189 **Original Article** Arab Journal for Security Studies 2023; Volume 39 Issue (2), 189-204

Naif Arab University for Security Sciences
Arab Journal for Security Studies
المجلة العربية للدراسات الأمنية
https://journals.nauss.edu.sa/index.php/ajss

AJSS

Digital Forensic Evidence in the Metaverse Technology

الدليل الجنائي الرقمي في تقنية الميتافيرس

رامي متولي القاضي
قسم القانون الجنائي، أكاديمية الشرطة، جمهورية مصر العربية

Ramy Metwally El-Kady
Criminal Law Department, Police Academy, Egypt.

Received on 25 Jul. 2023, accepted on 5 Sep. 2023, available online on 12 Dec. 2023.

Abstract

This study addresses digital forensic evidence in the metaverse technology.

The importance of this study is evident in the light of the legislative vacuum that exists in response to all forms of violations occurring in the metaverse world. There is no doubt that the current criminal laws are ineffective in addressing successive technological developments unless supplemented by existing criminal statutes.

The research aims to shed light on the metaverse technology, its dimensions, characteristics and risks of its use. It also intends to examine the potential criminal patterns that can emerge in metaverse technology and explore strategies to address them, including methods for collecting digital evidence within the metaverse technology.

The research yielded a set of results, the most notable of which include the lack of legal texts regulating the use of this technology and addressing the new forms of cybercrimes committed through it. Additionally, it highlighted the inability of existing legal texts to effectively address these issues, along with difficulties related to collecting evidence from metaverse crimes. This challenge arises due to the unique nature of these crimes and the substantial volume of data generated by the use of this technology. Gathering evidence encompasses multiple domains, such as the user's scope, service providers, and the metaverse platform itself. Furthermore, there are challenges in presenting this evidence before traditional courts, given its three-dimensional nature.

Keywords: *security studies, criminal law, metaverse, metacrimes, digital forensic evidence.*

المستخلص

تتناول هذه الدراسة موضوع الدليل الجنائي الرقمي في تقنية الميتافيرس، وتظهر أهمية هذه الدراسة جليةً في ضوء الفراغ التشريعي القائم في مواجهة كافة صور الانتهاكات التي تقع في تقنية الميتافيرس، فلا شك في أن القوانين الجنائية الحاليَّة تكون مكتوفة الأيدي في مواجهة تطورات تكنولوجية متلاحقة لا يمكن التصدي لها جنائيًّا، إلا من خلال نصوص جنائية قائمة.

وتهدف الدراسة إلى إلقاء الضوء على تقنية الميتافيرس وأبعادها وخصائصها ومخاطر استخدامها، وبحث الأنماط الإجرامية التي يمكن أن تنشأ في تقنية الميتافيرس وسبل مواجهتها، وتسليط الضوء على سبل جمع الأدلة الرقمية في تقنية الميتافيرس.

وقد خلصت الدراسة إلى مجموعة من النتائج من أبرزها: عدم وجود نصوص قانونية تنظم استخدام هذه التقنية، وتواجه صور الجرائم السيبرانية المستحدثة المرتكبة خلالها وعجز النصوص القانونية القائمة عن مواجهتها، وكذا وجود صعوبات تخص عملية جمع الأدلة المتحصلة من جرائم الميتافيرس بالنظر إلى طبيعتها الخاصة والكم الهائل من البيانات الناجمة عن استخدام هذه التقنية، وهو ما يستتبع جمع الأدلة من أكثر من نطاق؛ كنطاق المستخدم ومقدمي الخدمات ومنصة الميتافيرس ذاتها، فضلًا عن وجود بعض الصعوبات في عرض الأدلة المتحصلة من الميتافيرس أمام المحاكم العادية بالنظر إلى طابع

الكلمات المفتاحية: الدراسات الأمنية، قانون جنائي، تقنية الميتافيرس، جرائم الميتافيرس، الأدلة الجنائية الرقمية.

Production and hosting by NAUSS

* Corresponding Author: *Ramy Metwally El-Kady*
Email: dr.ramy_elkady@yahoo.com
doi: 10.26735/QMDY9278

هذه الأدلة الثلاثي الأبعاد، وأن نجاح جهات إنفاذ القانون في جمع الأدلة الرقمية حول جرائم الميتافيرس يتوقف على مدى تعاون الشركات الخاصة من مقدمي الخدمات ومشغلي منصة الميتافيرس، بما يضمن للمحققين النفاذ إلى البيانات المطلوبة لاستكمال التحقيقات.

وانتهت الدراسة إلى ضرورة تضافر الجهود الدولية لتعديل الاتفاقيات الدولية الخاصة بالجرائم السيبرانية، وعلى رأسها اتفاقية بودابست (الاتفاقية الأوروبية لمكافحة الجرائم السيبرانية)، أو التطلع لوضع اتفاقية دولية جديدة تنظم مسئولية مقدمي خدمات الميتافيرس وتلزمهم بالانصياع إلى التعاون في مكافحة الجرائم ومتابعة التعديات والانتهاكات وتبادل الأدلة والمعلومات المرتبطة بتلك الحالات، وتحديد القوانين واجبة التطبيق في تلك الحالات وضوابط الاستناد إليها.

The success of law enforcement agencies in collecting digital evidence related to metaverse crimes depends on the extent of the cooperation of private companies from service providers and operators of the Metaverse platform. This cooperation is crucial to ensure that investigators have access to the necessary data required to complete their investigations.

The research concluded that there is a need for international cooperation to amend existing international conventions on cybercrime, with leadership from the Budapest Convention (the European Convention for Combating Cybercrime). Alternatively, there is an aspiration to develop a new international convention that regulates the responsibilities of metaverse service providers, obliging them to cooperate in combating crimes, monitoring infringements and violations, exchanging evidence and information related to such cases, and defining applicable laws and the criteria for their enforcement.

1. المقدمة

تعرف البشريَّة في الوقت الراهن تحولًا تكنولوجيًّا هائلًا في تقنيات الشبكة المعلوماتيَّة الدوليَّة «الإنترنت» يسمى تقنية الميتافيرس، ويشهد العالم اهتمامًا متزايدًا بهذه التقنية الفريدة في ضوء اتجاه بعض الدول إلى تبني تجاربها الافتراضيَّة الخاصة بشأن تطبيق تقنية الميتافيرس؛ كاليابان والولايات المتحدة وكوريا الجنوبية وسنغافورة وأندونسيا (تقرير مركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء المصري، 2022، ص. 55)، واتجاه بعض الدول الأخرى إلى وضع إستراتيجيات للتوسع في استخدام هذه التقنية؛ كإستراتيجية دبي للميتافيرس بدولة الإمارات العربيَّة المتحدة، وفي مقابل هذا الاهتمام نجد بعض التكهنات بتزايد مخاطر استخدام هذه التقنية، التي قد تفتح الباب إلى عالم الجريمة بظهور أنماط جديدة من الجرائم الافتراضيَّة؛ حيث تفتح تقنية الميتافيرس المجال واسعًا للدخول في عالم ثلاثي الأبعاد عبر تقنيات الواقع الافتراضي والواقع المعزز بأجهزة استشعار في عالم مظلم، وتتيح للعصابات الإجراميَّة ارتكاب العديد من الجرائم السيبرانيَّة المستحدثة، فضلًا عن مخاطر انتهاك الخصوصيَّة للمستخدمين (جبريل، 2023، ص. 7)، ومن جانب آخر، يمثل التهديد المحتمل للجريمة في تقنية الميتافيرس مصدرًا للقلق في الواقع الإنساني؛ بالنظر للتشابه الكبير بينه وبين العالم الحقيقي، ومن ثم فإن الأحداث التي ستقع فيه يمكن أن تؤثر على العالم الحقيقي أيضًا (Seo et al., 2023:9468).

وفي سياق آخر، تشير بعض التقديرات الدوليَّة إلى أن سوق الميتافيرس سوف تحقق رواجًا اقتصاديًّا هائلًا، بالنظر للتوسع المستمر في أنشطته؛ إذ قدر حجم هذه السوق في عام 2021 بـ39 مليار دولار أمريكي، وفي عام 2022 بـ47 مليار دولار أمريكي، ومن المتوقع أن يصل حجم هذا السوق في عام 2030 إلى 679 مليار دولار أمريكي (مركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء المصري، 2022)، وهو ما يبرز بشكل جلي مدى التوقعات الاقتصادية الإيجابية المصاحبة لتقنية الميتافيرس وتأثيرها الكبير على الاقتصاد العالمي.

أهمية الدراسة

تنبع أهمية الدراسة من تناولها لأحد أبرز الموضوعات التكنولوجيَّة على الساحة العالميَّة في الوقت الراهن، ألا وهو تقنية الميتافيرس التي من المتوقع سطوع شمسها خلال الآونة المقبلة باعتبارها أبرز صور تطور شبكة المعلومات الدوليَّة التي تنقل البشريَّة إلى أبعاد تكنولوجيَّة جديدة، وعلى الرغم من وجود نصوص قانونيَّة تحكم مواجهة الجرائم في الفضاء السيبراني، فإن هذه القواعد من المتصور عجزها عن مواجهة الظواهر الإجراميَّة الحديثة عبر الميتافيرس، والتي تقوم على أبجديات غير تقليديَّة وعناصر مختلفة من حيث الأشخاص والوقائع والحدود المكانية والزمانية (جبريل، 2023، ص. 103)، وتبدو أهمية هذه الدراسة جليةً في ضوء الفراغ التشريعي القائم في مواجهة كافة صور الانتهاكات التي تقع في تقنية الميتافيرس، فلا شك في أن القوانين الجنائيَّة الحالية تكون مكتوفة الأيدي في مواجهة تطورات تكنولوجية متلاحقة لا يمكن التصدي لها جنائيًّا، إلا من خلال نصوص جنائيَّة قائمة تطبيقًا لمبدأ الشرعيَّة الجنائيَّة «لا جريمة ولا عقوبة إلا بنص»، ناهيك بأن كافة الإجراءات الجنائيَّة لمواجهة كافة صور الانتهاكات التي تقع في تقنية الميتافيرس يجب أن تكون بقانون تطبيقًا للمبدأ ذاته (الشرعية الإجرائية)؛ حيث ينظر إلى تقنية الميتافيرس بأنها ستنقل العالم إلى آفاق مختلفة وغير تقليديَّة ستثير بلا شك مشكلات غير محدودة من منظور القانون الجنائي.

كما تبرز أهمية بحث الدليل الرقمي في هذا العالم الافتراضي الجديد في ضوء الوسائل المستحدثة المستخدمة في الولوج له، والمتمثلة في أدوات الواقع الافتراضي أو الواقع المعزز والهواتف المحمولة ومنصات الألعاب؛ حيث تستخدم تلك التقنية أجهزةً وأدوات للإدراك والإحساس والاستدعاء، مثل: النظارات والقفازات والسترات ومستشعرات وحساسات تدمج بين تقنيات إنترنت الأشياء وتقنيات الواقع الافتراضي، والواقع المعزز والتقنية ثلاثية الأبعاد، ومن ثمَّ فمن المتوقع أن تزيد أهمية تلك المسألة في ظل التطورات المتوقعة لتنامي الميتافيرس، حين سيكون بمقدور المستخدم أن يخوض أي تجربة أو نشاط، وسيكون بمقدوره التعامل مع أي أمر يحتاج إليه من مكان واحد، هو الميتافيرس؛ إذ إن الميتافيرس عند وصولها للحالة المثالية الكاملة، فإنه سيمكن تطبيقها على أي شيء، ليصبح تقنية الميتافيرس هو التصور الافتراضي الجديد للحياة الإنسانية.

