فالمعلومات يمكن أن تشمل كيفية التعرف على الاحتيال، كيفية تأمين الحسابات، والتصرف في حالات الاعتداء.

- **تشجيع المشاركة المجتمعية:**

يجب أن تكون المجتمعات الافتراضية جزءًا من جهود التصدي للجرائم. يمكن تشجيع الأعضاء على الإبلاغ عن الأنشطة المريبة والمساعدة في تعزيز ثقافة الأمان. إن بناء شبكة دعم بين المستخدمين يسهم في تعزيز الوعي بالجرائم المحتملة وطرق الحماية.

- **تشجيع البحوث والدراسات الأكاديمية:**

إن القيام بأبحاث ودراسات مستمرة حول تطور الجرائم المرتبطة بالميتافيرس والتقنيات الناشئة ضروري لفهم التحديات المستقبلية وتقديم الحلول المناسبة؛ يجب على المؤسسات الأكاديمية ومراكز البحث التعاون مع الشركات التقنية لفهم سلوك المستخدمين وكيفية تحسين بيئات التفاعل الافتراضية. كما ينبغي تشجيع الأبحاث والدراسات حول

الجرائم في الميتافيرس الأمر الذي يساعد في فهم التطورات المستقبلية وكيفية التصدي لها، بالإضافة إلى إنشاء مجموعة من البيانات والمعلومات التي يمكن استخدامها لتطوير استراتيجيات أفضل.

ونافلة القول يتبين أن مواجهة الجرائم المرتبطة بالميتافيرس تتطلب جهدًا جماعيًا من الأطراف المعنية، بما في ذلك الحكومات، الشركات، والمجتمع المدني. بتبني هذه التوصيات، يمكننا العمل نحو بيئة أكثر أمانًا في الميتافيرس، مما يعزز من فوائد هذه التقنية الحديثة دون المخاطر المرتبطة بها.

كما تتبنى الباحثة التوصيات أشارت إليها أحد التقارير الدولية حول تهديدات الميتافيرس، والتي جاءت على النحو التالي:

(Gaming And The Metaverse ,2022:42-45)

- **الحكومات:**

يعد التنظيم الفعال أحد الأدوات المتاحة لغرض إطار منسق وشامل لسلامة الاطفال على منصات الألعاب الاجتماعية، ومنصات Metaverse، ويتعين على الحكومات استخدام هذه السلطة لتحقيق تكافؤ الفرص والتأكد من أن جميع المنصات توفر نفس المستوى الأساسي من سلامة المستخدمين، وسيتطلب ذلك من المشرعين والمنظمين إدراك الطبيعة المتغيرة للتقنيات، وتحديث متطلبات السلامة ليتناسب مع واقع العصر الرقمي الجديد. كما يجب تحديث المناهج الدراسية لتعليم الأطفال والمستخدمين السلوك المسئول في عالم ما وراء الطبيعة، وكيفية حماية أنفسهم.

- **المنصات:**

تحتاج المنصات إلى الارتقاء إلى مستوى واجبها في الرعاية ووضع السلامة في قلب عمليات تصميم وتطوير التجارب والتقنيات الرقمية. كما يجب على الشركات مع التطور التكنولوجي المستمر أن تتبنى نهج السلامة حسب التصميم، وتعزيز سلامة الأطفال ليس كفكرة لاحقة ولكن كجزأ لا يتجزأ من استراتيجية أعمالهم من أجل تقديم التجارب الممتعة والمفيدة حقًا للمستخدمين التي يعدونها.

