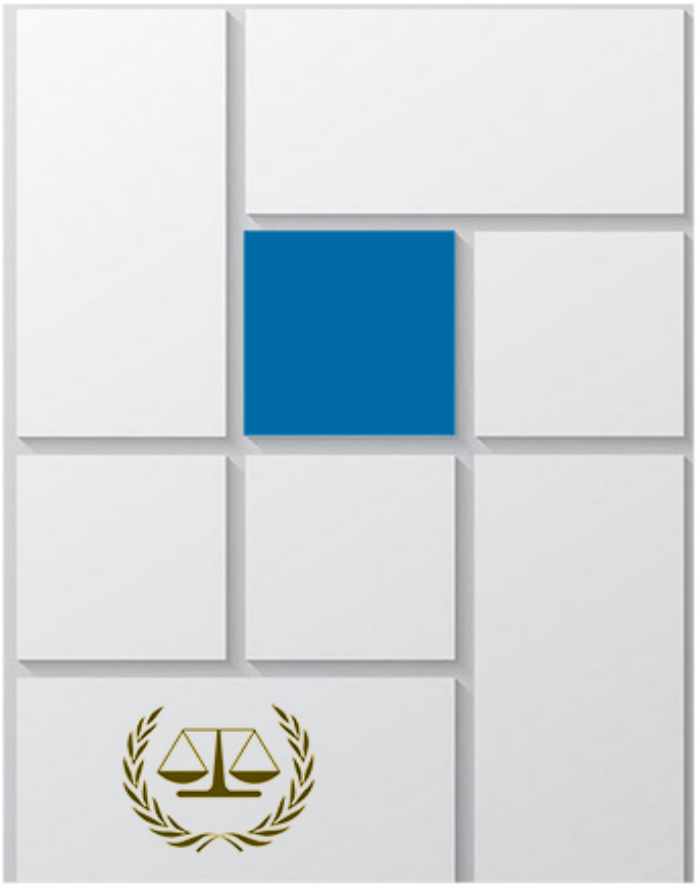
المركز العربي للبحوث القانونية والقضائية
مجلس وزراء العدل العرب
جامعة الدول العربية

الحماية القانونية لمستخدمي الميتافيرس

(دراسة مقارنة)



إعداد:
الأستاذ/ أيمن محمود مجيد الكبيسي
باحث قانوني - ماجستير القانون الخاص
مستشار قانوني
والدكتور حسن علي دبوق
أستاذ مشارك في القانون الخاص
الجامعة اللبنانية- بيروت

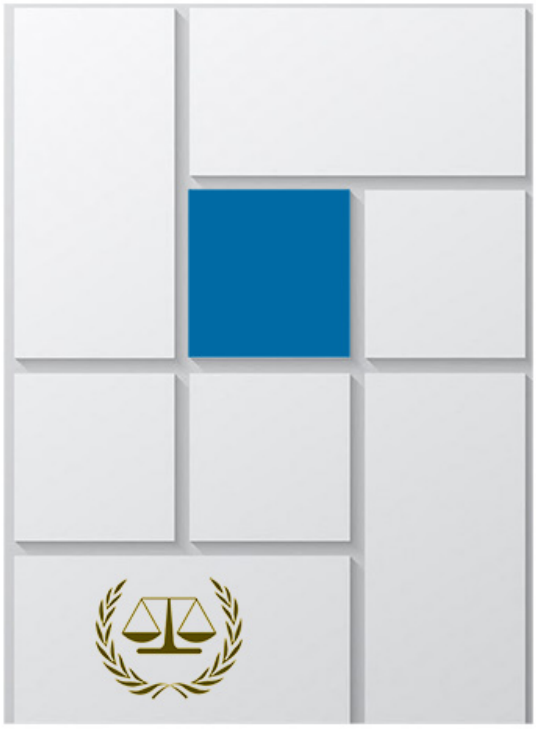
معهد دبي القضائي

مقدم إلى المركز العربي للبحوث القانونية والقضائية مجلس وزراء العدل العرب جامعة الدول العربية

المركز العربي للبحوث القانونية والقضائية
مجلس وزراء العدل العرب
جامعة الدول العربية

الحماية القانونية لمستخدمي الميتافيرس

(دراســة مقــارنــة)



إعداد:
الأستاذ/ أيمن محمود مجيد الكبيسي
باحث قانوني - ماجستير القانون الخاص
مستشار قانوني
والدكتور حسن علي دبوق
أستاذ مشارك في القانون الخاص
الجامعة اللبنانية- بيروت

معهد دبي القضائي

مقدم إلى المركز العربي للبحوث القانونية والقضائية مجلس وزراء العدل العرب جامعة الدول العربية

المركز العربي للبحوث القانونية والقضائية
مجلس وزراء العدل العرب
جامعة الدول العربية

الحماية القانونية لمستخدمي الميتافيرس
(دراســـة مقـــارنـــة)

إعـــــداد:

الأستاذ/ أيمن محمود مجيد الكبيسي
باحث قانوني - ماجستير القانون الخاص
مستشار قانوني
والدكتور حسن علي دبوق
أستاذ مشارك في القانون الخاص
الجامعة اللبنانية- بيروت
معهد دبي القضائي

مقدم إلى المركز العربي للبحوث القانونية والقضائية مجلس وزراء العدل العرب جامعة الدول العرب

منشورات المركز العربي للبحوث القانونية والقضائية
العنوان: بيروت -منطقة الأشرفية-شارع بيضون- مقابل فصيلة قوى الأمن الداخلي
الموقع الإلكتروني: www.carjj.org
البريد الإلكتروني: arab.league@carjj.org
تلفون: 009611200281 / 009611200283

فاكس: 009611200280

"إن المواقف والأفكار الواردة في هذا الكتاب تعبّر عن وجهة نظر ورأي المؤلف ولا تلتزم بها أية جهة أخرى"

مقدمة

منذ بداية دخول عالم الانترنت إلى بعض جوانب حياتنا اليومية في بدايات التسعينيات من القرن المنصرم، يعمل التقنيون والباحثون عن الاستثمار لجعل هذا الخدمة هو عالمنا، الذي لا يمكن الاستغناء عنه، وعلموا خلال الثلاثين عاماً ونيف على ربطنا بتلك التقنية شيئًا فشيئاً حتى لا يكاد هناك شخص في مدينة أو قرية أو حتى في الصحراء لا يستخدم تلك الخدمة، حتى أصبح من الصعب ولا أبالغ إن قلت من المستحيل التخلي عنه، أو ممارسة أي عمل دون أن تكون لهذه الخدمة ـــ الأنترنت ـــ دور فيه يزيد وينقص بحسب تلك الأعمال.