أضف إلى ذلك ما يتسم به الدليل الرقمي في تقنية الميتافيرس من خصوصية وطبيعة خاصة تميزه عن غيره من الأدلة الرقميَّة المتحصل عليها في الجرائم السيبرانية الأخرى، أو التي ترتكب عبر الوسائل الإلكترونية الأخرى، بالنظر للطابع الثلاثي الأبعاد لهذه التقنية الجديدة التي تنطبع بالتالي على الأدلة الرقميَّة الناجمة عنها، والتي تكون لها الطبيعة الثلاثية الأبعاد ذاتها، والتي تختلف عن غيرها من الأدلة الرقميَّة التي تكون ثنائية الأبعاد، فضلًا عن اتساع نطاق البحث عنها ليشمل نطاقات افتراضية موازية تشمل نطاقات (المستخدم - مقدم الخدمة - منصة الميتافيرس) بشكل أوسع نطاقًا من الفضاء الافتراضي التقليدي الذي توجد فيه الأدلة الجنائيَّة الرقميَّة الأخرى.

وإذا كان الواقع الحالي لم تعرض فيه بعد قضايا تتعلق بالميتافيرس أمام ساحات المحاكم؛ فقد سعى الباحث إلى العثور على قضايا خاصة باستخدام هذه التقنية في ارتكاب جرائم، ولكنه لم يعثر على قضايا واقعية، إلا أنه من المتوقع أن يشهد استخدام هذه التقنية إشكاليات جديدة من بينها إشكالية الدليل الجنائي الرقمي في عصر الميتافيرس، وذلك في ظل متغيرات تكنولوجية متسارعة يمضي فيها العالم نحو اعتماد كلي على الميتافيرس وبخطوات سريعة وصولًا لمرحلة الحياة الافتراضية.

إشكاليات الدراسة

تثير تقنية الميتافيرس عددًا من الإشكاليات القانونيَّة في سياق القانون الجنائي، من أبرزها: عدم وجود نصوص جنائيَّة تخص هذه التقنية والسلوكيات المخالفة المرتكبة عبرها، علاوة على عدم ملاءمة التكييفات الجنائيَّة التقليديَّة للجرائم الواقعة عبر تقنية الميتافيرس، وبصفة خاصة جرائم الاعتداء على الأشخاص، وكذلك بالنسبة لظرفي الزمان والمكان في جرائم الميتافيرس، فقد أوجدت الميتافيرس مفهومًا جديدًا لمسرح الجريمة، فالسلوك الصادر من فاعل واحد قد يحدث أثره في عدة أماكن في لحظة واحدة، بخلاف البعد الزمني للفعل الذي يختلف من دولة لأخرى بسبب التوقيتات بين الدول، فيرتب على ذلك اختلاف الوصف القانوني للفعل (جبريل، 2023، ص. 104)، ولا شك في أن الطابع المتغير والمتقلب لهذا الفضاء الافتراضي الجديد من شأنه التأثير في موثوقية الأدلة الرقميَّة المتحصلة عن الجرائم المستحدثة الواقعة داخله، وهو ما سوف ينعكس - دون أدنى شك - على كيفيات جمع الأدلة الرقميَّة واستخلاصها في هذا العالم الافتراضي.

تساؤلات الدراسة

تثير الدراسة العديد من التساؤلات ذات الصلة بكيفية وقوع الجرائم في تقنية الميتافيرس، ونوعية هذه الجرائم، وهل تختلف عن الجرائم الأخرى التي تقع في الفضاء الإلكتروني، وهل الطبيعة الخاصة للميتافيرس ستؤثر على طبيعة وشكل الأدلة الرقميَّة المتحصلة من الجرائم التي تقع في هذا الفضاء الافتراضي، وهل الأدلة الرقميَّة في الميتافيرس ستتأثر بهذه الطبيعة، ومن ثم سيختلف الدليل الرقمي المتحصل من الجرائم الواقعة في الميتافيرس عن غيره من الأدلة الرقميَّة المتحصلة في الفضاء السيبراني العادي، وما سبل وإجراءات جمع الأدلة الجنائيَّة المتحصلة عن جرائم الميتافيرس، وما حدود سلطات إنفاذ القانون على هذا العالم الذي تديره شركات من القطاع الخاص، وما حدود التعاون بين هذه الشركات وسلطات إنفاذ القانون في تقنية الميتافيرس، وهل سيكون لجهات إنفاذ القانون القدرة والصلاحيات لإنفاذ قوانين الدولة في الميتافيرس، التي تتحكم فيها المنصات الافتراضية المختلفة التي تتبع شركات القطاع الخاص، وهل ستصبح تحديات إنفاذ القانون فيما يتعلق بمنصات التواصل الاجتماعي هي ذاتها أم ستخلق تحديات أكبر من النواحي التشريعية والتنفيذية والعملية في مجال الملاحقة وإجراءات الضبط واستخراج الأدلة، إلى غير ذلك من التساؤلات القانونيَّة العديدة ذات الصلة بموضوع الدراسة، والتي تفرضها الطبيعة الخاصة لتقنية الميتافيرس، والتي دعت البعض إلى القول بأن منصة العالم الافتراضي (ميتافيرس) قد تجلب أبعادًا جديدة لمفهوم الجرائم السيبرانية، وأن هناك احتمالًا لوجود خطر ما بزيادة أنواع الجرائم السيبرانية، بل إنه من المتوقع كذلك تطوير أنواع جديدة كليًّا من هذه الجرائم.

والواقع أنه على الرغم من أن غالبية التساؤلات السابقة لا يجد لها الباحثون إجابة وافية في الوقت الحالي، فإنه من المتوقع في المستقبل

القريب أن تكون هذه الإجابات حاضرة في ضوء التطورات المتسارعة التي يشهدها تقنية الميتافيرس، وتبرز خطورة هذا العالم في أنه كلما زاد اعتماد الإنسان على التكنولوجيا، كان ذلك مجالًا خصبًا لتزايد أعداد الجرائم الافتراضية المتصور وقوعها في هذا العالم الجديد، ومن ثم تبرز أهمية بحث دور الدليل الرقمي في تقنية الميتافيرس؛ بالنظر لما ستؤول إليه حياة الإنسان في ظل هذا العالم الافتراضي الجديد، إلا أن كافة التساؤلات السابقة - من وجهة نظر الباحث- يمكن الإجابة عنها في الوقت الحاضر بأن الميتافيرس شأنه شأن البيئة المعلوماتيَّة السيبرانية الافتراضية، فإن أية جريمة تقع داخله، فهي جريمة سيبرانية تنطبق عليها كافة القواعد القانونيَّة الخاصة بالإثبات الجنائي في البيئة الافتراضية، وتنطبق عليها كذلك كافة القواعد القانونيَّة الخاصة بمقبولية وموثوقية هذا الدليل أمام القضاء الجنائي.

أهداف الدراسة

تهدف هذه الدراسة إلى تناول موضوع الدليل الجنائي الرقمي في عصر الميتافيرس، ويتفرع عن هذا الهدف مجموعة من الأهداف الفرعية، من أبرزها:

أ. إلقاء الضوء على تقنية الميتافيرس وأبعادها وخصائصها ومخاطر استخدامها.

ب. بحث الأنماط الإجراميَّة التي يمكن أن تنشأ في تقنية الميتافيرس وسبل مواجهتها.

ج. تسليط الضوء على سبل جمع واستخلاص الأدلة الرقميَّة في تقنية الميتافيرس.

فرضيات الدراسة

تتمثل فرضيات الدراسة في صعوبة جمع الأدلة الرقميَّة المتحصلة من الجرائم الواقعة في تقنية الميتافيرس، بالنظر إلى حداثة هذه التقنية، وأنها مازالت في طور التطوير، ولم تتكامل عناصرها بعد، وأنها وبالنظر إلى الاهتمام الدولي بهذه التقنية الجديدة قد يدفع بالعناصر الإجراميَّة إلى استغلالها في ارتكاب الأنشطة الإجراميَّة المختلفة بغرض التربح من ورائها، وهو ما سيلقي العبء على كاهل المحققين وأجهزة العدالة الجنائيَّة في مواجهة هذه الجرائم كأولوية أولى، وجمع الأدلة الجنائيَّة المتحصلة عنها لإدانة مرتكبيها.

2. منهجية الدراسة

تتمثل منهجية الدراسة في استخدام المنهج الوصفي التحليلي الذي يتناول ظاهرة تقنية الميتافيرس من كافة جوانبها وأبعادها، ويعرف المنهج الوصفي التحليلي بأنه: «دراسة الظاهرة كما توجد في الواقع ووصفها وصفًا وثيقًا يعبر عنها تعبيرًا كيفيًّا أو كميًّا؛ بغية الوصول إلى استنتاجات تسهم في فهم هذا الواقع وتطويره» (عبيدات وآخرون، 1996، ص. 220)، فهذا المنهج يهدف إلى بحث وتحليل تقنية الميتافيرس من جوانبها القانونيَّة، وقد تم الاستعانة في إعداد هذا البحث بالمراجع القانونيَّة المتاحة، من مؤلفات عامة في مجال القانون الجنائي، أو متخصصة في موضوع البحث، سواء أكانت مراجع عربية أم أجنبية ذات صلة بموضوع البحث.

2. 1 خطة الدراسة

تسير الخطة التفصيلية للدراسة على مطلبين: يتناول المطلب الأول ماهية الميتافيرس؛ وذلك في فرعين؛ حيث يعرض الفرع الأول تعريف الميتافيرس وخصائصها، ويتطرق الفرع الثاني إلى مخاطر تقنية الميتافيرس من الناحية الجنائيَّة، ويعرض المطلب الثاني ماهية الدليل الرقمي في تقنية الميتافيرس وإجراءات جمعه واستخلاصه؛ وذلك في فرعين، حيث يعرض الفرع الأول تعريف الدليل الرقمي وخصائصه، ويتطرق الفرع الثاني لإجراءات جمع الدليل الرقمي ومشروعيته ومقبوليته أمام القاضي الجنائي.

3. المطلب الأول: ماهية الميتافيرس

نتناول في هذا المطلب التعريف بتقنية الميتافيرس من خلال تناول تعريفها وخصائصها، ومخاطر استخدامها من الناحية الجنائيَّة؛ وذلك في فرعين على النحو التالي:

3. 1 تعريف تقنية الميتافيرس وخصائصها

نتناول في هذا الفرع تعريف تقنية الميتافيرس وخصائصها، والتصور الخاص باستخدامها، وذلك على النحو التالي:

تعريف الميتافيرس

تعددت التعاريف الاصطلاحية التي تصف الميتافيرس بحسب كيفية نظر الباحثين لها، فمنهم من ركَّز على اعتبارها شبكة معلوماتية، ونموذجًا مطورًا من شبكة المعلومات الدوليَّة (الإنترنت)، وهذا هو منظور مارك زوكربيرج الذي يعرف الميتافيرس بأنها: «الإنترنت المتجسد الغامر، والشيء الذي يمكن للناس القفز إليه، أو تحقيقه من خلال الواقع الافتراضي أو الواقع المعزز عند إثارة الاهتمام الدولي به»، بينما يعرفها راتان بأنها: «شبكة ضخمة ومترابطة من المساحات الافتراضية»، وهناك اتجاه آخر يعرفها بأنها منصة رقميَّة؛ حيث يذهب البعض لتعريفها بأنها: منصة جديدة تمامًا أو إطار عمل يجتمع فيه العالمان المادي والافتراضي، وهناك من يعرفها بأنها: «منصة رقميَّة

تشبه إلى حد كبير العالم الحقيقي ومتصلة به بشكل مكثف، يمكن للأشخاص الدخول إليها أو إحضار عناصر افتراضية عبر جهاز يعمل كوسيط من خلال مفهوم التوأمة الرقميَّة» (Seo et al., 2023:9468).

