الجرائم السيبرانية في الميتافيرس

"نحو استراتيجيات قانونية فعالة"

د. هاله محمد إمام

أستاذ مساعد كلية إدارة الاعمال- قسم الأنظمة- جامعه نجران

drhalaemam@gmail.com

hmemam@nu.edu.sa

(ISSN: 2537 - 0758)

الجرائم السيبرانية في الميتافيرس
"نحو استراتيجيات قانونية فعالة"

د. هاله محمد إمام

الملخص:

يشكل التطور السريع للتكنولوجيا في العصر الحديث وظهور الإنترنت أساساً لتغيير العديد من جوانب حياتنا. ومع ذلك، فإن هذه التطورات قد جلبت معها مشاكل وتحديات جديدة، أبرزها جرائم الميتافيرس التي تهدد أمن الأفراد والمؤسسات. يهدف هذا البحث إلى تحليل خطورة جرائم الميتافيرس وتأثيرها على الأمن السيبراني، بالإضافة إلى استعراض الحلول والتدابير الفعالة للتصدي لها والحد من انتشارها.

تُعتبر جرائم الميتافيرس من التحديات الأمنية الحديثة التي يجب على المجتمع العالمي مواجهتها بفعالية. تشمل هذه الجرائم استخدام التكنولوجيا لتنفيذ أنشطة غير قانونية تهدد الأمن السيبراني وتسبب خسائر كبيرة، مما يجعلها واحدة من أبرز التحديات التي تواجه المجتمعات المعاصرة. تمثل هذه الجرائم نوعاً من الجرائم المعلوماتية التي تعتمد على استخدام التكنولوجيا الحديثة لارتكاب أفعال إجرامية في الفضاء الرقمي.

تتميز الجريمة الافتراضية بالتطور السريع والتعقيد المتزايد، مما يتطلب من الباحثين والمتخصصين دراسة طبيعتها وأسبابها وتأثيراتها على المجتمع والأفراد. يعد فهم هذه الجرائم وآلياتها من التحديات المهمة في مجال الأمن السيبراني لضمان حماية فعالة للمعلومات والأنظمة الرقمية. تهدف هذه الدراسة إلى تسليط الضوء على الظاهرة المتزايدة للجريمة الرقمية وتحليل أبعادها وتأثيراتها الاجتماعية والاقتصادية والقانونية.

تُعتبر الميتافيرس منصة رقمية متطورة تجمع بين الواقع الافتراضي والعالم الحقيقي، مما يخلق بيئة مبتكرة تسمح بتفاعل المستخدمين عبر الشبكات الإلكترونية. تشكل هذه البيئة تحدياً للأمن والقانون، حيث يمكن أن تحدث فيها أنواع متعددة من الجرائم. تهدف هذه الورقة البحثية إلى تحليل الأطر القانونية المتاحة لمكافحة جرائم الميتافيرس وفهم كيفية التصدي لهذه الظاهرة بفعالية.

الكلمات المفتاحية: الميتافيرس، جرائم، خطورة.

Cybercrime in the metaverse" Towards effective legal strategies"

Summary:

The rapid development of technology in modern times and the emergence of the Internet form the basis for changing many aspects of our lives. However, these developments have brought with them new problems and challenges, most notably metaverse crimes that threaten the security of individuals and institutions. This research aims to analyze the seriousness of metaverse crimes and their impact on cybersecurity, in addition to reviewing effective solutions and measures to address them and limit their spread.

Metaverse crime is one of the modern security challenges that the global community must effectively address. These crimes include the use of technology to carry out illegal activities that threaten cybersecurity and cause significant losses, making it one of the most prominent challenges facing contemporary societies. These crimes represent a type of information crime that relies on the use of modern technology to commit criminal acts in the digital space.

Virtual crime is characterized by rapid development and increasing complexity, which requires researchers and specialists to study its nature, causes and effects on society and individuals. Understanding these crimes and their mechanisms is an important challenge in the field of cybersecurity to ensure effective protection of information and digital systems. This study aims to shed light on the increasing phenomenon of digital crime and analyze its social, economic and legal dimensions and impacts.

The metaverse is a cutting-edge digital platform that combines virtual reality and the real world, creating an innovative environment that allows users to interact over electronic networks. This environment poses a challenge to security and law, as multiple types of crimes can occur. This paper aims to analyze the legal frameworks available to combat metaverse crime and understand how to effectively address this phenomenon.

Keywords: metaverses, crimes, seriousness.

(ISSN: 2537 - 0758)

المقدمة

تُعتبر الميتافيرس من أحدث التطورات التكنولوجية التي تُحدِث تحولاً شاملاً في كيفية تفاعل البشر مع العالم الرقمي. فهي تمثل بيئة افتراضية ثلاثية الأبعاد يمكن للأفراد دخولها والتفاعل فيها من خلال شخصيات ثلاثية الأبعاد، مما يفتح آفاقاً جديدة للتواصل والتجربة الإنسانية. في عصرنا الحالي، أصبحت هذه البيئة الافتراضية أكثر أهمية من أي وقت مضى، حيث تبرز الفرص والتحديات المتعددة، ومن بين هذه التحديات تُعد جرائم الميتافيرس موضوعاً محورياً يتطلب التصدي له فهماً عميقاً للمفاهيم والحلول المتاحة.

تُعتبر الجريمة الرقمية أو الافتراضية من التحديات الحديثة التي ظهرت مع زيادة انتشار تكنولوجيا المعلومات والاتصالات. تعتمد هذه الجرائم على استخدام التكنولوجيا الحديثة لتنفيذ أنشطة غير قانونية تستهدف الأفراد أو المؤسسات أو المجتمعات بشكل عام. تشمل الجريمة الرقمية مجموعة واسعة من الأنشطة الإلكترونية غير القانونية، مثل الاحتيال الإلكتروني، اختراق الأنظمة، توزيع البرمجيات الخبيثة، التحريض على الكراهية، والتحرش الإلكتروني، بالإضافة إلى جرائم مثل سرقة الهوية، انتشار الأخبار الزائفة، والتشهير عبر الإنترنت، والتنمر.

يُعتبر التحرش الإلكتروني نوعًا جديدًا من السلوك المنحرف، حيث تُستخدم التكنولوجيا للتحرش بالآخرين بطرق متنوعة. ومع الاعتماد المتزايد على الإنترنت، والبريد الإلكتروني، والرسائل الفورية، وغرف الدردشة، أصبحت هذه المشكلة الاجتماعية تنمو بشكل ملحوظ، مما يؤثر على مستخدمي الكمبيوتر في جميع أنحاء العالم. لقد أدت التكنولوجيا الجديدة إلى تغييرات جذرية في حياتنا، مما يسهل إساءة استخدامها لتخويف وإكراه واستهداف الأشخاص.

على الرغم من أن التحرش الإلكتروني غالباً ما يتضمن شخصاً واحداً يلاحق آخر، إلا أن الأمر لا يقتصر على ذلك. فقد تطور هذا السلوك ليشمل أفعالاً مثل الاحتيال في سوق الأوراق المالية، وسرقة الهوية، والتحرش الجنسي، وسرقة البيانات، وتقمص الشخصيات، والاحتيال على المستهلكين، ومراقبة الحواسيب، وهجمات من قبل جماعات سياسية على خدمات الحكومة. والأكثر إثارة للقلق هو استخدام المواقع الإباحية والمتحرشين بالأطفال للتحرش الإلكتروني كوسيلة للعثور على ضحايا جدد.

أهداف البحث:

يهدف هذا البحث إلى التعرف على مفهوم جرائم الميتافيرس وتحليل أنواعها المختلفة، بالإضافة إلى دراسة تأثيراتها على المجتمع والفرد. كما يسعى البحث إلى تحليل الأطر القانونية المتاحة لمكافحة هذه الجرائم، مع اقتراح التدابير والسياسات اللازمة للوقاية منها والتصدي لها بفعالية.

أهمية البحث:

تتسبب جرائم الميتافيرس في تسريب البيانات الحساسة، والابتزاز الرقمي، وانتشار الأخبار الكاذبة، والتأثير على عمليات الانتخابات، بالإضافة إلى الاختراقات الهجومية والتحرش الافتراضي، مما يؤدي إلى آثار كارثية على الأفراد والمؤسسات والحكومات. تشكل هذه الجرائم خطورة كبيرة على الفرد والمجتمع، مما يجعل الموضوع محورًا هامًا للبحث والدراسة، يهدف البحث إلى وضع الحلول القانونية اللازمة للتصدي لهذه الجرائم من خلال فرض عقوبات رادعة والعمل على الحد منها نظراً لخطورتها.

منهج البحث:

استخدمت الباحثة المنهج الوصفي التحليلي، لوصف تلك الجرائم مع تحليل لأسباب انتشارها وطرق التصدي لها في ضوء التشريعات القانونية الحالية مع، وضع أطار مقترح للتشريعات الواجب صدورها لمواجهه هذا النوع من الجرائم المستحدثة.

خطة البحث:

الفصل الأول: جرائم الميتافيرس خطورتها وتأثيراتها علي الفرد والمجتمع.

الفصل الثاني: جرائم الميتافيرس في ضوء التشريعات وطرق التصدي لها.

