

## Criminally Illegal Use of Virtual Avatars in the Metaverse

Mohannad Walid Al-Haddad\* 

Department of Public Law, College of Law, Jerash University, Jerash, Jordan.

Received: 7/8/2025  
Revised: 15/9/2025  
Accepted: 8/1/2025  
Published: 25/2/2026

\* Corresponding author:  
[m11haddad@yahoo.com](mailto:m11haddad@yahoo.com)

Citation: Al-Haddad, M. W. (2026).  
Criminally Illegal Use of Virtual Avatars  
in the Metaverse. *Dirasat: Shari'a and  
Law Sciences*, 53(3), 12763.  
<https://doi.org/10.35516/Law.2026.12763>

### Abstract

**Objectives:** This study examines the criminally illegal use of virtual avatars in the metaverse, which has become an attractive environment for cybercrime due to the functional and interactive features of avatars. Such activities include offenses against property and persons, including virtual sexual exploitation. The study aims to assess the readiness of cybercrime law to confront avatar-related criminal activities in the metaverse and to propose a legal vision for applying criminal liability to these acts.

**Methods:** The study employed three research methods: a descriptive method to identify the phenomenon of criminal attacks involving virtual avatars; an analytical method to examine legal and jurisprudential positions on criminal liability for the illegal use of avatars; and a comparative method focusing on Jordanian cybercrime legislation, with reference to British law where relevant.

**Results:** The findings indicate that the metaverse represents an emerging technological environment that existing cybercrime laws are largely ill-equipped to regulate. Many forms of avatar-related misconduct fall outside current legal frameworks. The study emphasizes the need for Jordanian lawmakers to reconsider cybercrime legislation and to explore the adoption of a form of virtual legal personality for avatars to enable effective criminal accountability.

**Conclusions:** The study concludes that some metaverse-related attacks may fall under cybercrime law when their effects extend into the real world. However, other attacks remain unregulated despite their serious psychological impact on users, highlighting the need for explicit criminalization within future legal reforms.

**Keywords:** Metaverse technology, virtual world, augmented reality, avatars, cybercrime

### الاستخدام غير المشروع جزائياً للصُّور الرمزيّة الافتراضيّة "الافاتار" في تقنيّة الميتافيرس

مهند وليد الحداد\*

قسم القانون العام، القانون الجنائي، كلية الحقوق، جامعة جرش، جرش، الأردن

#### ملخص

الأهداف: الميتافيرس هو تمثيل تفاعلي افتراضي، حيث يتفاعل المستخدمون من خلال صور رمزية تربط الواقع المادي بالافتراضي، ويفضل مزايا الصُّور الرمزيّة في الميتافيرس، الأمر الذي جعل منها بيئة جاذبة للأنشطة الإجرامية. وقد تشمل هذه الأنشطة الاعتداء على الأموال، أو الأشخاص، كالاستغلال الجنسي الافتراضي على الصُّور الرمزيّة، ومن هنا حدّدت أهداف هذه الدراسة بمدى استعداد قانون الجرائم الإلكترونيّة لمواجهة الأنشطة العدائية التي فرضتها الصُّور الرمزيّة في الميتافيرس، لاسيما تلك التي تقع على ذات الصور الرمزيّة الافتراضيّة داخل تقنية الميتافيرس، ووضع تصوّر لأهم إشكاليات تطبيق المسؤولية الجزائية على تلك الاعتداءات.

المنهجية: اعتمدت هذه الدراسة على ثلاثة مناهج بحثية -المنهج الوصفي، القائم على تشخيص ظاهرة الاعتداء على الصُّور الرمزيّة، والمنهج التحليلي، بتحليل الموقف القانوني والفقهني من المسألة الجزائية عن الاستخدام غير المشروع للصور الرمزية، والمنهج المقارن، قانون الجرائم الإلكترونيّة الأردني، والاستشهاد مع القانون البريطاني، كلّما أمكن ذلك.

النتائج: من أهم نتائج الدراسة: أنّ تقنيّة الميتافيرس هي أحدث تكنولوجيا في الواقع الافتراضي، وهذا بطبيعة الحال جعل من نصوص قانون الجرائم الإلكترونيّة الحالية عاجزة عن مواجهة معظم الاعتداءات الواقعة على الصُّور الرمزيّة الافتراضيّة في الميتافيرس. وفي ضوء ذلك أوصت هذه الدراسة المشرّع الأردني بضرورة مراجعة قانون الجرائم الإلكترونيّة لضمان مواجهة فعالة لهذا النوع من الاعتداءات المستحدثة، والعمل على إمكانية مساءلة مزود الخدمة ومستخدمها عن الأفعال غير المشروعة.

الخلاصة: ثمة بعض الاعتداءات عبر تقنيّة الميتافيرس تخضع لقانون الجرائم الإلكترونيّة، ذلك إذا امتدت النتيجة الجرمية المتمثلة بالضرر الحدود الافتراضيّة، لتصل إلى الحدود الماديّة للمستخدم؛ إلا أنّ البعض الآخر من الاعتداءات لا ينطبق عليه القانون، بسبب انحصار الضرر على الصُّور الرمزيّة الافتراضيّة في الميتافيرس، والتي يقتضي تجريمها لجسامة أثارها النفسيّة للمستخدم.

الكلمات الدالة: تقنيّة الميتافيرس، الواقع الافتراضي، الصُّور الرمزيّة، الجرائم الإلكترونيّة.



© 2026 DSR Publishers/ The University of Jordan.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC) license <https://creativecommons.org/licenses/by-nc/4.0/>

## المقدمة:

## أولاً: موضوع الدراسة.

أحدثت تقنية الواقع الافتراضي "الميتافيرس" نقلة نوعية في مجال تقنيات التكنولوجيا، إذ تُقدم تجربة تفاعلية، تُمكن المستخدم من العيش في واقع مواز للواقع المادي، من خلال استخدام صُور رمزية "افاتار"؛ إذ تتيح مميزاتاً للمستخدم نقل الشُّعور بما في ذلك حاسة اللمس، فتمكّنه من استشعار وتلمس الأشياء والتفاعل مع غيره من المستخدمين في واقع يحاكي العالم المادي "الحقيقي". ومع نمو هذه التقنية، يكثر جانبها المُظلم، إذ يتم تزويدها في الغالب بالأشياء غير المنقولة، وغير المحسوسة، كالعُملة الافتراضية والرموز غير القابلة للاستبدال، ممّا يجعلها بيئة جاذبة للمجرمين الإلكترونيين، إذ يُمكن للمستخدم أن يُشوم بالاعتداء على صُورة رمزية لمستخدم آخر ومن خلالها يقوم المعتدي بالمساس بملكيّتها الفكرية أو أن يستخدمها في غسل الأموال، أو التدريب على أعمال إرهابية تحاكي الواقع المادي، أو السرقة، أو الإيذاء، أو الاعتداء الجنسي أو التزيف العميق لاسيما الافتراضي، وغيرها الكثير (Severgin,A,2023)، وهذه الاعتداءات تُشكّل تحدياً في قانون الجرائم الإلكترونية ممّا يتعيّن البحث في مدى كافية نُصُوبه للتصدي لهذا النوع من الاعتداءات الواقعة على الصُورة الرمزية الافتراضية، فضلاً عن عدم تحديد الاختصاص القضائي كون الاعتداء يقع في بيئة افتراضية غير تابعة لحدود أي دولة، ومعظم الاعتداءات التي تمس الصور الرمزية غير خاضعة لقانون، ومشكلة جمع الأدلة من الميتافيرس.

## ثانياً: أهمية الدراسة.

تتأتى أهمية الدراسة في حداثة استخدام تقنية الميتافيرس، وما ترتبه من تداعيات سلبية لمستخدميها، ممّا يستدعي ضرورة التأطير القانوني للمسؤولية الجزائية الناشئة عن الاعتداءات الواقعة على الصُور الرمزية في الميتافيرس، خاصةً في ظل غياب منح الهوية الرقمية -الشخصية القانونية- للصُورة الرمزية "الافاتار"، فيجعل من الأهمية بمكان البحث في إمكانية تطبيق قانون الجرائم الإلكترونية على الاعتداءات الواقعة في هذه التقنية، كما أن هذه الدراسة تأمل في تقدير درجة الموازنة بين الاعتداء الإلكتروني -التقليدي- وذلك الافتراضي.

## ثالثاً: مشكلة الدراسة وتساؤلاتها.

تمكّن تقنية الميتافيرس للمستخدم إجراء أنشطة افتراضية، وهذه الأنشطة تتم من خلال تقمص المستخدم لصُورة رمزية "افاتار" تعود للغير، وهذه الصُورة ليس لها هوية رقمية بالمعنى التقني أو القانوني، بحيث يصعب التوصل من خلالها إلى معرفة ماهية المستخدم الحقيقي -المعتدي-، الأمر الذي يصعب معه تعقبه في كل مرة يعتدي على الصُور الرمزية العائد للغير داخل تقنية الميتافيرس، ومن هنا، فإن مشكلة الدراسة الرئيسية تنحصر في غياب السند القانوني لتوصيف بعض الأنشطة العدائية الواقعة على الصُور الرمزية الافتراضية داخل الميتافيرس كاستخدامها في التزيف العميق والتصيد الاحتمالي والأنشطة الجنسية والمقامرة الافتراضية وغيرها من الاعتداءات غير المشروعة.

لهذا، فإن مشكلة الدراسة تكمن بطرح سؤال رئيسي يتمثل بمدى إمكانية المساءلة الجزائية عن الاعتداءات غير المشروعة الواقعة على الصُور الرمزية الافتراضية في الميتافيرس؟ وينبثق عن هذا التساؤل أسئلة فرعية تتمثل فيما يلي:

1. ما المشاكل القانونية -الموضوعية والشكلية- التي تثيرها هذه التقنية عند الاستخدام غير المشروع للصُور الرمزية؟
2. ما تقنية الميتافيرس والصُور الرمزية الافتراضية، وهل ثمة فرق بين الجرائم الإلكترونية وتلك المرتكبة على الافاتار؟
3. هل من المتصور حدوث اعتداءات على الصُور الرمزية الافتراضية في الميتافيرس وبواسطتها؟
4. ما صور الاعتداءات الواقعة على الصُور الرمزية في الميتافيرس؟ ومدى إمكانية تطبيق نصوص قانون الجرائم الإلكترونية على الاعتداءات الواقعة على الصُور الرمزية الافتراضية؟
5. هل يتصور تحقّق المساءلة الجزائية لمرتكبي الاعتداءات على الصُور الرمزية الافتراضية؟

## رابعاً: أهداف الدراسة.

تهدف هذه الدراسة إلى تسليط الضوء على موضوع حديث نسبياً من خلال إيجاد تعديل لبعض نصوص قانون الجرائم الإلكترونية، ممّا يجعلها تستوعب الاعتداءات الواقعة على الصُور الرمزية في الواقع الافتراضي "الميتافيرس"، كَوْن بعض الاعتداءات على الصُور الرمزية لم ينظمها القانون، ولاسيما تلك الاعتداءات التي لا يمتد أثارها للواقع المادي للمستخدم، كالمساس بحقوق الملكية الفكرية الافتراضية وغسيل الأموال والإرهاب الافتراضي والاعتداءات الجنسية الافتراضية والتزيف العميق... الخ، وهذا يخلق بعض الاشكاليات الموضوعية والشكلية التي تحول دون الملاحقة القضائية لمن يعتدي على الصُور الرمزية الافتراضية.