ويتفق الباحث مع الرأي الذي يرى تعريف الميتافيرس بأنها: «عالم افتراضي رقمي موازٍ ثلاثي الأبعاد، يتيح للمستخدم الدخول فيه بمساعدة أدوات معينة، وباستخدام صورة رمزية متحركة تمثله (أفاتار)، وذلك لإجراء بعض العمليات كالتسوق ومقابلة الأشخاص والألعاب، وغيرها الكثير من الأنشطة دون أن يتحرك من مكانه» (جبريل، 2023، ص. 16).

بينما من ناحية المدلول اللغوي، فكلمة ميتافيرس «Metaverse» تعني العالم الماورائي، وهي تتكون من شقين: الأول «meta» (بمعنى ما وراء، أو الأكثر وصفًا) والثاني «Verse» مصوغ من «Universe» وتفيد (ما وراء العالم)، وقد كان أول استخدام لهذا المصطلح في رواية الخيال العلمي «تحطم الثلج» (Snow Crash) عام 1992 التي كتبها نيل ستيفنسون؛ حيث يتفاعل البشر كشخصيات خيالية (Avatar) بعضهم مع بعض ومع برمجيات، في فضاء افتراضي ثلاثي الأبعاد مشابه للعالم الحقيقي (خليفة، 2022، ص. 8).

خصائص الميتافيرس

يتضح من التعريف السابق بعض الخصائص المتميزة لتقنية الميتافيرس، من أبرزها ما يلي:

- الميتافيرس عالم افتراضي موازٍ

تتميز تقنية الميتافيرس بأنها تخلق للمستخدم عالماً ثالثًا ما بين عالمين، الأول: عالم مادي ملموس، وهو الحياة الطبيعية التي يعيشها الإنسان، والثاني: عالم افتراضي خلقته التكنولوجيا الحديثة، وهو الفضاء السيبراني، فيأتي بعد ذلك الميتافيرس باعتباره عالماً افتراضيًّا موازيًا ثلاثي الأبعاد، يتيح للمستخدم الدخول فيه بأدوات تكنولوجية معينة، وباستخدام صورة رمزية متحركة تمثله، وهي عبارة عن شكل يختاره كل مستخدم، ويمكنه تكوين مساحته أو محتوياته الخاصة (أفاتار)؛ مما يعني ضمان عدم الكشف عن هويته والاستقلالية عن العالم، وتنقل الميتافيرس الفرد من مجرد مستخدم للإنترنت إلى جزء منه ومشارك فيه؛ حيث يشترك المستخدمون الذين يتحولون إلى صور رمزية في نفس التجربة والمكان والوقت، كما هو الحال في العالم الحقيقي، فتقنية الميتافيرس يتسم بخصيصة، تقوم على فكرة العالم الافتراضي الذي يُعدُّ في ظاهره مجرد خيال، ولكنه يحمل في طياته الكثير من التطبيقات الواقعية التي ستوفر للإنسان عالماً حضاريًّا متميزًا، ومن ثم فهي ليست حقيقة مطلقة، كما أنها ليست خيالًا مطلقًا، ولكنها عالم ثالث.

ويرى البعض أن استخدام تقنية الميتافيرس قد يحدث تطورًا كبيرًا في حياة البشر وسلوكهم، فبدلًا من أن تكون التفاعلات البشريَّة واقعيةً ومحسوسةً عبر التلاقي المادي، أو أن تكون غير مادية وغير محسوسة عبر التلاقي الرقمي من خلال شاشات الهواتف الذكية وأجهزة الكمبيوتر، فسوف يكون هناك طريق ثالث يسد الفجوة بين هذين العالمين الواقعي والرقمي، ليظهر عالم ثالث افتراضي موازٍ، يأخذ من الواقع شيئًا، ومن الخيال والإنترنت والتقنيات الذكية أشياء وخصائص أخرى (خليفة، 2022).

فمن خلال تقنية الميتافيرس يفتح الباب واسعًا لإنشاء عالم ثالث افتراضي، يستطيع فيه الأفراد إنشاء حياة افتراضية لهم عبر مساحات مختلفة من الإنترنت؛ بحيث تسمح لهم بالتلاقي والعمل والتعليم والترفيه بداخله، مع توفير تجربة تسمح لهم ليس فقط بالمشاهدة عن بعد عبر الأجهزة الذكية كما يحدث حاليًّا، ولكن بالدخول إلى هذا العالم في شكل صورة متحركة تمثل الشخص (أفاتار) في العالم الثلاثي الأبعاد عبر تقنيات الميتافيرس الافتراضية (جبريل، 2023).

- الميتافيرس من تطبيقات التكنولوجيا الحديثة

يمكن القول بأن الميتافيرس هي صورة متطورة من شبكة المعلومات الدوليَّة الإنترنت، بل إنها الجيل الحديث من هذه الشبكة التي تمكن الشخص من الدخول إليها، وممارسة حياة افتراضية متكاملة، تتيح له القيام بكافة الأنشطة والعمليات التي كان يباشرها في حياته المادية الطبيعية، فمن خصائص الميتافيرس أنها تعتمد في عملية استخدامها على تقنية تشفيرية تقوم على تكنولوجيا التناظر الإلكتروني على منصات الإنترنت، فيمكن للشخص أن يقوم بممارسة نشاطه عبر شبكة الإنترنت باستخدام أدوات معينة تساعده على الدخول إلى العالم الافتراضي، وعلى الرغم مما توفره هذه التقنية من سرية تامة، فإن غياب التنظيم القانوني الذي يحكمها يفقد مستخدميها الحماية اللازمة لهم؛ مما يعرضهم لعمليات النصب والاحتيال (جبريل، 2023، ص. 17)، وهو ما سيثير إشكالية حول كيفية استخلاص وجمع الأدلة في ظل هذه البيئة الرقميَّة الجديدة ذات التقنيات المعقدة.

الميتافيرس تعتمد على وسائل تكنولوجية معينة

تتسم بيئة الميتافيرس بأنها بيئة رقميَّة تعتمد على التقنيات في ابتكار المعاملات والخدمات، وتوفير قنوات جديدة لإنجاز المهام والتعاملات، ويمكن القول: إن الدخول إلى تقنية الميتافيرس له متطلبات معينة، من أبرزها: وجود خدمة إنترنت فائق السرعة

من الجيل الخامس وما يليه، تتيح للمستخدم الدخول في تقنية الميتافيرس، فضلًا عن وجود تقنيات الواقع الافتراضي والواقع المعزز من نظارات وسترات وقفازات وسماعات، يستخدمها الفرد خلال وجوده في تقنية الميتافيرس، وتنقله من مجرد مستخدم للإنترنت إلى جزء منه ومشارك فيه، وتساعده على مباشرة حياته الافتراضية داخل تقنية الميتافيرس، فمن خصوصيات الميتافيرس أنها تقنية تقوم على عنصرين مهمين هما: الإنترنت وأدوات الواقع الافتراضي والمعزز، وإذا تخلف عنصر منهما تتوقف تقنية الميتافيرس، وتصاب بالشلل؛ حيث توفر شبكة الإنترنت باستخدام الأجهزة الإلكترونية الحديثة العديد من الخدمات التي لا يمكن للإنسان العصري الحياة بدونها (جبريل، 2023).

ولقد أدَّى ارتباط الميتافيرس بشبكة الإنترنت إلى أن أصبحت بيئة الميتافيرس جزءًا من قرية كونية على الإنترنت، يحكمها واقع افتراضي، لا يخضع للمفاهيم التقليديَّة التي وضعت حدودًا جغرافية وسياسية للفصل بين الدول والأقاليم والقارات المختلفة، فهذه الفواصل لا تتلاءم مطلقًا مع مجتمع إلكتروني ينقسم إلى مواقع ويب ومنصات وشبكات إلكترونية.

ومن جانب آخر، تعتمد تقنية الميتافيرس على استخدام بعض الأدوات التقنية؛ كنظارات الواقع الافتراضي والواقع المعزز، وارتداء السترات والقفازات المزودة بأجهزة استشعار، يستطيع المستخدم من خلالها أن يعيش تجربة حقيقية، تعمل فيها هذه التقنيات الذكية كوسيط بين المستخدمين في تقنية الميتافيرس، لإيصال الشعور بالإحساس المادي، فيستطيع المستخدم من خلال القفازات أن يشعر بملمس الأشياء ودرجة حرارتها ووزنها، ويستطيع أن يرى بواسطة النظارة الخاصة الأشياء من حوله بصورة ثلاثية الأبعاد، كما يمكن أن يشعر فيها بالمؤثرات الجسدية الحسية من خلال السترة أو البدلة، كإحساس السقوط في المياه أو اللكمة في الوجه أو غيرها، من خلال المستشعرات الموجودة في السترات والقفازات التي يرتديها، فيحصل على تجربة أشبه بالواقعية حتى وإن كانت غير مباشرة (خليفة، 2022).

- التصور الخاص باستخدام تقنية الميتافيرس

حتى يمكن للقارئ تصور التساؤلات المطروحة؛ فإنه يجدر التنويه إلى طبيعة تقنية الميتافيرس الذي يقوم على إستراتيجية تكنولوجية جديدة تعتمد على التطور غير المسبوق في تطبيقات الجيل الثالث للأشياء web-3.0، والتي ستتيح لمواقع الويب والتطبيقات التعامل مع المعلومات بطريقة تحاكي الإنسان، من خلال تقنيات التعلم الآلي والبيانات الضخمة؛ حيث ستكون البيانات مترابطةً ببروتوكولات التعامل بطريقة لا مركزية، تعتمد على تقنيات سلاسل الكتلة block-chain والعملات الرقميَّة المشفرة crypto-currency، وسيتمكن المستخدمون من التفاعل مع الأدوات والمعدات والبيانات بشكل يعمل على إعادة تشكيل وسائل التواصل الاجتماعي؛ بما يسمح لمستخدميها بالانتقال والدخول والتفاعل داخل تقنية الميتافيرس بشكل تفاعلي في بيئة رقميَّة تحاكي البيئة الطبيعيَّة، أو المادية التي نعيش فيها من خلال استخدام المستخدمين لشخصيات رمزية «Avatar» للتعامل والتفاعل (حجازي، 2022).

ويوضح البعض التصور الخاص بتقنية الميتافيرس وكيفية التعامل والتعايش داخله، بأن الأمر يشبه تحويل شبكة الإنترنت إلى مجتمع يحيط بالشخص بواسطة خاصية ثلاثية الأبعاد، ومن ثم يدخل المستخدم إلى هذا العالم في صورته الافتراضية الرمزية (الأفاتار) وباستخدام تقنيات الواقع الافتراضي؛ كالنظارات والسترات والقفازات، ليجد نفسه داخل مجموعة من العوالم الافتراضية المترابطة التي لا نهاية لها، كما يمكنه الالتقاء بعدد كبير من الناس في صورتهم الرمزية (الأفاتار) كذلك، والتعامل معهم؛ بحيث يكون المستخدم للميتافيرس جزءًا من العالم الافتراضي، ومن الممكن في المستقبل القريب أن يصبح المستخدم مشاركًا وصانعًا لهذا العالم، إذا تم توفير مستلزماته من البدلة والنظارة وسماعة الرأس والقفازات، ومع إنترنت سريع من الجيل الخامس وما يليه ستتغير التقنية في تعاملها مع المستخدم ليتحول من مجرد مستخدم أو مشاهد إلى جزء لا يتجزأ من هذه الحياة الافتراضية (جبريل، 2023).

فبدلًا من الدخول إلى الفضاء السيبراني عبر شاشات الكمبيوتر وأجهزة الهواتف الذكية، كما هو الوضع الحالي في شبكة الإنترنت، سوف يتم الدخول إليه عبر نظارات الواقع الافتراضي، التي يتم استخدامها في ألعاب الفيديو حاليًّا، لكن بدلًا من استخدامها كوسيلة للتسلية، ستتم إعادة تصميمها لكي تصبح بديلًا للهواتف الذكية؛ فتصبح متصلة بالإنترنت، وسيتم دمج تقنيات الواقع المعزز معها التي تعرض المعلومات الخاصة كافة بأي شيء تقع عليه عينك في الواقع الحقيقي؛ وبذلك يتم دمج تقنية الواقع الافتراضي التي تغلب عليها التصميمات الرقميَّة، مع الواقع المعزز الذي يغلب عليه الواقع، فينشأ عالم مختلط هو المتيافيرس (خليفة، 2022).