الفصل الأول

جرائم الميتافيرس خطورتها و تأثيراتها علي الفرد و المجتمع

تمهيد:

يعود مصطلح الميتافيرس إلى الروائي نيل ستفنسون في روايته تحطم الثلج سنة ١٩٩٢ والذي يعبر فيه عن عالم افتراضي يتفاعل فيه البشر، وسبق كذلك رواية Ready Player One للمؤلف ارنست كلاين الذي تم تحويله إلى فيلم سينمائي عام ٢٠١٨ والذي تدور أحداثه في عام ٢٠٤٥ حيث يهرب فيه مراهق يهرب من عالمه

(ISSN: 2537 - 0758)

الكئيب إلى عالم آخر افتراضي بالكامل، وكذلك فيلم Summer Wars والذي هو فيلم كرتوني تدور أحداثه حول عالم افتراضي.

إن كلمة "ميتافيرس تجمع ما بين الكلمة الأولى هي "ميتا– (Meta) والتي تعني ما وراء، أما الكلمة الثانية فيرس (Verse) وهي كلمة تعني من العالم أو الكون، وبذلك يكون الاسم الكامل الكون الماورائي"، أو ما بعد الكون. هي في الأساس تكنولوجيا قديمة للواقع الافتراضي كان يستعملها الأطباء للتدريب على العمليات الجراحية، وكذا مساعدة الطيارين التدريب على القيادة[١].

أولا: تعريف الميتافيرس (العالم الافتراضي):

العالم الافتراضي هو عبارة تكنولوجيا تتيح إنشاء بيئة مشابهة للحقيقة بواسطة الحاسب الآلي وذلك بواسطة شاشة الحاسوب أو السماعات المجسمة للصوت أو النظارات و الأدوات الأخرى،وهي تعتمد على تقديم صورة مشابهة جدا للواقع في أماكن لا يمكن للإنسان الوصول إليها أو إنشاؤها[٢].

لا يوجد إجماع بشأن تعريف مصطلح الميتافيرس. ومع ذلك، لقد بذل العديد من العلماء محاولات لتعريفه. على سبيل المثال.

قام البعض بتعريف الميتافيرس على أنها بيئة افتراضية ثلاثية الأبعاد، وهو ما يتناقض مع المفهوم الأكثر شمولاً للفضاء الإلكتروني الذي يشمل جميع المساحات المشتركة عبر الإنترنت عبر جميع أبعاد التمثيل. وقد أكد علماء آخرون على البعد التجريبي للميتافيرس، الذي يسمح للناس بعيش محتوى الإنترنت مع الآخرين[٣].

يُعَدُّ الواقع الافتراضي اتصالًا يُنظر إليه كتفاعل بين شخصين أو أكثر، ويمكن أيضًا أن يكون الاتصال بين الإنسان والتكنولوجيا، وهو مكون أساسي كأساس للواقع الافتراضي. وهو العلاقة بين المستخدم والمحتوى، حيث يتم التركيز فيها على التجربة

---

[١] زعتر، نور الدين (٢٠٢٢) العالم الافتراضي الميتافيرس Metaverse" من منظور سيكولوجي. مجلة العلـــــــــــــــوم الإنســـــــــــــــانية مـــــــــــــــج ٩ ٢ ١٠٢٩ – ١٠١٦، .Record/com.mandumah.search//:http,1017p/1285730

[2] The VR Book human-centered design for virtual reality books, Jason Jerald, 2016, part 1, Chapter 1, page 7.

(3)Dionisio, J.D., Burns, W.G., & Gilbert, R. (2013). 3D Virtual worlds and the metaverse: Current status and future possibilities. ACM Comput. Surv., 45, 34:1-34:38. p 1-38 https://doi.org/10.1145/2480741.2480751

بدلاً من التكنولوجيا. والفرق بين البيئات الافتراضية والبيئات الواقعية هو التجريد الحسي، حيث تكون أكثر عرضة لاختبار الحياة الواقعية، بحيث يمكنك بشكل بسيط التحكم في كل شيء. وبناءً على ذلك، تستطيع أيضا الشخصيات غير القابلة للعب الشعور بأنها أقرب أن تستطيع اجتياح الفضاء الشخصي للمستخدم، مما يجعل الأمر مربكا في بعض الأحيان، باستخدام أجهزة الحاسب الآلي والمعدات الحسية المختلفة مثل سماعات الرأس والقفازات. ولا تقتصر تطبيقات الواقع الافتراضي على مجال الترفيه والألعاب فقط، بل تستخدم أيضا في مجال التعليم والطب فمثلا يقوم الجراحون بالتخطيط لعملياتهم والتدرب عليها، كما يمكن أيضا أستخدمها في المجال العسكري من أجل محاكاة بعض التدريبات العسكرية ضمن ظروف قاسية.

ثانيا: **العالم المختلط بين الواقع الافتراضي والمعزز**:

هو ما يجمع بين العالم الحقيقي والعناصر الرقمية. ومن خلاله، يمكنك التفاعل والتحكم بالعناصر المادية والافتراضية باستخدام تقنيات توليد الخيال والشعور. يتيح لك الرؤية والتدخل في العالم من حولك حتى ولو كنت تتفاعل مع بيئة افتراضية باستخدام يديك دون خلع سماعات الأذن. يمكنك من امتلاك رجل أو يد واحدة في العالم الحقيقي وأخرى في عالم وهمي. يتجاوز المفهوم التقليدي للحقيقة والوهم، ويمنحك تجربة قد تغير الطريقة اليومية التي تلعب أو تعمل به[٤].

الميتافيرس عالم افتراضي موازٍ للعالم المادي، لكن الاختلاف الرئيسي بين الحياة في العالم المادي والحياة في الميتافيرس يكمن في حقيقة أنه في الأخير، يتفاعل الأشخاص مع أفراد أو أشياء أخرى من خلال تمثيلات افتراضية لأنفسهم، تُعرف باسم الصور الرمزية. يمكن تعريف الصور الرمزية بأنها" أي تمثيل رقمي (رسومي أو نصي) له قوة (القدرة على تنفيذ الإجراءات) ويتم التحكم فيه بواسطة وكيل بشري في الوقت الفعلي، فإن الصورة الرمزية هي في الأساس صورة معكوسة لمستخدم الميتافيرس من البشر الموجود في العالم الحقيقي، ويتم ربط هذه الصورة بشكل مباشر والتحكم فيها من

---

[٤] جمعة مصطفى، إ. (٢٠٢٣). الجرائم المرتكبة باستخدام تقنيات التكنولوجيا الحديثة في القانون المصري (الواقع الافتراضي والواقع المعزز والمختلط) Crimes Committed Using Modern Technology Techniques In Egyptian Law (Virtual Reality, Augmented And Mixed Reality). مجلة كلية الشريعة و القانون بطنطا، ٣٨(١)، ١٩p.

(ISSN: 2537 - 0758)

قبل المستخدم من خلال المعدات المستخدمة وتأخذ الأنشطة البشرية داخل الميتافيرس نفس شكل تلك الموجودة في العالم المادي، مثل شراء أو بيع العقارات الافتراضية، أو حضور الحفلات الموسيقية الافتراضية، مثل السباق في بطولة خيول[٥].

ثالثا: **الشخصية الافتراضية داخل العالم الإلكتروني**:

نلاحظ أن الشخصية الافتراضية في العالم الالكتروني شخصية لها كيان واستقلال منفرد. وعلى الرغم من ذلك فأنها لا تمكن أن تكون تمثيل لمبدأ الإرادة الحرة، فالوصف القانوني للشخصية الافتراضية داخل العالم الإلكتروني يعد مسألة هامة تتعلق بتحديد الحقوق والواجبات المتعلقة بتلك الشخصيات والتي تتفاعل وتعيش في بيئة رقمية. تعتمد هذه القضية على القوانين والتشريعات المعمول بها في كل بلد وتتطلب دراسة دقيقة لهذه القوانين وتطبيقاتها في سياق العوالم الرقمية ففي العوالم الافتراضية، تمثل الشخصية الرقمية الكيان الذي يمثل الفرد داخل هذا العالم، ولها مظهر، وهوية، وتفاعلات كما لو كانت حقيقية، لكن يظل السؤال المهم وهو كيف يتم التعامل القانوني مع هذه الشخصية الرقمية؟

بعض القوانين قد بدأت تعترف بالشخصية الرقمية وتنظر إليها على أنها كيان قانوني بحد ذاته. يمكن أن تتضمن حقوقها وواجباتها القانونية الحماية من الاستخدام غير المصرح به، والخصوصية الرقمية، وحماية الملكية الفكرية فيما يتعلق بالمحتوى الذي تنشره.

من الجدير بالذكر أن هذا المجال متطور بسرعة، وتتغير القوانين باستمرار لتكييفها مع التطورات التكنولوجية الجديدة. لذا، يجب أن تكون هناك جهود مستمرة لدراسة وتحديث التشريعات والتنظيمات لتوفير الحماية اللازمة للأفراد والمجتمعات داخل العوالم الرقمي تثار تساؤلات كثيره حول الحقوق القانونية المتعلقة بها.