### خامساً: منهج الدراسة.

تعد هذه الدراسة من الدراسات الاستشرافية لمستقبل الدراسات القانونية المتخصصة في قانون الجرائم الإلكترونية، التي تسعى لابتكار منظور قانوني، وهذا بطبيعة الحال ينعكس على منهج البحث الذي يقتضي إتباعه عند إعداد هذه الدراسة حتى يتسنى لنا الإجابة عن مشكلة الدراسة وتساؤلاتها، حيث تم الاعتماد على ثلاثة مناهج بحثية، وهي:

1. المنهج الوصفي: من خلاله يتم تشخيص ظاهرة الاعتداء على الصُّور الرمزية أو كما تسمى بجرائم الخيال التقني من كافة جوانبها وعناصرها.
2. المنهج التحليلي: ذلك من خلال تحليل الموقف القانوني للوصول إلى منطق القانون الأمثل للتطبيق على هذا النوع الجديد من الاعتداءات، وذلك باقتراح نصوص قانونية لمعالجة الفراغ أو القصور التشريعي للاستخدام غير المشروع جزائياً للصُّور الرمزية.
3. المنهج المقارن: والذي يهدف إلى البحث عن التكييف الممكن للمسؤولية الجزائية لمرتكبي الاعتداءات على الصُّور الرمزية، وفقاً للقواعد العامة في قانون الجرائم الإلكترونية الأردني، والاستشهاد مع القانون البريطاني -كلما أمكن ذلك-.

### سادساً: الدراسات السابقة.

#### 1. دراسة:

Qin,H, et al(2025) *Identity, crimes, and law enforcement in the Metaverse*. Humanities and Social Sciences Communications volume 12, Article number:194.

تناولت الدراسة المعنونة ب:(الهوية والجرائم وتطبيق القانون في الميتافيرس)، طبيعة الميتافيرس، كمساحة جغرافية غير محدودة تمزج بين الموقعين المادي والافتراضي، وتُشكل تحديات جديدة لتطبيق القانون. ولمعالجة هذه التحديات، تدعم هذه الدراسة إرساء إطار قانوني دولي موحد؛ وتحديداً، من منظور جهات تطبيق القانون الدولي، وتُقدم الدراسة مناقشة شاملة حول المخاوف القانونية المتعلقة بالهوية، وأنواع الجرائم المحتملة، والتحديات التي تواجه تطبيق القانون الموحد في الميتافيرس.

#### 2. دراسة: Quintero,J.et al,(2024) *A scoping study of crime facilitated by the metaverse*. Futures journal,Volume 157.

هذه الدراسة المعنونة ب(دراسة نطاقية للجريمة يسهلها الميتافيرس) تبحث في الآثار الإجرامية والأمنية للتقنيات الناشئة عن الميتافيرس، والتي تضمنت مراجعة نطاقية حديثة للأدبيات الحالية من بريطانيا وأوروبا والقانون الدولي، وقد تم تحديد ما مجموعه 30 تهديداً إجرامياً في الأدبيات، كما استكشفت مدى وقوع الضرر الذي توقعه المشاركون ومدى تكرار حدوثه وقابليته للتحقيق في الجرائم ذات الطابع الجنسي، والجرائم ضد الأشخاص، وهذه الدراسة تُساعد الجهات المعنية على تحديد أولويات الجرائم التي يجب التركيز عليها في عالم الميتافيرس. ترتبط دراستنا بهاتين الدراستين من حيث أنهما يبينان ماهية الميتافيرس والعمل على حماية الافاتار من الاعتداءات الواقعة عليه، في حين تتميز دراستنا عن سابقتها بأنها تسلط الضوء على نوع جديد من الاعتداءات الإلكترونية، ولكنها غير مشمولة بقانون الجرائم الإلكترونية.

### سابعاً: مصطلحات الدراسة:

1. الواقع الافتراضي (VR) "Virtual reality": هو تقنية تفاعلية تُحاكي بيئة ثلاثية الأبعاد، يُمكن استكشافها والتفاعل معها باستخدام أجهزة إلكترونية متخصصة، مثل سماعات الرأس وأجهزة التحكم، ويُضفي هذا الواقع شعوراً بالتواجد، ويتيح للمستخدمين تجربة عوالم افتراضية أو سيناريوهات مُحاكاة والتفاعل معها، للواقع الافتراضي تطبيقات في مجالات مُختلفة، بما في ذلك الألعاب والترفيه والتعليم والتدريب وغيرها(Barta,S.et al.2024).
2. الواقع المعزز (AR) "Augmented reality": تقنية تدمج العالمين المادي والافتراضي، من خلال عرض الصُّور والمعلومات الرقمية في بيئة مادية، حيث يُتيح هذا الواقع للمستخدمين رؤية العالم الحقيقي، مع إسقاط أشياء رقمية عليه(Miraj,Z,2023).
3. الواقع الممتد (XR) "Extended reality": هو مصطلح شامل يشمل جميع التقنيات التفاعلية، بما في ذلك التقنيات الموجودة حالياً: الواقع المعزز، والواقع الافتراضي، والواقع المختلط، بالإضافة إلى التقنيات التي لم تُطوّر بعد(Karapatakis,A,2025).
4. الواقع المختلط (MR) "Mixed Reality": هو امتداد لواقع المعزز، متفوقاً على الواقع الافتراضي والواقع المعزز، الذي يوفر معلومات رقمية ثلاثية الأبعاد، تسمح للعنصرين بالتفاعل في الوقت الفعلي، بحيث يُمكن وضع الأشياء الافتراضية في الواقع المادي والتحكم فيها(Karapatakis,A,2025).

## ثامناً خِطّة الدراسة:

من خلال طرح مشكلة الدراسة وتساؤلاتها ووصف الافكار واستشراف فرضيات المسؤولية الجزائرية عن الاستخدام غير المشروع للصُّور الرمزيّة الافتراضية في الميتافيرس، ثم تقييم النتائج والتوصيات التي تساهم في إيجاد حلول لمشكلة الدراسة، وذلك وفقاً للتقسيم الآتي:

المبحث الأول: ماهية تقنية الميتافيرس، والصُّور الرمزيّة، وتميزهما عن الجرائم الإلكترونية.

المبحث الثاني: إشكالية تطبيق المسؤولية الجزائرية على الاعتداءات الواقعة على الصُّور الرمزيّة.

## المبحث الأول

### ماهية تقنية الميتافيرس والصُّور الرمزيّة وتميزهما عن الجرائم الإلكترونية

الميتافيرس هي أحدث تكنولوجيا موجودة في التقنيات الرقمية، بل يُمكن اعتبارها فكرة حديثة تكاد تكون غير معروفة لدى معظم مستخدمي الإنترنت، وهي تعمل بواسطة استخدام الصُّور الرمزيّة، لذا، كان لازماً بيان ماهية تقنية الميتافيرس والصُّور الرمزيّة، في المطلب الأول، والتمييز بين الجرائم الإلكترونية، والاعتداء على الصُّور الرمزيّة في الميتافيرس، في المطلب الثاني.

## المطلب الأول

### ماهية تقنية الميتافيرس والصُّور الرمزيّة

في عام 1992، استخدم نيل ستيفنسون "Neal Stephenson" مُصطلح "ميتافيرس" لوصف عالم افتراضي يتفاعل فيه الناس مع بعضهم البعض باستخدام الصُّور الرمزيّة الافتراضية "الافاتار" (Karapatakis,A,2025)، وبمرور الوقت، تحوّل تقنية الميتافيرس إلى مفهوم مُعقّد يُشبه الفضاء الإلكتروني، فتقنية الميتافيرس هي بيئة افتراضية تستخدم تقنيات تحاكي العالم الحقيقي من خلال الصُّور الرمزيّة، فهذه التقنية تعمل من خلال أدوات تكنولوجيا حاسوبية متصلة بالإنترنت، تسمى بالعالم الافتراضي "Virtual reality" VR- وهي نظارات محوسبة توفر بيئة ثلاثية الأبعاد تحيط بالمستخدم وتستجيب لأفعاله بطريقة طبيعية (Qin,H, et al.2025)، وعادةً ما تتصل بالواقع المعزز-AR "Augmented Reality"- وهي السترات والقفازات المزودة بمستشعرات لإيصال الشعور المادّي الذي ينقل المستخدم من الواقع الحقيقي إلى عالم شبه حقيقي (Quintero,J.et al,2024).

من هذا المنطلق كان لازماً بيان ماهية تقنية الميتافيرس في الفرع الأول، وماهية الصُّور الرمزيّة الافتراضية في الفرع الثاني.

## الفرع الأول

### ماهية تقنية الواقع الافتراضي "الميتافيرس"

يُمكن القول: إنّه ثمة غموض في تحديد معنى الميتافيرس، وربما يعود ذلك إلى أنّه ما يزال هناك المزيد من العمل ليتم انتشار هذه التقنية بشكل واسع (Lee.et al,2021). وحتى نحدّد المعنى الدقيق للميتافيرس يجب تحديد مفهومه، ومن ثم خصائصه، وأهم الاعتداءات الواقعة عبر تقنية الميتافيرس.

## أولاً: مفهوم تقنية الميتافيرس:

1. المفهوم اللغوي: الميتافيرس ليس كلمة عربية، وإنّما انجليزية "Metaverse"، تم إنشاؤها باستخدام مصطلحين الأول "الميتا" ويأتي من الكلمة اليونانية "meta" بمعنى "وراء" أو "ما بعد" والثاني "verse" مصاغ من "Univeres" بمعنى العالم أو الكون، ولذلك فإن ميتافيرس تعني "ما وراء الكون" أو "ما وراء العالم" (إبراهيم، م، 2024، ص16). كما عرّف معجم أكسفورد الإنجليزي بأنّ الميتافيرس مصطلح عام يستخدم لوصف تمثيل افتراضي للواقع يتم تنفيذه بواسطة برامج الواقع الافتراضي (رابط Metaverse). كما وعرف معجم اللغة العربية المعاصر "الميتافيرس"، بوصفه واقعاً تقريبياً افتراضياً بأنّه "محاكاة يولدها الحاسوب لمناظر ثلاثية الأبعاد لمحيط أو سلسلة من الأحداث تمكّن النّاطر الذي يستخدم جهازاً إلكترونياً خاصاً من أن يراها على شاشة عرض ويتفاعل معها بطريقة تبدو فعلية (رابط Metaverse).

## 2. المفهوم التقني:

بشكل عام، تتجنب الأوساط الأكاديمية تحديد مفهوم للميتافيرس بشكل صارم، والسبب بذلك يعود للتطور التكنولوجي السريع الذي يُغيّر خصائصها إلى حد ما، ورغم ذلك، عرّف البعض الميتافيرس بأنّه عالم ما بعد الواقع (Mystakidis,2022)، يتم فيه دمج الواقع المادّي مع البيئات الافتراضية بشبكة اجتماعية وترفيهية متصلة تضم تفاعلات مستمرة ومتعددة الأشخاص (Pandey,D.Gilmour,P,2024,P:211)، وتقوم تكنولوجيا الواقع الافتراضي مع الواقع المعزز والواقع المختلط والبيئات ثلاثية الأبعاد وتقنيات الذكاء الاصطناعي بالاندماج والتفاعل معاً لتكون صُورة رمزيّة (Avatar) الذي يقدم الأخير واقع مواز لواقع المادّي للمستخدم (Miraj,Z,2023). وبالنظر إلى هذا المفهوم يتبيّن أنّه يميل إلى المفهوم التقني المحض، وإن كان يستند بشكل أساسي إلى المنظورين الاجتماعي والترفيهي، كون محور تقنية الميتافيرس هو الترفيه والتواصل الاجتماعي في بيئة رقمية، بيد أنّه تجاهل طابعه الصناعي والتجاري ومهني (Karapatakis,A,2025).

