د. أميرة عبد العظيم محمد عبد الجواد
أستاذ القانون الدولي العام المساعد بجامعة الأزهر – الأستاذ المشارك بكليات الشرق العربي

إشكاليات إنفاذ القانون الدولي في عالم الميتافيرس

المراسلة: د. أميرة عبد العظيم محمد عبد الجواد
أستاذ القانون الدولي العام المساعد، جامعة الأزهر، مصر

معرف الوثيقة الرقمي (DOI): https://doi.org/10.54873/jolets.v3i2.161

البريد الإلكتروني: dr.amiraadny360@gmail.com

نسق توثيق البحث:
أميرة عبد العظيم محمد عبد الجواد، إشكاليات إنفاذ القانون الدولي في عالم الميتافيرس، بحث مقدم إلى المؤتمر العلمي الدولي الثالث: الجوانب القانونية للتحول الرقمي «الفرص والتحديات»، كلية القانون بالجامعة البريطانية، الفترة من ١٧–١٨ يونيو ٢٠٢٣، مجلة القانون والتكنولوجيا، المجلد ٣، العدد ٢، أكتوبر ٢٠٢٣، صفحات ١٦٣ – ٢٣٠

إشكاليات إنفاذ القانون الدولي في عالم الميتافيرس

د. أميرة عبد العظيم محمد عبد الجواد

الملخص:

ظهرت تقنية الميتافيرس في إعلان لرئيس شركة «ميتا»، كثورة تكنولوجية، تندمج فيها الحياة الواقعية مع واقع افتراضي وواقع معزز، كما ظهر معها تخوفٌ من سلبياتها على البشر. وتهدف هذه الدراسة إلى إلقاء الضوء على تقنية الميتافيرس بوصفها إحدى نتائج الذكاء الاصطناعي والثورة العلمية، مما يستلزم البحث عن سبل ووسائل المواجهة القانونية للإشكاليات التي تثيرها تقنية الميتافيرس، واستشراف نص قانوني دولي مناسب يحكم المستجدات التي تصاحب الجرائم المرتكبة عبر تقنية الميتافيرس، وتطبيقه على النزاعات التي تنشأ عبر هذه التقنية. ولعل أبرز هذه الإشكالات يتمثل في تحديد مدى انطباق قواعد القانون الدولي العام على تقنية الميتافيرس وهل تعد كافية أم لابد من تحرك المجتمع الدولي بوضع تشريعات دولية جديدة لتنظيم ومواجهة ما ينشأ عن تلك التقنية.

الكلمات الرئيسية: الميتافيرس، الواقع الافتراضي، إنفاذ القانون الدولي، إشكاليات الميتافيرس.

Challenges of Implementing the International Law in the Metaverse World

Amira Abdel Azim Mohamed Abdel Gawad

Associate Professor of Public International Law, Al-Azhar University, Arab East Colleges

Abstract:

The metaverse appeared in an advertisement by the president of Meta as a technological revolution, integrating real life with a virtual and enhanced reality, as well as a fear of its negative effects on humans. The aim of this study is to shed light on metaverse technology as a result of artificial intelligence and the scientific revolution, making it necessary to investigate ways and means of legally addressing the problems posed by metaverse technology and to identify an appropriate international legal text governing developments associated with metaverse crimes and its application to conflicts arising through this technology. The most notable problem is whether the rules of public international law apply to the metaverse and whether they are sufficient or whether the international community should act with new international legislation to regulate and address the resulting technology.

Keywords: Metaverse, Virtual reality, Enforcement of International Law, Metaverse problems

المقدمة:

يشهد العالم – حاليًا– ثورة كبيرة في تقنية المعلومات والاتصالات، ففي نهاية شهر أكتوبر ٢٠٢١ أعلن مارك زوكربيرج عن تغيير اسم شركته من «فيسبوك Facebook» إلى «ميتا Meta» وعن انطلاق مشروع العالم الافتراضي «الميتافيرس Metaverse» ، فهو بمثابة ثورة تكنولوجية تنقل العالم إلى آفاق جديدة وغير تقليدية عبر حياة افتراضية رقمية موازية.

ومن ثَمَّ يعتبر هذا الموضوع – بلا شك – من أهم الموضوعات التي تثير كثيرًا من الجدل في عصرنا الحالي؛ وذلك نظرًا للغموض الذي مازال يكتنف هذه التقنية؛ لذلك فإن أهمية السيطرة على مضمون الميتافيرس لا يقتصر على الجانب القانوني فقط، بل يمتد إلى مختلف جوانب الحياة الاقتصادية أو الاجتماعية أو السياسية.

وتعد تقنية الميتافيرس مساحة افتراضية تسمح للمستخدم بالتواصل والتفاعل مع غيره من المستخدمين، ويقوم عمل الجهة التي تتولى تشغيل التقنية على إدارة النشاط المعلوماتي وتوفير حيز خاص لكل مستخدم على حواسيبهم الآلية المرتبطة بشكل دائم بشبكة الإنترنت؛ ليستطيع من خلالها الاتصال والتواصل مع الآخرين. وستكون هذه الحياة افتراضية بصورة كلية، وهذا ما يخطط له مارك زوكربيرج المؤسس والرئيس التنفيذي لموقع فيس بوك، والذي من شأنه تغيير مستقبل البشرية بصورة مذهلة؛ كما يزعم مارك زوكربيرج نفسه.

ولا شك أن استخدام تقنية الميتافيرس ليس بالأمر المستغرب في عصرنا الحالي بعدما أصبحت وسائل التواصل الإلكترونية الوسيلة الأساسية للتواصل بين الأشخاص، وأصبحت المجتمعات البشرية أمام مرحلة جديدة من مراحل العلاقات الاجتماعية في الاتصال والتواصل بين أفراد المجتمع.

وتتيح تقنية الميتافيرس لمستخدم هذا العالم الافتراضي ثلاثي الأبعاد إجراء بعض العمليات مثل التسوق ومقابلة الأشخاص والألعاب وإنشاء العوالم الخاصة، وغيرها الكثير في هذا العالم، دون أن يتحرك من مكانه، وسوف تتوافر هذه الوظائف قريبًا مع

توفير مستلزمات الواقع الافتراضي المتطلبة لذلك، وأهمها البدلة والنظارة الخاصتين بهذه التقنية، ويقودنا ذلك إلى أن لتقنية الميتافيرس جوانب إيجابية وأخرى سلبية، ومن الجوانب الإيجابية ما تتيحه هذه التقنية من تطور مذهل في وسائل التواصل وسبل التعامل بين الأفراد والجماعات(١).

ومع ذلك فهناك مخاطر عدة لتقنيات الميتافيرس، فهي تفتح المجال واسعًا للدخول في عالم ثلاثي الأبعاد عبر تقنيات الواقع الافتراضي بأجهزة استشعار في عالم مظلم، فيفتح الباب إلى عالم الجريمة بصورة مخيفة، حيث يعيش البشر في عصر آخر وهمي وفي مكان آخر، ويتيح لعصابات الإنترنت ارتكاب العديد من الجرائم الإلكترونية المستحدثة. كما أن تقنية الميتافيرس ستتسبب في انتهاك خصوصية المستخدمين، وبدء حقبة جديدة من إقامة عالم افتراضي مواز للعالم الواقعي، تنقل الفرد من مجرد مستخدم للإنترنت إلى جزء منه ومشارك فيه(٢).

كما يجب ألا تظل الفجوة واسعة بين النظم القانونية وبين تقنية الميتافيرس، فلا بد من وجود مواجهة قانونية فورية؛ لمعالجة المخاطر التي تسببها هذه التقنية وما تحدثه من انتهاكات، كما يلزم الاستعداد التشريعي الجاد لما سيخلقه هذا العالم الافتراضي من أرضية خصبة لارتكاب الجرائم بصورة سهلة، بما يجعل الإمساك بالمجرم أمرًا صعبًا.

ولذا يعد هذا البحث استشرافًا لنهج القانون الدولي في تعامله واستخدامه لتلك التقنية الرقمية الافتراضية، ولاستغلال أفضل لمزاياها، وتسليط الضوء على الإشكاليات التي يمكن أن تثيرها؛ من أجل درئها والتقليل من تبعاتها.

الهدف من الدراسة:

تهدف هذه الدراسة إلى إلقاء الضوء على تقنية الميتافيرس بوصفها إحدى نتائج الذكاء الاصطناعي والثورة العلمية، وما هي سبل وسائل المواجهة القانونية التطبيقية للإشكاليات التي تثيرها تقنية الميتافيرس، واستشراف نص قانوني دولي مناسب

(١) انظر: المستشار الدكتور/ محمد جبريل إبراهيم، الميتافيرس والقانون الجنائي، دار النهضة العربية ، ط١، ٢٠٢٣، ص ٩.

(٢) انظر: د/ شريف يوسف خاطر، حماية الحق في الخصوصية المعلوماتية، دار الفكر والقانون المنصورة بمصر، ٢٠١٥، ص ٣٠.

يحكم المستجدات التي تصاحب الجرائم المرتكبة عبر تقنية الميتافيرس، وتطبيقه على النزاعات التي تنشأ عبر هذه التقنية.

أهمية الدراسة:

تستهدف هذه الدراسة رصد وتحليل إشكاليات استخدام تقنية الميتافيرس، بعدما أصبحت وسائل التواصل الاجتماعي وسيلة أساسية لتواصل أفراد المجتمع بعضهم مع بعض، فحلت محل الوسائل التقليدية، وأصبح من غير الممكن الاستغناء عنها، خصوصًا في ظل ما يشهده العالم من تطور تكنولوجي، فانتقلت التفاعلات والسلوكيات البشرية – من خلالها – من تفاعلات وسلوكيات مادية إلى افتراضية. وبما أن هذا الانتقال انطوى على كل مظاهر السلوك الإنساني (الإيجابية منها والسلبية)، فإن المحتوى الذي تتضمنه وسائل التواصل – ومنها تقنية الميتافيرس – قد يكون في حالات كثيرة غير متناسب مع القواعد الأخلاقية والاجتماعية التي يضعها المجتمع لنفسه، أو قد يكون غير متناسب مع أهواء فئة معينة من أفراد المجتمع، مما يطرح إشكالات تتعلق بمدى مشروعية المحتوى الذي يُبث عبرها[1].

لذا تتمثل الأهمية العملية لهذه الدراسة في تحديد مدى مشروعية الممارسات المرتقبة داخل تقنية الميتافيرس، وفي ضرورة توفير رد الفعل القانوني الدولي المواجه له، لكن نظرًا لأن شبكة الإنترنت تحتوى على تقنيات تمكّن صاحب المحتوى من إخفاء نفسه، بالإضافة إلى سرعة انتشار المعلومات التي تحتوي عليها، فقد وجهت الأنظار إلى المنصات التي تمتلك السيطرة على المعلومات التي تحتوي عليها، لاتخاذ إجراء بشأن هذا المحتوى.

والذي ينبغي العمل عليه أن تلاحق التشريعات المستجدات المتلاحقة والمتسارعة، ويسبق الفقه التشريع في ذلك الأمر، حيث يترقب الفقهاء الاكتشافات التكنولوجية الحديثة في محاولة لوضع حلول حاسمة للإشكاليات القانونية الناجمة عن هذه المستجدات، فيسترشد بها المشرع.

(١) انظر: د/ ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، ٢٠١٢، ص ٣٣.

وإذا كانت تقنية ميتافيرس – كما أوضح مارك زوكربيرج – تتيح للفرد أعلى مستوى من الحرية والرفاهية، فإن هذه الحرية يجب ألا تكون على حساب الاعتداء على حقوق الآخرين، وانتهاك خصوصياتهم وحرياتهم، ومن هنا تأتي أهمية الدراسة في أنها تعد محاولة لوضع الأطر التشريعية الدولية التي توفق بين هذين الاعتبارين المتناقضين[1].

مـن ثَمَّ تأتـي أهمية الدراسـة في أنها تتعلـق بالجانب القانـوني التطبيقي لمواجهة الميتافيرس، فالتشريعات القانونية ما زالت في موقف المتأهب لهذه التقنية، ولم يصدر حتـى الآن أي قانون يتنـاول هذه التقنية، ومن ثَـمَّ فالأنظار تتجـه إلى تطورات الوضع القانوني بشأن هذه التقنية.

إشكالية الدراسة:

إن الإشكاليـات التي يثيرها أي تطبيق أو تقنية إلكترونية حديثة هي كيفية الحد من السلوكيـات غير القانونية، من خلال تتبع التطبيقـات أو التقنيات لمراقبتها، وإذا كانت تشـكل خروجًا عن القانون، أو النظام العام، وذلـك بوضع تشريعات تنظم التعامل من خلال هذه التطبيقات والتقنيات وتحظر أو تمنع القيام بها من طرف مستخدمي وسائل التواصل الاجتماعي.

ومـن ثَمَّ تثير تقنية الميتافيرس العديد من الإشكاليـات: كيف يتم مواجهة الجرائم التـي يمكن أن تتم من خلال تلك التقنية، وكيـف يتم إثباتها، وكيف يحدث التعاون بين الـدول مع وجود الأنظمة القانونية المختلفة، واختلافهـم أيضًا في المعالجة التشريعية، وكذلـك كيـف يتم حفظ قواعـد البيانات داخل تقنيـة الميتافيرس، ومـن هنا لا بد من تحرك الدول لمعالجة الإشكاليات التي تنتج عن تقنية الميتافيرس.

والسـؤال الـذي يطـرح نفسه: هل الاتفاقيـات الدوليـة القائمة والمعمـول بها تكفي لمواجهـة الاعتداءات من قِبـل مستخدمي تقنية الميتافيرس، أم أنـه يتعين على المجتمع الدولي أن يكون على أهبة الاستعداد لمواجهة هذه الاعتداءات باتفاقيات دولية جديدة.

---

(١) انظـر: د/ أحمـد إبراهيم محمد إبراهيم: المسئولية الجنائية الناتجة عن أخطاء الـذكاء الاصطناعي في التشريع الإماراتي دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس، ٢٠٢٠ ، ص ٧.

والسبب في تفاقم الإشكالية أن محل الاعتداء إلى الآن غير واضح، سواء من حيث دلالته أو مفهومه، وإذا كان الاعتداء يتمثل في « تسلل الأفاتار إلى المواقع التي يمتلكها الأشخاص أو الهيئات على الشبكة العالمية للمعلومات، وإلحاق الضرر بهذه المعلومات أو سرقتها أو إتلافها بنشر الفيروسات، فإن هذا الاعتداء- وما نتج عنه من آثار تشمل في انتهاك للسرية المتمثلة في المعلومات وغصب لمكان افتراضي على الشبكة العالمية للمعلومات - يعد جريمة من الجرائم المعاصرة.

منهج الدراسة:

اتخذت الدراسة المنهج الوصفي التحليلي، الذي يقوم على أساس تحديد مفهوم تقنية ميتافيرس وخصائصها، وتحليل مزاياها وعيوبها، والإشكاليات التي يمكن أن تثار عبر تقنية ميتافيرس؛ بغية الوقوف على النص القانوني الدولي المناسب الذي يمكن أن يحكم هذه المستجدات، وتكوين نهج كامل عن هذه التقنية، ووضع إطار قانوني لها، بالإضافة إلى الاعتماد على المنهج المقارن في دراسة التشريعات التي نظمت مسؤولية منصات التواصل الاجتماعي عن المحتوى غير المشروع.

خطة الدراسة:

يتطلب تحقيق أهداف هذا البحث: بيان ماهية تقنية الميتافيرس، والنظر في العديد من الإشكاليات التي يمكن أن تثيرها تقنية الميتافيرس؛ فضلاً عن الآليات الدولية لمواجهة الجرائم الإلكترونية المرتكبة عبر تقنية الميتافيرس، **وفي ضوء ذلك يقسم البحث على النحو التالي:**

- **المطلب التمهيدي: ماهية تقنية الميتافيرس:**
- **الفرع الأول:** مفهوم تقنية الميتافيرس.
- **الفرع الثاني:** خصائص تقنية الميتافيرس.
- **الفرع الثالث:** طبيعة المحل الإلكتروني داخل تقنية الميتافيرس.

- **المبحث الأول: تحديد الإشكاليات القانونية لإنفاذ القانون الدولي على تقنية الميتافيرس:**
  - **المطلب الأول:** إشكالية حماية خصوصية البيانات داخل تقنية الميتافيرس.
  - **المطلب الثاني:** إشكالية مكافحة الجرائم الإلكترونية عبر تقنية الميتافيرس.
- **المبحث الثاني: الآليات الدولية لمواجهة الجرائم الإلكترونية المرتكبة عبر تقنية الميتافيرس:**
  - **المطلب الأول:** الصعوبات التي تواجه المنظومة القضائية إزاء الجرائم الإلكترونية.
  - **المطلب الثاني:** المعالجة التشريعية للجرائم الإلكترونية المرتكبة عبر تقنية الميتافيرس.
  - **المطلب الثالث:** تعزيز التعاون الدولي في ضوء اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.

وذلك على النحو التالي:

المطلب التمهيدي

ماهية تقنية الميتافيرس

تمهيد وتقسيم:

تعد تقنية الميتافيرس وسيطًا إلكترونيًا غير مادي، يتمثل في تطبيق يستخدم شبكة الإنترنت لإيجاد عالم افتراضي، يتواصل من خلاله المستخدمون بشكل غير مادي، عبر ما يقومون بإنشائه ومشاركته من مواد إلكترونية، ويدار هذا العالم الافتراضي بواسطة شركات تجارية في أغلبها؛ لذا ينبغي عدم الخلط بين «الخدمة» أو «المنصة»، وبين «الجهة المقدمة لتلك الخدمة»، فموقع فيسبوك دوت كوم Facebook.com ، أو تطبيق فيسبوك Facebook ، على سبيل المثال، يُمثل الخدمة المقدمة أو المنصة، بينما شركة فيسبوك تحولت مؤخرًا إلى شركة ميتا Meta [(١)].

إذن فمنصات التواصل الاجتماعي تتمثل في الوسائل التي تضعها الجهة المقدمة للخدمات رهن إشارة المستخدمين، ومما لا شك فيه أنّ تحديد ماهيتها يعد الخطوة الأهم نحو فهم طبيعتها القانونية، ومسألةً أوليةً مهمة لتحديد الإطار القانوني الذي ينظمها[(٢)].

لهذا سنتناول – في هذا المطلب– مفهوم تقنية الميتافيرس، وخصائص تقنية الميتافيرس، وطبيعة المحل الإلكتروني داخل تقنية الميتافيرس.

وتستلزم الدراسة في هذا المطلب تناوله وفقًا للتقسيم الآتى:

(١) انظر: أ/ زياد عبد التواب، ما وراء الميتافيرس: ذلك المجهول القادم، مجلة الديمقراطية، مؤسسة الأهرام، المجلد (٢٢)، العدد (٨٥)، يناير ٢٠٢٢، ص ١٦٢.

(٢) المرجع السابق، ص ١٦٤.

الفرع الأول

مفهوم تقنية الميتافيرس

تعرف تقنية الميتافيرس بأنها: تكنولوجيا تتيح مساحة افتراضية يتم فيها إنشاء الأفاتار Avatar (تجسيد لشخصياتنا رقميًّا في العالم الافتراضي والأغراض الرقمية)، فبدلاً من المشاهدة والتصفح للمحتوى الإلكتروني كما كان سابقًا، يتم في هذه التقنية الدخول والتجسد في هذا العالم الرقمي، والشعور بأنك موجود فعلاً مع شخص آخر أو في مكان آخر، وهو بمثابة عالم ثالث افتراضي يأخذ من الواقع شيئًا ومن الإنترنت والتقنيات الذكية أشياء وخصائص(١).

ويعود مصطلح الميتافيرس Metaverse إلى الروائي نيل ستفنسون Neal Stephenson في روايته «تحطم الثلج» Snow Crash سنة ١٩٩٢، والذي يعبر فيه عن عالم افتراضي يتفاعل فيه البشر، وسبق كذلك رواية One للمؤلف أرنست كلاين الذي تم تحويله إلى فيلم سينمائي عام ٢٠١٨ والذي تدور أحداثه في عام ٢٠٤٥؛حيث يهرب فيه مراهق يتيم من عالمه الكئيب إلى عالم آخر افتراضي بالكامل، وكذلك فيلم Summer Wars المعروض عام ٢٠٠٩، وهو فيلم كرتوني تدور أحداثه حول عالم افتراضي يدعى «أوزي»(٢).