رابعا: **حماية البيانات والخصوصية في العالم الافتراضي**:

تعتبر حماية بيانات الشخصيات الرقمية وخصوصيتها أمرًا بالغ الأهمية. يجب أن تكون هناك قوانين ولوائح تضمن حماية بياناتها ومنع الوصول غير المصرح به. وتعتبر

---

[٥] Earth2 التاريخ غير معروف) https://app.earth2.io/#thegrid/d3817c93-9b25-4e8e-9acc-fe718e416b22. تم الوصول إليه في ١٨ نوفمبر ٢٠٢٢

الخصوصية وخطر الاختراق في العالم الافتراضي هما مسألتان تتصاعدان في مجال الأمان السيبراني وانتهاكات الخصوصية. إذ تُشكّل البيئة الرقمية بيئة خصبة لهجمات الاحتيال والتلاعب ونشر الشائعات. وهناك أيضًا مراقبة ورصد لجميع الأنشطة الإلكترونية للمستخدم، حيث تم تطوير تقنيات لتتبع حركات اليد والعين لجمع بيانات بيو مترية خاصة بالمستخدم واستخدامها. وبالتالي يمكن استهداف المستخدم بإعلانات مستهدفة تتناسب مع شخصه واهتماماته. وبشكل عام، يمكن أن نقول أننا سنكون عرضة للكشف التام في عالم الميتافيرس، وتزداد خطورة مستلزمات هذا العالم إذا تم تطوير موصلات ومستشعرات إلكترونية تُزرع في الجسم والجهاز العصبي لقراءة الموجات الكهربائية للإنسان. ذلك يمكنها جعل الإنسان مكشوفًا تمامًا وعرضة للتأثير، وهذا هو ما يعمل عليه رائد الأعمال إيلون ماسك. ويجعل وجود البنية التحتية المادية للعوالم المتعددة في يد مجموعة من الشركات التكنولوجية الكبرى الأمور تحت سيطرة مخفية تجعلها عرضة للاستغلال وقد تكون موضوعًا للابتزاز والصراعات السياسية والأيديولوجية[٦].

والجدير بالذكر أن حقوق الملكية الفكرية مثل حقوق النشر والعلامات التجارية، التي تحمي المحتوى الذي يتم إنشاءه ونشره بواسطة الشخصية الرقمية. لذلك يجب تحديد المسؤولية القانونية للشخصيات الرقمية، بما في ذلك التصرفات والأفعال التي يمكن أن تؤثر على الآخرين أو تتسبب في أضرار.

خامسا: الانتهاكات داخل بيئة الميتافيرس:

يجب وضع عقوبات وتدابير قانونية للتصدي للانتهاكات ضد الشخصيات الرقمية، مما يشمل الاستخدام غير القانوني أو السرقة الإلكترونية، وبعد أن أصبح الواقع الافتراضي والواقع المعزز جزءًا لا يتجزأ من واقعنا المعاصر. ويعود ذلك إلى أن ما كان في السابق خيالًا علميًا أصبح الآن جزءًا من العالم الحالي. فعلى الرغم من أن بعض الجرائم قد لا تكون معروفة لدى مطوري البرامج أو غير موجودة، إلا أنها قد تكون محتملة في المستقبل نظرًا للتقدم التكنولوجي وتطوره، وتعتمد الأمور على ما ينص عليه القوانين واللوائح داخل الدولة، إذا ما كان الفعل يعد جريمة أم لا، وبعض الأفعال قد

[٦] زعتر، نور الدين (٢٠٢٢) العالم الافتراضي الميتافيرس Metaverse" من منظور سيكولوجي. مجلة العلوم الإنسانية مج.

(ISSN: 2537 - 0758)

تعتبر جريمة في بلد معين، بينما تمثل جريمة مكتملة الأركان في بلد آخر ويتوجب هنا تحديد مبدأ شرعية الجرائم والعقوبات، ومبدأ سريان القانون من حيث المكان وتنازع الاختصاص[٧].

سادسا: **تعريف جرائم الميتافيرس**:

بعد دخول الملايين من الأشخاص إلى ميتافيرس واستكشاف ميزاته، أصبح من المتوقع أن يظهر شكل جديد من أشكال الجريمة، يُعرف باسم جرائم الميتافيرس ويختلف هذا الشكل الجديد من الجريمة عن الجرائم التقليدية والجرائم السيبرانية .يمكن أن تتخذ جرائم الميتافيرس أحد ال شكلين اما الجرائم ضد الصور الرمزية في الميتافيرس،أو الجرائم المرتكبة ضد مستخدمي الميتافيرس والتي تسبب ضررًا جسديًا .ومن منظور قانوني، ومن هنا يثير هذا تساؤلات حول اختصاص القوانين وتنظيمها وإنفاذها في العوالم الافتراضية .يسلط ظهور جرائم الميتافيرس الضوء على الحاجة إلى اتخاذ إجراءات استباقية لمنع وتخفيف مثل هذا النشاط الإجرامي.[٨]

جرائم الميتافيرس أو الجريمة الافتراضية هي أي نشاط غير قانوني يتم تنفيذه عبر الإنترنت، مثل الاحتيال، والتجسس، والتهديد، والتشهير الرقمي، واختراق الأمان، وتوزيع البرمجيات الخبيثة، وغيرها، بهدف الحصول على مكاسب غير مشروعة أو التسبب في ضرر للأفراد أو المؤسسات. هذه الأنشطة تشمل استخدام التكنولوجيا والأنظمة الرقمية لارتكاب جرائم والتلاعب بالبيانات والمعلومات[٩].

---

[٧] جمعة مصطفى، إ. (٢٠٢٣). الجرائم المرتكبة باستخدام تقنيات التكنولوجيا الحديثة في القانون المصري (الواقع الافتراضي والواقع المعزز والمختلط) Crimes Committed Using Modern Technology Techniques In Egyptian Law (Virtual Reality, Augmented And Mixed Reality). مجلة كلية الشريعة والقانون بطنطا.51-2 ,38(1) ,

[٨] علي، أحمد عمرو، خليفة & ,ماهينور محمد. (٢٠٢٣). أركان الجريمة في الميتافيرس: دراسة في ضوء أحكام القانون الجنائي المصري .*المجلة الدولية للفقه والقضاء والتشريع*-735 ,(2)4 , p.٧٤٩755.

[9] Bocij, P., McFarlane, L., & McNally, R. (2012). Cyberstalking: Harassment in the Internet age and how to protect your family. ABC-CLIO

إن Metaverse، وهو عالم افتراضي يستخدم تقنيات غامرة مثل الواقع الافتراضي والواقع المعزز، لديه القدرة على إحداث ثورة في التفاعل البشري مع التكنولوجيا ومع بعضهم البعض، ولكنه يثير مخاوف أخلاقية بشأن الخصوصية والإدمان[١٠].

الجريمة الإلكترونية يمكن تحديدها على أنها الأفعال ذات الصلة الجنائية التي ترتكب باستخدام شبكات البيانات (وخاصة الإنترنت) يتمثل الجرائم الإلكترونية الكثيرة في اختراق الأجهزة وسرقة المعلومات، وكذلك احتيال البطاقات الائتمانية عبر الإنترنت والعديد من الأنواع الأخرى[١١]. يمكن القول بأن مفهوم الميتافيرس هو مصطلح يشير إلى بيئة رقمية ثلاثية الأبعاد تتيح للمستخدمين تفاعلًا مشابهًا للواقع الحقيقي. تشمل هذه البيئة العناصر الافتراضية مثل العوالم الافتراضية، والشخصيات، والأشياء، والتفاعلات بين المستخدمين.

يثار التساؤل هام جدا عن القانون الواجب التطبيق على المواقع الإلكترونية على شبكة الإنترنت، وتطبيقا للقواعد التي تحكم الاختصاص المكاني للجرائم، حيث أن جرائم الانترنت عابرة للحدود تخضع في كثير من الأحيان لأكثر من قانون، فإذا وقع السلوك في نطاق بلد معين والآثار الضارة التي تحققت في نطاق بلد آخر،فإن كلا البلدين يكون قانونه واجب لتطبيق على الواقعة. فلا يوجد مفهوم محدد يسمى "جرائم الميتافيرس". فهي قد يطلق عليها "جرائم الإنترنت" أو "جرائم الحاسوب"، والتي تشير إلى أنشطة إجرامية تتعلق بالتكنولوجيا والحوسبة والإنترنت.

وعلية يمكننا أن نقترح تعريف جرائم الميتافيرس بأنها (تلك الجرائم التي تقع داخل البيئة الافتراضية، وتشكل اعتداء بأي شكل من الأشكال عن حقوق و حريات الأفراد داخل تلك البيئة، تستوجب العقاب)، وعلية يمكننا استعراض أهم أنواع تلك الجرائم فيما يلي.

---

(10) A, J., Khanum, A., A, S., S, A., Latheef, A., & S, D. (2023). METAVERSE. *International Journal of Innovative Research in Information Security*. https://doi.org/10.26562/ijiris.2023.v0903.29.