3. 2 مخاطر استخدام الميتافيرس من الناحية الجنائيَّة

هناك بعض المخاوف من استخدام تقنية الميتافيرس، فضلًا عن وجود بعض التساؤلات ذات الصلة باستخدامها، وهو ما سوف نتناوله في هذا الفرع على النحو التالي:

مخاطر الميتافيرس

على الرغم من المزايا الكثيرة التي يزعمها مؤيدو الميتافيرس والتي من أبرزها: إزالة الحواجز الجغرافية بين الأشخاص بعضهم مع بعض، مع إمكانية العثور على أشخاص لديهم نفس الاهتمامات والأفكار والتعرف عليهم، وتطوير وسائل التواصل الاجتماعي، وخلق العديد من فرص العمل التجارية، وتوفير أشكال جديدة من التسويق والإعلان على منصات التواصل الاجتماعي، وتطوير منظومة التعليم والتعلم عبر الإنترنت، فإن واقع الميتافيرس ليس ورديًّا؛ حيث تعتبر السلبية الأبرز للميتافيرس هي سهولة ارتكاب الجرائم من خلالها؛ إذ يتم دخول الشخص إلى الميتافيرس بطريقة سرية مشفرة، ويتفاعل بصور رمزية قابلة للبرمجة مع غيره من الأشخاص في فضاء افتراضي ثلاثي الأبعاد، ويرى البعض أن هناك العديد من الجرائم التي قد ترتكب عبر الميتافيرس؛ كالجرائم الجنسية، والممارسات غير الأخلاقية، وتعمد إزعاج الغير، والسب والقذف، وانتهاك الآداب العامة، وخدش الحياء، والفعل الفاضح العلني، والإخلال بحياء امرأة في غير علانية، والتحريض على الفسق والدعارة، والاستغلال الجنسي للأطفال، واستراق السمع والبصر، والإخلال بالقيم الأسرية، والسرقة والنصب والاحتيال إلى غير ذلك من جرائم الأموال (المري، 2020، ص. 78)، ومن ثم يتوقع البعض ازدياد مخاطر الجرائم السيبرانية مع وجود تقنية الميتافيرس، إيذانًا بظهور مصطلح جديد هو جرائم الميتافيرس Metacrimes، فهذا العالم الجديد - الذي ما زال قيد التطوير- لا يتمتع بمستويات تأمينية متطورة؛ مما قد يجعله مسرحًا واسعًا لارتكاب العديد من الأنشطة غير القانونيَّة؛ مثل: انتحال الهوية والاحتيال والسرقة الافتراضية، وتخريب الأعمال والمقتنيات الفنية الافتراضية وغسل الأموال وتزييف العملات الافتراضية، واستغلال الأطفال في الدعارة والاتجار بالسلع غير القانونيَّة والمخدرات وغيرها (جبريل، 2023).

ونذكر من صور جرائم الميتافيرس المستحدثة جرائم انتحال الهوية؛ حيث يربط البعض بين استخدام الأفاتار في الميتافيرس وعمليات انتحال الهوية؛ حيث يمتلك المستخدمون هوية رمزية تمثلهم في تقنية الميتافيرس (أفاتار)، وتكون عادةً في شكل بشري ثلاثي الأبعاد، ويقوم المستخدمون بتخصيصها بشكل فريد من لون البشرة إلى الملحقات بالتفصيل عند التسجيل لأول مرة في الميتافيرس، ويتعرفون بعضهم على بعض من خلال الصورة الرمزية عند تكوين علاقة مع الآخرين أو إجراء المعاملات؛ لأن المستخدم يدخل فقط بيانات بسيطة؛ مثل: المعرف والعمر والجنس عند التسجيل في الميتافيرس، ونظرًا لأن جميع إجراءات الصورة الرمزية مكشوفة لجميع المستخدمين في الميتافيرس، فيمكن التعرف على الخصائص الفريدة، مثل: المظهر وأنماط السلوك والإيماءات من قبل المستخدمين لأغراض ضارة فقط، من خلال الملاحظة البسيطة، بالإضافة إلى ذلك، يتم عرض المعلومات الشخصية للمستخدم بسهولة للمستخدمين الآخرين على الميتافيرس؛ حيث يمكن استخدام النمط الفريد للصورة الشخصية والمعلومات الشخصية لانتحال الهوية أو هجوم الهندسة الاجتماعية، مثل: التصيد الاحتيالي والتهديد المستمر للحصول على مكاسب مالية؛ حيث يكون من الصعب تحديد هجمات الهندسة الاجتماعية أكثر من الواقع؛ لأن الميتافيرس ليس له قيود على تغييرات شكل الأفاتار (Seo et al., 2023 :9472).

هذا بالإضافة إلى جرائم السرقة الافتراضية، وهي فعل انتهاك للممتلكات الافتراضية للآخرين من خلال سرقة أشياء افتراضية في العالم الرقمي؛ حيث يشير البعض إلى أن هناك حالات تمت فيها معاقبة السرقة الافتراضية كعمل إجرامي في المحاكم الفعلية (Lodder,2011:79).

كما تشير بعض التقارير إلى إمكان وقوع الجرائم الجنسية في تقنية الميتافيرس، كجريمة الاغتصاب والتحرش الجنسي الافتراضية؛ حيث ادَّعت إحدى السيدات الإنجليزيات بتعرض الأفاتارة الخاصة بها للاغتصاب من أفتارات لأشخاص آخرين، وتعرضها لأضرار ومتاعب نفسية جسيمة نتيجة حادث الاغتصاب الذي مرت به أثناء تواجدها في تقنية الميتافيرس، ومطالبتها بمعاقبة هؤلاء الأفاتارات عن جريمة الاغتصاب التي قاموا بها (حجازي، 2022)، حيث تتلخص وقائع الحادثة في أن السيدة بمجرد دخولها تقنية الميتافيرس، وفي غضون دقيقة من الدخول تعرَّضت للتحرش اللفظي والجنسي من قبل أربعة شخصيات رمزية عن طريق الأفاتار الخاص بهم، ولم يكتفوا بالتحرش اللفظي أو الجنسي، ولكن تمادوا في الأمر، وتم اغتصاب الأفاتار الخاص بها (جبريل، 2023)، وذلك على الرغم من أن جريمة الاغتصاب على خلاف غيرها من جرائم العرض من الصعب تصور وقوعها في بيئة الميتافيرس بالنظر إلى افتراضها اتصالًا جنسيًّا مباشرًا غير رضائي يقع من ذكر على أنثى، وهو غير متصور في بيئة الميتافيرس.

فضلًا عن عمليات غسل الأموال الرقميَّة؛ حيث يمكن أن تكون الميتافيرس مساحةً مركزيةً أو مجالًا للاتصال بين غاسلي الأموال (Laue, 2011: 20)؛ حيث يمكن للجماعات الإجراميَّة غسل الأموال غير المشروعة والقيام بعمليات شراء وبيع للأصول الافتراضية على الميتافيرس عن طريق تحميل محتويات افتراضية إلى سوق الميتافيرس، ثم الشراء من خلال شركات وهمية أو شركات مشبوهة الملكية بالعملة المستخدمة فقط داخل الميتافيرس، أو ما تسمى بعملة الميتافيرسMetaverse Coin التي من المتوقع إساءة استخدامها في عمليات غسل الأموال غير المشروعة مستقبلًا؛ وذلك لأن المستخدم

يبتكر الصور الرمزية بشكل مجهول، ويمكن شراء عملة الميتافيرس بأموال حقيقية وأن تستبدل بها أموال حقيقية، فعلى سبيل المثال، يمكن للمجرمين شراء عملات الميتافيرس من خلال حسابات متعددة يحصلون عليها من مساهمين أو شركات مختلطة، وبيع أشياء افتراضية مزيفة تم وضعها سلفًا.

أضف إلى ذلك توقعات زيادة الهجمات السيبرانية (الإجراميَّة والإرهابية)؛ الأمر الذي يرتفع معه نسبة المخاطر المتوقع حدوثها على الأمن السيبراني، بسبب غياب الرقابة في هذا العالم الجديد؛ إذ إن مراقبة عدد كبير جدًا من المستخدمين في وقت واحد لن تكون بالمهمة السهلة، بل إنها تكاد أن تكون مستحيلة، خاصةً أن تلك التقنية حديثة، ولم يتم وضع ضوابط منظمة لتشغيلها حتى الآن، ومن ثم نخلص من ذلك إلى أن الميتافيرس قد يكون أحد المسببات في زيادة خطورة وانتشار الجرائم السيبرانية في عالمنا اليوم بشكل أكبر مما هو قائم في الوقت الحالي.

تساؤل حول مدى إمكان وضع بعض السلوكيات في تقنية الميتافيرس تحت وصف الجريمة

أثار البعض تساؤلًا مهمًّا بشأن مدى إمكان وقوع الجرائم داخل تقنية الميتافيرس، من منطلق قانوني منطقي، مفاده أن الميتافيرس عالم افتراضي خيالي، وأن القانون الجنائي لا يوجه إلا إلى السلوك المادي الخارجي في المجتمع الحقيقي، وما يترتب على ذلك من أن القانون لا يأخذ بالنوايا، ولا ينطبق على ما يجري داخل خفايا الإنسان أو أحلامه وأمنياته، كما أن القانون ليس له علاقة بمشاعر الإنسان النفسية التي لا تظهر للواقع، وتتخذ مظهرًا خارجيًّا، أو مخاوفه أو أوهامه التي لا تبدو في الحقيقة، ومن ثمَّ يمكن القول استنتاجًا لذلك بأن القانون قد لا يحكم ما يفعله الإنسان في العالم الافتراضي، ما دام لم يتسبب في ضرر للغير، أو لم يمثل سلوكًا يشكل جريمة وَفق نصوص القانون، ومن ثم ينتهي الرأي السابق إلى إخضاع تقنية الميتافيرس لحكم القانون، ومن ثم جواز المعاقبة على السلوكيات التي تتم عبر تقنية الميتافيرس مادامت تشكل سلوكًا مجرمًا وفق القانون (جبريل، 2023، ص. 62)، ويتفق الباحث مع الرأي السابق من منطلق اتفاقه مع المنطق القانوني السليم الذي يرتكز على طبيعة القانون الجنائي كأداة لضبط السلوك الاجتماعي للأفراد، والذي لا يحاسب الفرد على نواياه الداخلية غير المادية، وإنما يحاسبه على أفعالهم المادية الخارجية التي تشكل مخالفةً لحكم القانون واعتداءً على المصلحة القانونيَّة الجديرة بالحماية من جانب المشرع.