إن كلمة «ميتافيرس» Metaverse تجمع ما بين الكلمة الأولى هي «ميتا» (Meta) وتعني ما وراء، أما الكلمة الثانية «فيرس (Verse)» وهي كلمة مصاغة من العالم أو الكون، وبذلك يكون الاسم الكامل الكون الماورائي»، أو ما بعد الكون(٣).

وهي في الأساس تكنولوجيا قديمة للواقع الافتراضي، كان يستعملها الأطباء للتدريب على العمليات الجراحية، وكذا مساعدة الطيارين للتدريب على القيادة، وفي مجال محاكاة الأنظمة العسكرية(٤).

---

(١) انظر:د/ نور الدين زعتر، العالم الافتراضي «الميتافيرس Metaverse » من منظور سيكولوجي، مرجع سابق، ص ١٠١٧.

(٢) المرجع السابق ، ص ١٠٢٠.

(٣) المرجع السابق ، ص ١٠١٧.

(٤) محمد عبد العزيز المحمود، المسؤولية الجنائية عن إساءة استخدام وسائل التواصل الحديثة، رسالة دكتوراه، كلية العدالة الجنائية، جامعة نايف للعلوم الأمنية، الرياض، ٢٠١٤، ص ٥٣.

ويبقى القول إن مشروع الميتافيرس أحد مشروعات «فيس بوك» الواعدة، لكنها ما زالت قيد الاختبار المتوقع اكتماله خلال خمس سنوات من الآن كما تسعى «فيس بوك»، ويبدو أن «مارك زوكربيرج» الرئيس التنفيذي لشركة «فيسبوك» قد نجح بالفعل في إحداث الضجة اللازمة للإعلان عن مشروعه الجديد، وكأنه بديل محتمل لتطبيقات التواصل الاجتماعي التقليدية مثل «فيسبوك»، فمن أهم خصائص تقنية ميتافيرس أنها من نتائج الثورة التكنولوجية، والتي تبشر بنقل البشرية إلى طفرة غير مسبوقة في نطاق التواصل، كما تبشر بمستجدات لا نهاية لها[1].

الفرع الثاني

خصائص تقنية الميتافيرس

يغطي مصطلح ميتافيرس مجموعة متنوعة من الحقائق الافتراضية من بيئة العمل وأدواتها، والاجتماعات والتعليم عن بعد إلى الدفع الإلكتروني بالعملات المشفرة إلى صناعة الألعاب إلى المنصات الاجتماعية، لكن ضمن تصور مختلف تمامًا عما كانت عليه. ومما لا شك فيه أيضًا أن جائحة كورونا أثارت اهتمامًا كبيرًا بالبيانات الافتراضية المشتركة بكل المجالات، وعلى وجه الخصوص في التجارة الإلكترونية والدفع المالي الإلكتروني وفي مجال التعليم.

ومن أهم خصائص تقنية الميتافيرس ما يلي:

١- الميتافيرس عالم افتراضي ثلاثي الأبعاد:

تنبئ النظرة المستقبلية للميتافيرس - كوسيلة تواصل واتصال- عن توقعات لعديد من التطبيقات والاستخدامات المحتملة للميتافيرس، فمن المتوقع أنه عند الوصول إلى ميتا فيرس بالشكل المثالي سيكون وسيلة أساسية يُعتمد عليها في مجالات الحياة المختلفة.

ولن تقتصر الاستفادة من ميتافيرس على ممارسة الألعاب أو حتى عقد اجتماعات

(١) انظر: المستشار الدكتور/ محمد جبريل إبراهيم، الميتافيرس والقانون الجنائي، مرجع سابق، ص ٩.

العمل بشكل افتراضي، بل ستتأثر جميع الأنشطة التي يمارسها مستخدم الإنترنت بهذا العالم، فعلى سبيل المثال سيشهد التسوق الإلكتروني نقلة نوعية داخل هذا العالم، حيث يكون المستخدم قادرًا على معاينة أي شيء يريد شراءه عن قرب بدلاً من مجرد معاينة صور في الشكل التقليدي المعروف الآن للمتاجر الإلكترونية[١].

ويعد الميتافيرس عالمًا افتراضيًّا ثلاثي الأبعاد، فلا هو حقيقي، ولا هو خيالي، لكنه بين هذين العالمين، ويتيح للمستخدم الدخول فيه بمساعدة أدوات معينة، وباستخدام صورة رمزية متحركة تمثله (أفاتار)؛ وذلك لإجراء بعض العمليات، مثل: التسوق ومقابلة الأشخاص، والألعاب، وإنشاء العوالم الخاصة... وغيرها الكثير في هذا العالم بدون أن يتحرك من مكانه[٢].

ولقد قصد به نيل ستيفنسون في روايته المذكورة العالم الافتراضي المملوك من قِبل الشركات، حيث يتم التعامل مع المستخدمين النهائيين كمواطنين يعيشون في ديكتاتورية الشركات بصورة تجعل من الأفراد جزءًا من الإنترنت لا مستخدمين له[٣].

٢- إنشاء أفاتار مميز لكل شخصية:

في تقنية الميتافيرس ينشأ المحتوى من طرف المستخدمين أنفسهم، فالمستخدم هو الذي يحدد ماذا يريد أن يفعل من خلال تلك التقنية، ومن ثَمَّ فإن الخيارات التي يتخذها مستخدم تقنية الميتافيرس هي المحرك الأساسي للتفاعل بين المستخدمين داخل تلك التقنية.

فمع تطور ميتافيرس سيصبح كل نشاط إنساني في الواقع الحقيقي متاحًا بكل تفاصيله في العالم الافتراضي، الأمر الذي يعني أن الإنسان ربما يكون قادرًا على البقاء في العالم الافتراضي لفترات أطول، فهو إما يمارس إحدى الألعاب أو الرياضات مع أصدقاء من مختلف أنحاء العالم، أو يعقد اجتماعات افتراضية أو يتسوق ما يحتاجه من متاجر على الجانب الآخر من الكوكب.

---

(١) انظر: د/ نور الدين زعتر، العالم الافتراضي «الميتافيرس Metaverse» من منظور سيكولوجي، مرجع سابق، ص ١٠١٧.

(٢) انظر: د/ جميلة بن زاف: المجتمع الافتراضي ونهاية أطروحة القرية العالمية لماكلوهان بحث منشور في -مجلة علوم الإنسان والمجتمع المجلد (١١) العدد (١) السنة ٢٠٢٢، ص ٢٠٣.

(٣) انظر: د/ نور الدين زعتر، العالم الافتراضي «الميتافيرس Metaverse» من منظور سيكولوجي، مرجع سابق، ص ١٠١٩.

ووصف مؤسس شركة «ميتا»، مارك زوكربيرج «مشروع ميتافيرس» بأنها بيئة افتراضية شبه حقيقية، فبدلاً من النظر إليها من خلال الشاشة فقط يمكن الدخول إليها والتفاعل معها بشكل يبدو كالحقيقة بفضل السترات والقفازات التي يتم ارتداؤها والمزودة بأجهزة استشعار عبر عوالم افتراضية لا نهاية لها، حيث يمكن للناس الدخول لهذه العوالم والمجتمعات والالتقاء بالأصدقاء والتحدث إليهم، وكذلك اللعب معهم باستخدام نظارات الواقع الافتراضي، وارتداء سترات وقفازات مزودة بأجهزة استشعار حسية[١].

كما أعلنت شركة Meta «ميتا» بداية هذه السنة (٢٠٢٢) أنها ستنتج حاسوبًا خارقًا هو الأسرع في العالم وسيساعدها في التحضير لمنصة العالم الافتراضي «الميتافيرس». حسب Gibbs ٢٠٢١ فإن الميتافيرس Metaverse هي تجمع للتقنيات التي كانت تتلاشى منذ أعوام والتقنيات الآخذة في الظهور [٢].

٣- طبيعة العلاقة بين مُزوّد الخدمة – تقنية الميتافيرس- والمستفيد:

حتى يستطيع الشخص استخدام تلك التقنية ينبغي عليه – بدايةً – الموافقة على الشروط التي يضعها مُقدّم الخدمة لاستخدامها، ثم بعد ذلك التسجيل في التقنية، من خلال إدخال معلوماته الشخصية لإنشاء صفحة خاصة به تعرفه وتميزه عن بقية أفراد المجتمع، بحيث لا يستطيع الدخول إليها إلا باستخدام كلمة سرية خاصة به. وشروط الاستخدام التي يوافق عليها المستخدم تتضمن توجيهات ومعلومات يُقدمها مزود الخدمة لضمان الاستخدام السليم لتلك التقنية، وعدم الإضرار بالغير في أثناء ذلك، كما تتضمن –بالإضافة إلى ذلك – بيان الحقوق والالتزامات المتبادلة بين طرفي العلاقة[٣].

ولاستخدام أية وسيلة من وسائل التواصل لا بد من إنشاء حساب شخصي يتم التفاعل

(١) انظر: العالم الافتراضي «الميتافيرس Metaverse » من منظور سيكولوجي، مرجع سابق ، ص ١٠١٨.

(٢) المرجع السابق ، ص ١٠٢٠.

(٣) انظر: د/عبد الوهاب جودة الحايس، الآثار الاجتماعية لاستخدام وسائل الإعلام الاجتماعي على بعض جوانب الشخصية الشابة ، مجلة شؤون اجتماعية ، الإمارات العربية المتحدة، م ٣٢ ، ع ١٢٦، سنة ٢٠١٥، ص ٨٣.

من خلاله، فدخول العالم الافتراضي لوسائل التواصل يستدعي وجود شخصية متميزة لكل مستخدم داخل المجتمع المكوّن لها، من خلال الحساب الشخصي الذي ينشئه المستخدم عند الشروع في استخدامها، من خلال إدخال بعض المعلومات الشخصية التي تختلف من وسيلة تواصل إلى أخرى، مثل الاسم والصورة وتاريخ الميلاد، ومن دون هذه البيانات لا يمكن للأفراد أن يتعرفوا بعضهم على بعض وإجراء التواصل فيما بينهم، فالغاية الأساسية لوسائل التواصل هي ربط الأفراد بعضهم ببعض، وتسهيل التواصل فيما بينهم، ومازالت هذه السمة تميز وسائل التواصل عن غيرها من تلك التي يمكن أن تشبهها، وعلى العموم فإنّ أي موقع أو تطبيق يقوم على فكرة محتوى المستخدم، ويعطي مستخدميه إمكان التفاعل مع غيرهم، دون أن يشارك في تقديم المحتوى، يعتبر من وسائل التواصل الاجتماعي، حتى لو لم تكن الغاية الأساسية منه هي التواصل، مثل منصات الألعاب، على سبيل المثال[١].

وعليه فإن أي خدمة تُقدَّم عبر الإنترنت، وتتوافر فيها جميع العناصر السابق ذكرها، تعتبر بمنزلة وسيلة تواصل اجتماعي – ويدخل في ذلك الميتافيرس- ؛ فهذا المصطلح يُستخدم للتعبير عن فئة خاصة من مخرجات التقنية الحديثة، تقوم على المزاوجة بين تقنيات الاتصال والإنترنت، وينشئ بواسطتها الشخص شخصية افتراضية يتفاعل من خلالها مع غيره من الأشخاص سواء أكانوا من المرتبطين معه ضمن شبكة واحدة أم من غير المرتبطين معه ضمن هذه الشبكة، وهذا التفاعل يشبه نظيره في المجتمع المادي الحقيقي، غير أن وسائله هي نشر كل أشكال البيانات والمعلومات ومشاركتها، عوضًا عن التفاعل المادي المباشر[٢].

مما سبق يتضح أن وسائل التواصل الاجتماعي تتميز بمجموعة من الميزات التي تعطيها أهمية استثنائية، بالنظر إلى ما يترتب عليها من مخاطر، وما تطرحه من إشكالات قانونية قد لا نبالغ إذا قلنا إنها تتعلق – في بعض الأحيان – بكينونة المجتمع وأسسه العامة.

(١) انظر: د/ محمود محمد أبو فروة، منصات التواصل الاجتماعي ومسؤوليتها القانونية عن المحتوى غير المشروع، نشر مجلة القانون الكويتية العالمية، السنة العاشرة، العدد (٣)، العدد التسلسلي (٣٩)، ذو القعدة ١٤٤٣هـ/ يونيو ٢٠٢٢م، ص ١٧١.

(٢) المرجع السابق ، ص ١٧٢.

ونظرًا لكـون استفادة المستخدم من وسائل التواصـل مرهونة بموافقته على شروط الاستخـدام التـي يضعها مُقدِّم الخدمة، فـإنّ الإطار المنظم للعلاقـة بين الطرفين هو إطـار تعاقدي في الأساس، فاستخدام وسائل التواصل الاجتماعي يتم من خلال اتفاق يمنـح بموجبه أحد الطرفين (مُقـدِّم الخدمة) الطرف الآخـر (المستخدم) الحق في إنشاء صفحة شخصية على الموقع، أو البرنامج، أو التطبيق الإلكتروني المملوك للطرف الأول، لكـي يستخدمها للتواصل والتفاعل مع الغـير، بإرسال ومشاركة المعلومات بشكل إلكـتروني، ويتميز الاتفاق الذي يُنظم استخـدام وسائل التواصل الاجتماعي بأنّ مُقدِّم الخدمـة هو الذي يضعه ويُحدّد شروطه، ويمتلك إمكانية تعديله في أي وقت، ولا يمكن للمستخدم التفاوض بشأن تلك الشروط، أو الاعتراض على التعديلات التي تم إخطاره بهـا؛ لذلك نجد أغلبية الشروط التي يتضمنها تصـب في مصلحة مُقدِّم الخدمة، بما في ذلك الشروط التي تُحدد التزامات الأطراف ومسؤولياتهم[١].

ولا يملك المستخدم إلا الإذعان للشروط التي وضعها مُقدِّم الخدمة إذا ما رغب في الاستمرار في الاستفادة من وسائل التواصل؛ لأن أي إخلال بتلك الشروط يعطي مُقدِّم الخدمـة الحق في حذف المحتوى المخالـف، أو بموجبه أحد الطرفين (مُقدِّم الخدمة) الطـرف الآخر (المستخدم) الحق في إنشاء صفحة شخصية على الموقع، أو البرنامج، أو التطبيـق الإلكـتروني المملوك للطـرف الأول، لكي يستخدمها للتواصـل والتفاعل مع الغـير، بإرسال ومشاركة المعلومات بشـكل إلكتروني، على أن يستخدمها وفقًا للضوابط والمعايير التي يُحددها الطرف الأول[٢].

لذلك فإن الاتفاق المبرم بين المستخدم ومُقدِّم الخدمة يُمثل الإطار القانوني المنظم لعلاقـة الطرفين كل منهما بالآخر، والمحدّد الرئيسي للالتزامات المتبادلة بينهما، وأي إخـلال بهذا الاتفاق، من أي طرف سوف يؤدي إلى قيام مسؤوليته العقدية في مواجهة الطرف الآخر[٣].

---

(١) المرجع السابق، ص ١٧٨.

(2) Amanda De carlo, La Responsabilité de L›hébergeur Internet Visà- Vis des Tiers. Mémoire du diplôme de la Faculté Libre de Droit, d›Economie et de Gestion (FACO)JUIN 2008, p.5. https://www.lepetitjuriste.fr/wp-content/uploads/2011/05/La responsabilité de 1›hébergeur internet vis- à-vis des tiers.pdf, (Accessed on: 2/5/2023).

(3) Amanda De carlo, La Responsabilité de L›hébergeur Internet Visà- Vis des Tiers. Mémoire du diplôme de la Faculté Libre de Droit, d›Economie et de Gestion (FACO)JUIN 2008, p.5. https://www.lepetitjuriste.fr/wp-content/uploads/2011/05/La responsabilité de 1›hébergeur internet vis- à-vis des tiers.pdf, (Accessed on: 2/5/2023).

ويرى الفقه أنّ العلاقة بين مُزوِّد الخدمة والمستفيد هي أقرب إلى عقد إيجار الأشياء أو الإعارة، وفق طبيعة الخدمة، إذا كانت بمقابل أو مجانية؛ فمهمة مزوّد الخدمة تقتصر على تزويد مساحة خاصة لمتلقيها يمكن له استخدامها بحرية كاملة، وهو يمتلك كل البيانات التي يقوم بإضافتها أو مشاركتها، ما لم يثبت العكس، وبطبيعة الحال فإن استخدامه تلك المساحة ينبغي أن يكون وفقًا للضوابط والشروط المتفق عليها، بالإضافة إلى التزامه العام بعدم الإضرار بالغير أثناء هذا الاستخدام[١].

الفرع الثالث

طبيعة المحل الإلكتروني داخل تقنية الميتافيرس

يمكن أن تتمثل الاعتداءات داخل تقنية الميتافيرس، إما اعتداءً على المواقع الإلكترونية الموجودة على الشبكة العالمية للمعلومات، سواء فيما يتعلق بالمواقع التي يمتلكها الأشخاص كالحقوق الشخصية اللصيقة بذات الإنسان كالحق في السرية، وحقوق الملكية الفكرية، أو بالمواقع التي تمتلكها الهيئات والدول كالاعتداء على البيانات والمعلومات الخاصة بها. والاعتداء على المواقع الإلكترونية يعرف بالجريمة المعلوماتية، والتي يتم فيها التسلل للمعلومات للتجسس عليها أو النسخ، أو الحذف، أو التعديل، أو الإضافة، أو إتلافها[٢].

ويعتبر صاحب المعلومات أو مزود الموقع الإلكتروني بالبيانات المقدمة معتديًا عليه من جراء الولوج غير القانوني للموقع الإلكترونى، ويهدف من تقديم تلك المعلومات إما الربح المادي أو مجرد الاطلاع والتسلية، ودون النظر للقصد من ذلك، فتلك المعلومات لها حماية قانونية، وقد كفلت مختلف القوانين والاتفاقيات الحماية لتلك المعلومات.

ويمكن وصف المحل الإلكتروني الذي يقع عليه الاعتداء – وينطبق هذا أيضًا على الميتافيرس- بأنه المال الوجود على الحاسب الآلي، سواء فى صورة معلومات أو بيانات

(١) انظر: د/ رضا المتولي وهدان، النظام القانوني للعقد الإلكتروني والمسئولية عن الاعتداءات الإلكترونية، دراسة مقارنة في القوانين الوطنية وقانون الأونسيترال النموذجي والفقه الإسلامي، دار الفكر والقانون، ٢٠١٧، ص ١٣٠.

(٢)انظر: د/ أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٥، ص ٢٩.

إلكترونيــة، كذلك أى صورة يكون فيها موجودًا سواء علــى أقراص صلبة أو أسطوانات تكــون في طريقهــا للإدخال على الحاســب الآلي، فالمحل الإلكترونى هــو أى مدخلات إلكترونية قابلة للتعامل، ولها من القيمة المادية ما يجعلها قابلة للتملك وتكتسب الحماية القانونية[١].

كذلك فالمحــل الإلكترونى يتمتع بصفة التطور، فالمتابــع لنوعية الجرائم التي كانت تقــع على المحل الإلكتروني سيجد أن تلك الجرائم قد تطورت بشكل ملحوظ منذ القرن العشريــن إلى وقتنــا الراهن، ففي البداية كانت الجرائم تنحصــر في سرقة البيانات أو المعلومــات ثم تطورت إلى إتلاف البرامج العسكريــة ومنها إلى التدخل في البيانات الحكوميــة، وانتهى الأمر – حتى وقتنا- إلى النصب بأساليب مبتكرة – ومنها ما سيتم من خلال الميتافيرس[٢].

أيضًــا فالمحــل الإلكترونــى وعلــى الرغم من تطــوره الملحــوظ إلا أن لــه خصيصة لم تتبــدل حتى الآن، وهــى صعوبة إثبات الجريمــة الواقعة سواء عليــه أو به، فالتوصل للجــاني المُستخدم للمحــل الإلكتروني في تنفيــذ جريمته محاط بالكثــير من المشاكل أبسطهــا التأكد من قيام الجاني باستخــدام الحاسب الآلي فى تنفيذ جريمته، وكذلك محاولات التفرد الجنائي والتي تدفع الجاني لعدم الكشف عن الأسلوب المتبع في تنفيذ الجريمة[٣].

وأولى الخطــوات فــي ارتكاب الجرائــم الإلكترونية هــي بالولوج غــير المصرح به، فمقتحم الموقع الإلكترونى – الأفاتار- يدخل إلى الموقع بأسلوب غير مباح له دون النظر للهدف من هذا الولوج، ودون البحث في كيفية الاقتحام للموقع، سواء تم ذلك بأجهزة مخصصــة لذلك أو بالوسائل الفنية والتقنيــة واعتمادًا على خبرة المنفذ لذلك الولوج، وأهــم صور الولوج المعلوماتي الاعتراض غير القانوني – من الأفاتار- لبرامج الحاسب

(١) انظر: د/ ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، مرجع سابق، ص ٣٢.