لذا كان من الضروري أن تتدخل الدول كنوع من الحماية، سواءً كان لأمنها الداخلي، أو الخارجي، أو لحماية المستهلكين ومستخدمي تلك الخدمة من عواقبها، أو ممن يحاولون استعمالها بشكل سيء يضر بالمستخدم نفسه أو غيره، فظهرت قوانين تنظيم الاتصالات، وقوانين التجارة الإلكترونية، وقانون الجرائم الإلكترونية، وقوانين الخصوصية الشخصية، وقوانين حماية حقوق الملكية، وغيرها من القوانين مشفوعة بالرقابة الحكومية المباشرة التي تختلف من بلد لآخر معتمدةً على ما يكون جزءًا من بناء مجتمعها الاجتماعي، معتمدةً في ذلك على أجهزتها المختصة لنطاقات تعتبرها ضارة سواءً كانت اجتماعية أو تجارية، إلى أن جاءت الثورة التي أصفها بأنها الثورة الصناعية التقنية الخامسة، التي تزيد في خطورتها على جميع أنواع الأسلحة سواءً، اكانت النووية منها أو الهيدروجينية، إذ إن الأخير محصور في الاستخدام ومحدد الانتشار بضوابط على نطاق ضيق، وينحصر استخدامه من قبل الحكومات، تسبقها موافقات وتعهدات ورقابة لمنح استخدامها، أضف إلى ذلك أنه إذا ما أسيء استخدامه فهو مدمر للبشرية في نطاق مهما كبر يكون محدودًا، أما الثورة الجديدة التي تمثلت في ثورة التقنيات فإن خطرها متجسد في الدخول والتعدي على جميع مستخدمي التقنيات، فهو قابل للاستخدام من قبل الجميع وبأرخص الأثمان، هذا يجعل من الصعوبة بمكان الرقابة على هذه الثورة لتشعب المستخدمين، واختلاف الدول في نمط حياتها المبني على خليط لا محدود من التنوع، فبين اللامحدود والمحدود منطقة واسعة تتنوع فيه البشرية فيما تأخذ منه وفيما تتركه، ولعل الشواهد كثيرة، فباتت الأسرة الواحدة متنوعة في ميول أفرادها ثقافياً وفيما يعتقدونه، بعد أن كانت بلدانًا بأسرها تعيش بنمط واحد، ولعل من أحد تلك الأسباب بل من المؤكد كان للتقنية وما أظهرته من برامج التواصل الاجتماعي الأثر الأكبر في تكوين هذا الخليط، أضف إلى ذلك التنوع في القوانين المحلية والدولية ، فبينما نضع قانونًا يجرم ازدراء الأديان، ويحترم جميع معتقدات أفراد المجتمع المقيمين فيه، وما يؤمنون به، نرى في الجانب الآخر قوانين دول أوربية تبيح كل الأفعال المسيئة للآخر بحجة حرية التعبير، ونحن هنا أمام مفترق طرق وعر، فإما أن يكون هناك أطر عامة تتبناها الأمم المتحدة في الحقوق والحريات بحيث تراعي التباين الثقافي والاجتماعي للعالم بأسره، لا تلك التي تصاغ من الطرف الأقوى منفرداً، يشبه هذا النوع من الانفراد الاحتلال بطريقة أو أخرى، لذا أجد أنه في نهاية المطاف وآجلا أم عاجلا ستصبح القوانين المحلية تتقارب شيئاً فشيئاً لسد هذا البون الشاسع، وكذلك على الصعيد الديني لا يقف الفقه الإسلامي بعيداً عن هذا التطور، فلديننا في ديننا الحنيف الفقه الاستشرافي والي يعرف على أنه " التعرف

على الأحكام الشرعية للمسائل التي يتوقع حصولها، والحلول الشرعية للنوازل وآثارها والاستعداد المناسب لها." (1) لا سيما وأن

ومع ما ذكرنا استحدثت مخالفات يطلق عليه بالجرائم المستحدثة وعرفها كثير من الفقه تعاريف مختلفة نورد أحدها للتعريف بها ولسنا في مجال الخوض في تفاصيلها على أنها" **تلك الأنواع من الأفعال أو السلوكيات التي تشكل نمطاً إجرامياً، جديداً لم يكن مألوفاً من قبل، أو هي تلك الأساليب الإجرامية الحديثة المستخدمة لارتكاب جرائم معروفة من قبل**." (2)

لم تكن الثقافة القانونية مهمة وضرورية لكل أفراد المجتمع، إذ يهتم من لديه معاملات تجارية، حتى تلك الأعمال المدنية تجد من يحتاج إليها يهب إلى المتخصصين في القانون لتقديم المساعدة أو المشورة، أما نحن الآن أصبحت جميع تعاملاتنا اليومية هي تصرفات لها أثرها القانوني، علمنا أم لم نعلم، منها ما ينطوي تحت جرائم ازدراء الأديان، أو قانون مكافحة التمييز والكراهية، وغيرها، إذ أصبح من المعقول ونحن في عالم الميتافيرس في اجتماع افتراضي في بلد من البلدان وأفعل فعلًا مُجرمًا في ذلك البلد في حين أنه لا يُجرم في البلد الأصل الذي أنا فيه زمانًا ومكانًا واقعيًا.

لما تقدم يأتي القانون منظمًا، وهذا يعني أنه ينشأ بعد وقوع الحدث لا قبله، فيقوم المشرع بفهم الظاهرة ومعرفة جوانبها الحياتية ويكيفها لأي من الجوانب هي، ليقوم حسب تلك الظاهرة بمنعها أو الحد منها أو السماح بها في حالات أو الحث عليها، إلى أخره من الحالات التي تنتهي إلى تحقيق المصلحة العامة.