تساؤل حول مدى إمكان القول بمنح الأفاتار الشخصية القانونيَّة

ينبثق عن التساؤل السابق تساؤل آخر حول مدى تمتع أشخاص تقنية الميتافيرس، وبخاصة الأفاتار بالشخصية القانونيَّة، والإجابة عن هذا التساؤل أن القانون يمنح الشخصية القانونيَّة إلى الإنسان الطبيعي دون غيره من الجماد والحيوان، وأن القانون لا يخاطب رمز الشخص أو صورته أو أي شيء من الأشياء التي تمثله كصورته، أو الرمز الذي يدل عليه في تقنية الميتافيرس، ومن ثم يظل الشخص الحقيقي هو المسئول جنائيًا عن تصرفاته التي يرتكبها من خلال تقنية الميتافيرس، أما الأفاتار، وهو الرمز الذي يمثل الشخص الحقيقي، وما يقع منه من أفعال، وما يقع عليه من تعدٍّ، فلا يكون محل اعتبار إلا إذا كان صادرًا عن شخص حقيقي، أو صادرًا ضده، ومفاد ما تقدم أن الجرائم التي تقع على الأفاتار قد لا تمثل جريمة مطلقًا، كجريمة الاغتصاب، والتي لا يتصور وقوعها إلا على أنثى، وأن تتم على جسدها الحقيقي، وليس الرمز الخاص بها عبر تقنية الميتافيرس، وكذلك جريمة القتل، فلا تقع إلا على إنسان حي (جبريل، 2023، ص. 62)، والواقع أن الإجابة عن التساؤلات الأخيرة لها أهمية كبيرة في سياق القانون الجنائي، وأنه من المتوقع أن تتطور هذه القواعد بتطور تقنية الميتافيرس وتشعب استخدامها في كافة مناحي الحياة، وهو ما قد ينعكس على قواعد القانون الجنائي مستقبلًا، ويتوقع الباحث في ضَوء الإرهاصات السابقة أن يجد من الفقهاء مستقبلًا من قد ينادي بمنح (الأفاتار) الصورة الرمزية للإنسان داخل الميتافيرس شخصية قانونيَّة محدودة.

4. المطلب الثاني: ماهية الدليل الرقمي في تقنية الميتافيرس وإجراءات جمعه واستخلاصه

تلقي تقنية الميتافيرس الافتراضية الرقميَّة بظلالها على الدليل الجنائي المتحصل من الجرائم الواقعة بداخلها؛ حيث إن طبيعة مسرح جريمة الميتافيرس يتمثل في أنه عالم افتراضي لا حدود مكانية له، وينصب البحث فيه على وسائل وأدوات تتم بها الجريمة عبر أجهزة إلكترونية وشبكات إلكترونية دولية، باستخدام الأجهزة الإلكترونية، وفيما يتصل بالدليل الجنائي في تقنية الميتافيرس، فإنه ينقسم إلى قسمين: الأول: هو الدليل المادي المتحصل من استخدام أدوات الواقع الافتراضي والواقع المعزز؛ كالنظارات والسترات والقفازات والسماعات إلى غير ذلك، والثاني: هو الدليل الرقمي المتحصل من تقنية الميتافيرس الافتراضية وتطبيقات الهواتف الذكية، وسنتناول في هذا المطلب التعريف بالدليل الجنائي الرقمي، وإجراءات جمعه واستخلاصه، وذلك في فرعين على النحو التالي:

1.4 تعريف الدليل الرقمي وخصائصه

نتناول في هذا الفرع تعريف الدليل الجنائي التقليدي، ثم الدليل الرقمي وخصائصه، ثم نتطرق لأهميته في تقنية الميتافيرس، وذلك على النحو التالي:

تعريف الدليل الجنائي

يقصد بالأدلة الجنائيَّة الوسائل التي تربط الوقائع بإدانة أو براءة الأفراد أثناء المحاكمات الجنائيَّة، وهي مجموعة من القرائن التي من خلالها يمكن إثبات مجموعة من الحقائق التي تدور حول الجريمة، بالإضافة إلى القدرة على نسبتها إلى فاعل معين، أو هي: مجموعة من البراهين مقبولة بحكم القانون، لا يمكن أن يتم إثبات وقائع الجريمة إلَّا بواسطتها أمام الجهات القضائية، سواء أكانت المحاكم أم النيابة العامة، وهي تتنوع تبعًا لتنوع الجرائم، ومن ثم فالدليل الجنائي هو: «كل إجراء معترف به قانونًا لإقناع القاضي بحقيقة الواقعة محل الاتهام، وهذا الدليل إما أن يكون أثرًا من منطبع في نفس أو في شيء، أو يتجسم في شيء يدل على وقوع جريمة من جانب شخص معين» (نقض4/13/ 2021، الطعن رقم 14544 سنة 88 ق)، والدليل يتم الحصول عليه من مسرح الجريمة، والذي يعرف بأنه: «المكان الذي وقعت أو نفذت فيه الجريمة»؛ ونظرًا لما للأدلة من أهمية كبيرة عند الجهات القضائية للوصول إلى الحقيقة، فقد تم تقييدها بمجموعة من القيود والضوابط، وذلك يعني أنه يجب أن تقوم هذه الأدلة على البرهان والمنطق، وأن يقتنع بها العقل.

وقد تعددت تعاريف الدليل الجنائي لدى الفقه، فمنهم من عرفه بأنه: الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة (سرور، 1996، ص. 418)، ومنهم من عرفه بأنه: «الواقعة التي يستمد منها القاضي الرهان على إثبات اقتناعه بالحكم الذي ينتهي إليه» (نجيب، 2014 ص. 48)، والدليل يختلف عن الدلائل والأمارات التي توضع في مرتبة إثباتية أقل من الدليل، حيث تحتمل أكثر من وجه، ولا ينعقد بها اليقين القضائي (سلامة، 1996، ص. 191).

تعريف الدليل الرقمي

ذهب عدد من التشريعات إلى وضع تعريف للدليل الرقمي، نذكر منها التشريع المصري الذي عرف الدليل الرقمي بأنه: «أي معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة، أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتيَّة وما في حكمها، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة» (م1 من القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات)، ويلاحظ أن المشرع قد حرص على إبراز جوهر الدليل الرقمي، وهو المعلومات المستخرجة من الأجهزة التقنية، سواء أكانت أجهزة الحاسب الآلي أم شبكات المعلومات وما في حكمها.

خصائص الدليل الرقمي

يتسم الدليل الرقمي في تقنية الميتافيرس بعدد من الخصائص، أولها: أن التعامل مع الدليل الرقمي يتطلب دراية علمية وفنية متخصصة، فلا يمكن استخراجه أو حتى اكتشافه، إلا من خلال خبراء متخصصين (يونس، 2004)، وثانيها: أن الدليل الرقمي ذو طابع تقني، ويتكون من معلومات تتجسد في صورة إلكترونية، لا يتم إدراكها إلا باستخدام تقنية المعلومات (نجيب، 2014)، ومن ثم فالدليل الرقمي لا يكون إلا في بيئة رقميَّة (إبراهيم، 2020)، وثالثها: أن الدليل الرقمي يتكون من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة، لا تدركها الحواس العادية، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات HARDWARE، واستخدام نظم برامجية حاسوبية SOFTWARE (فرغلي، 2007)، فالأدلة الرقميَّة ليست أقل مادية من الدليل المادي فحسب، بل تصل إلى درجة التخيلية في شكلها وحجمها ومكان وجودها غير المعلن، فالدليل الرقمي يشمل كافة أشكال وأنواع البيانات الرقميَّة الممكن تداولها، بحيث يكون بينها وبين الجريمة رابطة من نوع ما، وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني (يونس، 2006)، ورابعها: أن الأدلة الرقميَّة ذات طابع ديناميكي فائق السرعة، تنتقل من مكان لآخر عبر شبكات الاتصال متعدية حدود الزمان والمكان (نجيب، 2014، ص. 55)، وخامسها: أنه يمكن استخراج نسخ من الأدلة الرقميَّة مطابقة للأصل، ولها القيمة العلمية والحجية الثبوتية ذاتها، وهذا الأمر لا يتوافر في الأدلة التقليديَّة؛ مما يشكل ضمانة شديدة الفاعلية للحفاظ على الدليل ضد الفقد والتلف والتغيير، عن طريق نسخ طبق الأصل من الدليل (فرغلي،2007)، وسادسها: أن الأدلة الرقميَّة يمكن استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها؛ مما يؤدي إلى صعوبة الخلاص منها، وهي خصيصة من أهم خصائص الدليل الرقمي، ويتم ذلك من خلال استخدام البرامج الحاسوبية التي وظيفتها استعادة البيانات التي تم حذفها أو إلغاؤها؛ مما يعني صعوبة إخفاء الجاني لجريمته عن أعين رجال العدالة الجنائيَّة (الحسيني، 2019)، وأخيرًا: يمكن من خلال الدليل الرقمي رصد المعلومات عن الجاني وتحليلها في الوقت ذاته، كما يمكن للدليل الرقمي تسجيل تحركات الفرد وسلوكياته وبعض الأمور الشخصية عنه (عبد المطلب، 2003).

أهمية الدليل الجنائي الرقمي في تقنية الميتافيرس

يمكن تأصيل أهمية الدليل الجنائي الرقمي في أن ذيوع استخدام التكنولوجيا في مناحي الحياة، وانتشار الأجهزة التكنولوجيَّة وشبكة الإنترنت أدَّى إلى استنتاج منطقي، مؤداه أنه من غير المتصور وقوع جريمة تقليديَّة أو مستحدثة، دونما أن يتخلف عنها أدلة رقميَّة يمكن التوصل من خلالها إلى تحديد مرتكب الجريمة، وإنه مع شيوع استخدام التكنولوجيات الجديدة، مثل: إنترنت الأشياء وشبكات الإنترنت المظلم، والتشفير العالي الدرجة والعملات الافتراضية، وصولًا إلى تقنية الميتافيرس في ارتكاب الجرائم، فمن المتوقع ازدياد أهمية الدليل الرقمي في الحقل الجنائي، وهو ما سيتطلب من جهات إنفاذ القانون إجراء تغييرات جذرية في طرق جمع الأدلة وآليات التعاون الدولي في المسائل الجنائيَّة، بالشكل الذي يتناسب وطبيعة هذه النوعية المستحدثة من الأدلة الجنائيَّة (Meiklejohn, 2013)، والتي تتسم بطابع خاص، وهو طبيعتها المعنوية المتغيرة، فالمعلومات المخزنة على الحواسب الآلية، أو على خوادم الحوسبة السحابية عبر شبكة الإنترنت هي معلومات متقلبة (Quéméner, 2014)، ويسهل العبث بها وتغييرها أثناء التحقيقات، بل إن هذه الأدلة ذات طبيعة هشة وقابلة للإتلاف من خلال سوء المناولة أو الفحص بطريقة غير سليمة (مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2013، ص. 230)، ومن ثم تبدو أهمية الدليل الرقمي جليةً، باعتباره الوسيلة التي تمكن سلطات إنفاذ القانون من معرفة كيفية وقوع الجريمة السيبرانية وإثباتها ونسبتها إلى مرتكبها، ولا سيما أنها ترتكب في بيئة افتراضية غير مادية (الصغير، 2002، ص. 11)، وكان من الواجب وضع قواعد وشروط محددة للتعامل مع هذه الأدلة الرقميَّة للتأكد من مقبوليتها أمام القضاء الجنائي، فضلًا عن اتخاذ احتياطات خاصة من أجل توثيقها وجمعها والحفاظ عليها وفحصها.

4. 2 إجراءات جمع الدليل الرقمي ومشروعيته ومقبوليته أمام القاضي الجنائي

نعرض في هذا الفرع مراحل جمع الدليل الرقمي في تقنية الميتافيرس، ثم نتناول مشروعية الدليل الرقمي ومقبوليته أمام القضاء الجنائي؛ وذلك على النحو التالي:

- مرحلة جمع البيانات والأدلة الرقميَّة في تقنية الميتافيرس

تتمثل أولى خطوات جمع الأدلة في جمع البيانات الخاصة بوقوع الجريمة في تقنية الميتافيرس، وهو ما يتطلب ضرورة التعرف على المصادر التي يبدو أن لديها أدلة، والتي يمكن أن تكون جهازًا ماديًّا أو نظامًا معلوماتيًّا أو خدمة، وبعد ذلك، يجب على الجهة المعنية بجمع الدليل (سواء أكانوا من مأموري الضبط القضائي أو الخبراء المختصين بجمع الأدلة الإلكترونية) الحصول على أدلة من المصادر، والتأكد من أنها بتنسيق ما يمكن نسخه بسهولة مع الحفاظ على الحالة الأصلية كصورة مع الحفاظ على سلامة البيانات (Seo et al, 2023).