(٢) انظر: د. عمر فاروق الحسيني، تأملات في بعض صور الحماية الجنائية لنظم الحاسب الآلي ، مقال مقدم للدورة التدريبية بفندق شيبارد المنظمة من اتحاد من ٧/ مايو، ١٩٩١

(٣) انظر: د/ ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية مرجع سابق، ص ٣٤.

الآلي، سواء أكانت برامج التشغيل للحاسب أم إدارته، وعند ذلك يبدأ المقتحم في ممارسة مختلف أنواع الجرائم سواء سرقة المعلومات، أو حذفها، أو تغيير بياناتها[١].

ففكرة ملكية الغير للمحتوى الموجود بالموقع الإلكتروني تظهر في تفعيل حق المؤلف وبسط الحماية المنصوص عليها في نصوص قانون حماية حق المؤلف، فأي انتهاك للمصنفات الموجودة على المحل الإلكتروني المعروض منها أو المخزن في الموقع يعد اعتداءً على حقوق المؤلف، سواء تم ذلك بالنسخ أو البيع أو العرض للجمهور للتحميل المجاني من شبكة الإنترنت[٢]. ولنضرب مثالاً على ذلك وهو إذا ما تم ولوج الأفاتار لموقع إلكتروني لإرسال بيانات شركة اقتصادية إلى منافسيها في أسواق التجارة العالمية، أو إرسال بيانات عسكرية خاصة بدولة إلى دولة أخرى أو جماعة معادية، وأيضًا ولوج الأفاتار لاختراق الحسابات البنكية، وقد يصل الأمر إلى إتلاف قاعدة البيانات الرئيسية للعملاء.

وتتمثل الإشكالية الأكبر في تفعيل حماية حق المؤلف في ظل تقنية الميتافيرس فى تحديد الشخص الذي استخدم الأفاتار ليقوم بالاعتداء على حقوق الملكية الفكرية، وإثبات ذلك الاعتداء عليه.

ومن ثَمَّ لابد من التدخل سواء على مستوى المجتمع الدولي أو التشريعات الوطنية لوضع تنظيم قانوني للجرائم المعلوماتية – وخاصة ما يحدث من خلال تقنية الميتافيرس- ، فالإشكالية لا تتعلق بالمخاوف من تطور المعلوماتية، بل في إيجاد إطار قانوني يحكم التعاملات خلالها، وتنظيم هذا التعامل باعتباره ظاهرة إنسانية اقتصادية اجتماعية لا يمكن أن تطور بنفسها دون وجود الكيان القانوني الذى يوضح مفهوم المجرم المعلوماتي والجريمة المعلوماتية.

أما بالنسبة لتصدي الأنظمة القانونية للجرائم المعلوماتية - وخاصة الولوج غير

(١) المرجع السابق، ص ٣٢.

(٢) انظر: د. فتوح الشاذلي و د. عفيفي أمل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفكرية ودور الشرطة والقانون، دراسة مقارنة ، منشأة المعارف، الإسكندرية ، ٢٠٠٨ ، ص ٥٧.

القانوني أو جريمة الاعتراض المعلوماتي- نجد أن النظامين اللاتيني والأنجلوساكسوني قد اتبعا أساليب تتفق في الهدف منها وهو الحماية، وإن اختلفت في كيفية التصدي، ففي المدرسة اللاتينية نجد أن المشرع النمساوي والبلجيكي والبرازيلي والتشيكي قد أقروا نظمًا قانونية تحدد الكيفية التي يتم بها مواجهة جرائم الكمبيوتر، ونجد تفرد المشرع الفرنسي بتقرير تشريعات لمواجهة الجرائم المعلوماتية مرتبطة بالعدالة والأخلاق[١].

أما عن النظام الأنجلوساكسوني فقد اختلف النظامان الأمريكي والبريطاني في الأساس المتبع في مواجهة الجريمة الإلكترونية، فقد واكب كل من المشرع الأسترالي والأيرلندي والنرويجي لتلك الاتجاهات، وقد كان النظام الذى انتهجه المشرع الأمريكي في البداية يعتمد على حق المؤلف والحماية المقررة للمؤلفات، وقد تم مؤخرًا إدخال مواد قانونية تهدف إلى حماية برامج الحاسب الآلي. أما النظام القانوني البريطاني فقد اتجه إلى حماية المحل الإلكتروني والحاسب الآلي وبرامجه، فقد تم إقرار قانون إساءة استخدام الكمبيوتر والذي نص على مفهوم الدخول المحظور على الكمبيوتر، سواء كان بغرض تسهيل ارتكاب الجرائم أو تبديل مواد الكمبيوتر[٢].

وقد كان الشرط الأساسي في تلك الجرائم أن تكون الخبرة الإلكترونية هى السبب الأساسي في ارتكاب تلك الجرائم، وهو شرط يحتاج إلى النظر والتأمل فى معيار الخبرة المتطلبة، وهل هي خبرة الرجل العادي أم أنها تطلب شروطًا خاصة[٣].

أما إذا ما تم التعرض للتشريعات العربية فقد اتفقت فيما بينها على حماية الحاسب الآلي من الاختراق وسرقة البيانات والتجسس على المعلومات، إلا أنه نظرًا لحداثة الدول العربية بتلك الأنظمة فهي ما زالت في طور النمو والتوسع فى مجال الحماية الجنائية، فهناك دول قد اتجهت إلى تقرير تشريع يختص بالجرائم الإلكترونية مثل مصر والإمارات كما أن هناك دولاً عربية كثيرة لم يصدر بها مثل ذلك التشريع كسوريا.

---

(١) انظر: د/ حمدي عبد الرحمن، المدخل لدراسة القانون المقارن، مذكرات لطلبة دبلوم القانون المقارن، كلية الحقوق، جامعة عين شمس القاهرة، ١٩٧٣م، ص ٢٥.

(٢) انظر: د/ ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، مرجع سابق، ص ٥١.

(٣) المرجع السابق، ص ٥١.

وفـي جريمة الإتلاف المعلوماتي يتم الاعتداء على الأدوات المادية أو محتوى البرامج والمعلومـات المنسوخـة، فهذا الاعتداء يقع علـى مال منقول مملوك للغير مـن شأنه أن يسبـب أضـرارًا لأصحابهـا، وقد اتجهـت غالبية الـدول إلى تجريم مثل هـذه الأفعال ومسؤوليـة المعتدي عن الإتـلاف الحادث بفعله والواقع على البيانـات، ومن الدول التي أصـدرت قوانين فـي هذا المجال فرنسـا وأمريكا وكندا وألمانيا والدانمارك ومصر، وقد سمَّته بعض الدول بالمال المعلوماتي كما هو فـي ألمانيا[١].

(١) انظر: د/ أحمد فتحي سرور، الوسيط في قانون العقوبات القسم الخاص، ط (٤)، ١٩٩١ دار النهضة العربية، ص ٣٧٣، ود/ أحمد حسام طه تمام، دار النهضة العربية، ٢٠٠٠، ص ٣٤٢، ٣٤٣

المبحث الأول

تحديد الإشكاليات القانونية لإنفاذ القانون الدولي على تقنية الميتافيرس

تمهيد وتقسيم:

تطور الحق في الخصوصية وحماية البيانات في الستينيات والسبعينيات نتيجةً للتأثر بتقنية المعلومات، وبسبب القوى الرقابية المحتملة لأنظمة الكمبيوتر، التي استوجبت وضع قواعد معينة تحكم جمع ومعالجة البيانات الخاصة، وفي هذا المجال فإن أول معالجة تشريعية في ميدان حماية البيانات كان عام ١٩٧٠ م، في هيس بألمانيا (Land Of Hesse In Germany) والذي تبعه أول قانون متكامل في السويد عام ١٩٧٣، ثم الولايات المتحدة عام ١٩٧٣، ثم ألمانيا على المستوى الفيدرالي عام ١٩٧٧ ، ثم فرنسا عام ١٩٧٨ [(١)].

وعلى الرغم من وجود العديد من المواثيق والمعاهدات الدولية العالمية والإقليمية التي تضفى مزيدًا من الحماية لحقوق الإنسان والتي من أهمها الحق في الخصوصية -ومنها خصوصيته داخل تقنية الميتافيرس وحماية حقه في عدم الاعتداء على البيانات الخاصة به- إلا أن هذه القواعد ستعجز عن مواجهة الظواهر الإجرامية الحديثة عبر الميتافيرس التي تقوم على أدوات غير تقليدية، وعناصر مختلفة من حيث الحدود المكانية والزمانية، وكذلك من حيث الأشخاص والوقائع.

وإذا كانت لم تعرض بعد نزاعات تتعلق بالميتافيرس على منصات القضاء وفي ساحات المحاكم؛ إلا أن الواقع يشهد أن استخدام هذه التقنية سيرتب إشكاليات عديدة عما قريب، يجدر التأهب لها والاستعداد لمواجهتها من كل من المشرع والفقه الدولي.

وقد بينت الأمم المتحدة التحديات التي تواجهها البلدان في إنفاذ قوانين حماية البيانات بشكل مناسب، والتي تشمل قضايا التمويل، وعدم القدرة على إنفاذ هذه القوانين بشكل مناسب (على سبيل المثال: قيود الموارد البشرية والتقنية)، وعدم كفاية

(١) انظر: د/ شريف يوسف خاطر، حماية الحق في الخصوصية المعلوماتية، مرجع سابق، ص ٣٠.

البنية التحتية لتكنولوجيا المعلومات والاتصالات، وعدم القدرة على التعامل مع الطلبات العابرة للحدود أو عدم الرغبة في ذلك[١].

ويختلف تطبيق مبادئ وقوانين الخصوصية وحماية البيانات في القطاعين العام والخاص بين البلدان وداخلها. على سبيل المثال، تم تنفيذ اللائحة العامة لحماية البيانات لتنسيق وتعزيز سلطات حماية البيانات لضمان التطبيق الفعال للقانون. وبالإضافة إلى قوانين حماية البيانات، قامت المنظمات الدولية والإقليمية بتطوير وتنفيذ لوائح حماية البيانات للمساعدة في جهود حماية البيانات. فعلى سبيل المثال، طورت منظمة التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC) إطار عمل الخصوصية، والذي يتضمن مبادئ وإرشادات لحماية البيانات بطريقة تتجنب العقبات التي تحول دون تدفق المعلومات بين الأعضاء، وقواعد الخصوصية عبر الحدود، وهي آليات اختيارية للتنظيم الذاتي تحدد معايير حماية البيانات لتبادل البيانات عبر الحدود بين الأعضاء. ومن المهم ملاحظة أن قوانين حماية البيانات والخصوصية الوطنية لها الأسبقية على هذه القواعد[٢].

لذلك وضعت منظمة التعاون الاقتصادي والتنمية دليلاً إرشاديًا لحماية الخصوصية ونقل البيانات الخاصة، والذي قرر مجموعة قواعد تحكم عمليات المعالجة الإلكترونية للبيانات، وهذه القواعد تصف البيانات والمعلومات الشخصية على أنها معطيات تتوافر لها الحماية في كل مرحلة من مراحل الجمع Collection والتخزين Storage والمعالجة Processing والنشر[٣].

وتتضمن التوجيهات المبادئ الثمانية الرئيسية لحماية الخصوصية أو الحق في حماية البيانات الخاصة، وهذه المبادئ هي: تحديد حصر عمليات جمع البيانات والاقتصار على طبيعة البيانات الشخصية وتحديدها وتحديد الغرض وحصر الاستخدام بالغرض المحدد وتوفير وسائل حماية وأمن المعلومات والعلانية والحق في المشاركة والمساءلة.

(١) تقرير الأونكتاد، ٢٠١٦، ص٩.

(2) https://www.apec.org/Publications/2005/12/APEC-Privacy-Framew ork

(3) Ghosh, Sumit., & Turrini, Elliot. (2010). Cybercrimes A Multidisciplinary Analysis. Germany: Springer. P326. https://www.oecd.org/mena/%D8%A7%D9%84%D8%B1%D8%A6%D9%8A%D8%B3%D9%8A%D8%A9/

ولقد لعب هذا الدليل دورًا رئيسيًا وكان الأكثر تأثيرًا في اتجاه الدول الأوروبية إلى إقرار تشريعات وطنية في مجال الخصوصية، ومنذ ذلك التاريخ تتابع هذه المنظمة موضوع الخصوصية وتضعه ضمن أجندتها السنوية، وتتابع تطورات التدابير التشريعية في هذه المجال. وفي عام ١٩٨١ وضع الاتحاد الأوروبي اتفاقية حماية الأفراد من مخاطر المعالجة الآلية للبيانات الشخصية، حيث تبنت لجنة وزراء من مجلس أوروبا منوط بها معالجة موضوع الخصوصية اتفاقية حماية الأفراد في نطاق المعالجة الآلية للبيانات الشخصية، وقد وقّعت على هذه الاتفاقية (٣١) دولة صدقت منها (٢١) دولة، وبتاريخ ٢٥ يناير ٢٠١٢ صدقت باقي الدول الموقعة على هذه الاتفاقية وانضمت إليها ثماني دول أخرى ليصبح عدد أعضائها (٣٩) دولة موقّعة ومصدقة على الاتفاقية[١].

وإذا دققنا النظر في كلٍّ من الاتفاقية السابقة وتوصيات منظمة التعاون الاقتصادي والتنمية، نجد أن الاتفاقية على خلاف توصيات منظمة التعاون الاقتصادي والتنمية، حيث إن الاتفاقية ملزمة للأعضاء الموقعين عليها، وينحصر نطاقها بالأشخاص الطبيعيين والملفات المعالجة آليًّا وتطبق على القطاعين العام والخاص، كما تقرر الاتفاقية عشرة مبادئ تمثل الحد الأدنى للمعايير التي ينبغي على الدول اتباعها وأهمها حماية الخصوصية المتعين على الدول الأعضاء تضمينها في تشريعاتها و قوانينها الداخلية التي تضعها، وهذه المبادئ مقاربة جدًّا لمبادئ منظمة التعاون الاقتصادي والتنمية، ولكن مع مزيد من التفصيلات، وتتمحور حول تحقيق العدل الاجتماعي، وقيود الجمع، والوقاية العلنية، وتأقيت الغرض وتحديد المدى، ومشاركة الأفراد. واستنادًا إلى هذه المبادئ الأساسية للحماية فإن قواعد الاتفاقية تغطي مسائل نقل وتبادل البيانات بين الدول المتعاقدة، وتمنع نقل أية معلومات خارج الحدود إلا للدولة التي تتوافر لها حماية موازية كاستثناءات من هذه القاعدة.

وقد بذل مجلس أوروبا جهودًا إضافيةً في هذا المجال من خلال لجنة الخبراء

(١) التوصيات الإرشادية تم إصدارها من قبل منظمة التعاون الاقتصادي والتنمية اهتمامًا منها بآثار الجرائم الإلكترونية السلبية على الحياة الاقتصادية مُنذُ عام ١٩٧٧م، وكان نتيجة هذا الاهتمام قواعد إرشادية وتوصيات للدول الأعضاء، كما بذلت مجهودًا لوضع تعريف للجريمة الإلكترونية.

العاملة في مجال حماية البيانات، وقد أصدرت هذه اللجنة سلسلة من الأدلة التوجيهية المعتمدة على الاتفاقية المذكورة، وهي ليست أكثر من توصيات موجهة إلى حكومات الدول الأعضاء، وتتعلق توصيات اللجنة بحماية قواعد المعلومات الطبية المعالجة إلكترونيًّا وقواعد المعلومات الخاصة المتعلقة بالأنشطة الطبية والإحصاءات وقواعد المعلومات الخاصة لأغراض التسويق وقواعد المعلومات الخاصة لأغراض الضمان الاجتماعي، وكذلك لأغراض البوليس والبيانات الجنائية وقواعد المعلومات الخاصة بأغراض التوظيف، وكذلك خدمات الاتصال، وقد عمل جزء من اللجنة المذكورة على موضوع البيانات المتعلقة بالقطاع المصرفي[1]. وتستلزم الدراسة في هذا المبحث تناوله وفقًا للتقسيم التالي:

المطلب الأول

إشكالية حماية خصوصية البيانات داخل تقنية الميتافيرس

والحق في حماية البيانات الشخصية يلتصق بالحق في الخصوصية الرقمية وهو «التسليم بحق الأفراد في التمتع بفسحة للتنمية الذاتية تقوم على مبدأي التفاعل والحرية، أو حقهم في مجال خاص يتسع لهم فيه التفاعل أو عدم التفاعل مع الآخرين، دون الخضوع لتدخل الدولة أو تدخل زائد يمارسه أفراد آخرون بلا دعوة»، وذلك وفقًا للتقرير السنوي لمفوض الأمم المتحدة السامي لحقوق الإنسان عن الحق في الخصوصية في العصر الرقمي[2]، ويشمل التقرير أيضًا الحياة الإلكترونية للأفراد، مساحة البيانات الشخصية التي تقع تحت بند الخصوصية.

وأكد على ذلك العالمي لحقوق الإنسان عام ١٩٤٨، نصت المادة (١٢) من الإعلان العالمي على أنه «لا يعرض أحد لتدخل تعسفي في حياته الخاصة، أو أسرته، أو مسكنه، أو مراسلاته، أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون

(١) انظر: د/ هلالي عبد اللاه أحمد (٢٠١١)، اتفاقية بودابست لمكافحة جرائم المعلوماتية (معلقًا عليها)، دار النهضة العربية، ط٢، ص ١٣٠.

(٢) التقرير السنوي بمفوضية الأمم المتحدة السامية، أثر التكنولوجيا الجديدة في تعزيز حقوق الإنسان وحمايتها في سياق التجمعات، بما في ذلك الاحتجاجات السلمية، ٣ يونيو ٢٠٢٠.

مـن مثل هذا التدخل أو تلك الحمـلات»، وسار على هذا الـدرب العهد الدولي للحقوق السياسية والمدنية عام ١٩٦٦، حيث قضت المادة (١٧) منه على نفس ما جاء به الإعلان العالمـي لحقـوق الإنسان. كما عقدت العديد مـن الاتفاقات الإقليميـة الخاصة بحماية حقـوق الإنسان كالاتفاقية الأوروبية لحقوق الإنسـان وحرياته الأساسية عام ١٩٥٠ وما تضمنتـه المادة الثامنة منها مـن توفير حماية للحق في حرمة الحياة الخاصة، وكذلك ما تضمنه ميثاق الأمم المتحدة [١].

أما على المستوى الإقليمي فقد اعترفت العديد من الاتفاقيات بالحق في خصوصية البيانـات والمراسلات، ويدخل ذلك عبر تقنيـة الميتافيرس، ونظمت قواعد حمايته كما هـي الحال فـي الاتفاقيـة الأوروبية لحماية حقـوق الإنسان والحريـات الأساسية لعام ١٩٥٠، حيـث قـررت في المادة الثامنـة منها ١- لـكل إنسان الحق فـي احترام حرمة حياتـه الخاصة وحرمة منزله ومراسلاتـه. ٢- يمنع تدخل السلطة العامة في ممارسة الإنسـان لحقـه المذكور إلا في الأحـوال التي يبينهـا القانون، وفي حالـة حماية الأمن القومـي للمجتمع الديمقراطي، أو لحماية سلامـة الناس، أو للمصلحة الاقتصادية، أو لمنـع حالات الفوضى أو ارتكـب الجرائم، أو لحفظ الصحة والأخلاق العامة، أو لحماية ورعاية حقوق وحريات الآخرين.

وفـي هذا الشأن قالت المفوضية الأوروبية لحقـوق الإنسان عام ١٩٧٦ إن الحق في احـترام الحياة الخاصة هـو الحق في الخصوصية، ووفقًا لـرأي اللجنة فإن الحق في احـترام الحياة الخاصـة لا ينتهي هنا، بل يمتد إلى الحق في تأسيس وتطوير العلاقات مـع الأشخاص الآخرين. وكذلك الاتفاقية الأمريكية لحقـوق الإنسان في المادة (١١)، والتي جاء نصها مطابقًا - تقريبًا- للنص المقرر في الإعلان العالمي لحقوق الإنسان.