(11) Laue, C. (2011). Crime potential of metaverses. In Springer eBooks (pp. 19–29). https://doi.org/10.1007/978-3-642-20823-2_2

(ISSN: 2537 - 0758)

سابعا: **أنواع الجرائم في الميتافيرس**:

تشمل جرائم الإنترنت مجموعة واسعة من الأنشطة الإجرامية التي تتعلق بالتكنولوجيا والحوسبة، وتشمل منها ولكن لا تقتصر على الاحتيال الإلكتروني، الاختراقات السيبرانية، الهجمات الضارة، سرقة البيانات، التجسس الإلكتروني، والتشهير على الإنترنت.

تتنوع الجرائم في الميتافيرس وتشمل عدة أنواع كثيره، منها على سبيل المثال:

١- **السرقة الرقمية:** اختراق الأمان الرقمي وسرقة البيانات الشخصية أو الأموال الرقمية.

التحرش والاعتداء الرقمي: التحرش أو الاعتداء على الآخرين داخل الميتافيرس[١٢].

٢- **الاحتيال والغش:** استخدام التلاعب والخدع للحصول على مكاسب غير مشروعة داخل الميتافيرس.

٣- **انتهاك حقوق الملكية الفكرية:** نسخ أو استخدام غير مصرح به للمحتوى المحمي بحقوق الملكية الفكرية داخل الميتافيرس[١٣].

ثامنا: **تأثيرات جرائم الميتافيرس**:

تأثيرات جرائم الميتافيرس تتضمن تأثيرات اقتصادية واجتماعية ونفسية. على الصعيدين الاقتصادي والاجتماعي، يمكن أن تؤثر هذه الجرائم بشكل كبير على الثقة في البيئة الرقمية والتجارة الإلكترونية، مما يؤثر على النمو الاقتصادي والثقافي. بالإضافة إلى ذلك، قد تؤدي جرائم الميتافيرس إلى زيادة مستويات التوتر والقلق النفسي لدى الأفراد والمجتمعات، نتيجة للانتهاكات الخصوصية والاختراقات والتلاعب بالبيانات الشخصية.

تاسعا: **خطورة جرائم الميتافيرس**

مع تزايد عدد مستخدمي الميتافيرس، سيتم ارتكاب جرائم باستخدام هذه التكنولوجيا، على غرار ما حدث مع الاستخدام الواسع النطاق للإنترنت. وفي الآونة الاخير بدأ

---

(12) 3 Smith, J. (2021). "Understanding the Metaverse: Concepts and Implications." Journal of Virtual Environments, 5(2), 120-135.

(13) 4 Jones, A., & Davis, B. (2022). "Metaverse Security: Challenges and Solutions." International Conference on Cybersecurity and Privacy, Proceedings, 45-52

يظهر خطورة الأمر بعد نشر الوقاعة التي كانت في كانون الأول (ديسمبر)، حيث ارتدت نينا جين باتيل، باحثة دكتوراه تبلغ من العمر ٤٣ عاما، سماعة رأس ودخلت عالم ميتا الافتراضي لترى ما كان يحدث في ذلك اليوم. وتقول باتيل "في غضون ثوان من وجودي هناك، وجدت ثلاث شخصيات افتراضية "أفتار" بالقرب مني فجأة بدأوا بالتقاط صور سيلفي مع باتيل، التي تعرضت لمضايقات في الميتافيرس،هي باحثة دكتوراه في جامعة ريدينج، تدرس "الأثر النفسي والفسيولوجي" الناتج عن الخوض في هذه العوالم الافتراضية الغامرة تعرف باتيل أفضل من معظم الناس كيف يكون الشعور إثر انتهاك يتم عبر التفاعل في تجربة رقمية(١٤).

"في الفضاء الافتراضي، يبدو أنه من المقبول أن يتصرف الناس بطريقة مختلفة عن تصرفاتهم في الحياة الواقعية"، كما تقول باتيل، ما يؤدي إلى مشكلات محتملة لانضباط السلوك الرقابي في مكان العمل في الميتافيرس. تقول، "إن التعليقات التي تلقيتها ردا على ذلك– في مدونة حول تجربتها–، تظهر أن هناك أشخاصا يعتقدون أن هذا السلوك ملائم في البيئات الافتراضية".

خلال فتره بسيطة سيتم الاستماع إلى قضايا جديدة مرتكبة في هذا العالم الافتراضي في المحاكم. على سبيل المثال، تخيل جريمة قتل يرتكبها مرتكب الجريمة الذي يقع على بعد آلاف الأميال. ومن غير المؤكد ما إذا كانت النظريات القانونية القديمة كافية للتصدي لمثل هذه الجرائم التي لم يسبق لها مثيل في تاريخ البشرية، ولتحديد خطورة جرائم الميتافيرس لابد أولا تحديد العوامل التي أدت الي ظهور تلك الجرائم

عاشرا: العوامل التي أدت الي ظهور جرائم الميتافيرس وتأثيراتها على الأفراد والمؤسسات:

هناك الكثير من الدوافع الاقتصادية والاجتماعية و الثغرات التكنولوجية التي أدت الي ظهور جرائم الميتافيرس فهو مصطلح يشير إلى الجرائم التي تتعلق بالتكنولوجيا والحوسبة السحابية وتخصصات الحوسبة الحديثة. يمكن تحديدها بناءً على مجموعة من العوامل التي أثرت على العالم وأدت إلى تزايد هذه الجرائم. **تتضمن العوامل الرئيسية التي أدت إلى ظهور جرائم الميتافيرس ما يلي:**

(14) https://www.aleqt.com/2022/02/28/article_2270971.html

(ISSN: 2537 - 0758)

١. **التطور التكنولوجي:** تقدم التكنولوجيا بسرعة، مما يجعلها أكثر تعقيدًا وتنوعًا. الابتكارات في مجالات مثل الحوسبة السحابية والذكاء الاصطناعي والإنترنت والأجهزة المتصلة أدت إلى توسع الفرص لارتكاب جرائم الميتافيرس.
٢. **زيادة الاعتماد على التكنولوجيا:** يعتمد المجتمع الحديث بشكل متزايد على التكنولوجيا في حياته اليومية وفي الأعمال والتواصل والمعاملات المالية. هذا يجعل الأفراد والشركات هدفًا للجرائم التي تستهدف التكنولوجيا.
٣. **نقص الوعي الأمني والتعليم السيبراني:** يمكن أن يؤدي نقص الوعي بأمان المعلومات والنقص في التدريب السيبراني إلى زيادة عرضة الأفراد والمؤسسات للهجمات السيبرانية.
٤. **الإدمان على الإنترنت والشبكات الاجتماعية:** يمكن أن يؤدي الإدمان على استخدام الإنترنت ووسائل التواصل الاجتماعي إلى سوء استخدام التكنولوجيا وارتكاب جرائم عبر الإنترنت.
٥. **المكاسب المالية:** تعد الجريمة المنظمة والهجمات السيبرانية والاحتيال على الإنترنت واحدة من الطرق التي يمكن من خلالها تحقيق مكاسب مالية بشكل سريع وسهل للمجرمين.
٦. **نقص التشريعات والتنظيمات الفعالة:** يمكن أن يؤدي نقص التشريعات الفعالة وتنفيذها إلى تقليل الردع وزيادة تكرار الجرائم الميتافيرس.

لمكافحة جرائم الميتافيرس، يجب تعزيز التوعية بالأمان السيبراني، وتطوير القوانين والتشريعات ذات الصلة، وتعزيز التدابير الأمنية للحد من هذه الجرائم، بالإضافة إلى تعزيز التعاون الدولي لمكافحة الجريمة عبر الحدود الرقمية.

تأثيرات جرائم الميتافيرس على الأفراد والمؤسسات:

تأثيرات جرائم الإنترنت على الأمن الرقمي تكون وخيمة ومتعددة، وتشمل ما يلي:

١. **فقدان البيانات والسرقة الهوية:** تتسبب جرائم الإنترنت في سرقة البيانات الشخصية والمالية، ويمكن استخدام هذه البيانات في ارتكاب جرائم أخرى مثل الاحتيال والسرقة الهوية.

٢. **تعطيل الخدمات والهجمات الضارة:** يمكن أن تؤدي الهجمات الضارة والاختراقات السيبرانية إلى تعطيل مواقع الويب والخدمات عبر الإنترنت، مما يتسبب في خسائر مالية وتعطيل العمليات الأساسية.
٣. **التجسس والتشهير:** يمكن استخدام الإنترنت للتجسس على الأفراد والمؤسسات، ونشر معلومات خاطئة أو مضللة تؤثر سلباً على سمعة الأفراد أو المؤسسات.
٤. **تهديدات الأمن القومي:** يمكن للهجمات السيبرانية على البنية التحتية الحيوية للدولة، مثل الكهرباء والمياه والمستشفيات، أن تهدد الأمن القومي.
٥. **الابتزاز الرقمي:** يمكن للمهاجمين تهديد الأفراد أو المؤسسات بنشر معلومات حساسة أو تعطيل خدماتهم ما لم يتم دفع فدية.
٦. **انتهاك الخصوصية والتطلُّع على البيانات الشخصية:** يتمثل تأثير آخر في انتهاك الخصوصية الشخصية والتجسس على الأفراد عبر جمع معلوماتهم دون إذن.
٧. يجب أن تعمل الحكومات والمؤسسات والأفراد على تعزيز الوعي بأمان الإنترنت واتخاذ تدابير أمنية فعالة للوقاية من جرائم الإنترنت والحد من تأثيراتها على الأمن الرقمي.
٨. **استهداف الصورة الرمزية:** قد لا يشكل في حد ذاته جريمة جنائية وفقًا لأطُرٍ قانونية معينة، حيث لا تتمتع الصور الرمزية بشخصية قانونية، وبالتالي لا تحظى بالحماية القانونية. ومع ذلك، في بعض الولايات القضائية، يمكن اعتبار مثل هذه الأفعال انتهاكًا للسلامة الأخلاقية للشخص.