ويشير البعض إلى وجود علاقة بين الأدلة المادية الموجودة في العالم الحقيقي ونظائرها من الأدلة الرقميَّة في تقنية الميتافيرس، فقد تحتوي بيانات الميتافيرس على أدلة تخص الجرائم التقليديَّة في العالم الحقيقي، بالنظر إلى التأثير المتبادل بينها وبين العالم الحقيقي، وعلى العكس من ذلك، يمكن أن تكون البيانات من العالم الحقيقي دليلًا عند التحقيق في حالة حدثت في الميتافيرس؛ لذلك سيحتاج المحققون إلى تحليل كل الأدلة من كلا العالمين في بعض الحالات (Seo et al., 2023).

ومن ثم يقسم الباحثون أدلة جرائم الميتافيرس بحسب مكان وقوع الجريمة وَفق أربعة فروض: الأول: جريمة أو مشكلة تحدث في الميتافيرس وجميع الأدلة بطبيعتها داخل الميتافيرس، والثاني: جريمة أو مشكلة تحدث في الميتافيرس، وبعض الأدلة خارج الميتافيرس، والثالث: جريمة أو مشكلة حدثت في العالم الحقيقي، وبعض أدلتها من الميتافيرس، والرابع: جريمة أو مشكلة حدثت عبر الميتافيرس والعالم الحقيقي، والأدلة من كليهما (Seo et al., 2023).

ومن جانب آخر، تتسم إجراءات جمع الأدلة الرقميَّة في تقنية الميتافيرس بخصوصية خاصة، ترتبط بالطبيعة الخاصة لهذا العالم؛ إذ إن إجراءات جمع الأدلة الرقميَّة تمتد لتشمل ثلاثة مصادر أو نطاقات مكونة لتقنية الميتافيرس، وهي أجهزة المستخدم، وخوادم مقدمي الخدمة، ومنصة الميتافيرس نفسها؛ حيث يمكن التمييز بين النطاقات الثلاث التالية:

نطاق المستخدم

يشتمل نطاق أو مجال المستخدم على كل ما يمكن للمستخدمين في العالم الحقيقي القيام به والأفاتارات التي يتحكمون بها في تقنية الميتافيرس، ويتكون نطاق المستخدم من طبقة اتصال، تمثل توصيل المستخدمين بالميتافيرس، وجميع إجراءات الاتصال وطبقة تفاعل، تمثل التفاعلات بين المستخدمين في الميتافيرس، ويمكن تنفيذ طبقة الاتصال من خلال نظارات الواقع المعزز أو السترات أو أجهزة الاستشعار؛ حيث يقوم المستخدمون بالوصول إلى الميتافيرس، والتواصل معه من خلال أجهزة مثل: نظارات الواقع المعزز والسترات القابلة للارتداء؛ حيث تحتوي هذه الأجهزة على معالجات وذاكرة متنقلة وذاكرة وصول عشوائي لأداء وظائفها، فنظارات الواقع المعزز على سبيل المثال تربط المستخدمين بالميتافيرس، على ذاكرة تبلغ سعتها 128 جيجابايت أو أكثر، ومن المتوقع أن يتم تخزين أنواع مختلفة من البيانات المتعلقة بالجريمة في ذاكرة تلك الأجهزة المستخدمة للتفاعل

مع العالم الحقيقي، أما بالنسبة للإجراءات والأساليب المستخدمة لجمع البيانات من هذه الأجهزة، فهي مماثلة لتلك المستخدمة مع إنترنت الأشياء والأجهزة المحمولة، إلا أنه بالنظر إلى التطورات التقنية المتلاحقة في مثل هذه الأجهزة التفاعلية، فإنه يجب أن يراعى في الاعتبار الأجهزة الطرفية التي يتم ربطها بهذه الأجهزة في العالم الحقيقي؛ حيث يتم نقل البيانات الخاصة بتلك الأجهزة التفاعلية على الأجهزة الأخرى (Seo et al., 2023).

نطاق الخدمة

يشمل نطاق الخدمة كل ما يتعلق بالخدمات التي تقدمها المنصة، بالإضافة إلى الخدمات التي تقدمها الأطراف الثالثة، وتتطلب طبقة الخدمة تقنيات؛ مثل: التجارة الإلكترونية، وأنظمة دفع p2p، وتكنولوجيا المصدر المفتوح، والعملات المشفرة؛ لأن محتويات التداول والتسوق يتم توفيرها كخدمات، فنظرًا للخدمات العديدة التي تقدمها الميتافيرس للمستخدمين في وقت واحد، والتي يصعب تشغيلها باستخدام موارد الميتافيرس فقط، فإنه يتم اللجوء إلى مقدمي الخدمات الخارجية لتوفيرها للمستخدمين؛ حيث يعتمد هؤلاء المقدمون على ما يوفره النظام الأساسي للميتافيرس من معلومات أساسية حول هذه الخدمات، مثل: العرض وتفاعلات المستخدم لتنفيذ وظائف الخدمة، والتي قد تكون موردًا أساسيًّا لتقديم الخدمة بسلاسة من جانبهم، وهو ما قد يشكل مصدرًا للمحققين في جمع واستخلاص الأدلة المتحصلة عن الجرائم الواقعة في تقنية الميتافيرس.

وقد يواجه المحققون صعوبات في الحصول على بعض البيانات التي تتصل بإدارة بيانات المستخدم؛ مثل: الخدمات المالية وخدمات الدفع، إذا كانت الخدمة المتضمنة في الحادث تستخدم مواردها الخاصة؛ حيث يتم تخزين البيانات في البنية التحتية للمزود، ولهذا السبب على المحققين طلب البيانات ذات الصلة من مزود الخدمة فورًا، وقد يكون إجراء جمع البيانات مستحيلًا، حينما لا يكون هناك التزام قانوني على مزود الخدمة بتوفير البيانات، ومن جانب آخر، قد يكون إجراء جمع البيانات ليس فقط في الميتافيرس، وإنما في العالم الحقيقي أيضًا، ومن ثم يجب على المحققين في هذه الحالة إرسال الطلب إلى مزود الخدمة بالنسبة للبيانات المخزنة خارج الميتافيرس (Seo et al., 2023).

نطاق منصة الميتافيرس

يشير نطاق منصة الميتافيرس إلى كل ما يعمل ويدير الميتافيرس، ويتضمن الوظائف المتعلقة بالنظام أو المسئول، فطبقة الفضاء الافتراضية هي جزء ينفذ ويدير «عالماً» افتراضيًّا ينشط فيه المستخدمون والخدمات، باستخدام تقنيات؛ مثل: التوائم الرقميَّة ورؤية الكمبيوتر من أجل وضع الميتافيرس بالقرب من العالم الحقيقي، وطبقة الإدارة عبارة عن تطبيق للنظام الذي يحافظ على الميتافيرس، ويتطلب تقنية الذكاء الاصطناعي للإدارة التلقائية للمشكلات الكبيرة جدًا، بحيث لا يستطيع البشر التعامل معها، وطبقة البيانات هي طبقة تدير جميع البيانات التي تم إنشاؤها وتخزينها على منصة الميتافيرس، وفي طبقة البيانات، هناك حاجة لتقنيات؛ مثل: سلاسل الكتل Blockchain، والحوسبة الحدية Edge Computing، ومفهوم السحابة لضمان سلامة واستقرار البيانات التي تصل إلى مستوى زيتا بايت وما بعده في الميتافيرس (Seo et al., 2023).

ونظرًا لأن الميتافيرس يحتوي على حجم من البيانات التي يجب توصيلها مع المستخدم، فمن الضروري أن يتم تخزين وإدارة البيانات المتعلقة بالكائنات المنفذة في الفضاء الافتراضي والمحتويات التي ينشئها المستخدم في الوقت الفعلي، وبالتالي فإن الميتافيرس يحتوي على كمية بيانات أكبر بكثير لمعالجتها وتخزينها من أي نظام أساسي آخر، وحينما تقع جريمة في الميتافيرس، فمن المحتمل صعوبة، بل استحالة الجمع والتحقق من جميع البيانات المخزنة على هذا النظام الأساسي؛ بالنظر لأن خوادم مركز بيانات الميتافيرس تستخدم تقنيات أساسية لسلسلة الكتل والحوسبة السحابية الموزعة في بلدان مختلفة، وبالتالي فإنه سيتم توزيع البيانات ذات الصلة عبر عدة خوادم من بلدان مختلفة، ولهذا يكون من الصعب فعليًّا الوصول إلى الخادم وجمع البيانات؛ نظرًا لقيود الوقت والمال، وبسبب المسافات الطويلة التي ينطوي عليها الأمر وإمكانية حدوث مشكلات قانونيَّة بين البلدان؛ لذلك على المحققين جمع الأدلة التي تم إنشاؤها بواسطة منصة الميتافيرس من خلال نظام الإدارة، ولا سيما نظام إدارة البيانات، ومن جانب آخر، على المحققين جمع البيانات المتعلقة بالجرائم فقط بشكل انتقائي عند النظر في الوقت والتكلفة، وقد يكون من الضروري أيضًا طلب البيانات ذات الصلة من نظام الميتافيرس مرة أخرى، بناءً على نتائج تحليل البيانات التي تم جمعها، وهو ما قد يتعين عليه إجراء هذه العملية بشكل متكرر، ومن ثم فإنه عند جمع البيانات على منصة الميتافيرس، فمن المهم تحديد البيانات التي سيتم جمعها من النظام خاصة، ومن الضروري كذلك تزويد النظام بوحدات أو معلومات لاختيار البيانات؛ مثل: موقع أو منطقة معينة من الميتافيرس والمحتوى المحدد والفترة المحددة (Seo et al., 2023:9479)، فلا شك في أن جمع البيانات الخاصة بجرائم الميتافيرس تتطلب من أجهزة إنفاذ القانون العمل على الثلاث نطاقات لجمع الأدلة المتحصلة عن الجرائم المرتكبة في سياق تقنية الميتافيرس.

مرحلة فحص واسترجاع الأدلة الرقميَّة في الميتافيرس

تتضمن مرحلة فحص الأدلة واسترجاعها استخراج وتقييم عناصر البيانات المتعلقة بالجريمة من مجموعة البيانات الخام التي تم جمعها، فقد تكون البيانات التي تم جمعها في شكل لا يمكنه نقل معلومات ذات مغزى بسبب التشفير أو الترميز أو الضغط، كما تتضمن هذه المرحلة أيضًا عملية تحييد تلك التي تعوق تفسير البيانات، ففي مرحلة جمع البيانات، تختلف أنواع البيانات التي يتم جمعها بواسطة المحققين في نطاقات (المستخدم ومقدمي الخدمة ومنصة الميتافيرس)، وذلك وَفق الاعتبارات الخاصة بكل نطاق، فبالنسبة لبيانات نطاق المستخدم، تختلف طريقة تفسير البيانات المجمعة باختلاف نظام التشغيل ونظام الملفات لمصدر البيانات، أما بالنسبة لبيانات نطاق الخدمة، فيمكن أن يختلف نوع البيانات وهيكل الدليل وتنسيق الملف بحسب كيفية تنفيذ المكدس الفني لإطار عمل الخدمة في النظام الأساسي الميتافيرس ونوع التخزين المحلي المقدم، فإذا كان الخادم يستخدم طريقة تشفير أو تنسيق ملف تم تطويره بواسطة المزود بدلًا من حزمة مقدمة من منصة الميتافيرس، فستكون هناك حاجة إلى أداة أو طريقة لتفسير البيانات المجمعة، وعندما تقوم إحدى الخدمات بضغط البيانات أو تشفيرها للحماية أو لزيادة كفاءة التخزين، يلزم البحث لتفسير البيانات، أما بالنسبة للبيانات التي يقدمها المزود في الخدمة باستخدام نوع مستقل من البنية التحتية، فيتم تحديد إجراءات استخراج وتقييم البيانات وفقًا لذلك النوع الذي يوفره المزود، أما بالنسبة لنطاق منصة الميتافيرس، فيتم تحديد إجراءات استخراج البيانات وتقييمها وفقًا لشكل البيانات المقدم، فإذا كان نظام إدارة البيانات يعمل على أساس التنقيب عن البيانات أو الذكاء الاصطناعي، فسيتم تنسيق البيانات المجمعة بشكل أكبر من البيانات التي تم جمعها من نطاق المستخدم (Seo et al., 2023).