تهدف اللائحـة العامة لحماية البيانات التي أصدرهـا البرلمان الأوروبي والمفوضية الأوروبيـة «GDPR» اختصـارًا لـ General Data Protection Regulation إلى تقنـين عمليـة استخدام بيانـات الأفراد من قِبل الشركات الكبرى أو التـي تقوم على حيازة أو

(١) انظر: د/ شريف يوسف خاطر، حماية الحق في الخصوصية المعلوماتية، مرجع سابق، ص ٣٠.

معالجة بيانات الأفراد، وذلك من خلال وضع الإطار القانوني الذي يؤسس تلك العلاقة ويحميها من الخلل، كما يشرع لوجود سلطة مستقلة تراقب تنفيذ الآليات بشكل سليم وتسعى إلى تطوير حماية بيانات الأفراد، وكذلك الحق في الخصوصية، بالتوازي مع حرية حركة البيانات.

وتتكون اللائحة العامة لحماية البيانات من (٩٩) مادة تتوزع على (١١) فصلاً، تختص بإدراج التعريفات العامة وأحكامها، والمبادئ المتعلقة بعملية المعالجة، وحقوق صاحب البيانات، ونقل البيانات الشخصية إلى دول ثالثة أو منظمات دولية، وتؤسس أيضًا لوجود سلطات مستقلة تقوم بالإشراف على العملية القانونية، وذلك بدايةً من الفصل السادس حتى الفصل الأخير، مع مراعاة إدراج سبل الانتصاف والمسؤوليات، وكذلك آليات دفع الغرامات في حالة المخالفة القانونية.

وتركز اللائحة على الشركات التي تقوم بمعالجة البيانات الشخصية للمستخدمين لأغراض مختلفة، فهي لا تعتبر بالأشخاص، وإنما تسعى إلى تقنين عمل الشركات، وهو الأمر الذي يختلف عن القانون المصري الذي ينطبق على الأفراد فضلاً عن الشركات. ورغم اختلاف الديباجات، يشترك القانون المصري واللائحة الأوروبية في اعتبار الآراء السياسية والصحة النفسية، وكذلك بيانات الأطفال ذات درجة أعلى من الخصوصية، يصنفها القانون المصري على أنها بيانات شخصية حساسة، أمَّا اللائحة الأوروبية فتقوم بحظر معالجة أو حفظ مثل هذه المعلومات. كما تؤكد كلتا الجهتين: القانون واللائحة، على عدم استحواذ الشركات على بيانات المستخدمين بدون موافقة مسبقة من الشخص المعني بالبيانات، وحقه في مراجعة البيانات الشخصية التي تستحوذ عليها الشركات، وكذلك حقه في تعديلها أو إلغاء التعاقد مع تلك الشركات. كما ضمَّت اللائحة، وأكدت على بعض الحقوق الفرعية التي تضمن حماية البيانات الشخصية كالحق في الخصوصية، والحق في التعامل مع البيانات الشخصية كمسح البيانات أو تعديلها، والحق في النسيان، والحق في المعرفة، والحق في الخصوصية حسب التصميم الافتراضي لها، والحق في إمكانية الحصول على البيانات وإمكانية نقلها[1].

(1) https://gdpr-info.eu/art-4-gdpr/

وأشار التقرير السنوي لمفوض الأمم المتحدة السامي لحقوق الإنسان عن الحق في الخصوصية في العصر الرقمي[١]، أيضًا إلى التدخلات من قِبل الحكومات، وكذلك مؤسسات الأعمال التي تقوم بجمع مليارات البيانات الشخصية لمستخدمي المعاملات الإلكترونية، بالإضافة إلى سماسرة المعلومات الذين يتاجرون بالبيانات الشخصية للمستخدمين، الذين يجدون أنفسهم في موقف يستحيل من خلاله تتبع مسار بياناتهم الشخصية والمعلومات المتعلقة بهم وكذلك مسار استخدامها، خاصةً أننا أمام قدرة فائقة لتحليل البيانات، وتدوينها، وتتبع مسار الحياة اليومية للمستخدمين والتفاصيل الخاصة بحياتهم التي قد لا يريدون الإفصاح عنها.

وقد جاء في التقرير الخاص بمفوضية الأمم المتحدة لحقوق الإنسان وتعزيز الحقوق المدنية والسياسية بتوضيح أثر التكنولوجيا في تعزيز حقوق الإنسان، وخاصة الحقوق المتعلقة بالمجتمع والاحتجاجات السلمية وألقى الضوء على ضرورة تقوية المجتمعات الديمقراطية لمبدأ حماية البيانات الشخصية المتعلقة بالأفراد وخاصة ذات التوجه السياسي، حيث تقوم الحكومات الهشة بتتبع الأفراد ذوي النشاط السياسي، سواء عن طريق البريد أو الهواتف أو المواقع الخاصة بهم، ومن ثَمَّ يؤكد على أهمية ترسيخ حماية البيانات الشخصية داخل القانون، وخاصة إذا كان المجتمع يريد الحفاظ على هويته الديمقراطية[٢].

بالإضافة إلى ذلك تستند صناعة القوانين الخاصة بحماية البيانات الشخصية إلى المعايير الدولية كأساس ومرجع لها، مثل المبادئ التوجيهية لمنظمة التعاون والتنمية في الميدان الاقتصادي، واللائحة العامة لحماية البيانات الخاصة باللائحة الأوروبية «GDPR» والتي أصبحت أخيرًا ضمن المراجع المستند إليها في صياغة قوانين حماية البيانات الشخصية.

---

(١) التقرير السنوي بمفوضية الأمم المتحدة السامية، أثر التكنولوجيا الجديدة في تعزيز حقوق الإنسان وحمايتها في سياق التجمعات، بما في ذلك الاحتجاجات السلمية، ٣ يونيو ٢٠٢٠.

(٢) انظر: الأمم المتحدة، الجمعية العامة، مجلس حقوق الإنسان، الدورة الرابعة والأربعون ١٥ حزيران/يونيه – ٣ تموز/يوليه ٢٠٢٠ البندان (٢ و٣) من جدول أعمال التقرير السنوي لمفوضية الأمم المتحدة السامية لحقوق الإنسان تعزيز وحماية جميع حقوق الإنسان ، المدنية والسياسية والاقتصادية والاجتماعية والثقافية، بما في ذلك الحق في التنمية.
https://documents-dds- ny.un.org/doc/UNDOC/GEN/G20/154/33/PDF/G2015433.pdf?OpenElement

ومحل الاعتداء الإلكتروني – بصفة عامة – هي المعلومات المخزنة على المواقع، وهذه المعلومات ملك للأفراد أو للهيئات العامة في الدولة، والمواقع التي احتوت المعلومات قد تكون مواقع مجانية أو مواقع بمقابل مادي؛ ولذلك فإن إساءة استخدام هذه المواقع يعد انتهاكًا لخصوصية الأفراد، وسرية الشركات التجارية، أو اختراقًا لشبكات الأمن القومي، فضلًا عن الجرائم في المجال الاقتصادي في القطاعات البنكية والمالية، حيث ترتكب بطرق ذات تقنية عالية، منتهكةً بذلك الحقوق الفكرية والذهنية المرتبطة بهذه المواقع، وهي محمية بموجب قواعد اتفاقية (T.R.B.S) الدولية[١].

فالمعلومات التي يتم الوصول إليها عن طريق اختراق الموقع الذي تضمنها ليست بالشيء الملموس أو القابل للقياس، حتى يتم تداولها أو انتقالها من شخص لآخر؛ ولكن التكنولوجيا غيرت طريقة التعامل مع المعلومات حتى أضحى التعامل معها رقميًّا وطريق الحصول عليها إلكترونيًّا ومن ثَمَّ تداولها وانتقالها كالشيء محل الملكية[٢].

فهناك ضرورة لا غنى عنها في حماية الحق في المعلومات المخزنة على المواقع في الشبكة العالمية للمعلومات، فالمعلومات أصبحت عصب الحياة الاقتصادية والسياسية والاجتماعية والعلمية، بل وأضحى استخدام تقنية المعلومات من سمات وضرورات حسن التنظيم في كافة المجالات، وقد تأثرت كافة أنواع الأنظمة بهذا نتيجة لتغير طبيعة ونموذج الأشياء محل الحماية من مادية إلى معنوية[٣].

وبتطبيق ذلك على تقنية الميتافيرس فلا بد أيضًا من حماية المعلومات المخزنة إذا تم إساءة استغلالها عن طريق استغلال هذه التقنية، والتي تتحول من خلالها التصرفات المادية إلى معنوية عن طريق استخدام الأفاتار.

فإذا أخذنا اختراق المواقع كنموذج للاعتداءات الإلكترونية؛ لأهميته وشيوعه وأوليته على بقية أنواع الاعتداءات الأخرى، ولتزايد ذلك سنويًا من حيث الإحصاء الدولي

---

(١) انظر: د/ محمد حسام الدين لطفي : الحماية القانونية لبرامج الحاسب الإلكتروني، بحث مقدم لمؤتمر الكويت الأول، القانون والحاسب الآلي ٤ – ٧ نوفمبر ١٩٨٩م كلية الحقوق ، منشورات مؤسسة الكويت للتقدم العلمي، ١٩٩٤م، ص ٣٧ .

(٢) المرجع السابق ، ص ٣٨.

(٣) انظر: أسامة عبد الله قايد : الحماية الجنائية وبنوك المعلومات ، دار النهضة العربية القاهرة ط (٣) ١٩٩٤م، ص ٤.

والمحلي؛ لأمكننا من خلاله أن نحدد بدقة محل الاعتداء الإلكتروني، وهو ما يحمله هذا الموقع، فالاختراق، تجاوز غير مشروع لمكان معين محمي بأداة حماية، أو هو التسلل إلى المواقع لإلحاق الضرر بالمعلومات المخزنة فيه أو سرقتها أو نشر الفيروسات به[1].

وهـذا أيضًا ما ينطبـق على الأفاتار داخل تقنية الميتافيرس؛ حيث يمكن استخدام الأفاتار لاختراق المواقع، والذي يعد تجاوزًا غير مشروع لمكان معين محمي بأداة حماية، وكذلـك تسلل الأفاتـار إلى المواقع لإلحاق الضرر بالمعلومات المخزنـة فيه أو سرقتها أو نشر الفيروسات به.

المطلب الثاني

إشكالية مكافحة الجرائم الإلكترونية عبر تقنية الميتافيرس

تعتمـد تقنية الميتافيرس على تحويـل الإنترنت إلى بيئة ثلاثية الأبعاد لا يقتصر دور المستخـدم لها علـى النظر إليها أمـام شاشته، بل الدخول في هـذه البيئة بنفسه حتى يصبـح أحـد عناصرهـا، ولتنفصل حواسه عن عالمـه الحقيقي فترة بقائـه في العالم الافتراضـي، ومن خلال ذلـك يمكنه الوصول إلى المعلومات بشـكل غير قانوني كسرقة المعلومات أو حذفها والاطلاع عليها، بل والتمكن من الوصول بواسطة الشبكة العنكبوتية إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها أو التلاعب بمعطياتها.

ولابـد من بـذل جهود عديدة لمكافحة الجريمة الإلكترونية مـن قِبل الدول والأفراد، وتتجسـد أولى طـرق مكافحة الجرائـم الإلكترونية عبر الإنترنت فـي الاستدلال الذي يتضمـن كلاً مـن التفتيش والمعاينـة والخـبرة، والتي تعـود إلى خصوصيـة الجريمة الإلكترونية عبر الإنترنت. أما ثاني سبل مكافحة الجريمة الإلكترونية وهي تلك الجهود الدوليـة والداخليـة للوقايـة من الجرائـم المستحدثة، فأمـا الدولية فتتمثـل في جهود الهيئـات والمنظمات الدولية والتي تتمثل في تتبع تطورات الجريمة الإلكترونية ومواءمة التشريعات لمكافحتها.

وهـذا الأمر هو ما دعا الدول الأعضاء في مجلـس أوروبا وغيرها من الدول الموقعة

(١) انظر: حسن طاهر داود، جرائم نظم المعلومات ، أكاديمية نايف العربية، ط (١)، ١٤٢٠هـ / ٢٠٠٠م، ص ٢٤.

على هذه الاتفاقية [١] لتوقيع الاتفاقية الدولية الأولى لمكافحة الإجرام عبر الإنترنت في العاصمة المجرية «بودابست» عام ٢٠٠١م، والمعروفة بـ «اتفاقية بودابست» [٢]؛ نظرًا لخطورة الجرائم الإلكترونية على الفرد والمجتمع وتنوع أشكالها، فالجريمة الإلكترونية لا تحدها حدود الدول، وهذا من أهم الأسباب التي دعت إلى تعاون الدول للحد منها والسيطرة عليها ومواجهتها، كما أن بعض الدول سنت قوانين وتشريعات وطنية تُجرم وتعاقب على الجريمة الإلكترونية، كالقانون الاتحادي لدولة الإمارات العربية المتحدة رقم ٢ لعام ٢٠٠٦م[٣] وبعض الدول أطلقت تشريعًا سمَّته نظام مكافحة الجرائم المعلوماتية كالمملكة العربية السعودية، فقد أصدرت المملكة بمرسوم ملكي رقم م/١٧ بتاريخ ١٤٢٨/٣/٨هـ نظام مكافحة جرائم المعلوماتية المكون من ست عشرة مادة، وفي إطار جهود دول مجلس التعاون لدول الخليج العربية لتعاون دول مجلس التعاون، فإنه من الجدير بالذكر أن نتطرق لوثيقة الرياض للنظام الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون الخليج العربي، والمتكونة من تسع وثلاثين مادة [٤]، أما

(١) أحمد ، هلالي عبد اللاه (٢٠١١)، اتفاقية بودابست لمكافحة جرائم المعلوماتية (معلقًا عليها)، مرجع سابق، ص ١٣٠. إدراكًا من الدول بمدى خطورة الجريمة الإلكترونية بوصفها جريمة عابرة للحدود، فقد تم التوقيع عليها من ثلاثين دولة في العاصمة المجرية «بودابست» حيث إن بعض الدول الموقعة أعضاء في الاتحاد الأوروبي، إضافة إلى كندا، اليابان، جنوب أفريقيا، الولايات المتحدة الأمريكية، وجاءت هذه الاتفاقية لتعالج إشكالية دولية الجريمة الإلكترونية وتجاوزها للحدود الدولية بما يساعد الدول على مكافحة هذه الجريمة وتعقب مرتكبيها والمساعدة على الاستدلال عليهم وضبطهم، كما تشمل جوانب عديدة من جرائم الإنترنت من بينها الإرهاب، عمليات تزوير بطاقات الائتمان ... وغيرها.

(٢) العبيدي، عمر عباس، (٢٠٢١م)، مكافحة الجرائم الإلكترونية كآلية لتعزيز الأمن الإقليمي، مصر: مركز الدراسات العربية، ص١٧٧، وتعد هذه الاتفاقية هي الأولى من حيث اختصاصها بالجريمة الإلكترونية، حيث اعتمد المجلس الأوروبي الطابع الدولي للجرائم الإلكترونية منذ العام ١٩٧٦، ففي العام ١٩٩٦، أنشأت اللجنة الأوروبية لمشاكل الجريمة (CDPC) لجنة خبراء للتعامل مع مشاكل الجريمة الإلكترونية، وعملت اللجنة بين العامين ١٩٩٧، و٢٠٠٠ على مشروع الاتفاقية التي اعتمدها البرلمان الأوروبي في الجزء الثاني من جلسته العامة في شهر نيسان / أبريل ٢٠٠١، وتم التصديق على الاتفاقية من قِبل ٣٠ دولة بحلول العام ٢٠١٠، ودخلت حيز النفاذ في ٢٣-١١-٢٠٠١.
https://rm.coe.int/budapest-convention-in-arabic/1680739173

(٣) العبيدي، عمر عباس، (٢٠٢١م)، مرجع سابق، ص٩٤، صدر هذا القانون في ٣٠-١-٢٠٠٦م وقد تلاه عدة قوانين لا تقل عنه أهمية، منها ما صدر في إمارة دبي رقم ٥ عام ٢٠١٢م والمعدل بقانون اتحادي رقم ١٢ لعام ٢٠١٦م وقد حل مكان المرسوم بقانون رقم ٥ لعام ٢٠١٢م في شأن مكافحة جرائم تقنية المعلومات المرسوم رقم ٣٤ لعام ٢٠٢١م في شأن مكافحة الشائعات والجرائم الإلكترونية الذي احتوى على ٧٤ مادة قانونية.

(٤) مجلس التعاون لدول الخليج العربية، (٢٠١٣م)، وثيقة الرياض للنظام الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون لدول الخليج العربية، الرياض: مجلس التعاون لدول الخليج العربية، الأمانة العامة، للاستزادة والاطلاع على الوثيقة، https://nshr.org.sa/wp-content/uploads/2013/10/وثيقة-الرياض-للنظام-القانون-الموحد-لمكافحة-جرائم-تقنية-المعلومات-لدول-مجلس-التعاون-لدول-الخليج-العربية-،-٢٠١٣.pdf

فيما يخص التعاون الدولي العربي، فقد تم إبرام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وكذلك العديد من الدول بذلت جهودًا كبيرة في هذا الصدد[١].

وعلى مستوى التعاون الأمني بين الدول فقد أسهم الإنتربول الدولي[٢] في كشف العديد من الجرائم الإلكترونية، منها العملية التي نسقها الإنتربول في ٢٠٢٠م لكشف برمجية خبيثة تستهدف مواقع للتجارة الإلكترونية، وأسفرت عن تحديد مئات المواقع الإلكترونية الإجرامية، وأفضت إلى اعتقال ثلاثة أشخاص يستخدمون هذه البرمجية في إندونيسيا [٣].

ومن أبرز جهود الدول أيضًا على المستوى الإقليمي ما قام به حلف شمال الأطلسي من عقد تحالف أطلق عليه «التحالف السيبراني»، لاختبار قدرات قوات الناتو في مجال مواجهة الجرائم الإلكترونية [٤].

وعلى مستوى الوكالات المتخصصة فقد عُنى الاتحاد الدولي للاتصالات بإنشاء

---

(١) هيئة الخبراء بمجلس الوزراء، (٢٠٠٧م)، نظام مكافحة جرائم المعلوماتية، المملكة العربية السعودية المرسوم الملكي رقم م/١٧ بتاريخ ١٤٢٨/٣/٨هـ.

(٢) عبد الحفيظ، أيمن (٢٠٠٥م)، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، مكتبة الكتب العربية، ص ٢١٤. المنظمة الدولية للشرطة الجنائية «الإنتربول الدولي» منظمة حكومية دولية فيها ١٩٥ بلدًا عضوًا. مهمتها أن تساعد أجهزة الشرطة في جميع هذه الدول على العمل معًا لجعل العالم مكانًا أكثر أمانًا. ولهذا، فهي تمكّن البلدان من تبادل البيانات المتعلقة بالجرائم والمجرمين والوصول إليها، وتقدم الدعم الفني والميداني بمختلف أشكاله.

(٣) الموقع الإلكتروني للإنتربول الدولي https://www.interpol.int/ar. وفي تقرير للإنتربول الدولي ذكر مدير مكافحة الجريمة الإلكترونية «السيد كريغ جونز»: «إن الشراكات المتينة والفعالة بين الشرطة وقطاع الأمن السيبراني بالغة الأهمية لتتمكن أجهزة إنفاذ القانون في العالم أجمع من الحصول على المعلومات التي تحتاج إليها لمواجهة نطاق وتعقيد التهديدات الإلكترونية في يومنا هذا، وإن هذه العملية الناجحة ما هي إلا مثال على قدرة أجهزة إنفاذ القانون على التكيف واستخدام التكنولوجيا الجديدة لدعم التحقيقات والتوصل في نهاية المطاف إلى الحد من تبعات الجريمة السيبرية على الصعيد العالمي، وأن التحقيقات جارية في بلدان أخرى حيث يواصل الإنتربول مساعدة الشرطة لمعرفة مكان هذه الخوادم وكشف مواقع الإنترنت الملوثة وتحديد هوية الجناة الضالعين».

(٤) والذي شاركت فيه ٢٧ دولة من أصل ٢٩ من حلف شمال الأطلسي، و٦ دول متحالفة أخرى هي، اليابان والجزائر والنمسا وفنلندا وإيرلندا والسويد، والتي عقدت في الفترة من ٢ إلى ٦ ديسمبر ٢٠١٩. وقد مثل هذه الدول ٧٠٠ مختص من المختصين في الأمن السيبراني والتقنيين، والمسؤولين العسكريين، والحكوميين، وممثلي قطاع الأعمال، وفي هذا الخصوص، أعلن الأمين العام لحلف الناتو، ينس ستولتنبيرغ أن جميع محاولات الهجوم السيبراني على شبكات الحلف المحمية تم صدها في الفترة الأخيرة، ولم يؤثر أي من الهجمات على أنشطة المنظمة، مؤكدًا أنه يتم صد الهجمات بشكل يومي. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/What_is_NATO_ara_iraq_20200507.pdf.