### 3. المفهوم الاصطلاحي:

عزف تقرير الإنترنت الدولي تقنية الميتافيرس "بأنها شبكات واسعة من التقنيات التي تشمل الواقع الافتراضي والواقع المعزز والحوسبة المتطورة وتهدف إلى تمكين الناس- في جميع أنحاء العالم وعبر صُور رمزية- من الوصول إلى بيئات افتراضية ثلاثية الأبعاد مشتركة باستخدام شبكة الإنترنت وأجهزة متنوعة ومتخصصة تلخص إحساساً بالوجود الافتراضي" (<https://www.google.com/search?q=>)، كما وعرفها البعض بأنها: "عالم رقمي قائم على الواقع الافتراضي، حيث يتفاعل البشر في الوقت الفعلي باستخدام صُور رمزية ثلاثية الأبعاد، وتتيح للمستخدم تجارب جديدة من خلال تمكينه التفاعل بشتى جوانب الحياة عبر الإنترنت" (Severgin,A,2023.P:38).

ويمكن أن نُقدم مفهوماً أبسط بكثير لوصف العديد من الأنشطة المتاحة في تقنية الميتافيرس باعتبارها شبكة إلكترونية قابلة للتشغيل المتبادل من العوالم الافتراضية بحيث تُمكن المستخدمين من الالتقاء بواقع هجين على نحو يُشبه الالتقاء في الواقع الحقيقي دون اعتبار للنطاق الجغرافي، والتي يُمكن تجربتها بشكل متزامن ومستمر من قبل عدد غير محدود من المستخدمين مع إمكانيةة الحضور وعقد اجتماعات ومؤتمرات والتعاقد والاتصالات والدفع الإلكتروني وغير ذلك.

ثانياً: أهم خصائص الميتافيرس.

1. **المتافيرس و اقع إفتراضي مواز:** تتميز تقنية الميتافيرس بأنها تقوم على فكرة الواقع الافتراضي، الذي يُعدّ في ظاهره مجرد خيال تقني، وفي حقيقته يضمّ الكثير من التطبيقات الواقعية (Mustawi,et al,2022)، فالمتافيرس تُكون للمستخدم عالماً ثالثاً ما بين عالمين، الأول: عالم مادي ملموس، وهو الحياة الطبيعية التي يعيشها البشر، والثاني: عالم إفتراضي كونه التقنيات الحديثة وهو الفضائي الإلكتروني، فتأتي تقنية الميتافيرس باعتبارها عالماً ثالثاً افتراضياً موازياً لثلاثي الأبعاد يُمكن للمستخدم من التجربة التفاعلية (Karapatakis,A,2025)، حيث يُقدم الميتافيرس مستوىً جديداً من التكنولوجيا يتيح للمستخدمين الانغماس التام في الواقع الافتراضي، وباستخدامها يُمكن التفاعل مع الأشياء الرقمية، واستكشاف أشياء يستحيل رؤيتها في العالم المادي كالخلية النانوية مثلاً (Song,C,&others,2023).

2. **حرية المحتوى الذي ينشئه المستخدم:** يعتمد الميتافيرس على المحتوى الذي يُنشئه المستخدم (UGC): فتمكّن هذه الخاصية المستخدمين من إنشاء محتوى وتعديله ومشاركته داخل الواقع الافتراضي في أغلب الأحيان (Sadeghi-Niaraki.A et al,2025)، وبشكل المحتوى الذي يُنشئه المستخدمون النظام البيئي الديناميكي للميتافيرس، ويُحفّز المحتوى التفاعل والابتكار من خلال الصُور الرمزية، ممّا يُمكنهم من صياغة نشاطاتهم الافتراضية بكل يسرّ وحرية (Kang,G,et al,2023).

3. **تسمح الميتافيرس التشغيل البيئي:** يُفهم الميتافيرس على أنه نظام بيئي يربط بين التطبيقات والخدمات المتعددة التي تُشكل جزءاً منه، وهكذا، تُعدّ قابلية التشغيل البيئي سمة أساسية أخرى لهذا التقنية، حيث يُمكن للمستخدمين التفاعل مع تطبيقات مختلفة في آنٍ واحد (Song,C,&others,2023)، ويُمكن للمستخدمين نقل صُورهم الرمزية وأصولهم وتجاربهم الافتراضية عبر منصات متعددة دون قيود في الميتافيرس (Geldenhuys,K,2024)؛ بمعنى آخر، سيُتاح "الانتقال" إلى مساحات افتراضية ذات مواضيع مختلفة، أو مقاطعة نشاط لبدء نشاط آخر دون مغادرة الميتافيرس، وعلى سبيل المثال، يمكن استخدام ونقل أصل رقمي تم شراؤه في واقع افتراضي إلى واقع افتراضي آخر داخل تقنية الميتافيرس (Dong,S,et al.2024).

وخلاصة القول أنّ تقنية الميتافيرس هي شبكة إلكترونية افتراضية تُمكن المستخدمين من الالتقاء بواقع هجين على نحو يُشبه الالتقاء في الواقع الحقيقي من خلال الصُور الرمزية، من دون اعتبار للنطاق الجغرافي. وهذا بطبيعة الحال جعل من هذه التقنية تنسم بالعديد من الخصائص، أهمها تكوين واقع افتراضي للواقع الموازي، وتكوين مساحة خاصة للمستخدم داخل الواقع الافتراضي، فضلاً عن التشغيل البيئي.

### الفرع الثاني

#### ماهية الصُور الرمزية الافتراضية "الافاتار"

الصُور الرمزية الافتراضية أو كما تسمى بصُور الذكاء الاصطناعي الرمزية أو بالشخصيات التمثيلية، والمشهورة بمصطلح الافاتار (Lisetti.C.2012)، يعود تاريخ نشأتها إلى الثمانينيات مع ظهور الشبكة الاجتماعية الأولى -الألعاب الإلكترونية- والتي كانت تعكس شخصيات المستخدمين بطريقة بدائية؛ ومع تقدّم التكنولوجيا في التسعينيات أصبحت الصُور الرمزية أكثر تطوراً وتعبيراً، حيث بدأت تستخدم في المنتديات والشبكات الاجتماعية المتكبرة، مثل (Yahoo Messenger) وفي تلك المرحلة بدأت الصُور الرمزية تعبر عن هوية المُستخدم الرقمية بشكل أكبر؛ ومع بداية الألفية الجديدة أصبحت الصُور الرمزية جزءاً لا يتجزأ من وسائل التواصل الاجتماعي والمنتديات-منصات الألعاب عبر الإنترنت، وفي الوقت الحاضر عرّفت الصُور الرمزية تطوراً كبيراً خاصةً عند ظهور تقنيات الواقع الافتراضي والواقع المعزّز في الميتافيرس، ممّا جعلها أكثر واقعية وفاعلية من ذي قبل، إضافةً إلى ذلك أصبح بإمكان المستخدمين الآن الدخول إلى عوالم افتراضية كاملة، والتفاعل مع بعضهم البعض من خلال صور رمزية تعبر عن حركاتهم بشكل دقيق (Barta,S,et al.2024). ومن هنا كان لازماً لتحديد ماهية الافاتار، تحديد مفهومه وخصائصه، وأهم الاعتداءات الواقعة

على الصور الرمزية، وذلك على النحو التالي.

### أولاً مفهوم الصُّور الرمزية الافتراضية "الافاتار":

1. المفهوم اللغوي: في اللغة العربية الصُّور الرمزية الافتراضية عبارة مركبة من ثلاث كلمات، تعنى صَوْرَ: بصوْر، تصوِراً، فهو مُصوِّر، والمفعول مُصوَّر، وصَوَّرَ الشَّيْءَ: جَعَلَ لَهُ صُوْرَةً، رَسَمَهُ، جَسَّمَهُ جَعَلَ لَهُ شَكْلاً وَصُوْرَةً؛ وتعني الرَّمْزِيَّةُ: اسم مؤنث منسوب إلى رَمَزَ، وهي: مَدَّهَبٌ فِي الْفَنِّ وَالْأَدَبِ يَعْتمِدُ الْإِيحَاءَ وَالتَّلْمِيحَ بِرُموذِهِ الْمُنبِثَةِ مِنَ الصُّوْرِ الْجَسِيَّةِ وَالْأَسَاطِيرِ، وَيَتَرَكُّ لِلْقَارِئِ مَجَالاً لِلتَّصَوُّرِ وَالخَيَالِ لِإِكْمَالِ الدَّلَالَةِ الرَّمْزِيَّةِ كَمَا تُوجِي بِهَا؛ وتعني افتراض: افتراض يفترض، افتراضاً، فهو مُفترض، والمفعول مُفترض، وافتراض أمراً: اعتبره قائماً أو مسلماً به، أخذ به في البرهنة على قضية أو حلّ مسألة" (<https://www.almaany.com/ar/dict/ar-ar/>) وبتجميع تلك الكلمات يُمكن القول أنها تعني صُوْر مجسمة ذات دلالات رمزية تمثيلية في عالم افتراضي غير ملموس.

أما المعنى الحر في اللفاتار، يأتي معناه من اللغة الهندوسية، وتعني الاستنساخ أو الولادة من جديد، والتي قد تكون على شكل إنسان أو حيوان أو طائر أو أي كائن حي آخر (Lisetti.C.2012). وفي قاموس اكسفورد ورد ذكر كلمة "أفاتار" وهي كلمة مشتقة من الكلمة السنسكريتية "أفاتارا" وتعني "الانحدار"، كما وتعني تقنياً "تجسيدا أو تجسيدا لشخص أو فكرة" ([https://www.oed.com/dictionary/avatar\\_n?tl=true](https://www.oed.com/dictionary/avatar_n?tl=true)).

2. المفهوم الاصطلاحي: هي بإتباع الشخصية الكترونية الرقمية الافاتار التي تُحاكي شكلاً بشرياً أو شخصية خيالية التي يختارها المستخدم لتمثيل نفسه داخل تقنية الميتافيرس في ألعاب الفيديو، أو على مواقع التواصل الاجتماعي، أو على منتديات الإنترنت، أو التقنيات (Barta,S.et al.2024).

وأكثر توضيحاً، هي صُوْر أو رموز أو رسومات متحركة تمثل شخصية المستخدم على الشبكة المعلوماتية-مواقع الويب-، ويُمكن أن تُكون الصُّور الرمزية عبارة عن أيقونات ثنائية الأبعاد كصُوْر للملفات الشخصية على منصات التواصل الاجتماعي والمنتديات، كما يُمكن أن تُكون على شكل صُوْر ثلاثية الأبعاد تستخدم في الميتافيرس، وهي تُمكن المستخدم من التعبير عن هويته الشخصية بشكل رقمي، ويُمكن تعديلها وتخصيصها لتشبه الشخص الحقيقي أو لصُوْر خيالية تعكس جوانب من شخصية المستخدم أو اهتماماته (Horne,C.2023).

### ثانياً أهم خصائص الصور الرمزية الافتراضية:

1. ارتباط الصور الرمزية بالذكاء الاصطناعي: الصُّور الرمزية ما هي إلا مجسمات متحركة رقمية للبشر، حيث تُحاكي حركاتهم والإيماءات وتعبيرات الوجه، وحتى صوت المستخدم، ممّا يجعلها الأداة المثالية لمحاكاة التفاعلات في الواقع الحقيقي في الميتافيرس، حيث تنشأ باستخدام الذكاء الاصطناعي، ممّا يُمكن استخدام هذه الصُّور الرمزية في سياقات مختلفة، سواءً للترفيه، أو لممثلي خدمة العملاء الافتراضيين، أو كمنثلي ذكاء اصطناعي في المحتوى التعليمي أو في مجالات القانون والصحة وغيرها من القطاعات المهنية والصناعية والتجارية (Cheong,B.2022).