تختلف الدول في سرعة الاستجابة لأسباب عدة منها عدم جاهزية أدوات التشريع أو الاهتمام والمواكبة، أو لأنها دول لا تسعى لأن تكون في مصاف الدول المتقدمة يحتذى بها، لذا نجد سرعة الاستجابة في دولة الإمارات العربية المتحدة لتلك المتغيرات سريعة ومواكبة للتغيرات بل وفي بعض الأحيان مستبقة متنبئةً (3)، وذلك لما لها من مكانة عالمية كونها منطقةً جاذبةً للاستثمار راعيةً لكل ما هو جديد، والأمثلة أكثر من أن يحصرها هذا البحث وليس هذا محله، لذا أقصرها على ما جاء مناسبًا لهذا البحث وموضوعه، فنرى مبادرة الشيخ محمد بن راشد في وضع استراتيجية الإمارات للذكاء الاصطناعي (Artificial Intelligence) ويعبر عنه باختصار (AI) أطلقتها الإمارات في أكتوبر من عام 2017 وبما ينسجم ومئوية الإمارات 2071 (4)، بل وتعدى الأمر ليكون هناك وزارةٌ مختصةٌ بذلك (5).

وفي مثل حالنا اليوم ونحن نتحدث عن الميتافيرس ومدى أهميتها البالغة فقد عقد ملتقى دبي للمتافيرس في سبتمبر من عام 2022 تحت رعاية مؤسسة دبي للمستقبل(6)، فإننا في حقيقة الأمر نتحدث عن تقنية تدخل في جميع مجالات الحياة وهي شيء من أشياء الذكاء الاصطناعي وأحد صوره، وقد تبنت 193 دولة أول اتفاق عالمي بشأن أخلاقيات الذكاء الاصطناعي (7)، ولأنها محل دراستنا وحسب ما ذكرنا أعلاه من أن القانون ليكون لا بد له من فهم الموضوع ودراسة تأثيره على جوانب الحياة لذا رأينا أن تكون خطة هذا البحث شاملة واضحة بقدر ما أمكننا الله وما استطعنا فإن كان فيها قصور فمن أنفسنا وما كان فيها من كمال فبتوفيق من الله.

إشكالية البحث:

نعلم جميعًا أن القانون يعتمد أركانًا محددة ليكيف الفعل بأنه جريمة فهناك الفعل والضرر والرابطة السببية بينهما أو العلاقة السببية كما يصفها البعض، كما أن للجريمة أركانًا، وهنا تكمن أهمية البحث حيث إن الأضرار في الذكاء الاصطناعي ومنها الميتافيرس هي أضرار متنوعة من حيث كونها مباشرة أو غير مباشرة، أو أضرارًا واضحة أو خفية، أو أضرارًا يمكن قياس حجم الضرر فيها وأخرى لا يمكن، بل قد تحدث الأضرار، ولا يمكنك إثباتها، أو إذا ثبتت فلا تجد تعويضًا عنها، كما أن صعوبات الإثبات في التقنيات هو أصعب منه عن عالم الواقع الملموس والمحسوس، من حيث ربط الفعل بالضرر (العلاقة السببية) فمن أضرار التقنيات ما هو صحي سواء كان من الأضرار الواضحة ـ كالتأثير على أذن الإنسان أو عينيه ـ ومنها ما هو خفي صعب التشخيص مثل التأثيرات النفسية، أو تأثيرات الموجات الإلكترونية، وكلاهما يحتاج إلى وقت قد يطول وقد يقصر تبعًا للكيفية التي يستخدم بها الأشخاص تلك التقنيات سواءً كان من حيث عدد الساعات أو طريقة الاستخدام أو نوع الأجهزة، كما أن التأثير يختلف من إنسان لآخر، هذا من ناحية ومن أخرى لما له من خطورة ما نحن والمستقبل وأبنائنا بصدده سواء كانت الصحية بنوعيها البدنية والنفسية، أو الأدبية والمعنوية، أو المادية المتمثلة في حفظ الحقوق والعيش بأمان، ذلك لما للشركات المتسابقة على الاستحواذ في مجال التقنية العالمية، والانفراد بها، ما يمكن أن يجعلنا ـ باعتبارنا مستهلكين لهذه الخدمات ـ فريسة لمطامع الربح والكسب والشهرة، فما نحن مقبلون عليه من التطور ـ إذا ما أسيء استخدامه ـ فستكون العاقبة جرائم لا يمكن وصفها كمًّا ولا نوعًا، هذا إذا مالم تكن هناك ضوابط وأخلاقيات واضحة ومحددة، ولعل ما قامت به الأمم المتحدة كما ذكرنا في مقدمة هذا البحث من تبنيها اتفاق أخلاقيات الذكاء الاصطناعي التي وقعت عليه 193 دولة، وما قام به الاتحاد الأوربي من سبق في تجييش مُشرعيه لتجهيز مشروع قانون الذكاء الاصطناعي وتمرريه والموافقة عليه أكبر دليل على ذلك.

يضاف إلى ذلك صعوبة المحافظة على بيانات (8) المستخدمين، وهذا أخطر ما يتعرض له المستخدمين العاديين فضلا عن مؤسسات مالية تم اختراقها ونهب أموالها، بالإضافة إلى ما تم تسريبه من بيانات ومعلومات تشكل خطرًا على الأمن القومي والعلاقات الدبلوماسية وتكشف الكثير من الأسرار، فلا أحد معصوم من هذا التسريب مهما كانت احتياطاته وبلغ حذره.

كما تدور محاور هذا البحث حول جرائم الميتافيرس، من حيث الماهية والقوانين الواجبة التطبيق فيها، ويحاول أن يقدم البحث الحلول القانونية لتلك الجرائم، ويرسم علاقة جرائم الميتافيرس بالقوانين السارية ذات العلاقة، مثل قوانين حماية البيانات الشخصية وقوانين مكافحة الشائعات والجرائم الإلكترونية، وقانون العقوبات.

أهمية البحث:

لا يخفى على الجميع أن هذه التقنية ما زالت في باكورة تطورها، لذا من الأهمية بمكان أن يكون المشرع مستوعباً لهذا التقنية وانعكاساتها الاجتماعية والاقتصادية والصحية على المجتمع، لا سيما وأن دستور الدولة هو من ضمن حقوق الفرد في سرية بياناته وحفظ معلوماته، وسلامته وصحته وتوفير بيئة آمنة له، لذا جاءت أهمية هذا البحث، في محاولة من الباحثين لإيجاد بعض الحلول.