فريق متخصص معني بالشبكات الذكية من أجل جمع وتوثيق المعلومات والمفاهيم التي ستكون مفيدةً من أجل إعداد توصيات لدعم تلك الشبكات في مواجهة التهديدات والجرائم الإلكترونية[١].

ومن أبرز الجهود الدولية سعي الأمم المتحدة من خلال وكالاتها وهيئاتها لوضع الإطار التشريعي للجرائم الإلكترونية، وكانت الانطلاقة في المؤتمر السابع عام ١٩٨٥م المنعقد بميلانو، الذي أكد على أهمية الاستفادة من التطورات العلمية والتكنولوجية في مواجهة الجرائم الإلكترونية بعد ذلك، وبرعاية منظمة الأمم المتحدة أكد وجوب حماية مخاطر التكنولوجيا، ووجوب التنسيق والتعاون بين الدول في المؤتمر التاسع في القاهرة عام ١٩٩٥م[٢].

وكذلك قرارات مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء ١٩٩٠ بشأن الجرائم ذات الصلة بالكمبيوتر[٣]؛ حيث حثت الدول أعضاء الأمم المتحدة على أن تكثف جهودها لمكافحة إساءة استعمال الحاسب الآلي، وذلك على المستويين الوطني والدولي[٤].

---

(١) الاتحاد الدولي للاتصالات هو وكالة متخصصة في قضايا تكنولوجيا المعلومات والاتصالات ونقطة التنسيق العالمية للحكومات والقطاع الخاص بشأن تطوير الشبكات والخدمات. ويتكون هذا الاتحاد من ١٩٣ دولة وما يزيد على ٨٠٠ من المؤسسات الأكاديمية والكيانات الخاصة، ويعتبر منبرًا «استراتيجيًا» للتعاون بين أعضائه باعتباره وكالة متخصصة داخل الأمم المتحدة حيث يعمل الاتحاد على مساعدة الحكومات في الاتفاق على مبادئ مشتركة تفيد الحكومات أو الصناعات التي تعتمد على تكنولوجيا المعلومات والبنية التحتية للاتصالات. ولوائح الاتصالات الدولية: الوثائق الختامية للمؤتمر الإداري العالمي للبرق والهاتف، الاتحاد الدولي للاتصالات الاسترجاع ٢٠٢٢/٩/١م.
http://www.itu.int/osg/spu/intset/

(٢) حسن، مريم محمد، (٢٠١٦م)، التنظيم القانوني لجريمة التجسس المعلوماتي، رسالة ماجستير، العراق: جامعة الكوفة، كلية القانون، ص١٦٢،

(٣) مؤتمر الأمم المتحدة لمنع الجريمة هو المحفل الأكبر والأكثر تنوعًا على مستوى العالم الذي يجمع الحكومات والمجتمع المدني والأوساط الأكاديمية والخبراء في مجال منع الجريمة والعدالة الجنائية. وكان لهذه المؤتمرات أثرها على مدار ستين عامًا، في سياسات العدالة الجنائية وفي تعزيز التعاون الدولي على التصدّي للمخاطر التي تهدّد العالم من جراء الجريمة المنظّمة العابرة للحدود الوطنية. من أجل التصدّي للتحدّيات الاجتماعية والاقتصادية وتعزيز سيادة القانون على الصعيدين الوطني والدولي ومشاركة الجمهور. وتعقد هذه المؤتمرات الدولية كل خمس سنوات ويعود منشؤها إلى عام ١٨٧٢م، وكانت هذه المؤتمرات تُعقد تحت رعاية اللجنة الدولية للسجون، التي أصبحت فيما بعد اللجنة الدولية للشؤون الجزائية والإصلاحية، ثم عقد مؤتمر الأمم المتحدة الأول في جنيف في عام ١٩٥٥م.
https://www.un.org/ar/events/crimecongress2015/.

(٤) تقرير الأمانة العامة للأمم المتحدة (منشورات الأمم المتحدة، (.A .٩١.IV الفصل الأول، الباب جيم-٩ ، مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، هافانا، ٢٧ آب/أغسطس – ٧ أيلول/ سبتمبر ١٩٩٠م، على المستوى الوطني=

كمـا أن تزايد الجرائم الإلكترونية بهذه الصورة دفع الجمعية العامة للأمم المتحدة إلى دعوة الدول إلى إبرام اتفاقية خاصة بمكافحة إساءة استعمال التكنولوجيا في عالم الجريمـة لسنة ٢٠٠٠م، والذي أكد الحاجة إلى التعزيـز والتنسيق والتعاون الدولي في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية [١].

أمـا على صعيـد الـدول الأوروبية، فقد بـدأت المحـاولات التشريعية لوضـع أحكام بخصوصـ مسؤولية متعهدي الإيـواء، ومن بينهم مزود وخدمـات وسائل التواصل بعد صـدور التوجيه الأوروبي رقم EC/٢٠٠٠/٣١ بخصوص بعض المسائل القانونية المتعلقة بالتجـارة الإلكترونية، والذي نصـ في المادتين (١٤ و ١٥) منه على بعض تلك الأحكام ورسـم حدودًا معينة للدول الأعضـاء بهذا الخصوص، ولعل من أهم الأحكام التي نص عليهـا التوجيه في هذا الصدد هو ما يسمى الملاذ الآمن Safe harbor الذي يقرر عدم توجيـه التشريعات الأوروبية من إلزام مـزودي خدمات التواصل، وغيرهم من متعهدي مسؤوليـة «متعهد الإيواء عن المحتوى غير القانوني الـذي يضعه المستخدم (٥٧) ، كما منع الإيواء، بالرقابة على المحتوى، أو البحث، أو التحقيق فيه إلا في حالات محدودة[٢].

والحقيقـة أن إعفاء منصـات التواصل من المسؤولية عن المحتوى غير المشروع، وفقًا

= حـث مؤتمـر هافانـا ١٩٩٠م الدول أعضـاء الأمم المتحدة على ضـرورة تجريم الأفعـال التي تنطوي علـى المساس بسلامة المعلومات أو البيانات المعالجة والمخزنة إلكترونيًا، كما دعا فيه الدول الأعضاء إلى النظر في عدد من التدابير، منها تحسين الأمـن الحاسوبـي واتخاذ تدابير وقائيـة، آخذة بعين الاعتبـار المشاكل المتصلـة بحماية الحُرمة الشخصيـة ومراعاة حقوق الإنسان وحرياته الأساسية وأي آليات تنظيمية تتعلق باستخدام الحواسيب.

أما جهود هذا المؤتمر على المستوى الدولي فنجد أنه قد حث الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الـدولي من أجل مكافحة الجرائم المتصلة بالكمبيوتـر بما في ذلك دخولها كأطراف في المعاهدات المتعلقة بتسليم المجرمين وتبـادل المساعـدة في المسائل الخاصـة المرتبطة بهذه الجريمة، وأن تتخـذ خطوات محددة نحو تحقيق هـذا الهدف، وذلك بضرورة وضع وتطوير معايير دولية لأمن المعالجة الآلية للبيانات، واتخاذ تدابير ملائمة لحل إشكاليات الاختصاص القضائي التـي تثيرهـا الجرائم الإلكترونية العابرة للحدود أو ذات الطبيعة الدولية، وإبرام اتفاقيات دولية تنطوي على نصوص تنظيم وإجـراءات التفتيش والضبـط المباشر الواقع عبر الحـدود، على الأنظمة الإلكترونيـة المتصلة فيما بينهـا والأشكال الأخرى للمساعدة المتبادلة مع كفالة الحماية في الوقت ذاته لحقوق الأفراد وحرياتهم وسيادة الدولة.

(١) قرار الجمعية العامة، الأمم المتحدة ٥٥/٦٣. (٢٠٠٢م). موقع الأمم المتحدة ٧-٣-٢٠٢٢م.
https://www.unodc.org/documents/treaties/a_res_56/121e.pdf

(٢) وقد جاء في المادة (١٥) من التوجيه الأوروبي:

«Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity....»

للتوجيه الأوروبي، يقوم على اعتبار أن الدور الذي تؤديه تقني محض ومحايد وليس لها أي دور إيجابي فعّال في ذلك المحتوى. كما أن عدم إلزامها – وفقًا لهذا التوجيه– بالرقابة الاستباقية على المحتوى من شأنه تعزيز فكرة الإعفاء من المسؤولية؛ لأن إلزامها بالرقابة الاستباقية من شأنه افتراض علمها بالمحتوى غير المشروع من جهة، ومن جهة أخرى قد يؤدى فرض هذا الالتزام إلى منح هذه المنصات سلطات واسعة نتيجة خوفها من التعرض للمسؤولية الناتجة عن أي محتوى غير مشروع (٥٣)، وقد أخذت الدول الأوروبية بهذا التوجيه، وأدرجت أحكامه ضمن تشريعاتها الوطنية.

وبناءً على ذلك فإن مكافحة الجرائم التي تتم من خلال سوء استخدام الميتافيرس تندرج تحت مسمى الجرائم الإلكترونية، والتي نظم المشرع لمكافحتها، قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ ولائحته التنفيذية رقم ١٩٦٦ لسنة ٢٠٢٠. وقد سبقه العديد من التشريعات التي تناولت تنظيم مجال التقنية المعلوماتية وكان من بينها قانون حماية الملكية الفكرية، وقانون التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات لتأمين معاملات الأفراد عبر شبكة المعلومات الدولية « الإنترنت» القانون رقم ١٥ لسنة ٢٠٠٤، وقانون تنظيم الاتصالات و تكنولوجيا المعلومات رقم ١٠ لسنة ٢٠٠٣ الخاص بتأمين ونقل وتبادل المعلومات.

ومن الضروري بناء الوعي الرقمي، وتعزيز أمن البيانات، استعدادًا لعالم الميتافيرس؛ لأن التقنية ما زالت في طور التكوين ولم تظهر إيجابياتها، كما لم تظهر سلبياتها بعد، ولكن سعي مارك زوكربيرج إلى التطبيق الفعلي للتقنية بإنشاء عالم افتراضي ثلاثي الأبعاد عبر ميتافيرس، 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 بُعد عبر الأجهزة الذكية، ولكن بالدخول إلى هذا العالم في شكل صورة متحركة تمثل الشخص أفاتار في العالم الافتراضي الثلاثي الأبعاد عبر تقنيات ميتافيرس، كما سيتيح عددًا من الفرص في مجالات التجارة والتدريب والتعليم والسياحة، وأيضًا عددًا من المخاوف في التأثير على الهوية والثقافة والتراث وحالة الاغتراب والتأثير على الجرائم، ومحاولات الانتحار،

والتطـرف، والإرهـاب، وتعزيز أمن البيانات، مـع استخدام الإعـلام والدراما لتعزيز المواطنة، وإعداد التشريعات المناسبة والبدء في إصدار عملة رقمية مشفرة.

ويمكـن أن يُحدث الميتافيرس ثورةً في جميع أنشطة الإنسان، وسيكون لها تداعيات تتعلـق بالإنسان وهويتـه وبخصوصية البيانات والمعلومات والمنظومـة الأخلاقية، ونشر العنف والإرهـاب والتطرف، لكن تلك التداعيات يمكـن استيعابها وتحويلها إلى فرص لحيـاة أكثر سعادةً ورفاهيـةً للإنسان، حـال استنفار ملكاته للتعامـل بطريقة إيجابية مـع التغيرات المحتملـة لشكل الحياة في عـالم الميتافيرس الذي سيشهـد مراحل أكثر تقدمًا[١].

ولم يقتصـر التطبيق الفعلـي للميتافيرس على الأفراد، بل سعت إلى ذلك الشركات والحكومـات، لا سيما بعد إعادة تسمية شركة فيسبوك باسم ميتا؛ بهدف التركيز على تطوير هذه التّقنيّة ، فقامت حكومة دولة جزيرة باربادوس، وهي جزيرة تقع في المحيط الأطلسـ، بالإعـلان عن قيام أوّل سفارة لها في هـذا العالم الافتراضي، ومن ثمّ يمكن اعتبار هذه الخطوة بداية التأريخ نحو إضفاء الشرعية على ميتافيرس[٢].

ولقـد صرّح سفـير جزيرة بابادوس فـي الإمارات العربية المتحـدة أن بلاده تعتزم التوسـع بقـوة إلى ما بعد هذا الجهد الأولي لبناء الهيـاكل وشراء الأراضي الرقمية في مجموعة متنوعة من العوالم الافتراضية، وبذلك ستصبح باربادوس أول دولة في العالم تعـترف بالأرض الرقمية ذات السيادة التـي ستكون متوافقة مع القانون الدولي وكذلك اتفاقية فيينا[٣].

(١) انظر: د/ إيهاب خليفة، مجتمع ما بعد المعلومات، تأثير الثورة الصناعية الرابعة على الأمن القومي، مركز المستقبل للأبحاث والدراسات المتقدمة، دار العربي للنشر والتوزيع القاهرة، ٢٠١٩، ص ١٢٥.

(٢) انظر الموقع على شبكة الإنترنت: https://arabic.sputniknews.com/20211115

(٣) اتفاقية فيينا للعلاقات الدّبلوماسيّة هي اتفاقيّة دوليّة أنشِئت بغية تحديد إطار العلاقات ، وما في ذلك من امتيازات البعثات الدّبلوماسيّـة وذلـك الدّبلوماسيّة بين دول العالم المستقل لتمكين الدّبلوماسيّين مـن أداء وظائفهم دون تخوف، وبعبارةٍ أخرى منحهـم الحصانـة الدبلوماسيّـة، وتعد بنودها العمـود الفقريّ الرّئيس للعلاقـات الدّوليّة، في العصـر الحديث. وقد دخلت اتفاقية فيينا حيّز التّنفيذ بشكل رسميّ في ٢٣ يناير عام ١٩٨٠.

المبحث الثاني

الآليات الدولية لمواجهة الجرائم الإلكترونية المرتكبة عبر تقنية الميتافيرس

تمهيد وتقسيم:

ابتداءً من عام ١٩٧٨ بدأت منظمة التعاون الاقتصادي والتنمية وضع أدلة وقواعد إرشادية بشأن حماية الخصوصية ونقل البيانات، وقد تم تبني هذه القواعد من قِبل مجلس المنظمة في عام ١٩٨٠ مع التوصية للأعضاء بالالتزام بها، ولا تعد هذه القواعد إلزامية وإنما مجرد إرشادات وتوصيات، وتغطي هذه القواعد الأشخاص الطبيعيين فقط وتطبق على القطاعين العام والخاص، وتتعلق أيضًا بالبيانات المعالجة آليًا أو غير المعالجة آليًا.

وبدأت أنشطة الإسكوا عام ٢٠٠٧م بهدف تطوير وتنسيق التشريعات الإلكترونية في المنطقة العربية وتطبيقها على أرض الواقع، ويجري التركيز على موضوع الأمن السيبراني ومكافحة الجريمة الإلكترونية؛ نظرًا لأهمية هذا الموضوع لتطوير وبناء مجتمع المعرفة في المنطقة العربية، فقد قامت الإسكوا بتنفيذ مشروع إقليمي تحت عنوان " تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية" بين عامي ٢٠٠٩ و٢٠١٢، حيث نتج عنه مجموعة من المخرجات أبرزها إرشادات الإسكوا للتشريعات السيبرانية. وقد توسعت هذه الإرشادات في الشق التشريعي، حيث قدمت نصوصًا نموذجية للقوانين السيبرانية تتيح للدول في المنطقة العربية الاستفادة منها وتكييفها أو الاعتماد عليها في صياغة قوانينها الوطنية[١]. وتستلزم الدراسة في هذا المبحث تناوله وفقًا للتقسيم التالي:

(١) الأمم المتحدة، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، دراسة بعنوان: «الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية»، E/ESCWA/TDD/2015/1 9 February 2015. على الرابط التالي: https://digitallibrary.un.org/record/1293274?ln=ar

المطلب الأول

الصعوبات التي تواجه المنظومة القضائية إزاء الجرائم الإلكترونية

مـن إشكاليات الجرائم المعلوماتية أنها تتميز في أكثر صورها بأنها مستترة وخفية لا يلاحظهـا المجنـي عليـه غالبًا، وقد لا يشعـر حتى بوقوعهـا، فهي غالبًا مـا تكتشف بمحض الصدفـة، ولذلك توصف بـ «الجريمة غـير المرئية»، ومما يزيـد الأمر تعقيدًا هـو أن الجريمة المعلوماتية إنما تتم عن بعـد، ومن ثَمَّ تتباعد غالبًا المسافات بين الفعل والنتيجة[١].

كمـا أن الدليل الرقمي في هذه الجرائم غالبًا ما يكون في صورة نبضات إلكترونية غـير محسوسـة، وهذا يتطلـب من المحقـق أن تكون لدية درايـة علمية كافيـة بأنظمة الحاسـب وماهيـة عملها؛ حتى يتسنـى له التعامل معهـا للبحث عن الأدلـة والمحافظة عليه.[٢]

كمـا أن المجـرم في هذه الجرائم يحاول -قدر الإمـكان- إعاقة الوصول إلى الدليل بشتـى الوسائل، فهو بعد ارتكاب جريمته يقوم بتزييـف البرامج، أو وضع كلمات سرية ورمـوز تعوق الوصول إلى الدليـل، أو يلجأ إلى تشفير التعليمـات؛ مما يصعب الوصول إلى دليل يدينه، حيث إن من السهل على المجرم - في أغلب الجرائم المعلوماتية - محو الدليـل في زمن قياسـي، ولا يستغرق ذلك سـوى دقائق معـدودة بالاستعانة بالبرامج المخصصة لذلك [٣].

كما تعد مراقبة المراسلات والتنصت على المحادثات الهاتفية من أخطر الإجراءات التـي قد يتم اللجـوء إليها في مرحلتي التحري وجمع الاسـتـدلالات والتحقيق القضائي لكشف الجرائم، أو الوصول إلى الحقيقة، ونسبة الجريمة إلى فاعلها.

---

(١) انظـر: د/ هشـام فريد رسـتم، قانون العقوبات ومخاطـر تقنية المعلومات، مكتبـة الآلات الحديثة، الطبعـة الأولى، ١٩٩٥م، ص٤٧٠.

(٢) انظر: د/ أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، مكتبة الكتب العربية ٢٠٠٥م، ص ٢١٤.

(٣) انظر: د/عزة على محمد الحسن، جرائم المعلوماتية في القانون السوداني، بدون ناشر، ص ١١.

لذلك استوجب أن تلحق تلك الإجراءات ضمانات، حتى لا تتعرض الحرية الشخصية والحياة الخاصة للاعتداء. وتتمثل هذه الضمانات في عدد من الضوابط يجب أن تتم المراقبة من خلالها. وقد أوضحت ذلك الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية لعام ١٩٩٠، حيث أشارت إلى أن: «لكل فرد الحق في أن تُحترم خصوصيته، وألا تتدخل السلطات العامة في ممارسة هذا الحق إلا وفقًا للقانون، ولمقتضيات المجتمع الديمقراطي، ولمصلحة الأمن القومي، أو الأمن العام، أو المصالح الاقتصادية للبلاد، أو لمنع الفوضى والجريمة، أو لحماية الصحة، أو الأخلاق، أو لحماية حقوق الآخرين وحرياتهم».

وكذلك أشار لذلك الدستور المصري في المادة (٤٥) إلى أن لحياة المواطنين الخاصة حرمة يحميها القانون، وأن للمحادثات الهاتفية وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا يكون مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، وفي مدة محدودة وفقًا لأحكام القانون.

فالغرض الذي من أجله أجازت التشريعات المراقبة للمراسلات والمحادثات الهاتفية هو تسجيل تلك المكالمات، أو ضبط هذه المراسلات التي تكون لها علاقة بإحدى الجرائم الجاري التحقيق بشأنها، ومن ثَمَّ لا بد أن تكون تلك الإجراءات ضرورية لكشف الحقيقة، وأن تتم إجراءات التنصت والمراقبة وفق ضوابط وشروط سنها القانون لصحة هذا الإجراء.