ويجب على المنصات إتباع الخطوات التالية:

- الاستثمار في الحلول التقنية التي تعمل على تحسن سلامة الأطفال على منصاتهم.
- التعرف على تحديات السلامة ومعالجتها.
- التعاون مع المُبتكرين والانخراط في تحالفات صناعية لتبادل أفضل الممارسات وضمان المعايير المشتركة، وتسهيل الحوار مع المنصات الأخرى والجهات التنظيمية والمجتمع المدني (على سبيل المثال تحالف Tect- Wepro العالمي، وتحالف التكنولوجيا).
- **الآباء وأولياء الأمور:**

يحتاج الآباء إلى التعرف على عادات أطفالهم الرقمية والمخاطر المُرتبطة بها بنفس الطريقة التي يفهمون بها مخاطر العالم غير المتصل بالإنترنت، وسيتطلب ذلك منهم استثمار الوقت لفهم وتنفيذ تدابير السلامة المناسبة عند الضرورة.

ويجب على الآباء الالتزام بما يلي:

- الدراية بالألعاب والتجارب التي يشارك فيها المستخدمين.
- التعرف على أدوات الرقابة الأبوية المتوفرة على المنصات التي يتصل بها أطفالهم.
- فهم المخاطر الكامنة في بعض هذه المنصات.
- إعلام أنفسهم والدخول في حوار حول المخاطر والتدابير الوقائية مع أطفالهم.
- حث ممثليهم على دفع التنظيم الفعال في مجال سلامة الأطفال.
- **المستثمرون:**

يحتل المستثمرون مكانة رئيسة في تطوير منصات جديدة، حيث تعتمد الشركات على رأس المال الجديد لتحقيق أفكارهم النمو، حيث أظهرت السنوات الأخيرة القوى التي يتمتع بها المستثمرون في تحويل اهتمام الشركات نحو التحديات المناخية والاجتماعية،

حيث يحدد المستثمرون مؤشرات الأداء الرئيسة (KPIS)، والتي تستخدم لتقييم ما إذا كانت الشركة تعتبر ناجحة أم لا، ولتقييم القيمة المحتملة لمنصة معينة، يمكن استخدام هذه القوة لتضمين مؤشرات الأداء الرئيسة لسلامة الأطفال كجزء من تقييمهم.

وذلك من خلال خطوات وإجراءات محددة تتمثل في:

- دمج اعتبارات سلامة الطفال في استثماراتهم المستحقة.
- العمل بشكل استباقي مع المستثمرين من خلال تبادل المعرفة بين الشركات وتسهيل إنشاء أفضل الممارسات.
- وفق تدفق الأموال إلى المشاريع التي تعتبر سلامة المستخدمين من الأطفال والشباب مبدأ أساسيًا.
- **الباحثون:**

أن الطبيعة الجديدة للألعاب الاجتماعية ومنصات الميتافيرس والعديد من التقنيات الأساسية (مثل سماعات الواقع الافتراضي) يترك لنا العديد من الأسئلة المفتوحة، ما تأثير الميتافيرس على حياة المستخدم الاجتماعية؟ كيف يؤثر الوقت الطويل الذي يقضيه استخدام سماعات الواقع الافتراضي على صحة الأطفال والمستخدمين؟ كيف تؤثر التجربة الغامرة على النمو المعرفي والاجتماعي والنفسي للأطفال، لا سيما في سياق الاستغلال والاعتداء الجنسي؟ ما الأطر القانونية التي ينبغي تطبيقها على الجرائم في الميتافيرس؟

فنحن في حاجة إلى مجتمع البحث لتزويد الحكومات والمنصات والمجتمع بالإجابات على العديد من هذه الأسئلة التي سيكون لها تأثير كبير على كيفية إدارة هذه المساحات واستخدامها.

ويجب على الباحثون العمل على:

- البحث في تأثير التجارب الغامرة (الواقع الافتراضي والواقع المعزز) على نمو الطفل حسب العمر وخاصة تأثير التجارب المؤلمة مثل الاستغلال والاعتداء الجنسي على الأطفال.

- دراسة مستفيضة في حجم التعرض للاستغلال والاعتداء الجنسي على الأطفال على منصات الألعاب.

- دراسة أليات تطوير الأطر القانونية لملاحقة الجرائم في منطقة ميتافيرس.