أهداف البحث

يحاول البحث عن الإجابة عن بعض الأسئلة التي تطرح نفسها إزاء هذه التقنية التي من الممكن أن تكون مفيدةً جداً للمجتمعات إذا ما استخدمت ضمن الأطر التي يضعها المشرع تحقيقاً للمصلحة العامة، ومن هذه الأسئلة التي يجيب عنها البحث:

- ماهية الميتافيرس وتعريفها؟
- ماهية الجرائم الإلكترونية، وحماية المستخدم، وحفظ البيانات الشخصية، وهل القوانين الصادرة قادرة على مجابهة الواقع والمستقبل؟
- هل نملك المؤسسات والأجهزة التي تؤمن لنا كشف تلك الجرائم؟
- وإذا ما كانت عناصر الجريمة فعلا ورابطة سببية وضررًا، فما الضرر الذي من الممكن أن يلحق للأفتار (Avatar؟) في عالم الميتافيرس، وكيف يمكننا ربط السببية بين الفعل والضرر
- وإذا كانت للجريمة ظرف زماني ومكاني فما حدود انطباقهما على الفعل الذي يعد جريمة في عالمنا المادي، إذا ما حصل في العالم الافتراضي الميتافيرس؟

المنهج المستخدم في البحث:

المنهج التحليلي، حيث سنحلل نوع وتصنيف الجرائم التي تحدث في عالم الميتافيرس، والحماية القانونية للمستخدم، والنظر في قوانين مكافحة الشائعات والجرام الإلكترونية وقوانين حماية البيانات الشخصية ومعرفة هل يمكن لهذه القوانين حماية المستخدم في عالم الميتافيرس؟

ولكل ما ذكرنا نجد من المناسب وضع الخطة الأتية:

المبحث الأول: الميتافيرس وحفظ البيانات الشخصية

المطلب الأول: تعريف وماهية الميتافيرس
الفرع الأول: تعريف الميتافيرس
الفرع الثاني: ماهية الميتافيرس
المطلب الثاني: ماهية البيانات الشخصية والحماية القانونية
الفرع الأول: ماهية البيانات الشخصية
الفرع الثاني: الحماية القانونية للبيانات الشخصية

المبحث الثاني: الجرائم الإلكترونية وجرائم الميتافيرس أنواعها وطبيعتها

المطلب الأول: الجرائم الإلكترونية وجرائم الميتافيرس
الفرع الأول: ماهية الجرائم الإلكترونية:
الفرع الثاني: طبيعة الجرائم الإلكترونية
المطلب الثاني: حماية المستخدم في جرائم الميتافيرس
الفرع الأول: الاختراق:
الفرع الثاني: الإضرار بأنظمة المعلومات

المبحث الثالث: المسؤولية القانونية في جرائم الميتافيرس والقانون واجب التطبيق

المطلب الأول: المسؤولية القانونية في جرائم الميتافيرس
الفرع الأول: المسؤولية القانونية على المستخدم في جرائم الميتافيرس
الفرع الثاني: المسؤولية القانونية لمزود الخدمة والوسيط ومن في حكمهم في جرائم الميتافيرس
المطلب الثاني: القانون واجب التطبيق في جرائم الميتافيرس
الفرع الأول: إثبات الجرائم الحاصلة في عالم الميتافيرس
الفرع الثاني: القانون الواجب التطبيق على جرائم الميتافيرس

ملخص البحث

تعرض هذا البحث إلى ماهية الميتافيرس وتعريفها وعلاقتها بالجرائم الإلكترونية، وكيف حمى قانون مكافحة الشائعات والجرائم الإلكترونية رقم 34 لسنة 2021 المستخدم من أنواع الجرائم التي من الممكن أن يتعرض لها في الميتافيرس، كما تعرض البحث لقانون حماية البيانات الشخصية رقم 45 لسنة 2021 وعلاقته بالميتافيرس، وبين البحث تعريفات البيانات الشخصية كما وردت في القانونين المشار إليهما، والفرق بين المعلومات والبيانات، وعلاقة جرائم الميتافيرس بالجرائم الإلكترونية وطبيعة تلك الجرائم، وكيفية إثباتها، كما ومن خلال البحث وجدنا أن المشرع الأمريكي في قانونه حفظ البيانات الشخصية راعى عدة جوانب، الدخول من حيث التصريح من عدمه، كما راعى مدة المكوث، واعتبر أن مجرد النظر أو قراءة البيانات الغير مصرح للشخص الاطلاع عليها يعتبر جريمة يعاقب عليها القانون، وهذا الذي لم يكن واضحًا في التشريع الإماراتي والمصري سواءً كان في قانون حفظ البيانات الشخصية أو في قوانين الجرائم الإلكترونية.

كما تناول البحث القانون الواجب التطبيق في جرائم الميتافيرس كأحد أنواع الجرائم الإلكترونية، والمسؤولية القانونية في تلك الجرائم، وطبيعتها، وكيفية حماية المستخدمين من خلال القوانين المنظمة وكذلك من خلال التوعية بأنواع تلك الجرائم والعقوبات المخصصة لها، ليكون هناك اكتمال بين مؤسسات الدولة وأفراد المجتمع في حماية أنفسهم.

مفاتيح البحث:

تعريف الميتافيرس، جرائم الميتافيرس، طبيعة الجرائم في الميتافيرس، حماية البيانات الشخصية، الجرائم الإلكترونية، القانون الواجب التطبيق، المسؤولية القانونية في جرائم الميتافيرس، المسؤولية القانونية على المستخدم في جرائم الميتافيرس، المسؤولية القانونية لمزود الخدمة والوسيط ومن في حكمهم في جرائم الميتافيرس

Summary of the research

This research is based on the nature and definition of the metaverse, its relationship to cybercrime, and how the Act of Anti-Rumor and Cybercrime No. 34/2021 protects the user from the types of crimes he may face in the metaverse.This research also studied the personal data protection law No. 45/2021 and its relationship with Metavers.Also, the definitions of personal data as stated in the two acts referred to, the difference between information and data, the relationship between Metavers and cyber crimes, the nature of such crimes, and how to prove them

In the course of the research, we found that the United States legislature, in the Personal Data Act, has taken into account several aspects, including authorized or non-authorized entry as well as the duration of the stay. The law considers that the mere consideration or reading of data by an unauthorized person is a punishable offense. This condition was not clear in the legislation of the United Arab Emirates and Egypt, whether it is in the personal data protection law or in the laws of cyber crimes.The research also examined the law applicable to metavers as one of the types of cybercrime, the legal responsibility for such crimes, the nature of the crimes, and how to protect users through law regulations as well as by raising awareness about the types of such crimes and the penalties allocated to them, so that state institutions and members of society are fully involved in protecting themselves.