ومن ثَمَّ نتناول في هذا المطلب الصعوبات التي تواجه السلطات أثناء التحقيق والإثبات في الجرائم الإلكترونية، وذلك على النحو التالي:

التحقيق الابتدائي:

يتمثل التحقيق الابتدائي في مجموعة الإجراءات التي تباشرها السلطة المختصة بتحقيق الدعوى عن جريمة ارتكبت لكشف الحقيقة، وذلك بالبحث والتنقيب عن الأدلة وتجميعها وتقديرها لإثبات حدوث الجريمة ونسبتها إلى المتهم، لتحديد مدى كفايتها لإحالة المتهم للمحاكمة، أو لنفي ذلك كأساس للأمر بإقامة الدعوى.

ولا شـك أن هناك مشكلات عمليـة وفنية تواجه الجهود المبذولـة لمكافحة الجرائم المعلوماتيـة -بصفة عامة- على المستوى الإجرائي، فمن ناحية يصعب الكشف عن هذه الجرائم، ومن ناحية أخرى قد يستحيل جمع الأدلة بشأنها، وهو ما يظهر عقبات عديدة فـي إجراءات التحقيق سواء خلال الانتقال والمعاينـة، أو ندب الخبراء، أو الشهادة، أو التفتيش والضبط.

فالمعاينـة، وإن كانت واردة في كافة الجرائم إلا أنها قد تكون دون جدوى، إذا كانت الجريمـة بطبيعتها لا تستلـزم هذا الإجراء، مثل الجرائم الإلكترونية، خاصة إذا ما تم الاقتصـار على الاطـلاع أو التنصت، دون أن يتعداه إلى معالجـة البيانات، إذ تتضاءل أهميـة المعاينة في هذه الحالة بسبـب طبيعتها الخاصة التي غالبًا لا تخلف آثارًا مادية تترتـب عليهـا أدلة جنائية من جهة، ومن جهة أخرى، فـإن المتهم بالجريمة المعلوماتية غالبًـا ما يكـون قد تخلصـ، أو أتلف الآثـار المادية للجريمـة، كما أن عـددًا كبيرًا من الأشخاص قد يكون تردد على مسرح الجريمة، وذلك ما بين فترة وقوع الجريمة وفترة اكتشافها مما يصعب معه تحديد الجاني[١].

وتحتـاج هـذه الجرائم إلى الخـبرة، والتي هي وسيلـة من وسائل الإثبـات التي يتم اللجوء إليها إذا اقتضى الأمر كشف دليل، أو تعزيز أدلة قائمة، كما أنها تعتبر استشارة فنيـة يستعين بهـا القاضي، أو المحقق فـي مجال الإثبات لمساعدته فـي تقدير المسائل الفنيـة، التي يحتـاج تقديرها إلى مسائل فنيـة لا تتوافر لدى عضـو السلطة القضائية المختص بحكم عمله وثقافته[٢].

ومن ثَمَّ تعد الجرائم المعلوماتية من الجرائم التي تتعلق بمسائل فنية وتقنية متطورة جـدًّا تحتاج إلى خبير على درجـة عالية من الذكاء والفطنة والخبرة الكبيرة في مجال

(١) انظر: أ/ أيها محمد التاج، التحقيق وجمع الأدلة في الجرائم المعلوماتية، مجلة العدل، وزارة العدل، السودان، مجلد (١١)، عدد (٢٦)، دار المنظومة، ٢٠٠٩، ص ٣٩٥.

(٢) انظر: عبد الحليم بن باردة، إجراءات البحث والتحري عن الجريمة المعلوماتية، مجلة الحقوق والعلوم الإنسانية، عدد (٢٣)، دار المنظومة، ٢٠١٥، ص ٨٢.

تخصصه، ولذا فإن أغلب جرائم المعلومات تحتاج إلى الاستعانة بالخبرة لمساعدة جهات التحقيق في كشف الجريمة وفي حصر الأدلة وترتيبها[١].

التفتيش:

بالنسبة للتفتيش فالمحل الذي يقع عليه التفتيش في الجرائم المعلوماتية هو جهاز الحاسب الآلي بمكوناته المادية، وشبكات الاتصال الخاصة به (الخادم، والمزود الآلي، والملحقات التقنية)، وقد يكون الشخص الذي يتم تفتيشه من مستخدمي أو مستغلي الحاسب الآلي، أو من خبراء البرامج، أو من مهندسي الصيانة والاتصالات، أو من مدير النظم المعلوماتية، أو أي شخص يكون بحوزته أجهزة، أو معدات معلوماتية، أو أجهزة محمولة، أو تليفونات متصلة بجهاز المودم[٢].

ومن ثَمَّ ففي نطاق الجرائم الإلكترونية لجهة التحقيق المختصة البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقًا لغرض الضبط. كما لها أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات، أو معلومات تتعلق بنظام معلوماتي، أو جهاز تقني، موجودة تحت سيطرته، أو مخزنة لديه، وكذا بيانات مستخدمي خدمته وحركة الاتصالات التي تمت على ذلك النظام، أو الجهاز التقني[٣].

وفى كل الأحوال، يجب أن يكون أمر جهة التحقيق المختصة مسببًا، ويكون استئناف الأوامر المتقدمة أمام المحكمة الجنائية المختصة منعقدة في غرفة المشورة في المواعيد، ووفقًا للإجراءات المقررة بقانون الإجراءات الجنائية، ويشترط القانون للقيام بهذا أن تصدر جهة التحقيق المختصة أمرًا مسببًا، لمأموري الضبط القضائي، لمدة لا تزيد على ثلاثين يومًا قابلة للتجديد لمرة واحدة، متى كان له أثر في معرفة الحقيقة[٤].

---

(١) انظر: د/ عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر، دار الكتب القانونية، ٢٠٠٧، ص ٣٢٩-٣٣١.

(٢) انظر: د/ أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، مرجع سابق، ص ٩٩.

(٣) المادة (٦، ف/ ٢) المعنونة بـ «الأوامر القضائية المؤقتة» الباب الثاني من قانون مكافحة جرائم تقنية المعلومات.

(٤) المادة (٦، ف/ ٣) نفس الموضع السابق.

ومـن ثَـمَّ، لابد من وجود هـدف من وراء اتخاذ تلـك الإجراءات، يتمثـل في إظهار الحقيقة، ولا يشترط أن تكون المراسلات المضبوطة صادرة من المتهم، بل يجوز أن تكون موجهة إليه، ويستوي أن يكون كشف الحقيقة لصالح المتهم، أو ضده، فغاية الإجراءات الجنائية الوصول إلى الحقيقة.

ولا شك في أن ضرورة تسبيب الأمر، أو الإذن بالمراقبة، يعد قيدًا على الجهة مصدرة هـذا الأمر، كذلك يعد التسبب ضمانًا لعدم انتهـاك حرمة الشخص محل المراقبة، إلا إذا كانت هناك أسباب جدية تبرر اتخاذ مثل هذا الإجراء، فلا يطلق العنان في إصدار هذا الأمر دون تحقق من توافر المبررات التي يستند إليها في مثل هذا الإجراء الخطير. كمـا حدد المشرع هذه الفترة الزمنية بما لا يتجاوز ثلاثـين يومًا، قابلة للتجديد، وذلك من طرف قاضي التحقيق، وطبقًا لمجريات هذا الأخير.

ويعـد الضبـط في مجـال الجريمـة المعلوماتية أثـرًا للتفتيش، وهو وضـع اليد على الدعائـم المادية المخزنة فيها البيانات الإلكترونية، أو المعلومات، التي تتصل بالجريمة المعلوماتية التي وقعت، وتفيد في كشف الحقيقة عنها وعن مرتكبيه.

ونصـت اتفاقية بودابسـت ٢٠٠١م لمكافحة الجرائـم الإلكترونية في المـادة (٢٣) على ضـرورة تبادل المعلومات ووجـوب التعاون الدولي بين الدول الأطـراف وتقليل ما يعوق ذلك [١]، ولضمـان سرعة التعاون الدولي فقد نصت الاتفاقية فـي المادة (٢٥) بأنه يمكن للدول الأطراف في حالة استعجالهم استخدام الوسائل السريعة كالفاكس والبريد الإلكتروني [٢].

كما ورد وجوب تبادل المعلومات الخاصة بكافة جوانب الجريمة في بنود المادة (١٨) من اتفاقيـة الأمم المتحدة لمكافحة الجريمة المنظمة العابـرة للحدود[٣]، ونصت المادة الأولى من اتفاقية الرياض العربية للتعاون القضائي العربي فيما يخص تبادل المعلومات

(١) المادة (٢٣) من اتفاقية بودابيست لمكافحة الجرائم المعلوماتية. (٢٠٠١م)، للاستزادة الاسترجاع ٢٠٢٢/٩/١٦م https://rm.coe.int/budapest-convention-in-arabic/1680739173.

(٢) الفقرة (٢) من المادة (٢٥) من اتفاقية بودابيست لمكافحة الجرائم المعلوماتية. (٢٠٠١م)، للاستزادة الاسترجاع ٢٠٢٢/٩/١٦م https://rm.coe.int/budapest-convention-in-arabic/1680739173.

(٣) المـادة (١٨) مـن اتفاقيـة الأمم المتحـدة لمكافحـة الجريمة المنظمة عـبر الوطنية والبروتوكـولات الملحقة بهـا، (٢٠٠٠م)، للاستزادة الاسترجاع، ٢٠٢٢/٩/١٦م.
https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-a.pdf

«تتبادل وزارات العدل لدى الأطراف المتعاقدة بصفة منتظمة نصوص التشريعات النافذة والمطبوعات والنشرات والبحوث القانونية والقضائية والمجلات التي تنشر فيها الأحكام القضائية، كما تتبادل المعلومات المختلفة بالتنظيم القضائي»[١].

وأقرت الاتفاقيات الإقليمية والدولية بأن نقل الإجراءات يُعد من صور التعاون القضائي الدولي، كمعاهدة الأمم المتحدة النموذجية فيما يخص نقل إجراءات المسائل الجنائية [٢]، وكما ورد في المادة (٢١) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ٢٠٠٠م[٣]، وما ورد في المادة ٩ من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي ١٩٩٩م[٤]، والمادة (١٦) من النموذج الاسترشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي ٢٠٠٣م[٥].

المطلب الثاني

المعالجة التشريعية للجرائم الإلكترونية المرتكبة عبر تقنية الميتافيرس

اختلاف الأنظمة القانونية للدول تُعد من الإشكاليات التي تواجه التعاون الدولي في مواجهته للجرائم السيبرانية، لما يترتب على ذلك من صعوبات في تطبيق القانون، بالإضافة إلى أن اختلاف أنظمة الدول في تحديد مفهوم الجرائم الإلكترونية يؤدي إلى اختلافهم في وضع العقوبات المناسبة لها، حيث إن سياسة التجريم تترتب على مفهوم الجريمة وأركانها وشروطها الواقعة على الجريمة ومرتكبها.

---

(١) اتفاقية الرياض العربية للتعاون القضائي(١٩٨٣م) والتي وافق عليها مجلس الوزراء العرب على بقراره رقم ١ بتاريخ ٦ إبريل ١٩٨٣، للاستزادة والاطلاع على الاتفاقية، الاسترجاع ٢٠٢٢/٩/١٦م، https://www.tahkeem.ae/contents/files/rule_c.pdf.

(٢) اتفاقية نقل الإجراءات في المسائل الجنائية معاهدة نموذجية بشأن نقل الإجراءات في المسائل الجنائية اعتمدتها الجمعية العامة للأمم المتحدة بموجب القرار رقم سي/١١٨ الصادر بتاريخ ١٩٩٠/١٢/١٤م.

(٣) المادة (٢١) من قرار الجمعية العامة، الأمم المتحدة ٥٥/٢٥، اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية. (٢٠٠٠م)، للاستزادة الاسترجاع ٢٠٢٢/٩/١٦م، https://www.unodc.org/pdf/crime/a_res_55/res5525a.pdf.

(٤) المادة (٩) من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي، والتي اعتمدت من قبل مؤتمر وزراء الخارجية دول المنظمة المنعقد في أواغادوغو المنعقد خلال الفترة من ١٩٩٩/٦/٢٨م إلى ١٩٩٩/٧/١م.

(٥) وافق أصحاب المعالي وزراء العدل على النموذج في اجتماعهم الخامس عشر المنعقد في الدوحة بتاريخ ٢٠٠٣/٩/٣٠م و١/١٠/ ٢٠٠٣م، وتم اعتماده من قبل المجلس الأعلى في دورته الرابعة والعشرين (الكويت، ديسمبر ٢٠٠٣)، لتسترشد به الدول الأعضاء عند إعداد اتفاقياتها في مجال التعاون القانوني والقضائي.

قصـور المعالجـة التشريعية للجرائـم السيبرانية، وذلك يعني عـدم كفاية القوانين وعدم وجود نظام قانـوني خاص بمواجهة الجرائم الإلكترونية لدى الدول، على الرغم من أن أول حادثة لإساءة استخدام الكمبيوتر حدثت في عام ١٩٥٩م، إلا أن التشريعات لم تبـدأ بوضـع قوانينهـا إلا بعـد ذلك بأعـوام عديدة، فبـدأت بعض الـدول بتحديث تشريعاتها في أواخر السبعينيات ومطلع الثمانينيات، لكنها لم تشمل كل ما يندرج تحت مسمى الجرائم السيبرانية، وبقيت إلى وقتنا الحاضر يتخللها بعض النقص(١).

يتبايـن موقـف القانـون المقـارن من دولـة لأخرى من حيـث القصور فـي المعالجة التشريعيـة، حيث إنه يتفـرع إلى عدة فروع، فهناك الدول التـي تحتوي دساتيرها على نصوص صريحة تكفل الحماية في مواجهة أخطار الجرائم السيبرانية، وهناك بعض الدول التي لجأت إلى وضع تشريعات خاصة بالحماية من الجرائم الإلكترونية(٢).

وكذلك انعـدام وجود نظام قانوني داخلي مختص بالجرائم الإلكترونية لدى الدول وعـدم قدرتها علـى ملاحقة التحديـث المستمر للجرائـم الإلكترونية وحصـر تفشيها ووضع حد نهائي لتوغلها، لا يمكنها من التوافق مع غيرها من الدول حول تجريم إساءة استخـدام التكنولوجيا مما يشـكل عائقًا كبيرًا أمام التعاون الدولي، حيث إن ترك هذه الجرائـم ليتم تطبيقها من قِبل جهات إنفاذ القانون لا يتلاءم مع الطبيعة التقنية لهذه الجرائـم(٣)؛ الأمر الـذي يجعلنا على يقين من فشـل التحقيقـات والمحاكمات باعتبار أن النصوص الجزائيـة والإجـراءات يسودها مبدأ الشرعية « لا جريمـة ولا عقوبة إلا بنـص». وعدم النص على جميع الجرائـم الإلكترونية -والتي تهـدد أمن الدول- يؤثر ذلك على متخذي القرار في مختلف المجالات وخاصة السياسية، وذلك مما يؤثر سلبًا علـى التوجه السياسي للدول والفكـر القانوني والتجريم والعقـاب في مختلف المجتمع الدولي(٤).

ويعـد مبدأ الشرعية الجنائية من المبادئ الثابتة الراسخة في القانون الجنائي في

(١) العبيدي، عمر عباس، (٢٠٢١م)، مصدر سابق، ص٧٧.

(2) Frayssinet, Jean. (1977). l'informatique et le secret des fichiers. France: Press Universitaires de France.P176.

(٣) خراشي، عادل عبدالعال، (٢٠١٥م)، مصدر سابق، ص٢٣٥.

(٤) موسى، سامح أحمد، (٢٠١٠م)، مصدر سابق، ص ٥١٨-٥٢٣.

معظم التشريعات الوطنية، فصلاحية القاضي الجنائي محدودة بالنص التشريعي، فهو لا يملك صلاحية إكمال تشريع ناقص، أو استبدال العقوبة، أو خلق نص تشريعي، أو القياس عليه؛ وذلك لضمان إرساء قواعد العدالة الجنائية.

لذلك استقر الفقه القانوني - في كثير من الدول- على ضرورة وجود نصوص قانونية مستحدثة تعمل على معالجة الجرائم المعلوماتية بصفة خاصة، وهو ما أوصى به المجلس الأوروبي لتشجيع الدول على اعتناق تشريع خاص للحد من الجريمة المعلوماتية، وهو ما دعا بعض الدول إلى تبني قانون خاص للحد من هذه الجريمة، بينما قام البعض الآخر بدمج بعض النصوص في قانون العقوبات التقليدي.

وأما بالنسبة لدور بعض الدول العربية في مواجهة الجرائم الإلكترونية نلاحظ أن دولة الإمارات العربية تبنت قانونًا مختصًّا بمكافحة الجرائم المعلوماتية، ويعد من القوانين النموذجية التي اشتملت على أغلب الجرائم المعلوماتية وصدر عام ٢٠٠٦ وتم تعديله عام ٢٠١٢، وتنص المادة (٨) من قانون مكافحة جرائم تقنية المعلومات ٢٠٠٦ على أن: «كل من تنصت، أو التقط، أو اعترض عمدًا دون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، يُعاقَب بالحبس وبالغرامة، أو بإحدى هاتين العقوبتين».

كما صدر نظام مكافحة الجرائم الإلكترونية في المملكة العربية السعودية عام ٢٠٠٧ وتم تعديله سنة ٢٠١٥ [(١)]. ويعاقب النظام السعودي في شأن مكافحة جرائم المعلوماتية على التجسس، حيث نصت المادة الثالثة منه على أن: « يعاقب بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد عن خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين كل شخص يقوم بالتنصت على ما هو مرسل عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي- دون مسوغ نظامي صحيح -، أو التقاطه، أو اعتراضه».

أما المادة السابعة فنصت على أنه: «يعاقب بالسجن مدة لا تزيد عن أربع سنوات

(١) انظر: ناصر بن محمد البقمي، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، مركز الإمارات للدراسات والبحوث الاستراتيجية، سلسلة محاضرات الإمارات، ١١٦، ص ٣٣-٤٠.

وبغرامــة لا تزيد عن ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب جريمــة الدخــول غير المشروع إلى موقــع إلكتروني، أو نظام معلوماتــي مباشرة، أو عن طريــق الشبكــة المعلوماتية، أو أحد أجهــزة الحاسب الآلي للحصــول على بيانات تمس الأمن الداخلي، أو الخارجي للدولة، أو اقتصادها الوطني».

وتجدر الإشــارة إلى أنه يمكن الاستعانة بالقانون العربــي النموذجي بشأن مكافحة جرائم الحاسوب والإنترنت وما في حكمها، حيث وضع هذا القانون القواعد الأساسية التي يتعين على المشرع العربي اللجوء إليها عند سن قانون وطني لمكافحة هذه الجرائم ســواء كان القانون الوطنــي مستقلًا لمكافحة هــذه الجرائم المستحدثــة أم كان تعديلاً لقانون العقوبات المطبق بالفعل في، أي دولة عربية. وقد أشار هذا القانون الاسترشادي لأنــواع الجرائم التي تقع بطريــق الحاسوب والإنترنت بصفة عامــة ومحددًا عقوباتها وأحــال إلى التشريــع الوطني كل ما يتعلق بأركان هذه الجرائــم، وكذلك العقوبات التي تطبق عليها [1].

وفــي القانون الفيدرالي للولايات المتحــدة الأمريكية، أقر المشرع حماية خاصة إزاء التنصت غير المشروع، حيث نص على أن: « غرامة قدرها عشرة آلاف دولار على الأكثر، أو بعقوبــة السجــن خمس سنوات على الأكــثر، أو بالعقوبتين معًــا، كل من: (١) يحاول التنصــت عن عمد علــى أي اتصال شفهــي، أو تليفوني، أو تلغرافــي، أو يكلف شخصًا للقيــام بذلــك، أو محاولة القيام بذلــك. (٢) يستخدم، أو يحــاول استخدام عن عمد، جهــاز إلكتروني، أو ميكانيكي، أو غــيره، للتنصت على اتصال شفهي، أو يكلف شخصًا آخر للقيام بذلك، أو محاولة القيام بذلك.

وفي المملكة المتحدة حيث لا توجد تشريعات مكتوبة تعالج ظاهرة الجرائم المعلوماتية، وذلك بسبب كــون النظام القانوني الإنجليزي يعتمد علــى السوابق القضائية، غير أنه فــي عــام ١٩٩٠ صدر فــي المملكة المتحدة قانون تحــت مسمى قانون إســاءة استخدام

(١) تم إعــداد هذا القانون الاسترشادي من قبــل لجنة مشتركة بين المكتب التنفيذي لمؤتمر وزراء العدل العرب والمكتب التنفيذي لمؤتمر وزراء الداخلية العرب في نطاق الأمانة العامة لجامعة الدول العربية وتم إقراره في عام٢٠٠٣.