تطوّر العوالم الافتراضية وتأثيرها:

في عصرنا الحالي، يشهد العالم تحولاً رقمياً مذهلاً يؤثر بشكل كبير على حياة الأفراد والمجتمعات. أحد أبرز هذه التطورات هو ظهور العوالم الافتراضية والتي تعتبر منصة للتفاعل والتواصل في بيئات ثلاثية الأبعاد تماماً كالعالم الحقيقي. يعود هذا التطور إلى التقدم الكبير في تكنولوجيا المعلومات والاتصالات.

أ- التأثيرات الإيجابية:

١. **توسيع الاتصال والتفاعل الاجتماعي:** تسمح العوالم الافتراضية بالتواصل مع الأشخاص من مختلف أنحاء العالم بشكل سهل وفعال. يمكن للأفراد إنشاء شخصيات افتراضية والتفاعل مع المجتمع العالمي بشكل غير محدود.

(ISSN: 2537 - 0758)

٢. **توسيع الفرص التعليمية والثقافية:** توفر العوالم الافتراضية بيئة للتعلم النشط والتجريبي، حيث يمكن للأفراد التفاعل مع المعرفة والثقافات بشكل مباشر. يعزز ذلك التفاهم والتقارب الثقافي.

٣. **دعم الأعمال والاقتصاد الرقمي:** يساهم استخدام العوالم الافتراضية في تعزيز الأعمال وتطوير الابتكارات الرقمية. تنشأ فرص جديدة للتسويق والتجارة الإلكترونية والتعاون العملي بين الأفراد والشركات.

٤. **تأثير على الصحة والعافية:** يظهر بعض البحوث أن استخدام العوالم الافتراضية يمكن أن يساعد في تحسين العافية العقلية والنفسية، حيث يمكن للأفراد الابتعاد عن الضغوط اليومية والتجربة العالم الرقمي بشكل ممتع ومفيد.باختصار فإن تطوير العوالم الافتراضية يعد تقدماً مهماً يؤثر إيجاباً على المجتمعات. لكن يجب أن نتعامل مع هذه التكنولوجيا بحذر ونضمن أن تكون هذه الابتكارات مفيدة ومحفزة لتحسين حياة الناس وتعزيز التفاهم والتقارب الاجتماعي.

٥. يقدم الميتافيرس إمكانيات تعليمية جديدة: ولكن التطوير المستقبلي ينبغي أن يعالج مخاوف الخصوصية ويضمن حل المشكلات بشكل تعاوني[١٥].

ب-التأثيرات السلبية:

يؤكد معظم مطوري مواقع التواصل الاجتماعي على أهمية إبعاد الأطفال عن هذا العالم حتى سن١٣عاماً لأنه هو العمر الأصعب، حيث تكون حياة الأطفال صاخبة وصعبة وعوالمهم الداخلية وأجسامهم في حالة تغير مستمر وكذلك عوالمهم الخارجية وعلاقاتهم، لذلك فهو ليس الوقت المناسب ليبدؤوا التعرف على العالم الافتراضي، فهم الأضعف في هذا العمر والأكثر عرضة لضغوط المؤثرات الخارجية المختلفة[١٦].

---

(15) Kye, B., Han, N., Kim, E., Park, Y., & Jo, S. (2021). Educational applications of metaverse: possibilities and limitations. Journal of Educational Evaluation for Health Professions, 18. https://doi.org/10.3352/jeehp.2021.18.32.

(16) Bakkaye, R., & Kerroum, M. (2019). تأثير مواقع التواصل الاجتماعي على الصحة النفسية والاجتماعية للطفل. مجلة التمكين الاجتماعي, 1(1), 44–51. https://doi.org/10.34118/sej.v1i1.796

حيث يجهل بعض الأهل هذه الحقائق ولا يفكرون قبل أن يسمحوا لأطفالهم باستخدام الهواتف المحمولة، وهناك الكثير من العوامل التي يحب أن تفكر بما قبل أن تساعد أطفالنا على يكونوا ملوكاً في ممالكهم الافتراضية في عالم مواقع التواصل الاجتماعي، البقاء حبيسي أسوار هذه المملكة إلى الأبد، حيث يفضلون أن يقوموا بكل هذا عن طريق الانترنت ومواقع التواصل الاجتماعي و يجهلون تماماً المعنى الحقيقي للعلاقات، تلك التي تبنى على العواطف بالنسبة لهم التواصل رقمياً مع آلاف الأشخاص هو مثل التواصل الفيزيائي.

الآثار الذهنية والإدراكية للعالم الافتراضي تظهر بوضوح في عالم الميتافيرس، حيث يتيح لنا هذا العالم دمج العالم الافتراضي والعالم المعزز معًا لصنع عالم ثالث، ممزوج بالبيانات الرقمية والأشكال والمعلومات. وقد يؤدي هذا التزامن بين العوالم المختلفة إلى تشتت العقل والارتباك، حيث يمكن للفرد أن يجد صعوبة في تمييز ما هو حقيقي وموجود فعلًا من ما هو مجرد تعزيز وإضافة إلكترونية. ونتيجة لذلك، يمكن أن يحدث تشتت ذهني وحالة دائمة من الشك، ونظراً لجاذبية ذلك العالم فإنه يبقى مشدوها إليه، ولكن يجد نفسه أمام التزامات مهنية أو دراسية في اليوم الموالي لذا فقد يلجأ إلى أدوية وعقاقير تعرضه للإدمان وآثار الضغط الجسمي والذهني والإصابة بالأمراض[١٧].

قد تؤدي العوالم الافتراضية إلى زيادة الجرائم على الإنترنت، لكنها لا تمتلك إمكانات كبيرة لظهور أشكال جديدة من الجرائم، وقد يؤثر استخدامها على السلوك في الحياة الواقعية من خلال القيم والمواقف[١٨]. يمكن لمهاجمي الواقع الافتراضي (VR) التحقق سراً من عشرات السمات الخاصة بالبيانات الشخصية من مستخدمين مجهولين على ما يبدو لتطبيقات metaverse مثل VRChat، مما يفرض مخاطر خصوصية فريدة تتجاوز تطبيقات الهاتف المحمول والويب التقليدية[١٩].

---

[١٧] بركات، مطاع. (٢٠٠٦). الواقع الافتراضي فرصه ومخاطره وتطوره: دراسة نظرية. مجلة جامعة دمشق للعلوم التربوية والنفسية، س ٢٢ ، ع ٢، ٤٠٧ – ٤٣٢. مسترجع من http://search.mandumah.com/Record/10647

[18] Laue, C. (2011). Crime Potential of Metaverses. , 19-29. https://doi.org/10.1007/978-3-642-20823-2_2.

[19] Nair, V., Garrido, G., & Song, D. (2022). Exploring the Unprecedented Privacy Risks of the Metaverse. *ArXiv*, abs/2207.13176. https://doi.org/10.48550/arXiv.2207.13176.

(ISSN: 2537 - 0758)

أظهرت العديد من البحوث تأثيرات نفسية وصحية كبيرة ناتجة عن استخدام التكنولوجيات التقليدية، على الرغم من ميزاتها المتواضعة مقارنةً بعالم الميتافيرس. وفي الوقت نفسه، نشهد تسارعا في إطلاق ونشر تقنيات العوالم الافتراضية المتقدمة دون إجراء دراسات متأنية حول مدى مناسبتها للسلوك الإنساني، وكذلك دون النظر إلى المخاطر والآثار الجانبية المحتملة.

الفصل الثاني

جرائم الميتافيرس في ضوء التشريعات وطرق التصدي لها

أولا: الأطر القانونية لمكافحة جرائم الميتافيرس

يتمحور هذا الجزء حول تحليل الأطُر القانونية المتاحة على مستوى الدولة والدول لمكافحة جرائم الميتافيرس، بما في ذلك القوانين واللوائح ذات الصلة، حيث تختلف الجرائم المرتكبة في الميتافيرس بطبيعتها مقارنة بالجرائم التقليدية والجرائم الإلكترونية الأخرى، بسبب الاختلاف الكبير في الوسيط، فهناك تفاوت بين جرائم الميتافيرس وينبغي للمشرع أن يكون أكثر يقظة للوتيرة غير المسبوقة التي تتطور بها التكنولوجيا الحديثة ويوكب تلك التكنولوجيا وذلك لتجنب أن تصبح القوانين ذات الصلة قديمة.