المبحث الأول: الميتافيرس وحفظ البيانات الشخصية

Metaverse and saving personal data

لعل ما حدث للعالم من أزمة كورونا كان أحد أهم أسباب تحفيز العالم للاتجاه إلى عدم حدودية التواصل وإنهاء الأعمال بالشكل التقليدي (Physical word)، أو قد يكون حدوثها لتحفيز العالم للقبول بهذه التقنية لما عاناه من عزلة عطلت تواصله بعائلته ومسيرته؟ سواءً العلمية أو التجارية، مما جعل الاتجاه إلى العالم الرقمي (Digital world) الذي بدأ بشكله البسيط من خلال مواقع التواصل الاجتماعي وتطبيقات الاتصال المسموعة والمرئية، ليتطور إلى ما نحن بصدده وهو العالم الافتراضي الميتافيرس (Metaverse) الذي يتجسد فيه الإنسان بشكله أو ما يختار أن ينوب عنه من تصاميم يوفرها التقنيون الهواة، أو الشركات، أو ينقل تراسميه من خلال أجهزة الماسح (Scanner) الضوئي ليجتمع مع من يريد حول العالم في الزمان والمكان الذي يحددانه متخطين الحدود الجغرافية، دون مشاق السفر وإجراءات الفيز والسماح والمنع، ويمكن أن يكون هذا الاتصال من خلال بناء واقع افتراضي من قبلهم، أو الاستعانة بواقع افتراضي صمم من الغير، كمن يختار واجهة أو خلفية لهاتفه النقال أو جهاز الحاسوب الشخصي.

ولدراسة هذا المبحث فقد خصص له مطلبان:

المطلب الأول: تعريف وماهية الميتافيرس. Definition and nature of the Metaverse

المطلب الثاني: ماهية البيانات الشخصية والحماية القانونية. The Notion of Personal Data and Legal Protection

المطلب الأول: تعريف وماهية الميتافيرس

Definition and nature of the Metaverse

لابد ونحن نبحث في هذا الموضوع أنه نبين بشكل مختصر تعريف الميتافيرس وماهيتها، كي نستطيع فهم هذا المصطلح وما يعنيه، ثم التعرف على أثره القانوني في واقعنا، وعلاقة القوانين والتشريعات، وما مدى حاجتنا إلى المزيد منها، وما ستعاجله تلك القوانين تماشيًا مع تلك الطفرة التكنولوجية الحديثة، لا سيما أن الجريمة لا تعرف الحدود، فقد انتقلت من العالم المادي إلى العالم الإلكتروني بصور مختلفة، فمن التجسس وسرقة البيانات إلى تسريبها وصولًا إلى غسيل الأموال والإرهاب.

هذا بالإضافة إلى أن تقنية الميتافيرس والسباق المحموم حول الاستحواذ على هذه التقنية، سيؤدي إلى الإخلال بكثير من النظم، ومنها المنافسة، إذ ستؤدي هذه الهيمنة إلى إساءة استخدام الوضع المسيطر من قبل المؤسسات المسيطرة على تلك التقنية، (9).

فهل تختلف الجريمة في عالمها الافتراضي عن تلك في العالم المادي الحقيقي؟

وسيتم دراسة هذا المطلب في فرعين:

الفرع الأول: تعريف الميتافيرس. Definition of Metaverse

الفرع الثاني: ماهية الميتافيرس. The Notion of Metaverse

الفرع الأول تعريف الميتافيرس
Definition of Metaverse

يرجع أصل مصطلح الميتافيرس إلى كلمتين (Meta) الذي يعني ما وراء أو ما بعد[10] وكلمة (Verse) التي في الحقيقة ترجمتها أنها كلمة يونانية قديمة، وظفها الروائي الأمريكي نيل تاون ستيفنسون (Neal Town Stephenson) [11] في إحدى قصصه عام 1992م حملت اسم "تحطم الثلج" (Snow Crash) التي تحولت إلى فيلم سينمائي، ليس كما أشارت إليها بعض المصادر أنها تعني الكون[12]، والشيء بالشيء يذكر فإن مصطلح الفضاء السيبراني، هو الآخر كان ناتجًا عن رواية أسمها نيورومانسر (Neuromancer) لأديب أمريكي واسمه ويليام غيبسون (William Gibson) عام 1984 ميلادية. ويرى البعض أن ظهور هذين المصطلحين وغيرهما هو محض صدفة من كاتبين أو أديبين، استشرفا المستقبل، وأعتقد أنّ ادعاء المصادفة بعيد جدًّا، وأن الصواب أن الشركات الكبرى ـ قبل طرحها لأي منتج له تأثير كبير على المجتمعات ـ تحاول قراءة الانطباعات والانعكاسات من خلال ما تسربه من معلومات من خلال الأفلام أو الشائعات، أو ما يسمى الفرضيات دون أن تأكيدها أو تنفيها، ومن المناسب ونحن بصدد هذين المصطلحين أن نعرف الفرق بينهما فالفضاء السيبراني أوسع وأشمل، وإنما الميتافيرس هي مستخدم لهذا الفضاء.

ولم تختلف تعريفات الميتافيرس بعضها عن بعض كثيرًا فجميع التعريفات مأخوذة من عمل التقنية ذاتها فقد عرفها البعض بأنها "عوالم رقمية بديلة لا يمكن تمييزها عن العالم المادي الحقيقي")[13].

وقال آخرون: إن الميتافيرس "هو عالم افتراضي مشترك يمكن للمستخدمين الوصول إليه من أي نظام أساسي عبر الإنترنت، وحيث يمكنهم التفاعل مع صورهم الرمزية الافتراضية. يمكن الوصول عبر الواقع الافتراضي أو الواقع المعزز أو مزيج من الاثنين معًا" [14]. وعرفها ستايلونز مايستكيديز (Stylianos Mystakidis) بأنها "عبارة عن بيئة متعددة المستخدمين دائمة ومستمرة يتم فيه دمج الواقع المادي مع الواقعية الرقمية، وهو يعتمد على تقارب التقنيات التي تتيح التفاعلات متعددة الحواس مع البيانات الافتراضية (VR) والواقع المعزز (AR)، ويتم تمثيل المستخدمين فيها بصورة رمزية يتم التفاعل بينها في الوقت الفعلي وبإحساس غامر يعيشه المستخدمين ويطلق على هذه الرموز آفاتور (Avatar)" [15].