مرحلة تحليل البيانات وإعداد التقارير الخاصة بالأدلة الرقميَّة في الميتافيرس

تقوم مرحلة التحليل على تحليل البيانات والأدلة المستخرجة من كل نطاق من النطاقات الثلاثة التي يعمل عليها المحققون في تقنية الميتافيرس، وتستخلص النتائج حول القضية من خلال تجميع النتائج؛ حيث يتم خلال هذه المرحلة الاعتماد على أكثر البيانات والمخرجات التي يجب فحصها في البداية، والتي تتوقف على نوعية الجريمة المرتكبة في الميتافيرس؛ حيث يعتمد تحديد الأولويات وترتيب تحليل البيانات والمخرجات المتحصلة على حدس المحقق وخبرته، فالأدلة التي تم جمعها من مصادر مختلفة في الميتافيرس قد يكون لها معنى في حد ذاتها، ولكن يمكن كذلك إنشاء معانٍ جديدة لها من خلال تحليلات الارتباط بينها وبين غيرها من المخرجات المتحصلة من نطاقات الميتافيرس الأخرى (نطاق المستخدم، نطاق الخدمة)، حيث يمكن للمحقق تحديد سلوك المستخدم في وقت معين من خلال ربط الأدلة المتحصلة من الثلاث نطاقات المختلفة للميتافيرس.

بينما تشير مرحلة إعداد التقارير إلى عملية تقديم وشرح الاستنتاج الذي ينتج عن مرحلة التحليل، ومن الجدير بالذكر أن هناك قلقًا بشأن كيفية تقديم الأدلة في شكل ثلاثي الأبعاد التي تم جمعها في الميتافيرس إلى المحاكم، فحينما يتم عرض البيانات ثلاثية الأبعاد في نموذج ورقي ثنائي الأبعاد يتم تقديمه إلى المحاكم في العالم الحقيقي، فقد يثار تخوف بشأن فقد بعض المعلومات أو تغيير مضمونها (Ebert et al., 2014)، وبخاصة بالنسبة للصور المجزأة ثلاثية الأبعاد أو لقطة واحدة لمشهد تم جمعه في الميتافيرس؛ حيث يمكن أن يصبح معنى المعلومات غامضًا اعتمادًا على الزاوية والمسافة التي تتعرض لها نظارات الواقع الافتراضي والمعزز؛ ولذلك يكون من الضروري دراسة المنهجية والاعتبارات الخاصة المتعلقة بالبيانات ثلاثية الأبعاد قبل أن يتم التعرف عليها كدليل في المحكمة (Seo et al., 2023).

وأخيرًا يواجه القائمون على التحقيقات الجنائيَّة في جرائم الميتافيرس بعض التحديات ذات الصلة التي من أبرزها: موثوقية الأدلة المتحصلة من تقنية الميتافيرس، ومقدار ومدى جودة البيانات الرئيسة التي تم جمعها، ففي نطاق منصة الميتافيرس، يجب جمع البيانات الضخمة والموزعة من الميتافيرس بشكل انتقائي مع مراعاة عنصر الوقت وكفاءة التكلفة، ونظرًا لأن جمع البيانات الانتقائي يعتمد على نظام إدارة البيانات لمنصة الميتافيرس، فقد تكون جميع إجراءات جمع البيانات غير شفافة، لذلك يجب -عند تقديم الأدلة في المحكمة- إثبات ملاءمة عملية جمع البيانات الانتقائية على منصة الميتافيرس، فضلًا عن وجود بعض المناقشات حول مدى موثوقية النتائج في تقنية الميتافيرس عندما يتم جمع البيانات بشكل انتقائي باستخدام تقنيات؛ مثل: التعلم الآلي والذكاء الاصطناعي.

فضلًا عن تقيد المحققين -في مرحلة جمع المعلومات من الميتافيرس- فيما يتعلق بوصولهم المباشر إلى مصادر البيانات بمدى تعاون الشركات المالكة للبيانات والمعلومات داخل منصة الميتافيرس؛ نظرًا لأن هذه الشركات قد تتحفظ على التعاون مع سلطات التحقيق وتقديم البيانات المطلوبة منها، ما لم تكن الشركة متورطة بشكل مباشر في القضية؛ وذلك لعدم وجود التزام قانوني عليها بالتعاون مع سلطات التحقيق والمحاكمة، وبالتالي لا يمكن جمع البيانات على منصة الميتافيرس إلا بالتعاون مع الشركة التي تمتلك البيانات، وينطبق الأمر ذاته على شركات الطرف الثالث من مقدمي الخدمة بالميتافيرس، إذا ما

قامت بتخزين البيانات خارج منصة الميتافيرس، مع الوضع في الاعتبار التزام هذه الشركات بمراعاة حقوق المشتركين في الخصوصية، ومن ثم امتناعها عن إفشاء أية بيانات تخصهم، حتى ولو كانت متصلة بتحقيقات أو محاكمات قائمة، ونذكر على سبيل المثال في عام 2016، رفض شركة أبل التعاون مع مكتب التحقيقات الفيدرالي عندما تم مطالبتها بتحليل بيانات الأيفون لإرهابي ميت بسبب مراعاتها لاعتبارات خصوصية المستخدم (Seo et al., 2023:9481).

أضف إلى ذلك تقلب وتغير حالة البيانات التي يتم إنشاؤها في الميتافيرس بشكل أكثر من البيانات المسجلة في العالم الحقيقي، فضلًا عن استحالة تسجيل جميع البيانات التي تحدث على الميتافيرس؛ كحركات جميع الصور الرمزية، بالإضافة إلى أن البيانات المتدفقة في الوقت الفعلي مثل: مؤتمرات الفيديو والمحادثات الصوتية كلها تكون متطايرة إذا لم يتم تسجيلها من جانب المستخدم، كما أنه ليس من السهل تطوير تقنية لمراقبة عشرات الآلاف من التيرا بايت من البيانات التي تم إنشاؤها في أجزاء من الألف من الثانية في تقنية الميتافيرس، ومن ثم إذا كان الميتافيرس لا يقوم بتشغيل نظام تسجيل منفصل أو مركز بيانات جنائي للاستجابات للحوادث، فيجب استخدام موارد الحوسبة الخاصة بنموذج الميتافيرس للتحقيق في الحوادث أو المشكلات.

كما يلزم توفير معلومات حول العملية التشغيلية للنظام المطور من أجل تطوير أداة تحليل مخصصة، فإذا لم تنشر الشركة المصنعة الوثائق الرسمية لنظام الملفات، فيجب على المحققين إجراء هندسة عكسية ضد النظام الثنائي لنظام التشغيل؛ الأمر الذي يتطلب الكثير من الوقت والجهد، ومن ناحية أخرى، إذا لم يكتمل تطوير تقنية التحليل، فلن يتمكن المحلل من جمع أو تحليل البيانات من جهاز الإدخال أو الإخراج.

هذا إلى جانب مسألة حماية الخصوصية للمستخدمين في الميتافيرس، ومدى إمكان السماح للمحققين بالوصول إلى المعلومات والأدلة المسجلة على الشاشات المحمولة على رأس المستخدم، بالإضافة إلى متابعة حركة المكونات الأخرى على الميتافيرس؛ حيث تؤدي الخلفيات دورًا مهمًّا في عملية التحقيق الجنائي، والتي غالبًا ما تتضمن معلومات غير مقصودة، مثل: حركات الأفاتارات الأخرى، والعلامات، والمناطق المحيطة، ومسرح الجريمة، كما أن المستخدم قد يقوم بكشف بعض المعلومات الشخصية الحساسة من خلال شاشة الخلفية كذلك، ويمكن ملاحظة إيماءات المستخدم وأنماط حركة الرأس، أو العينين من خلال الصورة الرمزية، كما يمكن استخدام هذه المعلومات لتتبع هوية المستخدم الفعلية خارج الميتافيرس من خلال تتبع العين في Avatar والتعرف على نمط الإيماءات باستخدام القياسات الحيوية (Pfeuffer et al., 2019) مثل: بصمات الأصابع وقزحية المستخدم، كما تؤدي تقنيات الحفاظ على الخصوصية الجديدة كاستنساخ الصورة الرمزية، والإغلاق، والتمويه، والنقل الفوري، والإخفاء إلى قيام المحققين في بعض الأحيان باتخاذ قرارات غير صحيحة، أو التسبب في حدوث ارتباك أثناء عملية التحليل (Falchuk et al., 2018).

مشروعية الدليل الرقمي

يستلزم الدليل الرقمي أن تكون وسيلة الحصول عليه مشروعة، بأن تكون إجراءات الحصول عليه قد تمت وفق القانون (نجيب، 2014، ص. 56)، وأن يكون التوصل إليه قد تم عن طريق إرادة حرة دون أي اعتداء على إرادة المتهم، أو إرادة الغير؛ كاستخدام العنف مع المشتبه به من أجل فك شفرة نظام معلوماتي، أو الوصول إلى دائرة حل التشفير، أو الوصول إلى ملفات البيانات المخزنة (نجيب، 2014، ص. 56)، ومن الجدير بالذكر أن الفقه والقضاء الجنائي يتوسعان في تحديد نطاق مشروعية الدليل الرقمي، بحيث لا تقتصر مشروعية إجراءات الحصول عليه على مجرد اتباع القواعد القانونيَّة المقررة، وإنما يجب أن تتفق كذلك مع القواعد الثابتة في وجدان المجتمع (منشاوي، 2012، ص. 552)، ومن القضاء المقارن، موقف محكمة النقض البلجيكية التي قضت بأن: «وصف الفعل غير المشروع لا يقتصر فقط على الفعل الذي يحظره القانون صراحةً، بل يشمل كل فعل يتعارض مع القواعد الجوهرية للإجراءات الجنائيَّة، أو المبادئ القانونيَّة» (الصغير، 2002، ص. 110).

مقبولية الدليل الرقمي أمام القضاء الجنائي

اتجه القضاء الجنائي في بعض الدول إلى وضع بعض القواعد أو المعايير لتقدير مدى قبول الأدلة الرقميَّة والتأكد من موثوقيتها، وبحث مدى إمكانية الارتكان إليها في الإجراءات القضائية، وتتبلور أبرز القواعد لتقرير مقبولية الدليل الرقمي أمام القضاء الجنائي في ضرورة تيقن المحكمة من سلامة الدليل الرقمي وصحته، وعدم تعرضه لأي محاولة للعبث به، ومن ثم يقع على عاتق سلطة الاتهام إثبات أن هذا الدليل بداءةً قد تم الحصول عليه بطريق مشروع، وإثبات ما يسمى باستمرارية الدليل؛ أي إن حالة المعلومات الرقميَّة كدليل لم يطرأ عليها أي تعديل أو تغيير يشكك في مصداقيتها في كشف وقائع الجريمة طوال فترة الإجراءات القضائية منذ تاريخ التحفظ عليه حتى صدور حكم في الدعوى.