2. الصُّور الرمزية توفر هوية رقمية "بصرية" للمستخدمين: تسمح تقنية الميتافيرس بالفصل بين الهوية الحقيقية للمستخدم وهويته الافتراضية، فهي تُمكن المستخدم من التفاعل والتواصل والتنقل في الواقع الافتراضي، إذ تزداد أهمية الهوية الرقمية في تفاعل المستخدم مع الآخرين ضمن إطار تقنية الميتافيرس، وألعاب الفيديو، والمساحات الافتراضية ثلاثية الأبعاد، ممّا يجعل من الصُّور الرمزية أداة تُسهل التفاعل الاجتماعي مع المستخدمين الآخرين، فكل مستخدم ينشئ في الميتافيرس صورة رمزية "أفاتار" أو أكثر، فضلاً عن ذلك، يُسهل اختيار الصورة الرمزية التعرف إليها فوراً من قبل المستخدمين، ذلك في حال رغب المستخدم للصورة الرمزية الكشف عن هويته الرقمية، وبذات الوقت، يصعب جداً تعقب آثارها حال وقوع اعتداء ما، خاصةً إذا كانت مُخصّصة ومُصمّمة بعناية فائقة لإخفاء هويته الرقمية (Lisetti.C.2012).

3. ارتباط الصور الرمزية مع الميتافيرس: تُمثل الصور الرمزية نقلة نوعية في الانغماس والتفاعل، فمن خلال تقنية الميتافيرس، يُمكن إنشاء صُوْر رمزية مطابقة تماماً لصُوْر المستخدم، ذلك باستخدام أحدث تقنيات التصوير الفوتوغراممترية. والجدير بالذكر يتيح دمج الصور الرمزية في مساحات ميتافيرس جمع معلومات وبيانات ضخمة حول تفاعل المستخدم وسلوكه، بحيث تترك هذه الصور الرمزية أثراً من التفاعلات والخيارات الإضافية، ممّا يسمح لمزودي الخدمة جمع أكبر قدر من المعلومات الشخصية عن المستخدم (Lisetti.C.2012).

### ثالثاً الاعتداءات الواقعة على الصُّور الرمزية الافتراضية في الميتافيرس:

رغم أنّ تقنية الميتافيرس في حقيقتها ما هي إلا تقنية إلكترونية تعتمد على خوارزميات وبرمجيات شأنها بذلك شأن البرامج الإلكترونية المحمية في قانون الجرائم الإلكترونية، والاعتداء على هذه التقنية من حيث تشفيرها أو اشغالها أو تعطيلها يرتب القانون على ذلك عقوبة جزائية وفقاً للمادتين (3/ب. 4/أ.ب) من قانون الجرائم الإلكترونية الأردني، إلا أنّ المساس بالصُّور الرمزية الافتراضية داخل تقنية الميتافيرس غير خاضع للرقابة القانونية، كونها تعيش داخل تقنية الميتافيرس، لهذا، يمكن تقسيم أوجه الاعتداء على هذه التقنية بنوعين من الاعتداءات؛ الأول مخالفة قواعد قانون الجرائم الإلكترونية، الواقعة في الكيان المادي وهي مُجرمة عموماً، والثاني الماسة بالصُّور الرمزية الافتراضية، وهي أفعال لم تُجرّم بعد. وبعقودنا أنّ مسألة تجريم-الاعتداءات على الصُّور الرمزية- يعتمد على إثبات الضرر، وهذا الأمر يمكن أن يتحقق كونها الصُّور الرمزية تمزج

بين الواقع المادي والافتراضي، مما يقتضي ضرورة إعادة النظر في تجريم الاعتداءات الحاصلة بواسطتها؛ ولإثراء عملية التجريم، سيتم العمل على تحديد جانباً من الجرائم الكبرى المحتملة عبر تقنية الميتافيرس على النحو التالي:

#### 1. جرائم الملكية الافتراضية:

في العوالم الافتراضية، يمكن للأفراد إنشاء وامتلاك وتعديل وتبادل العديد من الأشياء الافتراضية، مثل ملحقات الصورة الرمزية، والإبداعات الفنية، والعملات الافتراضية، مثل سلسلة الكتل والروبوكس الخاصة بالصور الرمزية (Huang RH, et al.2023)، حيث يُمكن إتلاف هذه الأشياء أو أخذها بطريقة غير مشروعة، على سبيل المثال، يمكن للأشخاص إتلاف الأعمال الفنية الافتراضية للافتاتار، مما يتسبب في تلف دائم إذا تم استبدال بياناتها الأصلية دون نسخة احتياطية، يمكنهم أخذ "سرقة" العناصر الإضافية أو عملات المنصة من خلال الاحتيال على معلومات الحساب، أو القرصنة (Seo.S.et al.2023).

وهنا كان لازماً التفريق بين الأشياء الافتراضية التي تخضع لرقابة قانون الجرائم الإلكترونية، وتلك التي لا تخضع له، فإذا كان الحرمان المماثل من شيء افتراضي ذي قيمة نقدية حقيقية، كأن يكون قابلاً للبيع أو الشراء بأموال حقيقية، يطبق عليه قانون الجرائم الإلكترونية كون أثر الجريمة تجاوز النطاق الافتراضي، مثل بعض الأعمال الفنية الافتراضية تبلغ قيمتها حالياً ملايين الدولارات، بينما الأشياء لا ينطبق عليها الحرمان، ولا تكون محلاً للجريمة الإلكترونية التي ليس لها قيمة نقدية حقيقية، مثل ملحقات الصورة الرمزية المجانية، وغير المحدودة في الألعاب الموجودة في الميتافيرس.

#### 2. غسيل الأموال والإرهاب الافتراضي:

هناك عملات مشفرة للميتافيرس، تُستخدم في العوالم الافتراضية المدعومة بتقنية بلوكتشين لشراء وبيع وتداول الأصول الرقمية، مثل الأراضي الافتراضية، وعناصر الصور الرمزية، ورموز كالمُتاجر والسلع والخدمات، وهذه العملات ذات قيمة نقدية يمكن تحويلها إلى نقد مادي (Huang,RH,et al.2023)، ومن خلال هذه العملات يمكن حدوث جريمة غسيل الأموال في ميتافيرس وفي المنصات الحالية، وتتم مرحلة غسيل الأموال في ثلاث مراحل؛ الأولى هي التنسيب، حيث يتم إدخال الأموال غير المشروعة إلى سوق "الميتافيرس" في شكل "أشياء" افتراضية، مثل العملات المشفرة، والثانية هي الطبقات، حيث يخفي المجرمون أصول الأموال عن طريق إنشاء دليل زائف من خلال سلسلة من المعاملات، مثل الشراء من خلال شركات وهمية (Seo.S.et al.2023)، والثالثة هي التكامل، حيث يتم إعادة الأموال ذات الأصول القانونية الآن إلى النظام الاقتصادي الرئيسي، مثل بيع الأصول الافتراضية، وقد تم استخدام العملات المشفرة، وهي خيارات قابلة للتطبيق لعملات ميتافيرس، لتسهيل غسل الأموال، وتمويل أنشطتهم الإجرامية ونشرها؛ لأنها أقل قابلية للكشف من خلال عدم الكشف عن الهوية أثناء إنشائها وسهولة تقسيمها إلى مبالغ صغيرة (Cheong,B.C.2022).

وفي سياق متصل تسلل الإرهاب بالفعل إلى العالم الافتراضي، حيث يستطيع الإرهابيون استخدام الواقع الافتراضي للتخطيط والتخطيط الاستراتيجي ومحاكاة الهجمات الإرهابية والتدريب عليها من خلال استخدام الصور الرمزية، ولعل الأمر الأكثر إشكالية هو إمكانية استخدام هذه المنصات أيضاً لأغراض التجنيد، إذ يمكن تقديم الدعاية الإرهابية بطرق أكثر وضوحاً وإقناعاً من وسائل الإعلام والمنصات الأخرى، ويُمكن للمنظمات الإرهابية استخدام الواقع الافتراضي لتدريب المجندين على استخدام الأسلحة، بالإضافة إلى تثبيط حساسيتهم تجاه الاحتمالات التي قد تنتج عن أفعالهم (Barta,S.et al.2024).

#### 3. الاستلاء على الهوية الافتراضية:

الاستلاء على الهوية الافتراضية هي شكل من أشكال انتحال الشخصية، حيث يستخدم الجاني المعلومات الشخصية لمستخدم الصورة الرمزية الافتراضية دون موافقة الأخير، إذ يُمكن أن تحدث سرقة الهوية الرقمية للصورة الرمزية من خلال اختراق الجاني لحساب مستخدم آخر ثم التظاهر بأنه صاحب الحساب للصورة الرمزية الخاصة به عبر تقنية الميتافيرس؛ فتوقع السرقة على مظهر الصورة الرمزية والإيماءات أو العملات أو السلع الافتراضية، أو من خلال اختراق الحسابات لابتزاز المستخدم، وذلك بالتهديد بنشر معلومات شخصية أو تعطيل البيئات الافتراضية ما لم تُدفع فدية (Cheong,BC.2022)، وربما لارتكاب الاحتيال الافتراضي، ذلك عند استخدام هويات أو معلومات زائفة لخداع الآخرين عبر تقنية الميتافيرس، وتشمل عمليات التصيد الاحتيالي، أو بيع سلع افتراضية مزيفة (Deng,M.et al.2023).

#### 4. المقامرة الافتراضية:

يُجرم قانون العقوبات الأردني المقامرة في المواد (393-395)، ولم ينص على تجريمها في قانون الجرائم الإلكترونية، ومع ذلك في حال ثبوت أن الشخص مارسها في المجال الإلكتروني يتم ملاحقته وفقاً للقواعد العامة باعتبار الوسيلة الإلكترونية ما هي إلا أداة لتحقيق النتيجة الجرمية المتمثلة بالمراهنة على شيء مادي. وتُعد إمكانات المقامرة بواسطة الصور الرمزية في الميتافيرس متعددة الاستخدامات، إذ يُوجد أماكن في الميتافيرس مخصصة للعب القمار بجميع أنواعه -الكازينوهات وصلالات القمار الافتراضية-، يُمكن للمستخدم من خلال الصورة الرمزية اختيار التواصل مع الآخرين والدخول في المراهنات، مثل سباق خيول الميتافيرس، أو مباريات رياضية افتراضية، أو ماكينات القمار الافتراضية، أو ألعاب الطاولة في الكازينوهات مثل البلاك جاك والروليت الافتراضي، وطبعاً تتم المقامرة من خلال منح المستخدم الفائز نقاط أو جوائز للافتاتار، وتتم المراهنة من

خلال استخدام العملات الافتراضية، مما يسهل ذلك عملية غسل الأموال، فضلاً عن ذلك السماح لجميع الفئات العمرية بالمشاركة في مقامرة الميتافيرس حتى من هم دون السن القانوني (Karapatakis,A,2025)

#### 5. الاعتداء الجنسي الافتراضي:

في الميتافيرس، قد يُجبر المستخدم على ممارسة الجنس رغماً عنه في العالم الافتراضي، فيمكن أن يتخذ الاعتداء الجنسي شكل لمس يوحي لصورة المجني عليه الرمزيّة، أو أفعال جنسية على صورته الرمزيّة دون موافقته (Bellini,O,2024). ومن المؤكد أنّ تجريم الاعتداء الجنسي الافتراضي ما يزال موضع نقاش فقهي غير محسوم، فالبعض أنكر إمكانية حدوثها؛ لأنّ المستخدمين في تقنية الميتافيرس ما هم إلا صوّر رمزيّة مكونة من رموز حاسوبية، ولا يمكن لهذه الرموز أن تسبّب ضرراً (Bellini,O,2024)، في حين قام البعض بتقييم الاعتداء الجنسي الافتراضي كواحد من أكبر عشرة مخاطر موجودة في الميتافيرس، معتمداً هذا التقييم على أثر الضرر النفسي الناجم عن الأفعال في الواقع الافتراضي، والأذى الناجم عن الأفعال الجسدية المحتملة من الضرر النفسي (Gómez-Quintero,J,et al.2024)، ونحن نميل للرأي الأخير، ونؤكد أن الحاجة لتنظيم قانوني لهذه التقنية باتت ملحّة. وناقلة القول هنا: إنّه يُمكن توقع طيفٍ واسع من الاعتداءات على الصور الرمزيّة الافتراضية في الميتافيرس، والتي يمكن التحقق في الواقع المادي، ولا تجد السند القانوني للتجريم في الواقع الافتراضي، منها على سبيل المثال لا الحصر جرائم خطف الصوّر الرمزيّة والفعل المنافي للحياة وترويج المخدرات الافتراضية... الخ، وإن كانت هذه الدراسة لا يتسع مجالها لتناول هذه المواضيع، إلا أنّ الإشارة إلى أهمها قد يفي بالغرض منها، لهذا، ينبغي أن يكون لقانون الجرائم الإلكترونية دور بارز في حماية الصوّر الرمزيّة الافتراضية في الميتافيرس.