وقد نستخلص تعريفًا مما سبق أن الميتافيرس **"تقنية تعمل بأدوات مساعدة يظهرون فيها على شكل أبعاد ثلاثية مشفرة أو مرمزة أفتار (Avatar) [16]، يختارون بمحض إرادتهم محل تواجدهم في واقع يفترضونه من بيئتهم الحقيقية أو يستعينون بواقع من تصميم الغير يرغبون التواجد به ليمارسوا مختلف أنشطتهم مع بعضهم البعض (NFT) [17] غير قابلة للاستبدال، ليحققوا مبتغاهم من هذا التجمع سواء أ كان تعليميًّا، أو تجاريًّا، أو ترفيهيًّا، أو اجتماعيًّا، أو بغرض إنجاز الأعمال"**.

الفرع الثاني: ماهية الميتافيرس
The Notion of Metaverse

من خلال التعريفات السابقة عرفنا إلى حدٍّ ما ماهية عمل الميتافيرس، ولم نكن بصدد التفصيل في كيفية عملها إلا ليكون لدينا تصورٌ كافٍ وواضحٌ، فالميتافيرس لا تتم إلا بوجود الشبكة العنكبوتية (Internet) والمتخصصون في هذا المجال يتحدثون عما سيكون أفضل في الجيل الخامس منها، وتأثيره في تحفيز الميتافيرس كعامل مساعد لسرعة نقل البيانات في هذا الجيل، بالإضافة إلى تطور الأدوات المساعدة للدخول إلى الميتافيرس بمختلف أنواعها.

تعمل الميتافيرس من خلال الجمع بين العالمين الافتراضي (Virtual Reality) الذي يختصر بـ (VR) وبين العالم المعزز أو الحقيقي (Augmented Reality) الذي يتم اختصاره بـ (AR)، لذا إنا كنا نفكر بالميتافيرس فيجب أن نراه على أنه بيئة للحياة الافتراضية تعيشها بجميع حواسك بدلًا من مجرد النظر إليه كما نتعامل مع الانترنت حاليًّا.

وللدخول إلى عالم الميتافيرس هناك أجهزة مساعدة وبروتوكولات ـ وليست محددة بما نراه اليوم فقط، ففي هذا العالم لك أن تتخيل أنه بدلًا من الجهاز الذي ترتديه اليوم على الرأس (AR) أو السماعة (VR) قد تكون مجرد عدسة لاصقة تضعها على عينيك وتقرأ افكارك وتنقلها إلى العالم الافتراضي.

ولعل من المناسب توضيح الفرق بين مصطلحين من خلال استعراض طريقة عمل كل منهما حيث يصعب التفريق بينهما للوهلة الأولى وهما أفتار (Avatar) ومصطلح (Non-Fungible Tokens) والذي يعبر عنه اختصارًا (NFT) كم يلي:

فكلا المصطلحين مشفرين ومرمزين بحيث يدلان على مالكهما، لكن الفرق بينهما أن أفتار (Avatar) هو نسخة من مالكه يبنى عن طريق فهم شخصية وسلوكيات المالك الحقيقي ويعبر عنه [18]، أما مصطلح (NFT) فهو من الممكن أن تكون صورة للشخص أو لأي شيء آخر، ويمكن تداولها وبيعها عن طريق العملات الرقمية، وقد تصل الصورة إلى ملايين الدولارات، والسبب في ذلك ندرتها. وعدم إمكانية نسخها، ويسجل في البلوكتشين [19] (Blockchain) جميع المالكين لها ويمكن من خلاله تتبع الأصول في شبكة الأعمال، ويمكن ـ أيضًا ـ أن يكون ملموسًا كالأشياء المادية، أو غير ملموس مثل الحقوق الأدبية والمعنوية.

المطلب الثاني: ماهية البيانات الشخصية والحماية القانونية
The Notion of Personal Data and Legal Protection

لعل من أبسط حقوق المستهلك هو حفظ بياناته وخصوصياته، وعدم تداولها أو نشرها أو استخدامها دون إذن منه، سواءً كانت لغرض الدراسة أو التسويق أو الإحصاء، ولعل القضاء مليء بتلك القضايا التي تبين فيها أن الشركات سربت أو استخدمت بيانات عملائها دون إذنهم، أظهرت فضيحة كامبريدج أنالاتيكا في عام 2014 أن بيانات أكثر من 87 مليون مستخدم لشبكة فيسبوك قد تم استخدامها دون تصريح لأغراض سياسية ومن أشهرها قضية الفيس بوك الذي تغير اسمه إلى (Meta) [20]، إذ تتفيأ الشركات الأمريكية بمضلة الحماية من القانون الذي يخولها أن تعالج المعطيات الشخصية لمواطنين غير أمريكيين مهما كان موقعهم في العالم وتخزينها لديها ولو خارج

التراب الأمريكي، كما يخول قانون (Cloud Act) [21] المؤسسات الحكومية الأمريكية الولوج إليها دون علم الأشخاص المعنيين، وهذا الجزء يخرق سيادة الدول وحقوق المستخدمين معاً.[22]