ويجب على القائمين على جمع الأدلة الرقميَّة من مسرح الجريمة اتخاذ الإجراءات اللازمة للحفاظ على سلامة الدليل الرقمي، بدءًا من

لحظة إنشائه ووصولًا لمرحلة تقديمه أمام المحكمة، وهو ما يعرف باستمرارية الدليل وثبات حالته وعدم تعرضه للتعديل أو التحريف أو العبث به؛ حيث يجب عليهم الحفاظ على استمرارية الأدلة على كل من الأجهزة المادية التي تحتوي على البيانات (عند تلقيها أو الاستيلاء عليها)، والبيانات المخزنة الموجودة على الأجهزة (وزارة العدل الأمريكية، معهد العدالة الوطني، 2007، ص. 16).

ويجب على سلطة التحقيق أن تعرض على المحكمة الإجراءات المطبقة للحفاظ على سلامة الدليل الرقمي، وتبيان الآلية المطبقة لحفظ الدليل وتوثيق التاريخ الزمني له، وأنه لم يطرأ عليه أي تغيير، ولم يتم العبث به، فيجب على النيابة العامة أن تعرض على المحكمة أن المعلومات الرقميَّة التي تم الحصول عليها من الجهاز هي بمثابة تمثيل حقيقي وسليم للبيانات الأصلية التي يتضمنها الجهاز (الصحة)، وأن الجهاز والبيانات المراد تقديمها كأدلة هي ذاتها التي تم اكتشافها في الأصل، وتم حفظها وتوثيق التاريخ الزمني لها (السلامة)، لما في ذلك من تأثير مباشر على المحكمة في ترجيح فكرة موثوقية الدليل الرقمي وجدارته بالثقة من جانبها (Marcella, J. et al., :2002:136)، ومن ثم مقبوليته أمام القضاء الجنائي، وللمحكمة في تحقيقها للدعوى بالجلسة سماع الشهود والخبراء ممن قاموا بجمع واستخلاص الأدلة الرقميَّة ومناقشتهم فيما أثبتوه بتقاريرهم للتثبت من صحتها وسلامتها، وأن الوصول إليها قد تم بطريق مشروع.

استعرضت الدراسة موضوع الدليل الجنائي الرقمي في عصر الميتافيرس من خلال مطلبين، تناولا ماهية تقنية الميتافيرس وإجراءات جمع واستخلاص الأدلة المتحصلة عن الجرائم التي ترتكب بداخلها، وقد تمخض البحث عن مجموعة من النتائج والتوصيات؛ وذلك على النحو التالي:

5. النتائج:

- ظهور تقنية الميتافيرس كعالم افتراضي موازٍ للعالم الحقيقي وسط تكهنات بإمكان إساءة استخدامها في ارتكاب المزيد من الجرائم السيبرانية، وانتهاك خصوصية المستخدمين في ظل عدم وصولها إلى الحالة المثالية لتشغيلها.
- عدم وجود نصوص قانونيَّة تنظم استخدام هذه التقنية، وتواجه صور الجرائم السيبرانية المستحدثة المرتكبة خلالها وعجز النصوص القانونيَّة القائمة عن مواجهتها.
- اهتمام العديد من الدول بتقنية الميتافيرس واتجاه بعضها إلى تبني تجاربها الافتراضية الخاصة بشأن تطبيق هذه التقنية.
- هناك توقعات بالتوسع في استخدام تقنية الميتافيرس في المستقبل القريب في المجالات الاقتصادية والتجارية بشكل كبير.
- وجود صعوبات تخص عملية جمع الأدلة المتحصلة من جرائم الميتافيرس بالنظر إلى طبيعتها الخاصة والكم الهائل من البيانات الناجمة عن استخدام هذه التقنية، وهو ما يستتبع جمع الأدلة من أكثر من نطاق؛ كنطاق المستخدم ومقدمي الخدمات ومنصة الميتافيرس ذاتها.
- نجاح جهات إنفاذ القانون في جمع الأدلة الرقميَّة حول جرائم الميتافيرس يتوقف على مدى تعاون الشركات الخاصة من مقدمي الخدمات ومشغلي منصة الميتافيرس، بما يضمن للمحققين النفاذ إلى البيانات المطلوبة لاستكمال التحقيقات.
- وجود بعض الصعوبات في عرض الأدلة المتحصلة من الميتافيرس أمام المحاكم العادية بالنظر إلى طابع هذه الأدلة الثلاثي الأبعاد.
- هناك احتمالية أن نجد في الفقه في المستقبل من ينادي بمنح الشخصية القانونيَّة المحدودة لكيانات الميتافيرس من الأفاتار للتعاطي مع التطورات المستقبلية لاستخدام هذه التقنية.

6. التوصيات:

- دعوة الدول إلى وضع إستراتيجيات تنظم استخدام تقنية الميتافيرس، وتحدد طرق التعامل معها والمجالات التي يجب أن يتم إنشاء الميتافيرس فيها من أجل تطويرها، والمجالات المحظورة فيها، وبما يضمن صياغة نمط من العلاقة المباشرة مع الشركات المطورة لتعزيز الدور الرقابي للدولة على مواطنيها داخل الميتافيرس من دون أن ينتقص ذلك من حقوقهم وحرياتهم الرقميَّة.
- تضافر الجهود الدوليَّة لتعديل الاتفاقيات الدوليَّة الخاصة بالجرائم السيبرانية، أو التطلع لوضع اتفاقية دولية جديدة تنظم مسئولية مقدمي خدمات الميتافيرس وتلزمهم بالتعاون في مكافحة الجرائم وتبادل الأدلة والمعلومات.
- إجراء التعديلات المناسبة لقوانين مكافحة جرائم تقنية المعلومات، بما يستوعب جرائم الميتافيرس وتحقيق مواجهة فعَّالة في مواجهة الجرائم السيبرانية المرتكبة داخل تقنية الميتافيرس.
- تعزيز التعاون الدولي القضائي والأمني، وتسهيل عمليات تبادل المعلومات بين الدول بهدف الحد من صور جرائم الميتافيرس وبخاصة في الدول التي بها خوادم تشغيل هذه التقنية المستحدثة.

الإفصاح عن تضارب المصالح

يعلن المؤلف أنه ليس لديه أي تضارب في المصالح للمقالة المنشورة.

الإفصاح عن تمويل البحث

يعلن (المؤلف) أن البحث المنشور لم يتلقَ منحة مالية من أية جهة تمويل في القطاعات العامة أو التجارية أو المؤسسات غير الربحية.

المصادر والمراجع

المراجع العربية

إبراهيم، خالد. (2020). الإثبات الإلكتروني في المواد الجنائيَّة والمدنية دار الفكر الجامعي، الإسكندرية.

الأوجلي، سالم. (2016). مقبوليَّة الدليل الرقمي في المحاكم الجنائيَّة، مجلة دراسات قانونيَّة، جامعة بني غازي، ليبيا، العدد 19، يناير 2016.

جبريل، محمد. (2023). التحديات القانونيَّة لتقنية ميتافيرس من الوجهة الجنائيَّة (دار الأهرام للإصدارات القانونيَّة، القاهرة).

حجازي، محمد. (2022). الميتافيرس والقانون (مجلة الأمن العام، القاهرة)، مقال منشور بالعدد 256، أكتوبر 2022.

الحسيني، أحمد. (2013). الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية (جامعة عين شمس، القاهرة)، رسالة دكتوراه.

خليفة، إيهاب. (2022). الميتافيرس مستقبل العمران البشري في عالم ما بعد الإنترنت (مركز المستقبل للأبحاث والدراسات المتقدمة، أبو ظبي)، سلسلة دراسات، العدد 17، نوفمبر 2022.

سرور، أحمد. (1996). الوسيط في قانون الإجراءات الجنائيَّة (دار النهضة العربيَّة، القاهرة).

سلامة، مأمون. (1996). الإجراءات الجنائيَّة في التشريع المصري، ج2 (دار النهضة العربيَّة، القاهرة).

الصغير، جميل. (1999). الجوانب الإجرائية للجرائم المتعلقة بالإنترنت (دار النهضة العربيَّة، القاهرة).

الصغير، جميل. (2002). أدلة الإثبات الجنائي والتكنولوجيا الحديثة (دار النهضة العربيَّة، القاهرة).

عبد المطلب، ممدوح. (2003). استخدام بروتوكول TCP IP في بحث وتحقيق الجرائم على الكمبيوتر (مركز البحوث والدراسات بأكاديمية شرطة دبي).

فرغلي، عبد الناصر. (2007). الإثبات الجنائي بالأدلة الرقميَّة من الناحيتين القانونيَّة والفنية: دراسة تطبيقية مقارنة (جامعة نايف العربيَّة للعلوم الأمنية).

مركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء المصري (2022): (اتجاهات العالم- تقنية الميتافيرس، القاهرة).

المري، بهاء. (2022). جرائم السوشيال ميديا (دار الأهرام للإصدارات القانونيَّة، القاهرة).

مكتب الأمم المتحدة المعني بالمخدرات والجريمة. (2013). دراسة حول الجريمة السيبرانية (منظمة الأمم المتحدة، نيويورك).

منشاوي، محمد. (2012). سلطة القاضي الجنائي في تقدير الدليل الإلكتروني (جامعة الكويت، الكويت) مجلة الحقوق، المجلد 36، العدد 2، يونيو 2012.

نجيب، هند. (2014). حجية الدليل الإلكتروني (المركز القومي للبحوث الاجتماعية والجنائيَّة، القاهرة)، المجلة الجنائيَّة القومية، المجلد 57، العدد الأول، مارس 2014.

وزارة العدل الأمريكية. (2007). الأدلة الرقميَّة الموجودة في حجرة المحكمة، دليل عمل لإنفاذ القانون والمدعين العامين، معهد العدالة الوطني.

يونس، عمر. (2004). الجرائم الناشئة عن استخدام الإنترنت (جامعة عين شمس، القاهرة)، رسالة دكتوراه.

يونس، عمر . (2006). مذكرات في الإثبات الجنائي عبر الإنترنت (جامعة الدول العربيَّة، القاهرة)، ندوة الدليل الرقمي التي نظمتها جامعة الدول العربيَّة، القاهرة، خلال الفترة (5-8 مارس 2006).

المراجع الأجنبية

Ebert LC, Nguyen TT, Breitbeck R, Braun M, Thali MJ, Ross S (2014) The forensic holodeck: an immersive display for forensic crime scene reconstructions. Forensic Sci Med Pathol 10(4):623-626.

Laue, C. (2011): Crime potential of metaverses, In book: K.Cornelius and D. Hermann (eds.), Virtual Worlds and Criminality, Springer-Verlag Berlin Heidelberg 2011, DOI: 10.1007/978-3-642-20823-2_2, pp 19-29.

Lodder, A.R. (2011): Conflict resolution in virtual worlds: general characteristics and the 2009 dutch convictions on virtual theft, pp 79-93.

Marcella, J., A., & Greenfield, R.S. (Eds.). (2002). Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes (1st ed.). Auerbach Publications. New York, https://doi.org/10.1201/9781420000115

Meiklejohn S. & others (2013): A fistful of bitcoins: characterizing payments among men with no

Quéméner, M. (2014): Les spécificités juridiques de la prevue numérique, Actualite Juridique Pénal (AJ Pénal "1"), Dalloz.

Seo, S., Seok, B. & Lee, C. (2023): Digital forensic investigation framework for the metaverse. J Supercomput 79, 9467-9485. https://doi.org/10.1007/s11227-023-05045-1.

Falchuk B, Loeb S, Neff R (2018) The social metaverse: battle for privacy. IEEE Technol Soc Mag 37(2):52–61.

names, in Proceedings of the 2013 ACM SIGCOMM conference on Internet measurement conference (New York, ACM, 2013).

Pfeuffer K, Geiger MJ, Prange S, Mecke L, Buschek D, Alt F (2019) Behavioural biometrics in vr: identifying people from body motion and relations in virtual reality. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow, Scotland Uk, pp 1–12.