#### المطلب الثاني

##### التمييز بين الجرائم الإلكترونية والاعتداء على الصوّر الرمزيّة في الميتافيرس

منذ عام 1995 ساد مصطلح الجريمة الإلكترونية، وحظي بقبول واسع في الأوساط الأكاديمية والعملية (Phillips.et al.2022) ومنذُ ظهوره، واجهت الأوساط الأكاديمية والمهنية تحدياً يتمثل في التوصل إلى إجماع بشأن مفهومه، وعلى الرغم من عدم وجود مفهوم موحد، إلا أنّه يُمكن تحديد مفهوم الجريمة الإلكترونية بأنّها: اعتداء على حق ماديّ أو افتراضيّ من خلال تكنولوجيا المعلومات والاتصالات. وبالرغم من أنّ هذا المفهوم يتجاهل السمات المميزة للجرائم الإلكترونية، إلا أنّه مع ذلك، يوفر إطاراً متعدّد الاستخدامات يستوعب مجموعة واسعة من الأنشطة الإجرامية الناتجة عن التقدم والتطور المتقلب للتكنولوجيا. ومن هنا كان لازماً بيان أوجه التشابه والاختلاف بين نوعي الجريمة الإلكترونية والاعتداء على الصوّر الرمزيّة في الميتافيرس، وذلك من خلال الفرعين التاليين.

#### الفرع الأوّل

##### أوجه التشابه بين الجريمة الإلكترونية والاعتداء في الميتافيرس

أولاً الأداة المستخدمة ذات طابع متطور باستمرار: كلٌّ من الجريمة الإلكترونية والاعتداء على الصوّر الرمزيّة تتطلب وجود أدوات تكنولوجياية متطورة، فعلى غرار الجرائم الإلكترونية، تنسم الاعتداءات على الصوّر الرمزيّة بدناميكيتها المتطورة، إذ توفر تقنية الميتافيرس، بيئة مواتية لارتكاب الجرائم الإلكترونية، فضلاً عن نشوء جرائم إلكترونية جديدة في الواقع الافتراضيّ (Dwivedi,Y.et al.2023). وتُعتبر مجموعة واسعة من التقنيات الحديثة، بما في ذلك تكنولوجيا المعلومات والاتصالات، والحوسبة السحابية، والذكاء الاصطناعي، والرؤية الحاسوبية، وسلسلة الكتل، والروبوتات- إنترنت الأشياء-، وتفاعل المستخدم، والواقع المعزز، أدوات تُسهل من حدوث الاعتداء على حقوق المستخدم للتكنولوجيا (Lee,L.et al.2021). ثانياً تقنية الميتافيرس تصلح لارتكاب بعض الجرائم الإلكترونية: دائماً ما تُؤدّد التكنولوجيا المتطورة عدداً متزايداً من الفرص الإجرامية، وهذا ينطبق على تقنية الميتافيرس (Dwivedi,Y.et al.2023)، حيث يُمكن تتبع نقاط الضعف التي تُسيبها تقنيات الميتافيرس، وتكون محلاً لحدوث جرائم إلكترونية لاسيما إذا تعدت آثارها الواقع الافتراضيّ، ومستّ الواقع الماديّ للمستخدم، ومن هذه الجرائم -كما سبق بيانه- انتهاك حق الملكية الفكرية، وسرقة الهوية الرقمية، وغسيل الأموال والإرهاب الافتراضي، والاعتداءات الجنسية... الخ (Marshall,A.Tompsett,B.2024)، وهذا يعني أنّ التطورات التكنولوجية المتلاحقة في الإصدارات القادمة من الميتافيرس يُرجّح أن تُفاقم نقاط الضعف في الأمن السيبراني بدلاً من أن تقضي عليها.

ثالثاً تجاوز الحدود الزمانية والمكانية: لا يعكس في الجرائم الإلكترونية وتقنية الميتافيرس سمة الزمانية والمكانية الفائقة للفضاء الإلكتروني فحسب، بل يُضيق أيضاً الفجوة بين العوالم الحقيقية والافتراضية من خلال البنى والمحاكاة المجسمة- الهولوجرافية؛ باعتباره بيئة تفاعلية عبر الإنترنت، يتجاوز مستخدمي الوسائل الإلكترونية وتقنية الميتافيرس القيود المادية والزمنية التي تحكّم التفاعلات الشخصية في الواقع الماديّ (Wang,Y.et al.2022)، ويُمكن لمستخدمي الوسائل الإلكترونية، وأيضاً تقنية الميتافيرس الانخراط في تفاعلات عابرة للحدود الوطنية مع الآخرين باستخدام مجموعة متنوعة من الوسائط، بالإضافة إلى ذلك، فإن ظهور المحاكاة المجسمة- التمثيلات الافتراضية للكيانات المادية- يحجب الحدود بين المساحات الفعلية والافتراضية، من خلال استخدام المحاكاة المجسمة- التوائم الرقمية "الهولوجرافية"-، هذه السمة المكانية والزمانية المفرطة، التي تُسهّلها المحاكاة المجسمة يُمكن استخدامها لارتكاب جرائم إلكترونية (Lee,L.et al.2021).

## الفرع الثاني

## الاختلاف بين الجريمة الإلكترونية والاعتداء في الميتافيرس

أولاً التنظيم القانوني: رغم أن تقنية الميتافيرس في حقيقتها ما هي إلا تقنية إلكترونية تعتمد على خوارزميات وبرمجيات شأهاً بذلك شأن البرامج الإلكترونية المحمية في قانون الجرائم الإلكترونية وفقاً للمادة (2) منه، والاعتداء على هذه التقنية من حيث تشفيرها أو اشغالها أو تعطيلها يرتب القانون على ذلك عقوبة جزائية وفقاً للمادتين (3/ب. 4/أ.ب) من نفس القانون؛ إلا أن المساس بالصور الرمزية داخل تقنية الميتافيرس غير خاضع للرقابة القانونية، وعلّ السبب أن هذه الاعتداءات لا تمتد آثارها للواقع المادي للمستخدم. لهذا، تُقسم أوجه الاعتداء على هذه التقنية بنوعان من الاعتداءات (Seo.S.et al.2023)؛ الأول مخالفة قواعد قانون الجرائم الإلكترونية، الواقعة في الواقع المادي وهي مُجرّمة عموماً، والثاني الماسة بالصور الرمزية الافتراضية، وهي أفعال لم تُجرّم بعد (Huang RH,et al.2023).

ثانياً وقوع الضرر: إن الضرر المتصور في الجرائم الإلكترونية قد يكون مادي أو معنوي أو كليهما معاً، وتأكيداً لذلك، باستقراء خطة المشرع الأردني يتبين أن قانون الجرائم الإلكترونية تبنى فكرة وقوع الضرر بصفة عامة في المادة (38) التي نصّت "... وألحقت أضراراً بأبي من مصالحها أو مواطنها أو المقيمين فيها..." وإن كان النص المتقدم يتعلق بالاختصاص القضائي بيد أن شرط الملاحقة، وانعقاد الاختصاص، يتطلب تحقق الضرر. وإن كان شرط الضرر الحاصل على الصور الرمزية يكون معنوياً فحسب، ولا يمتد للضرر المادي.

وتطبيقاً لذلك، قضت محكمة بداية عمان بصفتها الاستئنافية في الأردن اشتراط وقوع الضرر في جريمة الذم والقدح والتحقيب الإلكتروني، وقضت بالحكم على للمتضرر بالتعويض عن الأضرار المادية والمعنوية (رقم 2023/2435، بداية عمان بصفتها الإستئنافية)، وبالرجوع إلى نص المادة (38) أعلاه يتبين أن القانون لم يحدّد نوع الضرر مادي أو معنوي، ويفهم من ذلك أن المطلق يأخذ على إطلاقه، وبالتالي الجرائم الإلكترونية أي من الضربين يتم الملاحقة، بينما في الواقع الافتراضي وقوع الضرر الناتج عن الاعتداء على الصورة الرمزية، ولم يمتد أثره للواقع المادي لا يطبق القانون عليه، بسبب غياب النموذج التجريبي لبعض الأنشطة في الميتافيرس؛ فمن غير المرجح أن يُسبب القتل الافتراضي موتاً فعلياً يتجاوز موت الصورة الرمزية، حتى لو حدثت وفاة فعلية عند موت الصورة الرمزية.

ولتبسيط المسألة يُمكن أن تقع جريمة القتل، إذا مات أحد مستخدمي الواقع الافتراضي في الحياة الواقعية نتيجة أفعال حصلت في الواقع الافتراضي، ولاسيما إذا لم تتوافر لدى الشخص المتسبب في القتل النية الإجرامية المطلوبة، فإن المستخدم الذي يعلم بضعف قلب صديقه، ورهيبته من الثعابين، ونظراً لواقعية نظارات الواقع الافتراضي الخاصة به، ثم يسقط الصورة الافتراضية لصديقه في حفرة تُعاين افتراضية، يُسأل عن قلة الاحتراز بالتسبب بالوفاة وفقاً لاحكام المادة (343) عقوبات إذا توفي فعلاً؛ كما يُمكن تصوّر ظروف أخرى قد تكون فيها هذه النتيجة مُتعمدة نتيجة القصد الاحتمالي المنصوص عليها في المادة (64) عقوبات. ونفس الشيء ينطبق في حال حدوث عنف يتسبب بالإيذاء، فمن المرجح أن يُنظر إلى أي إصابة أو تأثير جسدي آخر موجود خارج الواقع الافتراضي بنفس الطريقة كما لو كان ناتجاً عن تفاعلات في الواقع المادي. إذا أصيب شخص ما عن طريق الخطأ بسبب اصطدامه بجدار مرتدياً خوذة الواقع الافتراضي، فهذه إصابة عرضية، بينما إذا استخدم شخص ما الواقع الافتراضي لخداع مستخدم للمشي من سطح أو التعثر على درج لإيذائه، فهو ليس أقل واقعية أو أقل عنفاً من الوسائل الأخرى للتسبب في مثل هذه الإصابات.

ثالثاً: إخفاء هوية المستخدم: من المعروف أنه يسهل تحديد هوية المستخدم لمرتكب الجرائم الإلكترونية من خلال تحديد (IP) العنوان الرقمي للمستخدم (Gómez-Quintero, et al.2024)، حيث لا يُمكن للمستخدم إنشاء أكثر من عنوان رقمي بوقت وتاريخ محدد، وتحديد هوية مرتكب الجريمة الإلكترونية من خلال المسجلات الرقمية (Logs)، ومصادر الرسائل الإلكترونية والأثار الرقمية (McGlynn,C.Rigotti,C.2025)، وبالتالي يسهل ذلك على الأجهزة الأمنية تعقبه. بيد أن تحديد هوية المستخدم في الميتافيرس تكون اختيارية من المستخدم، ممّا يُمكن له إخفاء هويته، ويعود ذلك أساساً إلى مخاوف تتعلق بالخصوصية في المجال الإلكتروني (Beltrán,M.et al.2023)، فمرونة الهوية يخلق درجات متفاوتة من عدم الكشف عن هوية المستخدم الفعلي، وهذا يُمكن مجرمي الميتافيرس من التهرب من الرقابة القانونية (Cheong,B.2022) بسبب عدم الكشف عن هويتهم وصعوبة تتبع المعاملات يُسهل ارتكاب الكثير من الجرائم كغسيل الأموال والاحتيال والإرهاب وغيرها (Pandey,D.Gilmour,P,2024).