الكمبيوتر، تناول المسئولية الجنائية الناشئة عن الجرائم المعلوماتية في القسم الثامن عشر من خلال ثلاثة بنود، تضمن البند الأول الدخول المحظور على مواد الكمبيوتر، وتناول الثاني الدخول الثاني المحظور بقصد التسهيل والتحريض على الجرائم، واحتوى الثالث جرائم حظر تبديل، أو تحويل مواد الكمبيوتر[١].

وتمت معالجة الجرائم الإلكترونية في القمة العالمية لمجتمع المعلومات التي أُقيمت في تونس عام ٢٠٠٥م، حيث أكدت على ضرورة التعاون الدولي لمواجهة الجرائم السيبرانية، استجابةً لتكليف رؤساء الدول والحكومات وغيرهم من قادة العالم، والدول الأعضاء المشاركين في القمة العالمية لمجتمع المعلومات، أعلن الأمين العام للاتحاد في عام ٢٠٠٧م إطلاق البرنامج العالمي للأمن السيبراني (GCA) [٢]، كإطار للتعاون الدولي للحفاظ على الأمن السيبراني[٣].

ويوفر الاتحاد الدولي للاتصالات «ITU» الذي يضم ١٩٢ دولة و٧٠٠ شركة من القطاع الخاص والمؤسسات الأكاديمية منبرًا «استراتيجيًا» للتعاون بين أعضائه باعتباره وكالة متخصصة داخل الأمم المتحدة [٤]. ويعمل الاتحاد على مساعدة الحكومات في الاتفاق على مبادئ مشتركة تفيد الحكومات والصناعات التي تعتمد على تكنولوجيا المعلومات والبنية التحتية للاتصالات. وقد وضع الاتحاد الدولي للاتصالات مخططًا لتعزيز الأمن السيبراني العالمي يتكون من أهداف رئيسية تتمثل في[٥]:

- وضع استراتيجيات لتطوير نموذج التشريعات المعلوماتية يكون قابلاً للتطبيق محليًا وعالميًا بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة، ولتحديد الحد الأدنى المقبول عالميًا في موضوع معايير الأمن ونظم تطبيقات البرامج والأنظمة، لوضع آلية عالمية للمراقبة والإنذار المبكر مع ضمان قيام التنسيق عبر

(١) لمزيد من التفصيل انظر د. أحمد خليفة الملط، مرجع سابق، ص١٦٨ وما بعدها، ود/ شيماء عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، بدون ط، ٢٠٠٧، ص٩٤-٩٧.

(٢) الأجندة العالمية للأمن السيبراني (Global Cybersecurity Agenda)، هي إطار التعاون الدولي تعمل على تعزيز الأمن السيبراني ويتمثل دورها الأساسي في بناء الثقة والأمن في استخدام التكنولوجيا والاتصالات في مجتمع المعلومات.

(3) Gercke, Marco. (2012). Previous Source. P120-121.

(٤) الموقع الرسمي للاتحاد الدولي للاتصالات «ITU»: http://www.itu.int

(5) Weber, Rolf H & Heinrich, Ulrike I. (2012). Anonymization. New York. USA: Springer.P54.

الحـدود، وإنشاء نظام هوية رقم عالمي وتطبيقه، وتحديـد الهيكليات التنظيمية اللازمة لضمان الاعتراف بالوثائق الرقمية للأفراد عبر الحدود الجغرافية.

- تطوير استراتيجية عالمية لتسهيل بناء القدرات البشرية والمؤسسية لتعزيز المعرفة والدرايـة في مختلـف القطاعات وفي وضع المجـالات المعلوماتية، تقديم المشورة بشـأن إمكانية اعتماد إطار استراتيجي عالمي لأصحاب المصلحة من أجل التعاون الدولي والحوار والتعاون والتنسيق في جميع المجالات التي سبق ذكرها[١].
- توظيـف الخبراء وتدريبهم لمواكبة أحدث التطورات التكنولوجية وفهمها وتطوير القوانين الوطنية وفق ذلك.
- لابد من تكاتف الجهود الداخلية والدولية لإنشاء منظمات دولية وإقليمية، وإبرام اتفاقيـات ثنائية وجماعية وتكـون متخصصة مهمتها الأساسيـة التنسيق بشأن مواجهة الجرائم الإلكترونية واحتوائها ومحاولة التخفيف منها، وتبادل الخبرات بين الدول كافة، وخاصةً التي لها خبرات واسعة في هذا المجال ومكافحتها لتلك الجرائم.
- التأكيـد على تفعيل قواعد الاتفاقيات الدولية الخاصة بتسليم المجرمين وتفعيلها في كل دولة لخصوصية الجرائم الإلكترونية ولصعوبة إثباتها ومتابعة مرتكبيها وسهولة إتلاف أدلتها ولكونها لا تترك آثارًا مادية على ساحة الجريمة.
- مساعـدة البلدان بعضها البعض في هذا الشأن لمحاربة تلك الجرائم، والتي يتم من خلالها أبشع ما يمكن تصوره «الإرهاب» الذي لا يعرف دينًا ولا وطنًا، والذي من الممكـن أن يذهب ضحيته الملايين من البشر الأبرياء، والذي لا يعرف حينها الدولـة الناميـة من الدولة المتقدمـة، ومن هذا المنطق صـدرت «دعوات للتعاون الدولي من أجل حماية البشرية ».

وأخـيرًا فلابد في الإطار التقني من ضرورة تشفـير البيانات وإخفائها، والاهتمام

(١) لمزيد من المعرفة في هذا الشأن انظر الموقع الإلكتروني: www.itu.int/about/pages/default.aspx

ببروتوكولات الحماية، ونظم منع المتطفلين، للاحتفاظ بسرية المعلومات عن الجميع، باستثناء الذين لديهم صلاحية الاطلاع عليها، ومن ثَمَّ يتم تأمينها باستعمال أساليب متطورة لا يتم اكتشافها، ولابد من تكامل البيانات، بمعنى التأكد من أن المعلومات لم تتغير من قِبل أشخاص غير مخولين، والتحقق من الشخصية.

المطلب الثالث

اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية

تُعد اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية اتفاقية عالمية، والتي صدرت عن الجمعية العامة لمنظمة الأمم المتحدة في الثاني عشر من شهر إبريل عام ٢٠٠٠م، رقم (٦٣/٥٥)[١].

أشارت الجمعية العامة لإعلان منظمة الأمم المتحدة موضحة حرصها على تكثيف الجهود الدولية لمواجهة الجرائم العابرة للحدود ومن ضمنها الجرائم الإلكترونية [٢]، السبب وراء عقد هذه الاتفاقية من قبل منظمة الأمم المتحدة هو تزايد الجرائم التي تُرتكب عن طريق استعمال التكنولوجيا بشكل هائل وما يترتب على ذلك من آثار سلبية، وأكدت على ضرورة تعزيز التنسيق والتعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، بالإضافة إلى دور المنظمات الدولية [٣].

أشار قرار الجمعية العامة رقم (١٢١/٤٥) لعام ١٩٩٠م، المؤيد لتوصيات مؤتمر منظمة الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين والذي عُقد في هافانا، وكان هناك قرار خاص بالجرائم المُرتكبة عبر الإنترنت، أكد فيه على الدول بضرورة تكثيف الجهود الدولية لمواجهة إساءة استعمال التكنولوجيا[٤]، وطلب القرار من الدول

(١) للاستزادة والاطلاع على القرار، الاسترجاع ٢٠٢٢/١٠/٩م.
https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/563/17/PDF/N0056317.pdf?OpenElement

(٢) الفيل، على عدنان. (٢٠١١م). الإجرام الإلكتروني. بيروت: منشورات زين الحقوقية، ص ٣٣٠.

(٣) مزغيش، سمية، (٢٠١٤م)، جرائم المساس بالأنظمة المعلوماتية، رسالة ماجستير، قسم القانون، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، ص٥٤.

(٤) تقرير الأمانة العامة عن مؤتمر منظمة الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين (١٩٩٠م)، الاسترجاع ٢٠٢٢/١٠/١٠م

الأعضاء التأكد من أن قوانينها الجنائية وافية لمواجهة الجرائم السيبرانية، وبناءً على القرار نشرت الأمم المتحدة دليلاً بعنوان «منع ومكافحة جرائم التكنولوجيا»[١].

بيّن من خلال مواد الاتفاقية أنه يجب على الدول أن تضمن عدم توفير قوانينها ما يحمي الذين يسيئون استعمال تكنولوجيا المعلومات لأغراض إجرامية وما يوفر لهم الملاذ الآمن، بل على العكس ينبغي أن تنسق جميع الدول المعنية إنفاذ القوانين دوليًا، من حيث التحقيق والمقاضاة الدولية، تبادل المعلومات والمساعدة، بالإضافة إلى حماية حريات الأفراد والمحافظة على أمن الحكومات وعلى سرية البيانات، بمكافحة إساءة استعمال التكنولوجيا؛ لأن آثار الجرائم الإلكترونية لا يمكن حصرها، فهي خطرة ومدمرة بمختلف مستويات الخطورة [٢].

اعتمدت الجمعية العامة للأمم المتحدة في عام ٢٠٢١م قرارًا كان هدفه مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، أكد القرار على مراعاة الصكوك الدولية القائمة والجهود المبذولة على الصعيدين الوطني والدولي، وذلك لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، ولاسيما ما قام به فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن الجرائم السيبرانية[٣].

ونخلص من ذلك أنه نظرًا للطبيعة الخاصة للجريمة المعلوماتية، وللوسائل الخاصة المستعملة في ارتكابها، فمما لا شك فيه أن هناك صعوبةً في الحصول على أدلة معلوماتية؛ وذلك نظرًا لسهولة محو الأدلة وإتلافها في زمن قصير، والدليل المعلوماتي يطلق على الأدلة المستمدة من وسائط ترتبط بتقنية المعلومات، وكلها تدور حول

https://www.unodc.org/documents/congress/Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders.pdf

(1) Brenner, Susan W. (2010). Cybercrime Criminal threats from Cyberspace. California USA: Praeger. P174.

(٢) الفتلاوي، أحمد عبيس، (٢٠١٦م)، مصدر سابق، ص٦٢٨.

(٣) قرار الجمعية العامة للأمم المتحدة رقم (٢٨٢/٧٥). من الدورة الخامسة والسبعين عام (٢٠٢١م)، الاسترجاع ٢٠٢٢/١٠/١١م

https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/133/49/PDF/N2113349.pdf?OpenElement

استخدامات الحاسب الآلي وتطبيقاته، وشبكة الإنترنت وغيرها من التقنيات الحديثة، ويتعلق -بالطبع - بالجريمة المعلوماتية[١].

ولذا يتم البحث فيها عن العمليات الإلكترونية والتي تتمثل في: التشفير، والأكواد السرية، والنبضات، والأرقام، والتخزين الإلكتروني... وغيرها، وفي كثير من الأحيان يصعب أن تخلف آثارًا مادية يستدل من خلالها على الجريمة، ولعل هذه هي الطبيعة المرئية للأدلة المتحصلة من الجرائم الإلكترونية والتي تجعل من الصعب على المحقق تطبيق إجراءات الإثبات التقليدية[٢]. وأيًّا ما كان الأمر، فإنه يجب مراعاة أن تكون هذه الأدلة قد تم الحصول عليها بطريقة مشروعة، وأن يتم الحصول عليها وفقًا للقواعد والضوابط العامة التي يفرضها القانون [٣].

ويشترط ألا تكون الأدلة المتحصلة من الحاسب الآلي أدلة ظنية، وأن تقترب من الحقيقة قدر الإمكان، ويترتب على ذلك أن تخضع كافة المخرجات الإلكترونية إلى تقدير المحكمة، وأن تقوم المحكمة باستنساخ الحقيقة[٤].

ويمكن القول إن النظم القانونية تختلف في موقفها من الأدلة بحسب الاتجاه الذي تتبناه، فهناك اتجاه يحدد حصرًا الأدلة التي يجوز للقاضي الاعتماد عليها بالإثبات، كما يحدد القيمة الإقناعية لكل دليل، ويقتصر دور القاضي على مجرد فحص الدليل للتأكد من توافر الشروط التي حددها القانون، فهذا النظام مقيد يحدد من صلاحية القاضي، وهذا النظام ينتمي للدول الأنجلوسكسونية، مثل: بريطانيا، والولايات المتحدة الأمريكية.

أما الاتجاه الآخر، فهو نظام الإثبات الحر الذي يتمتع القاضي بحرية مطلقة في شأن الوقائع المعروضة عليه، ومدى فعاليتها للإثبات، ففي مثل هذا النظام لا تثار

(١) انظر: د/ عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص٧٠٩.

(٢) انظر: د/ إبراهيم قسم السيد أحمد طه، الجريمة المعلوماتية في القانون السوداني، ط١، ٢٠١٦، ص ٦٠-٦١.

(٣) انظر: د/ عبد الإله أحمد هلالي، حجية المخرجات الكمبيوترية في الإثبات الجنائي، ط١، دار النهضة العربية، القاهرة، ١٩٧٧، ص ١٢١-١٢٢.

(٤) انظر: د/ أسامة بن غانم العبيدي، الإثبات بالدليل الإلكتروني بالجرائم المعلوماتية، مرجع سابق، ص ٦١.

مشكلة الأدلــة اليقينية، والظنية؛ لأن الموضوع يخضع للسلطة التقديرية للقاضي، وهذا ما أخذت به الأنظمة اللاتينية[١].

ونخلص من ذلك أن التحقيق والإثبات في الجرائم الإلكترونية تحكمه نفس قواعد التحقيــق والإثبــات في أية جريمة غــير إلكترونية، مــع مراعاة ما نصــت عليه قوانين مكافحة الجرائم المعلوماتية بصفة خاصة.

(١) انظر: د/ خالد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، مرجع سابق، ص ٢٣٧-٢٣٨.

الخاتمة

عند انطلاق مشروع العالم الافتراضي «الميتافيرس Metaverse» والذي هو بمثابة ثورة تكنولوجية تنقل العالم إلى آفاق جديدة غير تقليدية يتم فيها الدمج ما بين العالم الحقيقي الذي نعيش فيه والعالم الافتراضي، ويتم فيها إنشاء الأفاتار Avatar تجسيد لشخصياتنا رقميًّا في العالم الافتراضي والأغراض الرقمية.

ولا شك أن هذه التقنية ستحدث تأثيرًا في مختلف المجالات الاقتصادية والاجتماعية وغيرها، سواء على مستوى الأفراد أو الجماعات، وسيترتب عليها العديد من السلوكيات الاجتماعية السلبية المرتبطة باستخدامها، منها ما يرقى إلى درجة الجريمة، مثل: جرائم القرصنة والإرهاب والتجسس، والحض على العنف والكراهية والتمييز... وغيرها، بل إن تأثيرها قد يمتد إلى بنية المجتمع نفسه، وينتج عنها مخاطر جسيمة على مستوى المساس بالنظام العام بكل مجالاته في الدولة، وكذلك على صعيد القيم والمبادئ الاجتماعية والأخلاقية التي تقوم عليها المجتمعات.

ولما كانت نتيجة الاستخدام غير المشروع عالمية وتؤثر في إقليم أكثر من دولة مما يؤثر على أمنها واستقرارها، أصبح تنظيم هذا السلوك مشكلة دولية تحتاج لتعاون الدول لمواجهتها، من أجل تحقيق أهدافها ومصالحها بالإضافة إلى مصالح أفرادها.

الأمر الذي يتطلب من الدول العمل جاهدةً للتعاون لمواجهة الإشكاليات التي يمكن أن تحدث عبر تقنية الميتافيرس وفق إطار الغرض منه الإحاطة بالإشكاليات ومواجهتها والسيطرة عليها من خلال خطوات جِدية ومحددة من شأنها أن تحد من مخاطرها، وتقلل آثارها على الأمن والسلم الدوليين.

ومن خلال هذه الدراسة تم بيان مفهوم الميتافيرس، وما هي الإيجابيات التي نستشرفها من هذه التقنية، والسلبيات التي يجب أن نتوقاها، وكذلك الجانب القانوني التطبيقي لمواجهة الميتافيرس، ونتعرض -كذلك- لضرورة التعاون الدولي من الناحيتين التشريعية والأمنية فيما يتعلق بتطبيق الميتافيرس.

من خلال ما عُرِض وإتمامًا للفائدة أذكر أهم النتائج والتوصيات التي توصلت إليها خلال البحث والدراسة في هذا الموضوع:

أولًا- النتائج:

١- نظرًا لاختلاف التشريعات الدولية والدراسات الفقهية في تحديد نطاق الجرائم المعلوماتية، حيث إن تعدد المفاهيم القانونية غير واضحة ولا محددة بالنسبة للتقنيات المعلوماتية وخاصة فيما يتعلق بتقنية الميتافيرس، بالإضافة لتطور وتغير المفاهيم المتعلقة بالجرائم المعلوماتية مع تطور تكنولوجيا الاتصالات والمعلومات باستمرار، خاصةً وأن للجرائم المعلوماتية خصائص وصورًا تميزها كليًّا عن الجرائم التقليدية، بدايةً بأسلوب ارتكابها مرورًا بمرتكبها والمادة المستخدمة لارتكابها وصولًا لمدى آثارها حيث إنها عابرة للحدود، كما أنها صعبة الاكتشاف والإثبات؛ لما تمتاز به من سرعة وسهولة من حيث ارتكابها؛ لذلك تحتاج لخبراء ومختصين في التحقيق.

٢- من أهم المبادئ القانونية الدولية لمواجهة الجرائم المعلوماتية، التعاون الدولي لأنه مهما بلغت قوة وصلابة الدول، فهي لا تستطيع أن تواجه الجرائم المعلوماتية وحدها بجهودها الداخلية، لذلك لا غنى لها عن التعاون مع الدول أو على الأقل دولة أخرى، لطبيعة تلك الجرائم المتطورة والمستمرة بالتقدم، وتوسع مداها إقليميًّا وعالميًّا؛ مما يجعل من المستحيل السيطرة عليها، حيث إنه لا يمكن تعقب مرتكبي الجرائم إلا داخل حدود الدولة، وبما أنها عابرة للحدود، فإن من أهم مقومات نجاح مواجهتها التعاون الدولي بجميع صوره.

٣- يعد التعاون الأمني الدولي وسيلة مهمة وفعالة في مواجهة الجرائم المعلوماتية، به تكمل أجهزة الدول الأمنية بعضها، فعند وجود ثغرة لدى جهاز أمني لدولة معينة، تسد هذه الثغرة دولة أخرى بتعاونهم لمواجهة الجرائم العابرة للحدود.

٤- لفت الانتباه لدور المنظمة الدولية للشرطة الجنائية «الإنتربول» الفعال في مساعدة الدول الأعضاء لمواجهة الجرائم المعلوماتية، والتي لا تحدها الحدود.

٥- يُعد التعاون القضائي الدولي من التدابير المانعة لوقوع الجرائم الدولية عامةً والجرائم المعلوماتية خاصةً؛ لأن مرتكبي هذه الجرائم على علم تام بأن الجهات القضائية الدولية ستتعاون عن طريق المساعدات القضائية وتبادل المعلومات ونقل الإجراءات بالتالي لا مفر لهم، فإن استطاعوا الفرار من دولة مُعينة ستلاحقهم الدولة الأخرى، وذلك يعود للتعاون القضائي الدولي سواءً كان بالإنابة القضائية أو سماع الشهود أو إلقاء القبض على مرتكبي الجرائم المعلوماتية أو تسليم المجرمين.

٦- للاتفاقيات الدولية النصيب الأكبر في تأسيس القوانين المواجهة للجرائم المعلوماتية، كما أن للاتحاد الأوروبي ومجلس أوروبا دورًا مميزًا وجهدًا واسعًا في مواجهة الجرائم المعلوماتية، ويظهر لنا ذلك من خلال اتفاقية بودابيست «اتفاقية الجرائم المعلوماتية» لعام ٢٠٠١م.

٧- من الجهود الدولية التي كان لها دور في مواجهة الجرائم المعلوماتية الاتفاقيات العربية، مثل الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠م.

٨- دور المنظمات الدولية الفعّال، فعلى سبيل المثال: بذلت منظمة الأمم المتحدة جهودًا عظيمة لمواجهة الجرائم المعلوماتية، فأصدرت القرارات عن طريق الجمعية العامة ومجلس الأمن، وعقدت الاتفاقيات، كما عقدت المؤتمرات عن طريق المجلس الاقتصادي والاجتماعي للأمم المتحدة، وكذلك منظمة التعاون الاقتصادي والتنمية كونها أول منظمة اهتمت بالجرائم المعلوماتية على المستوى الدولي، ولا يخفى دور الاتحاد الدولي للاتصالات في الحفاظ على أمن الاتصالات وعدم إساءة استعمالها.