بالإضافة إلى ما سبق يجب على أصحاب المصلحة إتباع الخطوات التالية والالتزام بالإجراءات والمسئوليات المحددة وتتمثل في:

- **ضمان السن:**

يجب أن يطلب من منصات الألعاب الاجتماعية تنفيذ أدوات ضمان السن حتى تتمكن من تحديد ما إذا كان هناك قاصرين على منصاتها. ويمكن لمنصات الألعاب الاجتماعية اختيار طريقة ضمان العمر التي تعتبرها مناسبة لمنصاتها. وينبغي السماح للجهات التنظيمية بالمطالبة بأساليب ضمان أكثر صرامة، على سبيل المثال إذا قررت أحدى المنصات الإعلان عن إنها منصة لمن هم فوق ١٨ عامًا.

- **تقييم المخاطر:**

ستسمح المعلومات المتعلقة بالتوزيع العمري للمنصات الاجتماعية بإجراء تقييمات المخاطر المستمرة المناسبة للعمر، وصياغة تدابير السلامة المضادة. مثل هذه التقييمات تعمل على تعزيز السلامة من خلال التصميم في جميع مراحل التطور، وينبغي أن يطلب من المنصات توثيق تدابير المخاطر هذه ومشاركتها مع الجهات التنظيمية عندما يطلب منها ذلك.

- **الوصول لمرتكبي الجرائم الجنسية:**

ينبغي للقوانين أن تحظر على مُرتكبي الجرائم الجنسية ضد الأطفال المسجلين على المنصات، والتي تجذب الأطفال بشكل خاص. ورغم أن التنفيذ يمثل حاليًا تحديًا تقنيًا؛ فإن التشريعات الحالية توفر مسارات للمضي قدمًا.

في المملكة المتحدة تتمتع المحاكم بالفعل بسلطة تنفيذ قدرة مرتكب جريمة جنسية مدان على الوصول إلى الإنترنت دون تثبيت برامج مراقبة الكمبيوتر.

إن إدراج منصات الألعاب الاجتماعية التي تركز على الأطفال في قائمة الأنشطة المحظورة لمرتكب الجرائم الجنسية، يوفر أيضًا لإنفاذ القانون السلطة التشريعية لمقاضاة وإنفاذ الانتهاكات المحتملة ضد هذا التنظيم.

- **تطبيق ضوابط وسائل التواصل الاجتماعي:**

إذا كانت خدمات الألعاب توفر وظائف مثل الدردشة والتواصل مع الأصدقاء، فإن جميع اللوائح المطبقة على وسائل التواصل الاجتماعي، مثل قانون حماية خصوصية الأطفال على الإنترنت في الولايات المتحدة أو توجيه التجارة الإلكترونية للاتحاد الأوروبي يجب أن تطبق عليها أيضًا.

- **القيود المناسبة للعمر:**

يجب أن تعرض المنصات والتقنيات الاجتماعية تجربة فريدة تعتمد على الفئة العمرية لمراعاة احتياجات السلامة المختلفة للفئات العمرية المختلفة. كما يجب دائمًا تشغيل مجموعة من وظائف السلامة الأساسية بشكل افتراضي لجميع القاصرين الذين تقل أعمارهم عن ١٣ عامًا ولا يتم رفعها إلا بموافقة الوالدين. ويجب أن تشتمل هذه بشكل خاص قدرة الغرباء على التواصل مع الأطفال في مساحات مشفرة وغير خاضعة للإشراف (على سبيل المثال الدردشة الصوتية غير الخاضعة للإشراف).