## المبحث الثاني

## إشكالية تطبيق المسؤولية الجزائية في الاعتداءات الواقعة على الصور الرمزية

قد تُشبه الصور الرمزية الافتراضية "الافتاتار" شخصية ومظهر المستخدم في الواقع المادي أو تختلف عنه بشكل كبير، وهذا يطمس الحدود بين الواقع والوجود الافتراضي، لأنه يمنح المستخدمين حرية إعادة تشكيل هويتهم بما يتجاوز قيود الواقع المادي، لهذا، نجد أن مجرمي الجرائم الإلكترونية حوّلوا تركيزهم إلى الاستخدام غير المشروع لتقنية الميتافيرس؛ ونتيجة لذلك، يُمكن للصور الرمزية أن تُنشئ المزيد من الاعتداءات الافتراضية المتطورة، وهذا يتطلب تحقق اركان الاعتداء من حيث نهوض الركن المادي القائم على إتيان المستخدم لنشاط التعدي من قبل المستخدم والمساس بحقوق صور رمزية مملّكة للغير والركن المعنوي القائم على القيام بهذا الاعتداء بسوء نية. وأضحّت هذه التقنية تُشكّل تحدي جديد عند

تطبيق قواعد المسؤولية الجزائية عليها، ولاسيما ما تُمثله من إشكاليات موضوعية وأخرى شكلية، وهذا موضوع دراستنا في المطلبين التاليين.

### المطلب الأول

#### إشكاليات المسؤولية الجزائية الموضوعية المتعلقة بالصُّور الرمزيّة الافتراضيّة

يتطلب تطبيق أحكام المسؤولية الجزائية المتعلقة بالاستخدام غير المشروع للصُّور الرمزيّة الافتراضيّة في تقنيّة الميتافيرس، العديد من المتطلبات الموضوعية لعلّة أهمّها: ملائمة الاعتداءات على الصُّور الرمزيّة لقانون الجرائم الإلكترونيّة، وحماية المعلومات الشخصية سيرانياً للصُّور الرمزيّة الافتراضيّة، وهذين غير متحقّقين على الاغلب. وليبيان ذلك سيتم بحثه في الفرعين التاليين.

### الفرع الأول

#### إشكالية عدم خضوع بعض الاعتداءات على الصُّور الرمزيّة لقانون الجرائم الإلكترونيّة

بالرجوع لقانون الجرائم الإلكترونيّة الأردني تخلص احكامه من تنظيم الاعتداءات على الصُّور الرمزيّة الافتراضيّة في الميتافيرس، باستثناء جريمة واحدة حصراً المنصوص عليها في المادّة (3/13) المتعلقة في الاستغلال الجنسي للقاصرين أو المرضى النفسيين أو العقليين، وكان المحتوى صوراً أو تسجيلات أو رسومات أو غيرها مثيرة جنسياً لأعضاء جنسية أو أفعال جنسية افتراضية أو بالمحاكاة، نجد أنّ المشرع استخدم مصطلحات عامة كتلك "الصُّور، الرسومات، افتراضية، بالمحاكاة" وهي الأساس الفني لتقنيات الواقع الافتراضيّ، فالصُّور الرمزيّة الافتراضيّة هي التي تحاكي الواقع في تقنيّة الميتافيرس، ومحاكات القاصرين والمصابين بأمراض نفسية أو عقلية من خلال الاعتداء الجنسي على الصُّور الرمزيّة الافتراضيّة الخاصة بهم، ويعد ذلك فعلاً مُجرماً ومُعاقباً عليه في قانون الجرائم الإلكترونيّة الأردني.

وانطلاقاً من المادّة (3/13) من قانون الجرائم الإلكترونيّة، التي حاصرت الحماية الجزائية على الفئات الثلاثة -الأطفال، المرضى النفسيين، المرضى العقليين- وهذا، يقودنا لطرح سؤال ما مدى إمكانية القياس في قانون الجرائم الإلكترونيّة لمعاقبة الاعتداء على الصُّور الرمزيّة الافتراضيّة المتقاربة من الجرائم الإلكترونيّة؟ الإجابة عن هذا التساؤل تكمن في أنّ قانون الجرائم الإلكترونيّة هو قانون خاص، وفي حال خلو النص من تحديد الأفعال المُجرّمة، يعتبر الفعل مُباحاً، لاسيما الاعتداء على الصُّور الرمزيّة في الميتافيرس لا يخضع لرقابة قانونيّة -خلافاً للمادّة (3/13) أنفة الذكر- كون الاعتداء يمس الشخصية الكرتونية الافتراضية، وليس شخص المستخدم، وهذه المسألة تستند للمادّة (3) قانون العقوبات، باعتبارها قواعد عامة، التي اقرت مبدأ "لا جريمة ولا عقوبة إلا بنص"، لذا، حتى يُعتد بالسُّلوك ويصاغ بطابع التجريم لا بُدّ من النص عليه في القانون صراحةً، ومن هنا يغدو القول بالقياس في التجريم أمراً مخالفاً للقانون إذا كانت الغاية منه التجريم أو التشديد، بسبب تخلف نص التجريم المتعلق بالاعتداء على الصُّور الرمزيّة للغير، فلا مسؤولية جزائية على تلك الاعتداءات، ما عدا الحالة المنصوص عليها في المادّة (3/13) أنفة الذكر.

وتوضيحاً لما تقدم، إذا تجاوز الاعتداء نطاق الصُّور الرمزيّة، ومس الواقع المادّي للمستخدم، بحيث تجاوز نطاق الميتافيرس، فهذا السُّلوك يكون محلّاً للمساءلة الجزائية، كأن يقوم شخص بإتلاف حساب صورة رمزية لمستخدم بغير رضاه، هنا تنطبق عليه حكماً المادّة (3/ب) من قانون الجرائم الإلكترونيّة، بينما لو بقيت نتيجة الاعتداء منحصرة على الصُّور الرمزيّة في الميتافيرس فحسب، ولم يرتب أثراً في الواقع المادّي فلا مسؤولية جزائية على هذا الاعتداء؛ كأن يتفق مجموعة من المستخدمين للصُّور الرمزيّة على الاعتداء على صورة رمزية أثناء لعبة معيّنة في الميتافيرس بسبب انتماءه للدولة ما، هنا يقتصر أثره الاعتداء على الجانب الافتراضي دون أن يمتد للمادّي، ممّا يجعل من محلّها غير صالحاً لموضوع الجريمة الإلكترونيّة (Brenner,S,W.2020).

ونافذة القول هنا، أنّ الاعتداءات التي تقع على الصُّور الرمزيّة تفتقر إلى تحقيق النتيجة الإجرامية المادية الملموس، حيث لا تُعتبر الصُّور الرمزيّة الافتراضية أشخاصاً طبيعيين أو معنويين بالمعنى القانوني (McGlynn,C.Rigotti,C.2025). فالألفاظ والإيماءات والإشارات التعبيرية النابية التي تصدر عن بعض المستخدمين ضد الصُّور الرمزيّة للغير أثناء ممارسة نشاط ما في الميتافيرس، بهدف إثارة النعرات العنصرية أو إثارة الكراهية كاستبعاد لاعب بسبب جنسيته أو دينه أو عرقه أو لونه، فجميع هذه الأنشطة تبقى ضمن نطاق الواقع الافتراضي، ولا تمتد للواقع المادّي للمستخدم، ممّا يحول من إمكانية تطبيق قانون الجرائم الإلكترونيّة عليها.

### الفرع الثاني

#### إشكالية الأمن السيبراني للمعلومات الشخصية في الصُّور الرمزيّة

صُممت تقنيّة الميتافيرس؛ لتكون بيئة تفاعلية، وحتى تحقّق هذه التقنيّة الغاية من وجودها تتطلب جمع كميات ضخمة من المعلومات الشخصية لمستخدمها، ويتصدر غياب التشريعات الناظمة لكيفية استخدام هذه المعلومات قائمة أكثر تهديدات الأمن السيبراني إلحاحاً في تقنيّة الميتافيرس. ويُمكن تحديد أبرز التهديدات الأمنية السيبرانية للصُّور الرمزيّة الافتراضيّة في الميتافيرس على النحو التالي:

أولاً: بيئة غير خاضعة لقانون الجرائم الإلكترونيّة: بات معلوماً أن الاعتداء على الصور الرمزيّة في الميتافيرس غير خاضعة لرقابة القانون، وهذا الأمر مقلّماً للغاية نظراً لكمية المعلومات الشخصية لمستخدمي الصُّور الرمزيّة التي يتخلّى عنها -عمداً أو سهواً- في الميتافيرس، حيث سيتمكن مزودوا

خدمة الميتافيرس من الوصول إلى معلومات المستخدمين الحيوية، وموقعهم، ومعلوماتهم المالية، ومجموعة كبيرة من المعلومات الأخرى؛ فضلاً عن إمكانية مزودي الخدمة والمستخدمين لتقنية الميتافيرس استغلال هذه المعلومات أو استخدامها لأغراض إجرامية (Huang RH, et al.2023)، فمثلاً، تشترط شركة ميتا أن يكون لدى المستخدم للصورة الرمزية حساب في منصة "فيسبوك"، وتُمكن هذه الخاصية الشركة من جمع معلومات شخصية تتعلق بالمستخدمين (Beltrán, M. et al.2023)، وما يزيد الأمر تعقيداً أنّ معظم مزودي خدمة الميتافيرس لم يتعهدوا بالحفاظ على المعلومات الخاصة للمستخدمين، الأمر الذي يجعل من تلك المعلومات معرضة لخطر الاستغلال غير المشروع، ولاسيما عند نقلها بين مشغلي المنصات، أو بين التطبيقات الإلكترونية داخل الميتافيرس (Cheong, B.2022). لهذا، تعتبر حماية الصور الرمزية بما تشمله من معلومات شخصية تُشكل تحدياً كبيراً نظراً لُقصور نطاق قانون الجرائم الإلكترونية في شمولها.

ثانياً: اختراق نقطة النهاية للواقع الافتراضي: يتطلب الدخول إلى الصور الرمزية في الميتافيرس استخدام سماعة رأس للواقع الافتراضي، وسماعات الواقع الافتراضي أجهزة مزودة ببرامج ذكاء اصطناعي متطورة، فعند استخدامها، تعمل على جمع كميات هائلة من المعلومات الشخصية للمستخدم -بما في ذلك الاحتفاظ في التسجيلات الصوتية وتسجيل حركات المستخدمين وردود أفعالهم الجسدية، بل وحتى أنماط الموجات الدماغية- مما يُمكن مجرمو الميتافيرس من شن هجمات سببرانية على المعلومات الشخصية، فيجعل المستخدمين عرضة للابتزاز والقرصنة والاحتيال الافتراضي وغيرها من الاعتداءات داخل الميتافيرس وخارجه (Deng, M. et al.2023).