ليس هذا وحسب بل لعل من المناسب القول إن سلامة المستهلك لهذه التكنولوجيا لا يقل أهمية من حماية بياناته الشخصية، إن الاستخدام المفرط للتكنولوجيا الرقمية يرتبط بالعديد من المشاكل النفسية والعقلية، حيث أن هاته العوالم الافتراضية قد تسبب الهلوسات والإدمان الإلكتروني، يرى العالم (Born. Zyss) أن التكنولوجيا قد تقود إلى تداخل بين الواقع الافتراضي والواقع المعزز [23]، فالشركات تبحث عن أقل التكاليف وأكبر الأرباح، ولو كان هذا على حساب المستهلك، ناهيك عن الأعطال الممكنة الحدوث، والشواهد في هذا الإطار كثيرة، فعلى سبيل المثال ما حصل من هاتف سامسونج من أعطال في البطارية تسبب انفجار الهاتف (Galaxy Note 7)، والخسائر التي تسبب بها سواءً كانت على الصعيد البشري أو المادي، واعترفت الشركة بتحملها المسؤولية الكاملة عن تلك الخسائر، دون أن تلقي اللوم على الشركة الموردة للبطاريات، أو تبرر خطأها كما تفعل بعض الشركات، كذلك ما ورد من عقوبة فرضتها هيئة الرقابة الفرنسية لمراقبة المنـــــافسة على شـــركـــة أبل وتقدر تلك الغرامة بـ (27) مليون دولار[24]، وذلك لأنها لم تخبر مستهلكيها بتخفيض سرعة الهاتف مما اعتبرته الهيئة غشًّا وخداعًا للمستهلك، والقضايا في حقيقة الأمر أكثر من أن تحصر، ومن المخيب للآمال في حقيقة الأمر أنه لم يكن لشرق أو سطنا أي عقوبات تفرض على تلك الشركات.

لذا أولتها القوانين عناية فائقة إذ وردت في قانونين مستقلين لأغلب القوانين، فترد في قانون الجرائم الإلكترونية وترد في قانون منفصل تحت مسمى قانون حفظ البيانات، ومن الأمثلة على ذلك قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي، وقانون حماية البيانات الشخصية رقم (45) [25]، وقانون حماية البيانات الشخصية المصري [26]، ونظام حماية البيانات الشخصية السعودي [27]، وكذلك لائحة الاتحاد الأوربي (General Data Protection Regulation) واختصارها بـــ (GDPR) التي وضعت القواعد المتعلقة بحماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية [28]،ولعل من المناسب تناول هذا المطلب في فرعين:

الفرع الأول: ماهية البيانات الشخصية. The Notion of Personal Data

الفرع الثاني: الحماية القانونية للبيانات الشخصية. Legal Protection of Personal Data

الفرع الأول: ماهية البيانات الشخصية
The Notion of Personal Data

تتنافس الشركات في طرق وكيفية تجميع أكبر ما يمكن من المعلومات والبيانات حول أي شيء يمكن أن تجعل منه مادة للربح، ولا شك أن ما نراه من تصاعد في التكنولوجيا ليس إلا عبارة عن بيانات ومعلومات، فالذكاء الاصطناعي (AI) ليس وليد الصدفة أو اللحظة، بل هو عبارة عن حلقة في سلسلة التطور الاستراتيجي، والدليل على ذلك أننا نرى معظم الابتكارات التي نراها الآن قد تم مشاهدتها في أفلام الخيال العلمي، وكأنها تمهيد نفسي للإنسان لما سوف يحدث.

وإن كنا نتحدث عن حفظ المعلومات أو البيانات الشخصية فإننا نتحدث عن شقين أخلاقي وقانوني، من حيث إننا مأمورون دينيًا واجتماعيًا بعدم التنصت أو إفشاء أسرار الغير أو التدخل في شؤونهم، وقانونيًّا لعقاب من يخالف تلك الأخلاق الاجتماعية التي وإن تعددت المجتمعات إلا أنها ثابت من ثوابت العموم.

ولعلنا نعرف خطورة ما نحن مقدمين عليه، إذا ما عرفنا أن اتفاقية درع الخصوصية (Privacy Shield) التي عقدت بين الولايات المتحدة الأمريكية وبين الاتحاد الأوربي في عام 2016 بصفتها إطار قانونيًّا مناسبًا لتنظيم عمليات تبادل البيانات الشخصية للمستخدمين عبر المحيط، لأغراض محددة، بين الاتحاد الأوربي والولايات المتحدة الأمريكية لم تعد سارية بعد قرار محكمة العدل التابعة للاتحاد الأوربي بعدم نفاذ تلك الاتفاقية، وأنها لم تعد صالحة لمتطلبات حماية البيانات في الاتحاد الأوربي، في حال نقل البيانات الشخصية من الاتحاد إلى الولايات المتحدة الأمريكية(29).

وبعد ذلك أقامت منظمات أوربية ونشطاء في مجال حماية البيانات والخصوصية دعاوى قضائية على المكتب الإقليمي لفيس بوك سابقًا ــ حاليًا Meta ــ وأبل في إيرلندا، طالبت فيها بعدم تمرير بيانات الأوربيين إلى وكالة الأمن القومي الأمريكية والتيقن من مستوى حماية هذه البيانات حفاظًا على خصوصية الأوربيين، ولكن وكالة مراقبة البيانات الإيرلندية (ODPC) رفضت الدعوى على أساس أن شركة ميتا (Meta) مسجلة في اتفاقية الملاذ الآمن (EU Safe Harbor Agreement) التي أقيمت عام 2000 بين الولايات المتحدة الأمريكية والاتحاد الأوربي (30).

ولكي نعرف المقصود بالبيانات الشخصية، لزم أن نعرف ماذا قصد المشرع بالبيانات الشخصية في قانون حماية البيانات الشخصية الإماراتي وكذلك قانون مكافحة الشائعات والجرائم الإلكترونية؟

قسم المشرع الإماراتي في قانون حفظ البيانات الشخصية الإماراتي في مادته (1) البيانات الشخصية كما ورد في تعريفاتها كالآتي:

تعريف البيانات الشخصية:

"أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق ربطه ببعض العناصر، مثل الاسم أو الصوت أو الصورة أو الرقم التعريفي، أو بيانات معرف الإنترنت أو الموقع الجغرافي، أو من خلال الإشارة إلى واحد أو أكثر من الخصائص المادية أو الفيسيولوجية أو الثقافية أو الاجتماعية لهذا الشخص الطبيعي." (31)

تعريف البيانات الشخصية الحساسة:

أي بيانات تكشف بشكل مباشر أو غير مباشر عن عائلة الشخص الطبيعي، أو أصله العرقي، أو آرائه السياسية أو الفلسفية أو معتقداته الدينية، أو سجل السوابق الجنائية الخاص به، أو بيانات القياسات الحيوية البيومترية الخاصة به، أو أي بيانات تتعلق بصحة هذا الشخص، وتشمل حالته الجسدية أو النفسية أو الذهنية أو العقلية أو البدنية أو الجينية أو الجنسية، بما في ذلك المعلومات المتعلقة بتوفير خدمات الرعاية الصحية له التي تكشف عن وضعه الصحي.