والجدير بالذكر أن كلا من الفعل الإجرامي والقصد الجنائي يحدثان بنفس المعنى التقليدي المنصوص عليه في المراجع القانونية. لكن قد يكون هناك بعض الغموض القانوني فيما يتعلق بالجرائم المرتكبة في الميتافيرس حتى الآن، لا يمكن للجرائم السيبرانية أن تسبب ضررًا جسديًا للإنسان. وذلك لأن العوالم السيبرانية يمكن استخدامها كوسيلة لارتكاب جريمة تقليدية مثل التعدي على ممتلكات الغير أو السرقة أو العنف أو يمكن أن تكون موضوعًا للسلوك الإجرامي. ولا يوجد دليل على أن الأذى الجسدي يمكن أن يحدث من خلال أي من إساءة استخدام التكنولوجيا السيبرانية المذكورة مما يجعل الموضوع أكثر تعقيداً.

وتشير إلى القوانين واللوائح التي وضعتها الدول على مستوى وطني ودولي لمكافحة الجرائم في الميتافيرس. تتضمن هذه القوانين معايير العقوبات والتصدي لأنواع محددة من الجرائم. حيث تركز تلك القوانين واللوائح التي تهدف إلى حماية البيانات الشخصية

والخصوصية في الميتافيرس، وتحديد كيفية جمع ومعالجة البيانات بشكل مشروع[٢٠]. وكيفية تنفيذ العقوبات والإجراءات القانونية عند حدوث جرائم في الميتافيرس، بما في ذلك التحقيق والمحاكمة وتنفيذ العقوبات[٢١]. ولكن ينبغي للقانون الجنائي أن ينظم الاستخدام غير العلاجي للواقع الافتراضي الغامر (VR) بسبب إمكاناته الضارة المحتملة، بما في ذلك جمع البيانات، وإعادة خلق التجارب الجسدية عقليًا، والتلاعب بالأفراد[٢٢]. حيث توفر تقنية الواقع الافتراضي فرصًا جديدة للمجرمين للتلاعب بمشاعر الضحايا ووعيهم عن بعد، مما يتيح ارتكاب العديد من الجرائم عن بعد[٢٣].

تحليل النظم القانونية والتشريعات المعمول بها لمكافحة جرائم الميتافيرس في مختلف الدول:

أمثلة على بعض الدول والتشريعات ذات الصلة بالميتافيرس مع توضيح أرقام القوانين

١ – الاتحاد الأوروبي:

قانون حماية البيانات العام ١٧٢٥/٢٠١٨ (GDPR): هذا القانون يعد من أهم التشريعات على مستوى العالم في مجال حماية البيانات الشخصية. ينظم جمع ومعالجة البيانات الشخصية ويحدد حقوق المستهلكين فيما يتعلق ببياناتهم الشخصية. [الاتحاد الأوروبي، اللائحة العامة لحماية البيانات (GDPR)، ١٧٢٥/٢٠١٨][٢٤].

---

[٢٠] العجمي، ف. (٢٠٢٠). "الميتافيرس والتحديات الأمنية: دراسة تحليلية." مجلة الأمن السيبراني، ٨(٣)، ٢٤٥-٢٦٠

[٢١] اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا). (٢٠٢١). "تقرير حول التحول الرقمي والتحديات الأمنية: التركيز على الميتافيرس والعوالم الافتراضية."

[22] González-Tapia, M. (2023). Virtual emotions and Criminal Law. *Frontiers in Psychology*, 14. https://doi.org/10.3389/fpsyg.2023.1260425.

[23] Dremlyuga, R., & Kripakova, A. (2019). Crimes in virtual reality: myth or reality?. *Actual Problems of Russian Law*. https://doi.org/10.17803/1994-1471.2019.100.3.161-169.

[24] https://eur-lex.europa.eu/legal-content/AR/TXT/?uri=celex%3A32018R1725

(ISSN: 2537 - 0758)

٢- الولايات المتحدة الأمريكية:

قانون الاحتيال والاعتداء الإلكتروني (Computer Fraud and Abuse Act - CFAA): يُعتبر هذا القانون من القوانين الهامة في مكافحة الجرائم الإلكترونية في الولايات المتحدة. يحظر الوصول غير المشروع إلى الأنظمة الإلكترونية والتلاعب بالبيانات والأجهزة. [الولايات المتحدة الأمريكية، قانون الاحتيال والاعتداء الإلكتروني (CFAA)][٢٥].

٣- الصين:

قانون الجريمة الإلكترونية هناك جهود الصين في تنظيم ومكافحة الجرائم السيبرانية. حيث ينص على تعزيز أمن الشبكات وحماية البيانات الشخصية وتقديم إرشادات للشركات التكنولوجي الصين، قانون الجريمة الإلكترونية

يعتبر هذا القانون محورياً في تنظيم الأنشطة الرقمية ومكافحة الجرائم الإلكترونية. يحدد متطلبات الأمن السيبراني، ويشدد على حماية البيانات الشخصية وأمن الشبكات الإلكترونية

ومن أهم الإجراءات التي قامت بها الصين هي:-

- **التوعية والتثقيف:**

تعتمد الحكومة الصينية على حملات التوعية والتثقيف لرفع الوعي بأهمية الأمن الرقمي ومكافحة الجرائم الإلكترونية. تُنظم ورش العمل والحملات التوعية في المدارس والمؤسسات الحكومية والقطاع الخاص.

- **التعاون الدولي:**

تعمل الصين على تعزيز التعاون الدولي من خلال مشاركتها في المحافل الدولية المختصة بأمن المعلومات ومكافحة الجرائم الإلكترونية. يشجع هذا التعاون على تبادل المعرفة والخبرات بين الدول، تجلب تلك الخطوات الصينية إلى الأمام الضوء على أن الحلول لمكافحة جرائم الميتافيرس تتطلب جهدًا مشتركًا بين القطاعات المختلفة والتعاون

(25) https://www.law.cornell.edu/uscode/text/18/part-I/chapter-47

الدولي. تسعى الصين جاهدةً لتحقيق التنسيق الفعال والتوعية لضمان أمن المعلومات وتقليل وقوع الجرائم الإلكترونية[٢٦].

٤- اليابان:

قانون حماية البيانات الشخصية في القطاع الخاص (APPI): يحمي هذا القانون البيانات الشخصية وينظم كيفية جمعها واستخدامها في القطاع الخاص. [APPI قانون حماية البيانات الشخصية في القطاع الخاص][٢٧].

تعتبر اليابان من الدول التي تسعى بجدية لمكافحة جرائم الميتافيرس وتعزيز الأمن الرقمي. إليك بعض الجوانب الرئيسية لتجربتها:

- **توجيه الجهود القانونية:**

قد اتخذت اليابان خطوات قانونية هامة، حيث وضعت قوانين تنظم استخدام الميتافيرس وتحدد العقوبات لمن ينتهكها، مما يعزز رد الفعل القانوني ضد الجرائم الرقمية.

- **تعزيز التوعية العامة:**

تقوم الحكومة اليابانية بحملات وبرامج توعية تستهدف المواطنين والشباب لزيادة الوعي بأمان المعلومات ومخاطر الميتافيرس، وتشجيع السلوكيات الآمنة عبر وسائل التواصل وورش العمل.

- **تعزيز الشراكات مع القطاع الخاص:**

تقوم اليابان بتعزيز التعاون بين الحكومة والقطاع الخاص، بما في ذلك شركات التكنولوجيا ومزودي الخدمات الرقمية، لضمان الحماية الفعّالة ضد الجرائم الإلكترونية.

تعكس تجربة اليابان في مكافحة جرائم الميتافيرس أهمية توجيه الجهود في مجالات القانون والتوعية والشراكات لتحقيق أمن رقمي محسّن ومجتمع رقمي آمن.

٥- روسيا:

قانون حماية البيانات الشخصية الفيدرالي (Ф3-152): ينظم هذا القانون جمع ومعالجة البيانات الشخصية في روسيا. [قانون حماية البيانات الشخصية الفيدرالي (Ф3-152)][٢٨].

---

(26) http://www.npc.gov.cn/npc/index.html
(27) https://www.ppc.go.jp/en/privacy/related-laws/pdf/29_english.pdf

(ISSN: 2537 - 0758)

٦- كوريا الجنوبية:

قانون تنظيم الاتصالات السلكية واللاسلكية (KCCMA): يهدف هذا القانون إلى تنظيم وحماية البيانات الشخصية في كوريا الجنوبية. [قانون تنظيم الاتصالات السلكية واللاسلكية (KCCMA)][٢٩].

نجد أن هذه التشريعات تحمي البيانات الشخصية وتنظم جمعها واستخدامها، وهي جزء أساسي من مكافحة الجرائم في الميتافيرس وتعزيز الأمن الرقمي.

بالنسبة للدول العربية تتخذ خطوات هامة لمكافحة جرائم الميتافيرس وضمان الأمن الرقمي. يمكن تحديد بعض الدول العربية التي تبرز في هذا المجال بناءً على جهودها واهتمامها بأمن المعلومات ومكافحة الجرائم الرقمية:

١. الإمارات العربية المتحدة:

تعتبر الإمارات من الدول الرائدة في اتخاذ إجراءات حاسمة لمكافحة جرائم الميتافيرس وتعزيز الأمن السيبراني. تقوم بتطوير القوانين واللوائح ذات الصلة وتعزز التوعية العامة حول خطورة جرائم الميتافيرس[٣٠].