ثالثاً: الاستيلاء على الهوية الرقمية للمستخدم سرقة الهوية: يتم ذلك من خلال اختراق نقاط النهاية للواقع الافتراضي أو شن حملة تصيد احتيالي تهدف إلى الحصول على الكلمات السرية للوصول إلى المحفظة المالية والأصول الافتراضية للمستخدمين، وهذا يتيح للمخترقين السيطرة على الصور الرمزية والوصول الكامل للمعلومات الشخصية الرقمية، وإجراء عمليات الشراء والبيع بصفتهم المستخدم الأصلي (Cheong, B.2022). رابعاً التزييف العميق الافتراضي (Deepfake): هو برنامج يعتمد بشكل أساسي على الذكاء الاصطناعي، ويُستخدم لإنشاء صور وأصوات ومقاطع فيديو غير حقيقية مُضَلَّلة، يجمع التزييف العميق الصور والأصوات المزيفة ويدمجها باستخدام خوارزميات التعلم الآلي، ونتيجة لذلك، يُنشئ أشخاصاً ووقائع غير موجودة أو لم تحدث في الواقع (الرابط، FortiGuard Labs) ولما كانت تقنية الميتافيرس تعتمد على الذكاء الاصطناعي، الأمر الذي سهّل للمستخدمي الصور الرمزية إنشاء صور وأصوات ومقاطع فيديو غير حقيقية تتعلق بالغير، مما يجعل من الصعب التحقق من هوية شخص المستخدم أو المزيف، لاسيما لأنّ تقنية الميتافيرس تُمكن المستخدم من تغيير مظهر صورته الرمزية، وهذا يجعل من التعرف إلى هويته الافتراضية غير مؤكدة (McGlynn, C. Rigotti, C.2025).

وبالتالي، من السهل استخدام الصور الرمزية في الميتافيرس في التزييف العميق وبشكل خاص لأغراض عداثية، كتضليل مستخدمي الميتافيرس بنشر معلومات أو اشاعات كاذبة، ومثال ذلك ظهور فيديو مُرَوَّر بالتزييف العميق لصور رمزية تعود لشخصية مشهورة وهو يفعل شيئاً لم يفعله في الحقيقة، وهذا بطبيعة الحال يتطلب تدخل تشريعي لتجريم مثل هذه الأفعال.

## المطلب الثاني

### إشكاليات المسؤولية الجزائية الشكلية المتعلقة بالصور الرمزية الافتراضية

مسألة تطبيق قوانين الواقع المادي في الواقع الافتراضي مسألة معقدة، إذ تثير تساؤلات حول الاختصاص القضائي والسيادة، وتطبيق القوانين على الواقع الافتراضي؛ وجمع أدلة الاعتداءات على الصور الرمزية، وهذه التساؤلات سيتم الإجابة عنها في الفرعين التاليين.

### الفرع الأول

#### مشكلة تحديد السيادة والقانون والاختصاص القضائي في الميتافيرس

من المؤكد أنّ تقنية الميتافيرس تضم أشخاصاً يتبنون صوراً رمزية خاصة بهم، بالإضافة إلى أراض ومنازل وشركات في الواقع الافتراضي، ويُشترى هذا الواقع الافتراضي بالعملة المشفرة الرقمية أو الرموز غير القابلة للاستبدال "NFTs"، وهذا يُنشئ بيئة جاذبة لمجرمي الميتافيرس (Manxuan.W. Et al.2024)، وذلك بسبب عدم وجود دولة أو شركة أو منصة واحدة تملك أو تُشغّل الميتافيرس، بل على العكس، فالميتافيرس، مثل الإنترنت، تُطور وتُدار من قِبل جهات متعددة (Cheong, B.2022)، وهذا يخلق مشكلة قانونية تتعلق بعدم وجود أي سيادة أو قانون أو سلطة قضائية على هذه التقنية، لذا، فإن غياب سلطة مركزية أو هيئة مُتحكّمة يجعل الواقع الافتراضي للميتافيرس مغامرة محفوفة بالمخاطر بالنسبة للمستخدمين، وهذه المخاطر يُمكن اجمال أهمها بما يلي:

#### أولاً غياب سيادة الدولة والقانون في الميتافيرس:

يُعد مفهوم السيادة مثيراً للاهتمام في القانون، فالسلطة السيادية وحدها هي القادرة على تنظيم شؤون الدولة، والدولة هي من تُحدّد وتوزع الولاية القضائية ضمن حدودها الإقليمية (Manxuan.W. Et al.2024)، ولكن في تقنية الميتافيرس الأمر مختلف تماماً، فهي تقنية عالمية، لا يُمكن تقييد الولاية القضائية بأي حدود مادية تابعة للدولة (Kalyvaji, M.2023)؛ ولاسيما أنّ استخدامات وتطبيقات تقنية الميتافيرس تتجاوز حدود الكرة

الأرضية، ومع ذلك، فإنّ هناك رأي يعتبر تصرفات الصُّورة الرمزيّة في الواقع الافتراضي متصلةً بشكل مباشر لتصرفات مستخدميها، ممّا يتعيّن مجازاته وفقاً لقانون بلد المستخدم (Cheong,B.2022). ونعتقد أنّ هذا الرأي جانب الصواب من حيث أنّ سلوك الصُّورة الرمزيّة يكون أقرب إلى شخصية كيان في الواقع الافتراضي، والاعتداء يكون بين الصُّور الرمزيّة فحسب وليس المستخدمين، كما أنّ آثار الاعتداء لم تتجاوز حدود تقنية الميتافيرس، إضافةً إلى ذلك، فإنّ كون الواقع الافتراضي يُنشأ ويُدار من قِبَل جهات خاصة غير تابعة لدولة معينة يزيد الأمور تعقيداً، إذ يكون لهذه الشركات شروط خدمة وضوابط خاصة بها يُتوقع من المستخدمين اتباعها. ووفقاً لقانون الجرائم الإلكترونية الحالي، فإنّ سيادة الدولة على تقنية الميتافيرس محدودة جداً، بسبب عدم وجود شخص أو كيان واحد يُمكنه حيازة التقنية. وبالتالي، تبقى مشكلة سيادة الدولة قائمة، نتيجة صعوبة تسمية سلطة سيادية واحدة، يُمكنها ممارسة صلاحيات تنظيم تقنية الميتافيرس.

لهذا، بات بحُكم المؤكد أنّ لا ينطبق قانون الجرائم الإلكترونية الحالي بشكل كامل على تقنية الميتافيرس، ويعود ذلك إلى عدم وضوح مفهوم تقنية الميتافيرس التي تأخذ في التوسع بشكل كبير، كما أنّ خاصيّة تغيير الصُّور الرمزيّة بسهولة يُجنّب مجرمي الميتافيرس من المسؤولية الجزائية.

### ثالثاً غياب تحديد الاختصاص القضائي في الميتافيرس:

الاختصاص القضائي، بشكل عام، يعني تطبيق القوانين على منطقة محددة، مع ذلك، فإنّ الحدود الإقليمية لتقنية الميتافيرس غير واضحة أو حتى قابلة للقياس (Barta,S.et al.2024)، وبالرجوع إلى خطة المشرع الأردني نجد نص بالمادة (38) من قانون الجرائم الإلكترونية على أنّ الاختصاص القضائي ينعقد للقضاء الأردني حال حدثت الجريمة في الخارج، وألحقت أضراراً بمصالحها أو مواطنها أو المقيمين فيها أو ترتبت آثار الجريمة فيها. إذ لا خلاف على أنّ الجرائم التي تمتد آثارها من الواقع الافتراضي، وتمس الكيان المادّي للمستخدم هي من اختصاص القضاء الأردني، بينما الاعتداءات التي تقع على الصُّور الرمزيّة، وتبقى داخل التقنية غير خاضعة للرقابة القانونية أو القضائية للأردن، وبالرغم من حداثة إصدار قانون الجرائم الإلكترونية لسنة 2023م، إلا أنّ استبعاد العديد من تقنيات الواقع الافتراضي من نطاق التطبيق، ولم ينظّم الاعتداءات الواقعة على الصُّور الرمزيّة، باستثناء المادة (3/13) منه، ممّا جعل من إطاره القانوني غير شامل لجميع الجرائم الإلكترونية والافتراضية.

ومن هنا، نُولي انتباه مشرعنا بتضمين فقرة على المادة (2) من قانون الجرائم الإلكترونية إيراد عبارة "الصُّور الرمزيّة الافتراضية وكل ما ينشأ عن تطورات تكنولوجيا الواقع الافتراضي والمعزز"، وفي هذا الصدد، يُقدم قانون الاتصالات البريطاني لعام 2003 نموذجاً مُحتملاً لمعالجة الجرائم الافتراضية، حيث يُعاقب بموجب المادة (127) على الاستخدام غير السليم لشبكات الاتصالات العامة؛ وقد يُحمّل التفسير الواسع لهذه الأحكام الشخص الطبيعي المسؤولية عن أفعال صُّورته الرمزيّة الافتراضية. علاوةً على ذلك، يُناقش قانون السلامة على الإنترنت البريطاني لسنة 2023 الذي يُلزم بإجراء تقييمات منتظمة للمخاطر لمعالجة المواد غير المشروعة، لتعزيز السلامة على الإنترنت على المنصات، لتوسيع نطاق تركيزه؛ ليتجاوز المحتوى ليشمل أضرار الاتصال مثل الاعتداءات الجنسية الإلكترونية في الميتافيرس (الرباط، Bruno,D).

### الفرع الثاني

#### إشكالية جمع أدلة الاعتداءات على الصُّور الرمزيّة

يُعدّ التحقيق في الميتافيرس مهمةً صعبةً؛ لأنّه لا يقتصر على فحص ملفات مختلفة عبر أنظمة متعددة فحسب، بل يتطلب تحليل أنظمة إلكترونية متنوعة ضمن بيانات افتراضية مختلفة، وربط هذه البيانات ببعضها البعض، لاستخلاص أدلة قانونية، ومن الأمثلة التي توضح تعقيدات التحقيق في ميتافيرس، إخفاء لوحة رقمية نادرة من متحف افتراضي، هنا ينبغي أن يُجري المحقق تحقيقاً شاملاً يتضمن مراجعة سجلات الأمان في المتحف الافتراضي، وتتبع معاملات سلسلة الكتل -البلوك تشين-، وفحص التفاعلات داخل التقنيات الافتراضية والأسواق المترابطة؛ كما ينبغي أن يُحلّل معلومات الأدوات الحديثة المادية من أجهزة مثل القفازات ونظارات الواقع الافتراضي لتأكيد أيّ أنشطة ضارة للصُّور الرمزيّة الخاصة بالمستخدم، ويعتمد فحص السجلات الافتراضية أو الأجهزة على السجلات التي يُسجلها المُزودون أو البائعون، وما إذا كانت هذه السجلات متاحة للفحص؛ في هذا المثال، إذا لم تحتفظ منصة الميتافيرس والمتحف الافتراضي بسجلات، فسيكون من المستحيل التحقق من الأنشطة التي سبقت السرقة، بما في ذلك معلومات عن المستخدم الجانح. إذا لم تكن سجلات قفازات اللمس أو نظارات الواقع الافتراضي موجودة أيضاً، فسيكون من المستحيل التحقّق من الأنشطة التي وصفها المستخدم أثناء النشاط العدائي (Seo,S.et al.2023).

وهذه التقنية تستلزم تطوير منهجيات وأدوات مبتكرة مصمّمة لتتبع وفحص البصمات الرقمية للمستخدم، وجمع الأدلة الجرمية التي تم استخدامها (Manxuan.W.Et al.2024)؛ فمثلاً تتم السرقة من صُّورة رمزيّة نتيجة تقديم هدية، حيثُ تقترب صُّورة رمزيّة من صُّورة رمزيّة أخرى لتقديم حقيبة افتراضية كهدية، فتقبل الصُّورة الرمزيّة الهدية، لكنّها تكتشف بعد ساعات قليلة سرقة جميع الأصول الرقمية الافتراضية المرتبطة بحسابها في الميتافيرس ومحفظتها الرقمية؛ لأنّ الهدية الافتراضية ما هي إلا رمزاً غير قابل للاستبدال (NFT) خبيثاً مُدمجاً فيه شيفرة عدائية، ممّا سهّل سرقة الأصول الرقمية للصُّورة الرمزيّة (Seo,S.et al.2023). ومن أبرز الإشكاليات التي تواجه محققو الميتافيرس والأمن السيبراني في جمع الأدلة الافتراضية، إخفاء الهوية الرقمية، وكيفية التحقّق منها (McGlynn,C.Rigotti,C.2025)، وصعوبة تتبع الأصول الرقمية كوتّها تحتوي على الملايين من

عناوين الدخول المحمّية (Manxuan.W.Et al.2024)، وتنوع مصادر المعلومات بشكل يصعب حصره، فضلاً عن غياب المعايير الوطنية والدولية المنظمة لتقنية الميتافيرس (Seo,S.et al.2023).