٩- هناك إغفال وقصور في المعالجة التشريعية للدول لمواجهة الجرائم المعلوماتية على المستوى الدولي، حيث إن بعض الدول لم تضع نصوصًا صريحة في قوانينها خاصةً بالجرائم المعلوماتية ولم تُعد قوانين خاصة لإساءة استخدام وسائل التكنولوجيا، ويشكل هذا الإغفال عقبة أمام التعاون الدولي وتحديًا لمواجهة

هـذه الجرائم دوليًّا، مما قد ينتج عنـه إفلات مرتكبيها من العقاب باستغلالهم الفراغـات الموجودة فـي القانون، ولكن في المقابل عمـل المجتمع الدولي جاهدًا للتغلـب على هـذا الإغفال والقصـور بسن القوانـين الجديـدة أو بالتعديل على القوانـين الموجودة عن طريق إضافة بنود خاصـة بالجرائم المعلوماتية والدخول فـي الاتفاقيات الدولية التي تهـدف لمواجهة الجرائم المنظمـة والعابرة للحدود والجرائـم المعلوماتيـة، حيـث إن الجرائـم المعلوماتيـة تُعد جزءًا مـن الجرائم المنظمة والجرائم العابرة للحدود.

١٠- يعـد اختـلاف النظـم القانونيـة مـن الإشكاليـات المهمة التـي تواجـه التعاون الـدولي، ويترتـب على هـذه الاختلافـات مشاكل فـي تطبيق القانـون من حيث التجريم والإجراءات القانونية والمحاكمـات وتوقيع العقوبات، وسعت الاتفاقيات والمعاهـدات الدولية للتقريب بين الأنظمة الداخلية للدول وسد الثغرات، فركزت الجهود الدولية على تحقيق المواءمة بين التشريعات والأنظمة للتغلب على إشكالية اختلاف النظم القانونية للدول في مواجهة الجرائم المعلوماتية.

١١- تثير الجرائم المعلوماتية إشكالية الاختصاص القضائي بشقيه الإيجابي والسلبي علـى المستويين الوطني والدولي؛ مما يعوق التعاون الدولي، وللتغلب على إشكالية الاختصـاص القضائي يجب اعتبـار جميع الجرائم المعلوماتيـة دولية وإدخالها ضمن الاختصاص القضائي العالمي حتى وإن كانت قد ارتكبت داخليًّا.

١٢- تعد الإنابـة القضائية من إشكاليات التعاون القضائـي، حيث تعترضها إشكالية فكـرة السيادة والبطء في إجراءات الإنابـة القضائية، وللتغلب عليها تم التعاون بـين سيـادات الدول؛ حيـث إن الإنابـة القضائية تتـم اعتمادًا علـى الاتفاقيات والمعاهـدات فيمـا بين الدول، أما فيمـا يخص بطء الإجراءات فـإن الإنابة تتم بالاتصـال المباشر والاتصال المرئي والمسموع بـين السلطات القضائية اختصارًا للوقت وطول الإجراءات.

١٣- يواجه التعاون الدولي لتسليم المجرمين السيبرانيين عقبات، كاشتراط ازدواجية

التجريم والتزاحم في طلبات التسليم، ووضعت التطورات التشريعية الدولية الحلول للتغلب على إشكاليات التعاون الدولي فيما يخص تسليم المجرمين، حيث إنها اعتبرت شرط ازدواجية التجريم متحققًا بتجريم الفعل في الدول دون الالتفات للتفاصيل الأخرى، أما فيما يخص تزاحم طلبات التسليم فما زالت تختلف بحسب الدول؛ حيث إن أولويات الدول مختلفة، فتقرره الدولة المطلوب منها التسليم حسب معاييرها التقديرية.

ثانيًا- التوصيات:

١- ضرورة عقد مؤتمر دولي بقيادة الأمم المتحدة، والنظر إلى جميع الإشكاليات المتعلقة بالجرائم المعلوماتية وخصائصها وصورها، حيث يجب العمل على إنشاء تعريف جامع مانع مُعترَف به من جميع الدول الأطراف، حيث إن هذا من شأنه أن يزيح عقبات عديدة لمواجهة هذه الجرائم المعلوماتية.

٢- من الضروري تكثيف جهود التعاون الدولي بجميع أنواعه لتحصين الفضاء المعلوماتي ورصد كل الاستخدامات غير المشروعة له، والتصدي لها قضائيًّا وإجرائيًّا، حيث إن تكثيف التعاون الدولي من شأنه أن يحيط مخاطر الجرائم المعلوماتية ويسيطر عليها.

٣- إصدار اتفاقية دولية مستقلة تخص الجرائم المعلوماتية فقط لتسد جميع الثغرات الحالية متضمنة نصوصًا موضوعية تُجرم جميع الأفعال غير المشروعة في تكنولوجيا المعلومات وإجرائية توضح إجراءات التفتيش والضبط والانتقال؛ لتساعد الجهات القضائية لإجراء التحقيقات المناسبة والملاحقات القضائية والمحاكمات لتوقيع العقوبات المناسبة أو إجراء التسليم.

٤- ضرورة تعزيز التعاون مع المنظمات والمؤسسات الدولية لمواجهة الجرائم المعلوماتية، مثل: العمل مع المنظمة الدولية للشرطة الجنائية وتوسيع نطاق آليات القانون الجنائي للجرائم التقليدية بتطويرها وتشكيلها فيما يتناسب مع الجرائم المعلوماتية واتساع شبكات الاتصال العالمية، حيث إن الآليات الحالية

تتـم ببطء وتمر بعدة إجراءات وتعقيـدات تجعلها غير ملائمة لطبيعة الجرائم المعلوماتية.

٥- حـث الـدول التي لم تنضـم بعد علـى الانضمـام للاتفاقيات الدوليـة الخاصة بمواجهـة الجرائـم المعلوماتيـة كاتفاقية بودابسـت لعـام ٢٠٠١م، وحث الدول العربية على إنشاء اتحادات عربية دولية هدفها مواجهة الجرائم المعلوماتية من خلال منظمة عربية، لتسهيل تداول المعلومات فيما بين الدول العربية وإجراءات البحث والتحري في الجرائم المعلوماتية، بالإضافة لتفعيل الأمن الوقائي.

٦- لنجاح التعاون الدولي ينبغي التدخل على المحور الداخلي أولًا بملاءمة التشريعات الداخليـة بسـد أي فراغ وثغـرة تعتريها، وذلـك بإنشاء قوانـين وأنظمة داخلية جديـدة مختصة بالجرائم المعلوماتية، أو تحديـث النصوص التقليدية بالنص صراحةً على جميع صور الجرائم المعلوماتية لتتم مواجهتها بطريقة فعّالة، ومن ثَـمَّ التدخل على المحـور الدولي بإبرام الاتفاقيات الدوليـة الجماعية والثنائية، لإيجـاد أساس تشريعي موحد يضمن توحيد تجـريم الأفعال التي تُشكل جريمة سيبرانيـة، كما يجـب أن يستمر تحديث الأنظمة واللوائـح التي تكافح الجرائم المعلوماتية في جميع الدول.

٧- ينبغـي تفعيل قنوات الاتصال واعتماد الاتصال المباشر بين السلطات القضائية الدوليـة للتغلب على إشكالية بطء الإجراءات والتعقيد في تسليم طلبات الإنابة القضائية الدولية.

٨- ينبغـي عقد اتفاقيـة تتضمن أولويـات تسليم مرتكبي الجرائـم العبرة للحدود بوجه عـام، والجرائم المعلوماتية على وجه الخصوص، بشكل واضح ومُفصل؛ ليتـم اتباعها من جميع الـدول فتتحقق مصلحة الجماعـة بعدالة دون أن تقدم الدولة المطلوب منها التسليم مصلحتها على مصالح باقي الدول، مما من شأنه أن يُخـل بميزان العدالـة، كما أن توضيـح أولويات التسليم مـن شأنه أن يجعل عملية التسليم مُنَظَّمَة وواضحة.

٩- تدريس الجرائم المعلوماتية كمقرر علمي في الكليات ذات العلاقة، لِتُصبح لدى الطلاب خلفية جيدة عن الجرائم المعلوماتية وطبيعتها وأساليب ارتكابها وكيفية التعامل معها، كما يجب عمل دورات للضباط والقضاة عن تفاصيل التعامل مع الجرائم المعلوماتية.

١٠- نشر الوعي عن طريق تكثيف دور الإعلام والمؤسسات المدنية الأخرى بتوضيح المخاطر الناتجة عن سوء استخدام التكنولوجيا، وما يترتب عليه من أضرار تلحق بالمجتمعات والأفراد، ووجوب اتخاذ الاحتياطات الوقائية لحماية البيانات والمواقع سواءً كانت شخصية أو كانت تخص مؤسسات الدولة كونه موظفًا في أحد قطاعاتها.

قائمة بأهم مراجع البحث

المراجع العربية :

أولًا - الكتب:

- **د/ إبراهيم قسم السيد أحمد طه**، الجريمة المعلوماتية في القانون السوداني، ط١، ٢٠١٦.
- **د/ أحمد إبراهيم محمد إبراهيم**، المسئولية الجنائية الناتجة عن أخطاء الذكاء الاصطناعي في التشريع الإماراتي دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس ٢٠٢٠.
- **د/ أحمد حسام طه تمام**، دار النهضة العربية، ٢٠٠٠.
- **د/ أحمد خليفة الملط**، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٥.
- **د/ أحمد فتحي سرور**، الوسيط في قانون العقوبات القسم الخاص ، ط (٤)، ١٩٩١، دار النهضة العربية.
- **أسامة عبد الله قايد** ، الحماية الجنائية وبنوك المعلومات ، دار النهضة العربية، القاهرة، ط (٣)، ١٩٩٤م.
- **د/ أسامة بن غانم العبيدي**، التفتيش عن الدليل في الجرائم المعلوماتية.
- **د/ أيمن عبد الحفيظ**، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، مكتبة الكتب العربية ٢٠٠٥م.
- **أ/ أيها محمد التاج**، التحقيق وجمع الأدلة في الجرائم المعلوماتية، مجلة العدل، وزارة العدل، السودان، مجلد (١١)، عدد (٢٦)، دار المنظومة، ٢٠٠٩.
- **د/ إيهاب خليفة**، مجتمع ما بعد المعلومات، تأثير الثورة الصناعية الرابعة على الأمن القومي، مركز المستقبل للأبحاث والدراسات المتقدمة، دار العربي للنشر والتوزيع، القاهرة، ٢٠١٩.

- **أ/ زياد عبد التواب،** ما وراء الميتافيرس: ذلك المجهول القادم، مجلة الديمقراطية، مؤسسة الأهرام، المجلد ٢٢، العدد ٨٥، يناير ٢٠٢٢.
- **د/ جميلة بن زاف،** المجتمع الافتراضي ونهاية أطروحة القرية العالمية لماكلوهان بحث منشور في مجلة علوم الإنسان والمجتمع، المجلد (١١)، العدد (١)، السنة ٢٠٢٢.
- **د/ حسن طاهر داود،** جرائم نظم المعلومات ، أكاديمية نايف العربية، ط (١)، ١٤٢٠هـ / ٢٠٠٠م.
- **د/ حمدي عبد الرحمن،** المدخل لدراسة القانون المقارن، مذكرات لطلبة دبلوم القانون المقارن، كلية الحقوق، جامعة عين شمس، القاهرة، ١٩٧٣م.
- **د/ خالد الحلبي،** إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت.
- **د/ رضا المتولي وهدان،** النظام القانوني للعقد الإلكتروني والمسئولية عن الاعتداءات الإلكترونية، دراسة مقارنة في القوانين الوطنية وقانون الأونسيترال النموذجي والفقه الإسلامي، دار الفكر والقانون، ٢٠١٧.
- **د/ سمية مزغيش،** جرائم المساس بالأنظمة المعلوماتية، رسالة ماجستير، قسم القانون، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، (٢٠١٤م).
- **د/ شريف يوسف خاطر،** حماية الحق في الخصوصية المعلوماتية، دار الفكر والقانون، المنصورة، ٢٠١٥.
- **د/ شيماء عطا الله،** الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، بدون ط، ٢٠٠٧.
- **د/عبد الحليم بن باردة،** إجراءات البحث والتحري عن الجريمة المعلوماتية، مجلة الحقوق والعلوم الإنسانية، عدد (٢٣)، دار المنظومة، ٢٠١٥.

- **د/ عبد الفتاح بيومي حجازي**، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت ، دار الكتب القانونية، ٢٠٠٧.
- **د/ عبد الإله أحمد هلالي**، حجية المخرجات الكمبيوترية في الإثبات الجنائي، ط١، دار النهضة العربية، القاهرة، ١٩٧٧.
- **د/عبد الوهاب جودة الحايس**، الآثار الاجتماعية لاستخدام وسائل الإعلام الاجتماعي على بعض جوانب الشخصية الشابة ، مجلة شؤون اجتماعية ، الإمارات العربية المتحدة، م ٣٢ ، ع ١٢٦، سنة ٢٠١٥.
- **د/ على عدنان الفيل**، (٢٠١١م)، الإجرام الإلكتروني، بيروت: منشورات زين الحقوقية.
- **د/عزة على محمد الحسن**، جرائم المعلوماتية في القانون السوداني، بدون ناشر.
- **د/ عمر عباس العبيدي**. مكافحة الجرائم الإلكترونية كآلية لتعزيز الأمن الإقليمي. مصر: مركز الدراسات العربية، (٢٠٢١م).
- **د. عمر فاروق الحسيني**، تأملات في بعض صور الحماية الجنائية لنظم الحاسب الآلي ، مقال مقدم للدورة التدريبية بفندق شيبارد المنظمة من اتحاد من ٧/ مايو، ١٩٩٠.
- **د. فتوح الشاذلي و د. عفيفي أمل عفيفي**، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفكرية ودور الشرطة والقانون ، دراسة مقارنة ، منشأة المعارف، الإسكندرية ، ٢٠٠٨.
- **د/مريم محمد حسن**، التنظيم القانوني لجريمة التجسس المعلوماتي، رسالة ماجستير، العراق: جامعة الكوفة، كلية القانون، (٢٠١٦م).
- **المستشار الدكتور/ محمد جبريل إبراهيم**، الميتافيرس والقانون الجنائي، دار النهضة العربية ، ط١، ٢٠٢٣.

- **د/ محمد حسام الدين لطفي**، الحماية القانونية لبرامج الحاسب الإلكتروني، بحث مقدم لمؤتمر الكويت الأول، القانون والحاسب الآلي ٤ – ٧ نوفمبر ١٩٩٤م كلية الحقوق ، منشورات مؤسسة الكويت للتقدم العلمي، ١٩٩٤م.
- **د/ محمود محمد أبو فروة**، منصات التواصل الاجتماعي ومسؤوليتها القانونية عن المحتوى غير المشروع، نشر مجلة القانون الكويتية العالمية، السنة العاشرة، العدد (٣)، العدد التسلسلي (٣٩)، ذو القعدة ١٤٤٣هـ/ يونيو ٢٠٢٢م.
- **د/ ناصر بن محمد البقمي**. مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، مركز الإمارات للدراسات والبحوث الاستراتيجية، سلسلة محاضرات الإمارات (١١٦).
- **د/ نايل نبيل عمر**، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، ٢٠١٢.
- **د/ نور الدين زعتر**، العالم الافتراضي «الميتافيرس Metaverse» من منظور سيكولوجي، مجلة العلوم الإنسانية، الناشر: جامعة العربي بن مهيدي – أم البواقي، المجلد (٩)، العدد (٢)، ٢٠٢٢.
- **د/ هشام فريد رستم**، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، الطبعة الأولى، ١٩٩٥م.
- **د/هلالي عبد اللاه أحمد**، اتفاقية بودابست لمكافحة جرائم المعلوماتية (معلقًا عليها)، دار النهضة العربية، ط٢، (٢٠١١).

ثانيًا- القرارات والمعاهدات والاتفاقيات الدولية:

- **ميثاق الأمم المتحدة (١٩٤٥م)**، الأمم المتحدة، اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، دراسة بعنوان:«الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية»

- E/ESCWA/TDD/20159 1/ February 2015.

- الأمم المتحدة، الجمعية العامة، مجلس حقوق الإنسان، الدورة الرابعة والأربعون ١٥ حزيران/يونيه – ٣ تموز/يوليه ٢٠٢٠ البندان (٢ و٣) من جدول أعمال التقرير السنوي لمفوضية الأمم المتحدة السامية لحقوق الإنسان تعزيز وحماية جميع حقوق الإنسان ، المدنية والسياسية والاقتصادية والاجتماعية والثقافية، بما في ذلك الحق في التنمية.
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، (٢٠١٠م).
- اتفاقية الأمم المتحدة لمكافحة الفساد، (٢٠٠٣م).
- https://shortest.link/a9nq.
- الاتفاقية المتعلقة بالجريمة الإلكترونية اتفاقية مجلس أوروبا «بودابست»(٢٠٠١م)،
- https://shortest.link/9Gzh.
- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والبروتوكولات الملحقة بها، (٢٠٠٠م)، الاسترجاع ١٦/٩/٢٠٢٢م.
- https://shortest.link/9Gzp.
- اتفاقية الرياض العربية للتعاون القضائي، (١٩٨٣م).٣٠/١٠/١٩٨٥م
- https://www.tahkeem.ae/contents/files/rule_c.pdf.
- اتفاقية تسليم المجرمين بين دول الجامعة العربية، (١٩٥٣م).
- https://dftp.gov.ps/uploads/1623136174.pdf
- معاهدة نموذجية بشأن نقل الإجراءات في المسائل الجنائية، (١٩٩٠م).
- http://hrlibrary.umn.edu/arab/b051.html

- مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، (٢٠١٨م).

- https://shortest.link/9GzA.

- مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية، (٢٠١٥م).
- https://shortest.link/a9xd.

- قرار الجمعية العامة للأمم المتحدة رقم (٦٥/٢٣٠)، من الدورة الخامسة والستين مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، (٢٠١٠م).
- https://shortest.link/9GIq.

- المرسوم الملكي رقم (م/١٧) بتاريخ ١٤٢٨/٣/٨هـ، نظام مكافحة جرائم المعلوماتية.
- https://shortest.link/a9pV.

- القانون الأساسي للمنظمة الدولية للشرطة الجنائية (الإنتربول)، (٢٠٠٨م).
- https://www.legal-tools.org/doc/5b26fd/pdf/

- قرار مجلس وزراء الداخلية العرب رقم (٤١٧) بالدورة (٢١) في عام (٢٠٠٤م). من قانون الامارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، الاسترجاع ١٠/١٠/٢٠٢٢م.
- https://shortest.link/a9ry.

- وثيقة الرياض للنظام (القانون) الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون لدول الخليج العربية. (٢٠١٣م).
- https://shortest.link/a9sv

- الموقع الإلكتروني للإنتربول الدولي.
- https://www.interpol.int/ar.

- الموقع الإلكتروني لمنظمة شرطة الويب.
- http://www.web-police.org.

- الموقع الإلكتروني لمنظمة حلف الشمال الأطلسي

- https://shortest.link/a9uE.

- الموقع الإلكتروني للاتحاد الدولي للاتصالات.

- http://www.itu.int/osg/spu/intset/

المراجع الأجنبية:

- Amanda De carlo, La Responsabilité de L'hébergeur Internet Visà- Vis des Tiers. Mémoire du diplôme de la Faculté Libre de Droit, d'Economie et de Gestion (FACO)JUIN 2008, p.5. https://www.lepetitjuriste.fr/wp-content/uploads/201105//La responsabilité de 1'hébergeur internet vis- à-vis des tiers.pdf, (Accessed on: 22023/5/).

- Brenner, Susan W. (2010). Cybercrime Criminal threats from Cyberspace. California USA: Praeger.

- Gercke, Marco. (2012). Previous Source.

- Weber, Rolf H & Heinrich, Ulrike I. (2012). Anonymization. New York. USA: Springer.

- Ghosh, Sumit., & Turrini, Elliot. (2010). Cybercrimes A Multidisciplinary Analysis. Germany: Springer. P326.

- Frayssinet, Jean. (1977). l'informatique et le secret des fichiers. France: Press Universitaires de France.