٢. المملكة العربية السعودية:

تسعى المملكة العربية السعودية إلى تعزيز أمن المعلومات ومكافحة الجرائم الرقمية من خلال تحديث التشريعات وتعزيز التوعية بمخاطر الميتافيرس وطرق الحماية[٣١].

٣. مصر:

تسعى مصر إلى تعزيز الوعي بأمن المعلومات ومكافحة جرائم الميتافيرس من خلال تنظيم حملات توعية وورش عمل تثقيفية[٣٢].

---

(28) Распоряжение Председателя СФ ФС РФ от 11.09.2013 N 200рп-СФ (ред. от 19.11.2020) "О порядке уведомления представителя нанимателя о фактах обращения в целях склонения федерального государственного гражданского служащего Аппарата Совета Федерации,... \ КонсультантПлюс (consultant.ru)

(29) https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53254&lang=ENG

(30) www.ncsi.gov.ae

(31) https://sdaia.gov.sa/ar/default.aspx

(32) https://www.ntra.gov.eg/

٤. المغرب:

تضع المغرب جهودًا كبيرة لمكافحة جرائم الميتافيرس وتحقيق أمن المعلومات من خلال تطوير القوانين وتعزيز التعاون الدولي في هذا المجال(٣٣).

تعمل هذه الدول العربية وغيرها على تطوير القوانين والتشريعات وتعزيز التوعية بمخاطر الميتافيرس، وتشجيع البحث والتطوير لمكافحة الجرائم الرقمية وتحقيق أمن المعلومات.

التحديات والآفاق المستقبلية في مكافحة جرائم الميتافيرس

يتناول هذا الجزء التحديات التي تواجه مكافحة جرائم الميتافيرس ويسلط الضوء على الآفاق المستقبلية في هذا المجال.

الجدير بالذكر أن مشكلة تحديد الجريمة في العوالم الافتراضية حيث أن الحدود القانونية والتعريفات تعتمد على الأنظمة القانونية والتشريعات الوطنية، مما يعقد عملية تحديد تلك الجريمة(٣٤).

- **التحديات:**

١. **التقنيات المتقدمة:** تطور التقنيات يجعل من الصعب رصد ومكافحة الجرائم في الميتافيرس بشكل فعال.
٢. **التشفير والتمويه:** استخدام التشفير والتمويه يجعل من الصعب التعرف على الأنشطة الإجرامية.
٣. **نقص التنسيق الدولي:** تحتاج الجهود الدولية المشتركة لتعزيز التعاون لمكافحة جرائم الميتافيرس.
٤. **متطلبات الأمان والخصوصية:** تتطلب تحديات الأمن والخصوصية في Metaverse إجراء مسح شامل لمعالجة مخاوف التوسع والتشغيل البيني والخصوصية، مع معالجة اتجاهات البحث المستقبلية(٣٥).

---

(33) cndh.ma

(34) Laue, C. (2011). Crime potential of metaverses. In *Springer eBooks* (pp. 19–29). https://doi.org/10.1007/978-3-642-20823-2_2

(35) Wang, Y., Su, Z., Zhang, N., Liu, D., Xing, R., Luan, T., & Shen, X. (2022). A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Communications Surveys & Tutorials*, 25, 319-352. https://doi.org/10.1109/COMST.2022.3202047.

(ISSN: 2537 - 0758)

- **الآفاق المستقبلية:**

١. **التطور التكنولوجي:** مع التطور التكنولوجي المستمر، يمكن أن تظهر حلول فعّالة لمكافحة الجرائم في الميتافيرس.
٢. **تعزيز التعاون الدولي:** تعزيز التنسيق والتعاون الدولي يمكن أن يسهم في مكافحة الجرائم بشكل أفضل.
٣. **توعية الجمهور والتعليم:** زيادة الوعي بين المستخدمين حول مخاطر جرائم الميتافيرس يمكن أن يقلل من وقوعها.
٤. **تطوير النظام القانوني:** إن تطوير نظام قضائي إلكتروني شامل وقانون جنائي نموذجي في العالم الافتراضي أمر ضروري للتنظيم القانوني للعلاقات الاجتماعية في العالم الافتراضي، ومعالجة قضايا مثل الاختصاص القضائي والقانون والجريمة[٣٦].

إن تكنولوجيا الواقع الافتراضي، جنبًا إلى جنب مع الأجهزة اللمسية، تفتح المجال أمام أنواع جديدة من الجرائم، تجمع بين الجرائم التقليدية والجرائم الإلكترونية، مما يتطلب إطارًا قانونيًا خاصًا لمعالجة هذه التحديات[٣٧].

ثانيا: اقتراح سياسات وتدابير فعالة للوقاية من جرائم الميتافيرس ومكافحتها:

١. تشديد التشريعات وتحديثها:

يجب مراجعة وتحديث التشريعات لتكون متناسبة مع التطورات التكنولوجية، وتضمن معاقبة الجرائم الرقمية بشكل فعال ومنع انتهاكات الخصوصية والتلاعب الإلكتروني.

٢. تعزيز التوعية والتثقيف:

ينبغي توجيه حملات توعية وبرامج تثقيف للمستخدمين حول مخاطر الميتافيرس وأفضل السلوكيات الرقمية، وكيفية الحماية من الاحتيال والتلاعب.

---

(36) Kostenko, O., Zhuravlov, D., Dniprov, O., & Korotiuk, O. (2023). METAVERSE: MODEL CRIMINAL CODE. *Baltic Journal of Economic Studies*. https://doi.org/10.30525/2256-0742/2023-9-4-134-147.

(37) Dremliuga, R., Prisekina, N., & Yakovenko, A. (2020). New Properties of Crimes in Virtual Environments.. https://doi.org/10.25046/aj0506206.

٣. تعزيز التعاون الدولي:

يتعين تعزيز التعاون بين الدول والمنظمات الدولية لتبادل المعرفة والخبرات وتطوير استراتيجيات مشتركة لمكافحة جرائم الميتافيرس بشكل فعّال.

٤. تطوير التكنولوجيا الأمنية:

العمل على تطوير حلول تكنولوجية تعزز الأمان السيبراني وتقلل من فرص الاختراقات تجدر الإشارة إلى أن هذه السياسات والتدابير تهدف إلى تعزيز أمن المعلومات والحد من الجرائم في الميتافيرس. يتعين على الدول تبني هذه الإجراءات وتكييفها وفقاً لظروفها الخاصة.

الخاتمة والنتائج:

أن العالم الافتراضي يمثل تحديًا متزايدًا للمجتمع اليوم، مع تطور التكنولوجيا وتفشي الإنترنت. تنامي هذا العالم يعتمد بشكل كبير على تقدم التكنولوجيا وتبني المستخدمين لها. ومع ذلك، فإنه يترتب علينا أيضًا التعامل مع الجرائم الرقمية والتحديات الأمنية التي تنشأ عنها.

تظهر الحاجة الملحة لوضع تشريعات وقوانين فعالة تعالج جرائم العالم الافتراضي بشكل جدي وتعمل على تطبيق العقوبات على المرتكبين. بالإضافة إلى ذلك، يجب تعزيز التوعية والتثقيف لدى المستخدمين حول مخاطر جرائم العالم الرقمي وكيفية الوقاية منها.

تعد مشكلة جرائم العالم الافتراضي تحديًا عالميًا، يتطلب تعاوناً دولياً قوياً لمحاربتها بنجاح. يجب أن يتبنى المجتمع الدولي استراتيجيات مشتركة للتصدي لهذه الظاهرة وتبادل المعرفة والخبرات لمواجهتها بفعالية.

لابد تكثيف الجهود المشتركة لمحاربة جرائم الميتافيرس وتقديم الحماية للمجتمع العالمي. يتعين أن نعمل معًا لتطوير استراتيجيات فعالة للتصدي لهذه الجرائم وتحقيق أمن سيبراني مستدام. وأن البحث والتحليل الدقيق لجرائم الميتافيرس وتأثيراتها الاجتماعية والجريمة فيها يتطلب التعاون بين علماء الجريمة والعلماء الاجتماعيين والخبراء التكنولوجيا.

(ISSN: 2537 - 0758)

يعد التركيز على مكافحة جرائم العالم الافتراضي أمرًا ضروريًا للحفاظ على أمن وسلامة المستخدمين في هذا العالم الرقمي الذي يتزايد تطوره بسرعة. يجب تبني استراتيجيات متكاملة تجمع بين القوانين الفعالة والتوعية والتعاون الدولي لضمان حماية فعالة للمجتمع الرقمي.