#### الخاتمة:

خلّصت هذه الدراسة إلى أنّ الصُّور الرمزيّة الافتراضيّة في تقنيّة الميتافيرس، هي بيئة رقمية سريعة التطور قد تُغيّر جذرياً كيفية تفاعل البشر مع التقنيات الرقمية ومع بعضهم البعض، وقد أدى تفاعل الصور الرمزية الافتراضية في الميتافيرس إلى تطبيق تعليمات خاصة صادرة عن مزودي الخدمة، وإن كان ذلك ليس بحلاً مثالياً، إلا أنّ الإطار القانوني للمزود قد يكون أحد الحلول لمعالجة مشكلة المسؤولية الجزائية حال الاعتداء على الصُّور الرمزيّة الافتراضيّة في الميتافيرس. ومن هذا المنطلق، يُمكن استخلاص أهم النتائج والتوصيات على النحو التالي:

#### أولاً النتائج:

1. استكشفت هذه الدراسة أنّ أطرنا القانونية الحالية، ونُحْص بالذكر قانون الجرائم الإلكترونيّة غير مهياً على الإطلاق لمواجهة الاعتداءات الفريدة التي طرحها الصُّور الرمزيّة الافتراضيّة في الميتافيرس؛ وهذا جعل من هذه الدراسة تُعدّ خطوة حاسمة نحو فهم وتطوير إطار قانوني شامل مُصمّم خصيصاً للصُّور الرمزيّة في الميتافيرس، مع التركيز على أهم الإشكاليات التي تواجه مسألة تجريم الاعتداءات الواقعة على الصُّور الرمزيّة.

2. توصّلت الدراسة إلى أنّه، يُمكن توقع طيفٍ واسع من الاعتداءات على الصور الرمزية الافتراضية في الميتافيرس، والتي يُمكن أنّ تتحقّق في الواقع المادّي ولا تجد السند القانوني للتجريم في الواقع الافتراضي، فعلى سبيل المثال غسيل الأموال، والإرهاب، العنف، والاعتداء الجنسي، وإن كانت هذه الدراسة لم يتسع نطاقها لتناول هذه المواضيع، إلا أنّ الإشارة إلى أهمها قد يفي بالغرض منها.

3. تطمس الصُّور الرمزيّة الافتراضيّة في تقنيّة الميتافيرس-من خلال طبيعتها التفاعلية- الحدود الفاصلة بين الواقعيين الافتراضي والمادّي، ممّا يُنشئ تعقيدات جديدة في تحديد طبيعة النشاط العدائي وتنظيمه.

#### ثانياً: التوصيات:

1. يُؤكد نقاشنا في هذه الدراسة على ضرورة وضع مفهوم للصُّور الرمزيّة الافتراضيّة في قانون الجرائم الإلكترونيّة، يتضمن مفهوم قانوني مُبتكر للاعتداء الافتراضي، الذي يتجاوز حدود أضرار الواقع المادّي لتشمل العواقب المتعدّدة للأنشطة الواقعة في العالم الافتراضي، وهذا يتطلب من مُشرّعنا أن يُضمن المادة (2) من قانون الجرائم الإلكترونيّة عبارة "الصُّور الرمزيّة الافتراضيّة وكل ما ينشأ عن تطورات تكنولوجيا الواقع الافتراضي والمعزز". وتعريفها بالنص التالي: "بيّنها الشخصية الكرتونية الرقمية الافاتار التي تُحاكي شكلاً بشرياً أو شخصية خيالية التي يختارها المستخدم لتمثيل نفسه داخل تقنيّة الميتافيرس في ألعاب الفيديو، أو على مواقع التواصل الاجتماعي، أو على منتديات الإنترنت، أو التقنيات".

2. تقترح هذه الدراسة، ادراج الاعتداءات الواقعة على الصُّور الرمزية في الميتافيرس ضمن نطاق قانون الجرائم الإلكترونيّة حيث استطاعت الدراسة أن تُحدّد بعض الأنشطة العدائية على أنّها واقعة فعلاً، في حين أنّ النص عليها ووجودها ونطاقها غير محدّد حالياً في القانون.

3. أنّ مسألة تجريم الاعتداءات الواقعة على الصُّور الرمزيّة تتطلب من المشرع اعتماد إثبات الضررين المادّي و/أو المعنوي، وهذا الأمر يُمكن أن يتحقّق كونّ الصُّور الرمزيّة تمزج بين الواقع المادّي والافتراضي، ممّا يتعين بالضرورة إعادة صياغة نص المادة 38 من قانون الجرائم الإلكترونيّة بإضافة كلمة أو "افتراضية" ذلك عقب عبارة "... أو بأي وسيلة نشر إلكترونية..." وفي حال تم ذلك التعديل، نكون بصدد نص قانوني يجرم الأنشطة العدائية الواقعة على الصُّور الرمزيّة ضمن نطاق قانون الجرائم الإلكترونيّة.

4. هناك حاجة إلى تشريع دولي تابعاً لمنظمة دولية مستقلة يُعنى بتجريم الاعتداءات الواقعة على الصُّور الرمزيّة في تقنيّة الميتافيرس، وينبغي أن يستند هذا التشريع إلى معايير وقواعد دولية متفق عليها بين الدول.

#### المصادر والمراجع

إبراهيم، م. (2024). *التحديات القانونية لتقنية ميتافيرس من الوجهة الجزائرية*. ط1، دار الأهرام للنشر والتوزيع والإصدارات القانونية، مصر.

## REFERENCES

- Barta, S., et al. (2024). Avatar creation in the metaverse: A focus on event expectations. *Computers in Human Behavior*, 156, Article 108192. <https://doi.org/10.1016/j.chb.2024.108192>
- Bellini, O. (2024). Virtual justice: Criminalizing avatar sexual assault in metaverse spaces. *Mitchell Hamline Law Review*, 50(1), 3.
- Beltrán, M., et al. (2023). A privacy threat model for identity verification based on facial recognition. *Computers & Security*, 132.
- Brenner, S. (2007). Cybercrime: Re-thinking crime control strategies. In Y. Jewkes (Ed.), *Crime online* (pp. 12–28). Willan Publishing.
- Brenner, S. W. (2020). Fictional crime: The role of criminal law in virtual worlds. *Vanderbilt Journal of Entertainment and Technology Law*, 11, 75–94.
- Bruno, D. (n.d.). Online. <https://www.gov.uk/government/publications/online> (Accessed July 24, 2025).
- Cheong, B. C. (2022). Avatars in the metaverse: Potential legal issues and remedies. *International Cybersecurity Law Review*, 3(2), 467–494.
- Deng, M., et al. (2023). Social engineering in metaverse environment. In *2023 IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud) / 2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom)* (pp. 150–154). IEEE.
- Dong, S., et al. (2024). The metaverse review: Exploring the boundless realm of digital reality. *Computers, Materials and Continua*, 81(3), 3451–3498.
- Dwivedi, Y., et al. (2023). Exploring the darkverse: A multi-perspective analysis of the negative societal impacts of the metaverse. *Information Systems Frontiers*, 25, 2071–2114. <https://doi.org/10.1007/s10796-023-10400-x>
- FortiGuard Labs. (n.d.). Deepfake. <https://www.fortinet.com/resources/cyberglossary/deepfake> (Accessed September 19, 2025).
- Geldenhuis, K. (2024). Meta crime in the metaverse: Nothing sci-fi about this reality. *Servamus Community-Based Safety and Security Magazine*, 117(11).
- Gómez-Quintero, J., et al. (2024). A scoping study of crime facilitated by the metaverse. *Futures*, 157, Article 103338.
- Horne, C. (2023). Regulating rape within the virtual world. *Lincoln Memorial University Law Review*, 10(2), 159–176.
- Huang, R. H., et al. (2023). The legal nature of cryptocurrency as property: Accounting and taxation implications. *Computer Law & Security Review*, 51, Article 105860. <https://doi.org/10.1016/j.clsr.2023.105860>
- INTERPOL. (2022). *Technology assessment: Report on the metaverse*. <https://www.interpol.int> (Accessed July 22, 2025).
- Kalyvaji, M. (2023). Navigating the metaverse business and legal challenges: Intellectual property, privacy, and jurisdiction. *Journal of Metaverse*, 3(1), 87–92.
- Kang, G., et al. (2023). Security and privacy requirements for the metaverse: A metaverse applications perspective. *IEEE Communications Magazine*, 1–7.
- Karapatakis, A. (2025). Metaverse crimes in virtual (un)reality: Fraud and sexual offences under English law. *Journal of Economic Criminology*, 7.
- Lee, L.-H., et al. (2021). All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. *IEEE Access*, 14(8), 1–66. <http://arxiv.org/abs/2110.05352>
- Lisetti, C. (2012). 10 advantages of using avatars in patient-centered computer-based interventions for behavior change. *ACM SIGHIT Record*, 2(1). <https://doi.org/10.1145/2180796.2180820>
- Marshall, A., & Tompsett, B. (2024). The metaverse—Not a new frontier for crime. *Wiley Interdisciplinary Reviews: Forensic Science*, 6(1), e1505.
- McGlynn, C., & Rigotti, C. (2025). From virtual rape to meta-rape: Sexual violence, criminal law and the metaverse. *Oxford Journal of Legal Studies*, Volume X. <https://doi.org/10.1093/ojls/gqaf009>
- Miraj, Z. (2023). The legal status of metaverse law and its implementation in modern era. In *Proceedings of the 9th Bandung Creative Movement International Conference on Creative Industries (BCM 2022)*. Bandung, Indonesia.
- Mustawi, J., et al. (2022). BlockNet: Beyond reliable spatial digital twins to parallel metaverse. *Patterns*, 3(5).

- Mystakidis, S. (2022). Metaverse. *Encyclopedia*, 2(1), 486–497. <https://doi.org/10.3390/encyclopedia2010031>
- Pandey, D., & Gilmour, P. (2024). Accounting meets metaverse: Navigating the intersection between the real and virtual worlds. *Journal of Financial Reporting and Accounting*, 22(2), 211.
- Phillips, K., et al. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Sciences*, 2(2), 379–398. <https://doi.org/10.3390/forensicsci2020028>
- Qin, H., et al. (2025). Identity, crimes, and law enforcement in the metaverse. *Humanities and Social Sciences Communications*, 12, Article 194.
- Sadeghi-Niaraki, A., et al. (2025). A groundbreaking taxonomy of metaverse characteristics. *Artificial Intelligence Review*, 58(8), 243–296.
- Seo, S., et al. (2023). Digital forensic investigation framework for the metaverse. *The Journal of Supercomputing*, 79, 9467–9485.
- Seo, S., et al. (2023). Digital forensic investigation framework for the metaverse. *The Journal of Supercomputing*, 79(9).
- Severgin, A. (2023). Legal nature of the metaverse. *Digital Law Journal*, 4(4), 36–53. <https://doi.org/10.38044/2686-9136-2023-4-4-1>
- Song, C., et al. (2023). Exploring the key characteristics and theoretical framework for research on the metaverse. *Applied Sciences*, 13. <https://doi.org/10.3390/app13137628>
- Wang, M., et al. (2024). Metaverse security and forensic research. In *Proceedings of the 13th International Conference on Computer Engineering and Networks* (pp. 423–435).
- Wang, Y., et al. (2022). A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials*, 25(1), 319–352.
- المعاني. (n.d.). *Metaverse*. <https://www.almaany.com/ar/dict/ar-ar/> (Accessed July 7, 2025).