قائمة المراجع

أولًا: المراجع العربية:

- إبـراهيم، حنـان محمد الحسـيني أحمـد (٢٠٢٣): الإجـرام الميتافيرسـي، مجلـة العلـوم القانونيـة والسياسية، المجلد (١٢) العدد (٢).Doi: https://doi.org/10.55716/jjps.2023.12.2
- بكوش & هروال، محمد أمين وهبة (٢٠٢١): خصوصية المجرم الإلكتروني- مجرم الإنترنت نموذجًـا-، مجلـة البحـوث فـي الحقـوق والعلـوم السياسـية، المجلـد (٧) العـدد (١)، ص ٧٤-٨٣.
- البداينـة، ذيـاب موسـي & الخريشـة، رافـع (٢٠١٣): نظريـات علـم الجريمـة، المـدخل والتقيـيم والتطبيقات. دار الفكر، المملكة الأردنية الهاشمية.
- البداينـة، ذيـاب موسـي، (٢٠١٤): الجـرائم الإلكترونيـة، المفهـوم والأسـباب، الملتقـى العلمـي: الجـرائم المسـتحدثة فـي ظـل المتغيـرات والتحـولات الإقليميـة والدوليـة خـلال الفتـرة مـن ٢-٤ /٢٠١٤/٩، عمان، المملكة الأردنية الهاشمية.
- تقيـيم التهديـد العـالمي (٢٠٢٣): تقيـيم حجـم الاسـتغلال والاعتـداء الجنسـي علـى الأطفـال عبـر الإنترنت ونطاقها من أجل تقييم طبيعة الاستجابة، Weprotect Global AULANCE.
- دهشان، يحيى إبراهيم متولي (٢٠٢٢): جرائم الذكاء الاصطناعي وآليات مكافحتها مجلة روح القوانين، مجلد (٣٤)، العدد (١٠٠) أكتوبر.
- زايد، أحمد عبدالله (٢٠١٧): جرائم الكمبيوتر والإنترنت في المجتمع المصري: دراسة لأبعادها النفسية والاجتماعية والقانونية. القاهرة، المركز القومي للبحوث الاجتماعية والجنائية.
- الـزنط، يحـي عطـوة (٢٠٢٢): الممارسـات العمليـة لأمـن نظـم المعلومـات الحكوميـة ومنهجيـة مكافحة الجرائم السيبرانية. جامعة الدول العربية، لمنظمة العربية للتنمية الإدارية، القاهرة.
- سعيد، وليد سعد الدين محمد (٢٠٢٢): المسؤولية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي، المجلة العلمية لبحوث الإذاعة والتليفزيون، عدد (٤) عين شمس.
- سليمان وأخرون، محمد (٢٠٢٣): الميتافيرس، الفرص والتحديات الأمنية، سلسلة دراسات أمنية، جامعة نايف العربية للعلوم الأمنية.
- سـليمان، علـي حمـود، جمعـة وفتحـي، هبـة الله حمـد (٢٠٢٣): الآثـار النفسـية والاجتماعيـة للميتافيرس وعلاقتها بالترابط المجتمعي: دراسة ميدانية على عينة من المستخدمين والخبراء، المجلة المصرية لبحوث الرأي العام، مجلد (٢٢) العدد (٢) ١٨٣ – ٢٣٦ مسترجع من http://Search Mandumah.Com / Recard/ 1453593