في النهاية، يجب أن ندرك أن الحماية في العالم الرقمي تعد تحديًا مستمرًا، ويتوجب علينا أن نظل دائمًا ملتزمين بتحقيق بيئة آمنة ومأمونة للجميع في هذا العالم المتقدم تكنولوجي. ولا يزال النظام القانوني في كثير من دول العالم لا يغطي تلك الجرائم ولا يسن لها العقوبات الرادعة، وهذ الأمر يمثل تحديًا خاصة عندما يتعلق الأمر بالتعامل مع الجرائم المرتكبة في العالم الخارجي. حيث إن طبيعة الميتافيرس من الجانب الفني تزيد الأمور تعقيدًا، حيث يخضع المستخدمون للفصل بين جسدهم المادي ووعيهم، ويخضع كل مستخدم لمجموعة مختلفة من المحفزات.، فمن غير المرجح أن تتحمل المحاكم أي مسؤولية جنائية عن الجرائم المرتكبة ضد مجرد تجسيديات دون أي ضرر يلحق بشخص حقيقي خارج نطاق الميتافيرس، وذلك بسبب عدم الاعتراف بقوانين العقوبات لكثير من الدول لمصلحة الصورة الرمزية التي يمكن حمايتها جنائيا. ومع ذلك، إذا امتد الضرر إلى ما وراء حدود الميتافيرس وأثر على المستخدم في العالم الحقيقي، فسيكون التدخل القانوني ملحاً ولأن القواعد الجزائية الحالية قد لا تكون كافية من الناحية القانونية لمعالجة هذه الجرائم.فيجب سن قانون خاص لتعريف جرائم الميتافيرس وتحديد العقوبات عليها .كما ينبغي تعديل قانون الإجراءات الجنائية بحيث يحدد الطريقة الصحيحة لإثبات الجرائم والحصول على الأدلة، مع مراعاة الطبيعة التقنية لهذا العالم الافتراضي.

التوصيات والمقترحات:

يمكن تحديد أهم توصيات تحسين الأطُر القانونية والتدابير الأمنية لمكافحة جرائم الميتافيرس فيما يلي:-

١- **تعزيز التعاون الدولي:** تشدد التوصيات على أهمية تعزيز التعاون والتنسيق الدولي في مجال مكافحة الجرائم في الميتافيرس، وتطوير آليات فعالة لتبادل المعلومات

والتعاون القانوني بين الدول، ينبغي تعزيز التعاون بين الدول لمواجهة جرائم العالم الافتراضي وتبادل المعرفة والخبرات في هذا المجال مما يسمح بالحد من تلك الجرائم والسيطرة عليها علي الصعيد الدولي..

٢- **تحديث القوانين واللوائح:** يشدد على ضرورة مراجعة وتحديث القوانين واللوائح القائمة لتكون متسقة مع التطورات التكنولوجية والتحديات الجديدة التي تطرحها الميتافيرس.

٣- **تشديد التشريعات والقوانين الرقابية:** يجب تعزيز التشريعات لمعاقبة جرائم العالم الافتراضي وتحديثها بشكل دوري لمواكبة التطورات التكنولوجية، وخاصه اذا كانت الضحية في البيئة الافتراضية هي الأطفال.

٤- **توعية المستخدمين والتثقيف:** ينصح بتعزيز حملات التوعية والتثقيف حول مخاطر جرائم الميتافيرس بما في ذلك التوجيه للمستخدمين بشكل سليم حول السلوكيات الآمنة داخل هذه البيئة الرقمية. ويجب تعزيز الحملات التوعية للمستخدمين بشأن جرائم العالم الافتراضي وكيفية الوقاية منها والإبلاغ عنها، توعية الوالدين للأطفال بمخاطر البيئة الافتراضية، وعدم الانخراط فيها وترك الواقع الحقيقي.

٥- **تعزيز الرقابة الأمنية:** فرض تشريعات رقابية علي التطبيقات المختلفة للواقع الافتراضي، مما يعزز الأمان في البيئة الافتراضية، وفتح قنوات الإبلاغ عن الانتهاكات التي تحدث داخل البيئة الافتراضية، ومواكبه الانتهاكات المختلفة بتشريعات حاسمة.

(ISSN: 2537 - 0758)

المراجع

المراجع العربية:

١. جمعة مصطفى، إ. (٢٠٢٣). الجرائم المرتكبة باستخدام تقنيات التكنولوجيا الحديثة في القانون المصري (الواقع الافتراضي والواقع المعزز والمختلط) Crimes Committed Using Modern Technology Techniques In Egyptian Law (Virtual Reality, Augmented And Mixed Reality). مجلة كلية الشريعة والقانون بطنطا.51-2 ,(1)38 ,

٢. Bakkaye, R., & Kerroum, M. (٢٠١٩). تأثير مواقع التواصل الاجتماعي على الصحة النفسية والاجتماعية للطفل. مجلة التمكين الاجتماعي، ١(١)، ٤٤–٥١. https://doi.org/10.34118/sej.v1i1.796

٣. العجمي، ف. (٢٠٢٠). "الميتافيرس والتحديات الأمنية: دراسة تحليلية." مجلة الأمن السيبراني، ٨(٣)، ٢٤٥–٢٦٠

٤. اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا). (٢٠٢١). "تقرير حول التحول الرقمي والتحديات الأمنية: التركيز على الميتافيرس والعوالم الافتراضية".

٥. علي، أحمد عمرو، خليفة، & ماهينور محمد. (٢٠٢٣). أركان الجريمة في الميتافيرس: دراسة في ضوء أحكام القانون الجنائي المصري. المجلة الدولية للفقه والقضاء والتشريع.

٦. زعتر، نور الدين (٢٠٢٢) العالم الافتراضي الميتافيرس Metaverse" من منظور سيكولوجي. مجلة العلوم الإنسانية مج.

٧. بركات، مطاع. (٢٠٠٦). الواقع الافتراضي فرصه ومخاطره وتطوره: دراسة نظرية. مجلة جامعة دمشق للعلوم التربوية والنفسية، س ٢٢، ع ٢، ٤٠٧– ٤٣٢. مج.

المراجع الأجنبية:

1. A, J., Khanum, A., A, S., S, A., Latheef, A., & S, D. (2023). METAVERSE. *International Journal of Innovative Research in Information Security*. https://doi.org/10.26562/ijiris.2023.v0903.29.

2. Bocij, P., McFarlane, L., & McNally, R. (2012). Cyberstalking: Harassment in the Internet age and how to protect your family. ABC-CLIO.
3. Dionisio, J.D., Burns, W.G., & Gilbert, R. (2013). 3D Virtual worlds and the metaverse: Current status and future possibilities. ACM Comput. Surv.,
4. Dremlyuga, R., & Kripakova, A. (2019). Crimes in virtual reality: myth or reality?. *Actual Problems of Russian Law*. https://doi.org/10.17803/1994-1471.2019.100.3.161-169.
5. esign for virtual reality books, Jason Jerald, 2016.
6. González-Tapia, M. (2023). Virtual emotions and Criminal Law. *Frontiers in Psychology*, 14. https://doi.org/10.3389/fpsyg.2023.1260425.
7. Jones, A., & Davis, B. (2022). "Metaverse Security: Challenges and Solutions." International Conference on Cybersecurity and Privacy, Proceedings.
8. Kostenko, O., Zhuravlov, D., Dniprov, O., & Korotiuk, O. (2023). METAVERSE: MODEL CRIMINAL CODE. *Baltic Journal of Economic Studies*. https://doi.org/10.30525/2256-0742/2023-9-4-134-147.
9. Kye, B., Han, N., Kim, E., Park, Y., & Jo, S. (2021). Educational applications of metaverse: possibilities and limitations. *Journal of Educational Evaluation for Health Professions*, 18. https://doi.org/10.3352/jeehp.2021.18.32.
10. Laue, C. (2011). Crime potential of metaverses. In Springer eBooks
11. Laue, C. (2011). Crime potential of metaverses. In Springer eBooks
12. Nair, V., Garrido, G., & Song, D. (2022). Exploring the Unprecedented Privacy Risks of the Metaverse. *ArXiv*, abs/2207.13176. https://doi.org/10.48550/arXiv.2207.13176.
13. Smith, J. (2021). "Understanding the Metaverse: Concepts and Implications." Journal of Virtual Environments, 5(2),
14. Wang, Y., Su, Z., Zhang, N., Liu, D., Xing, R., Luan, T., & Shen, X. (2022). A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Communications Surveys &*

(ISSN: 2537 - 0758)

Tutorials, 25, 319-352. https://doi.org/10.1109/COMST.2022.3202047.
15. Dremliuga, R., Prisekina, N., & Yakovenko, A. (2020). New Properties of Crimes in Virtual Environments.. https://doi.org/10.25046/aj0506206.

مواقع الانترنت:

1. https://www.aleqt.com/2022/02/28/article_2270971.html
2. https://eur-lex.europa.eu/legal-content/AR/TXT/?uri=celex%3A32018R1725
3. https://www.law.cornell.edu/uscode/text/18/part-I/chapter-47
4. http://www.npc.gov.cn/npc/index.html
5. http://www.npc.gov.cn/npc/index.html
6. https://www.ppc.go.jp/en/privacy/related-laws/pdf/29_english.pdf
7. Распоряжение Председателя СФ ФС РФ от 11.09.2013 N 200рп-СФ (ред. от 19.11.2020) "О порядке уведомления представителя нанимателя о фактах обращения в целях склонения федерального государственного гражданского служащего Аппарата Совета Федерации,... \ КонсультантПлюс (consultant.ru)
8. https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53254&lang=ENG
9. www.ncsi.gov.ae
10. https://sdaia.gov.sa/ar/default.aspx
11. https://www.ntra.gov.eg/
12. cndh.ma
13. https://doi.org/10.1145/2480741.2480751