- عبدالصادق، عادل (٢٠٢٢): أي تأثير الميتافيرس على مستقبل الإنسان في العصر الرقمي، مركز المعلومات ودعم اتخاذ القرار، أفاق مستقبلية، العدد (٢).
- العلوي & التوزاني، سكينة الأمراني، محمد (٢٠٢٣) مستقبل الذكاء الاصطناعي: الميتافيرس نموذجًا. مجلة القانون والأعمال، العدد (٨٨) ٢٥٦- ٢٧٨. مسترجع من http://search.mandumah.com/Record/1361491
- علي، مروة سليمان.(٢٠٢٢): إسهام نظرية الأنشطة الروتينية في فهم الجرائم السيبرانية: دراسة استطلاعية. المجلة المصرية للعلوم الاجتماعية والسلوكية. العدد السادس، أكتوبر.
- القنبري، محمد قيس عادل (٢٠٢١): المراجعة الداخلية في عالم ميتافيرس بين آفاق الواقع الافتراضي وإمكانيات الواقع المعزز منصة المراجعة الداخلية.
- مصطفى (٢٠١٥) خالد حامد: الشرعية الإجرائية بين حقوق الضحية والمتهم، مجلة الشريعة والقانون، العدد (٦١)، العدد (٤) جامعة عجمان، الإمارات العربية المتحدة.
- مصطفى، إسلام مصطفى جمعة (٢٠٢٢): الجرائم المرتكبة بمستخدم تقنيات التكنولوجيا الحديثة في القانون المصري (الواقع الافتراضي والواقع المعزز والمختلط)، مجلة كلية الشريعة والقانون، العدد (٣٨) الإصدار الأول ٢/١.
- الهيئة السعودية للبيانات والذكاء الاصطناعي، (٢٠٢٣): التقنيات الحديثة المعتمدة على البيانات والذكاء الاصطناعي، المملكة العربية السعودية.
- وثيقة الأمم المتحدة (١٩٩٧م/16/e/cn) الفقرة (أ) إعلان المبادئ الأساسية لتوفير العدالة لضحايا الجريمة وإساءة استعمال السلطة ١٩٨٥م، وتم الإشارة إليها فيما بعد باسم وثيقة الأمم المتحدة وعنوانها (A. conf/144/20).
- يحيي، ربيع محمد (٢٠٢٢): الميتافيرس الفرص والمخاطر وسيناريوهات المستقبل. الطبعة الأولى، الإمارات العربية المتحدة، مركز الإمارات للدراسات والبحوث الاستراتيجية.

ثانيًا: المراجع الأجنبية:

- Argun,Ugur&Murat Daglar (2016):Examination of Routine Activies Theory by the property Crime international Journal of Human Scinces.vol (13) Issue 1,ISSN
- Bale , Ajay sudhir (et. al), (2022): A Comprehensive study on Metaverse and its Impacts on Human – computer Intevaction Volume 2022, Article ID3247060, 11 Pages **https:// doi. Org/ 10. 1155/2022/3247060. P. 1-11**.
- Berastegui,Pierre,(2024):Working in the Metaverse:what are the risks ? European Economic Employment and Social Developments, (ETUI) www.etui.org/publications.
- Blake, John, (2024):Online Crime In the Metaverse ,Astudy onClassification,Predication,andMitigation Strategies. **Doi:10.4018/979-8-3693-0220-0.ch004.**
- Council of Europe and EEEI ,SA (2024):The metaverse and its impact on human rights the rule of law and democracy.Information socity deparment .
- Cristea,Andi-Lucian,(2023): Risks and opportunities of the Metaverse.Committee On Culture,Science Education and Media.Council of Europe.
- DAWES CENTER ROR FUTURECRIMEATUCL, (2024):Crime Facilitated by the Metaverse (s) Dawes.

  https://doi.org/10.1016/j.futures.2024.103338. DRCF, (2023): Immersive Technologies Foresight Paper.
- Elliptic Metaverse Report, (2022): The Future Of Financical Crime In The Metaverse,Fighting Crypto-Crime In Web 3.0.ELLIPTIC.
- EUROPOL, (2022): Policing in the Metaverse: Whet law enforcement needs To know, An Observatory Report From the Europl innovation Lab. leuxembourg: bubli Cutions office of the European Union, Doi: 10. 1813/82062.
- Gaming and the Metaverse ,the alarming Rise of Online Sexual Exploitaion and Abuse of Children Within the new digital frontier.(2019), Bracket Capital & UNICRI.
- Gomes – Quintero, Juliana [et. al] ,(2024): A Scoping Study of crime Facilitated by The Metaverse.Futures157 (10338), **https: //doi.Org/10.1016/j.Futaverse 2024. 10333. P.1 – 22.**

- Haber,Eldar,(2024): The Criminal Metaverse,Indiana law Journal: Vol (99) Issue3,**https://www.Repository:Law. indiana.edu/ilj/vol99/iss314.**
- Henz, Patrick(2022): The Social Im Poct of the Metaverse. Discover Avtifical Intelligence 2-19.**https://doi.Org/10.1007/544163-022-00032-6.**
- Hinz, Michael, (2023);Risks the Metaverse Poses For Children and Adolescents:An Exploratory Content Analysis , The Netherland. **https: doi.org / 10.1016/ j.futures 2024. 103338.**
- https://www.unodc.org/e4j/ar/cybercrime/module-1/key-issues/cybercrime-in-brief.html.\ https://datareportal.com/reports/digital-2025-global-overview-report، وقت الزيارة ٢٨ يناير الساعة ١٠:٣٠م
- Huq,Numaan,[et.al],(2022); Metaverse Or Metavers Cybersecurity threats Against the Internet of Experiences. Trend MicroResearch. Management Framework International, Journal of Cyber.
- Hsieh, Ming-Li,& Wang, S.Y.K (2018): Routina Activities in avirtual Space: International journal of cyber Criminology,12(1),333-352**.** **doi:10.5381/zenodo.495776**.
- Marshall,AngusMckenzie& Tompsetl ,Brian Charles (2023):The Metaverse – Not a New Frontier For Crime WIRES Forensic, Wilau**.** **Doi: 10.1002/ WFS 2. 1505.**
- Mclntosh,Verity(2024):What do policy makersneed to Know about harassment in the metaverse ? Digital Cultural Research Centre,University of the west of England ,Bristol ,United Kingdom.
- Minpark,Sang&Gabkim,young,(2022):Ametaverse:Taxanomy Components, Applications, and open challenges.
- Miro,(2014): The Encyclopediab of Theoretical Criminology. https://onlinelibrary.wiley.com/doi/full/10.1002/9781118517390.wbetc19
- National research Foundation of Korea.IEEE acces Multidis ciplinany:National Research foundation of Korea. IEEE Access Multidisciplinary: Rapid Review: open Access. Journal **10.1109/Access.2021.3140175**.
- Ortiz, Laur (2022):Rsks of the Metaverse" A VRChat Study Case.The Journal of Intelligence Coflict and warfare 5(2)53-128**.** **Doi:10.21810/jicw.v5i2.5041**

- Rapid Review: open Access Journal 10. 1109/ Access. 2021. 3140175.
- Responsible Metaverse Alliance,(2023): policing in the Metaverse: Prevetion, Disription, and Enforcement Challenges, Discussion Paper 1of 3 Policing in the Metaverse.
- Rickli, jean-marc& Mantellassi, Fedrrico,(2022): Our Digital Future: The Security Implication of Metaverse. Geneva Centre for Security Policy. Issue (24) ,www.gcs.ch.
- Singh, Prabal Pratap,(2024): Cyber Crimes in metaverse, International Journal of science and Research (IJSR) Volume (13) Issue (2), P. 93-96.

  Doi:https://dx.doi.Org/10. 21275/ Mr24130195237.
- Smaili, Nadia & Raymond, Audrey de Rancourt (2024): Metaverse: Welcome to the new fraud marketplace, Journal of financial crime. Vo1. 31 No. 1. Emerald publishing limited. 188 – 200. **Doi. 10. 1108/ JFC – 06 – 2022- 2024**
- Stavola, J & Chol, Kyung-shick,(2023):Victimization by Deepfake in the metaverse: Building a Practical Mangement Framework. Interenational Journel of Cyber security Intelligince and Cyber crime, Vo1 6, ISSN 2 Page 3-20 **Doi:https://doi.Org.110.52366/2578- 3289.1171**
- UNICEF,(2023):Metaverse Extended Reality and Children. United Nations Childrens fund ,UNICEF.
- Wang, yuntao & Su, Zhou &Yan,Miao:(2023)Social Metaverse: Challenges And Solution, IEEE Internet Of Things Magazine ,china.
- Wang,Yuntao[et.al,] (2022): Asurvey On Metaverse Fundamentals, Security and Privacy **arXiv:2203.02662V4[ES,C R].**