تعريف البيانات الشخصية البيومترية:

البيانات الشخصية الناتجة عن المعالجة باستخدام تقنية محددة تتعلق بالخصائص الجسدية أو الفسيولوجية أو السلوكية لصاحب البيانات، التي تسمح بتحديد أو تؤكد التحديد الفريد لصاحب البيانات، مثل صورة الوجه أو بيانات البصمة.

صاحب البيانات:

الشخص الطبيعي موضوع البيانات الشخصية.

لم يذهب بعيدًا المشرع في قانون حفظ البيانات الشخصية المصري في الفصل الأول المادة (1) فعدد البيانات الشخصية والمعالجة [32] والبيانات الشخصية الحساسة، وكذلك الشخص المعني بالبيانات، وكذلك ذهب المشرع في نظام حماية البيانات الشخصية السعودي، إلا أنه فصل أكثر في تعريفات كان الأولى تركها لتشرح في اللائحة التنفيذية.

وتطرق كما أسلفنا قانون مكافحة الشائعات والجرائم الإلكترونية تعريف البيانات الشخصية في المادة (1) بأنها "**المعلومات أو البيانات الخاصة بالأشخاص الطبيعيين متى كانت مرتبطة بحياتهم الخاصة أو تحدد هويتهم أو يمكن من خلال ربط هذه المعلومات والبيانات بطريقة مباشرة أو غير مباشرة تحديد ومعرفة هوية الشخص**"، ونلاحظ من خلال تعريف أنه تعمد العموم والشمولية.

عرفت لائحة الاتحاد الأوربي (GDPR) [33] في المادة (4) الفقرة (1) البيانات الشخصية على أنها " **أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديد هويته**"، وحددت الشخص الطبيعي " **هو الشخص الذي يمكن التعرف عليه، بشكل مباشر أو غير مباشر، ولا سيما بالرجوع إلى معرف مثل الاسم أو رقم التعريف أو بيانات الموقع أو معرف عبر الإنترنت أو إلى واحد أو أكثر من العوامل المحددة للعوامل الجسدية أو الفسيولوجية أو الهوية الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لذلك الشخص الطبيعي**".

الفرع الثاني: الحماية القانونية للبيانات الشخصية

Legal Protection of Personal Data

لعل أبرز وأهم ما يبحث المستخدمون عنه هو حماية بياناتهم الشخصية، لما لها من أهمية كبيرة سوءً من الناحية الأمنية أو من حيث شعورهم بالخصوصية، إذ لا يخفى على الجميع ما تعنيه البيانات والمعلومات من تأثير على الأسواق، بل ويمكن من خلالها دراسة احتياج المستخدمين والمتاجرة بمعلوماتهم بين الشركات، ولا نعني هنا بالبيانات ذلك المعنى السطحي الذي يشمل المعلومات العامة من أسم أو عمر أو اهتمامات أو غيرها، بل يجب أن نمضي بعيداً، ففي دراسة أجرتها مجلة (Nature) في أكتوبر 2020 خلصت إلى أن تتبع بيانات الواقع الافتراضي ووضعية الجسم والحركات يعد مصدراً قوياً للمعلومات من خلال إنشاء روابط بين حركات معينة للجسم والإبداع والتعلم والسمات السلوكية الأخرى، [34] لذا أولت الأمم المتحدة هذا الجانب واعتبرته جزءًا من حقوق الإنسان، فأصدرت المبادئ التي تستند إليها الخصوصية وحماية البيانات الشخصية رقم (A/196/77)، ناقشت تلك المبادئ القانونية والشرعية والمشروعية، والموافقة والشفافية، والغرض، والإنصاف والتناسب، والتقليل إلى الحد الأدنى، والجودة، والمسؤولية، والأمن، واعتبرها أنها تشكل أساس النظام القانوني للخصوصية وحماية البيانات الشخصية (35).

كما طبقت اللائحة العامة لحماية البيانات (GDPR) منذ 25 مايو 2018 في جميع أنحاء الاتحاد الأوروبي. وتهدف إلى حماية الحقوق والحريات الأساسية للأشخاص الطبيعيين، وعلى وجه الخصوص، حقهم في حماية بياناتهم الشخصية، دون تقييد حرية حركة هذه البيانات داخل الاتحاد الأوروبي (المادة 1). وعلمت اللائحة العامة على توسيع نطاق حماية البيانات المحلي والإقليمي (المادة 2 و3). كما وتحدد اللائحة 26 مفهوما، بعضها جديد والبعض الآخر ليس جديدا (المادة 4). في حين أن المواد من 5 إلى 11 تجمع المبادئ العامة، بينما تخصص المواد من 85 إلى 91 أحكامًا محددة. (36)

حماية البيانات والمعلومات الشخصية في قانوني حماية البيانات الشخصية وقانون مكافحة الشائعات والجرائم الإلكترونية

1. قانون حماية البيانات الشخصية الإماراتي

بداية حدد القانون نطاق سريان القانون في المادة (2) والمستثنى منه، وفي المادة (4) حدد حالات المعالجة المسموح بها دون موافقة صاحب البيانات أو المعلومات، وذكرها على سبيل الحصر وليس المثال، ثم تحدث في المواد (16،17) عن حق تقييد المعالجة أو إيقافها، ووضح في المادة (5) الضوابط الخاصة بمعالجة البيانات الشخصية، وفي المادة (6) شروط الموافقة على معالجة البيانات.

2. قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي

عنون مادته (6) بالاعتداء على البيانات والمعلومات الشخصية والمادة (13) إذا ما تم جمع ومعالجة البيانات والمعلومات الشخصية بالمخالفة للتشريعات، وعرف في ذات القانون في المادة (1) البيانات أو المعلومات، والبيانات والمعلومات الحكومية، والبيانات والمعلومات الشخصية كما أوردناها سابقًا، والمعلومات والبيانات السرية (37).

وفرض عليها العقوبات القاسية، ويبقى القول إذا ما كانت تلك العقوبات رادعة أو لا نحتاج إلى دراسة ميدانية معمقة، ورغم ما تناولته القوانين من حماية، يبقى السؤال محور تلك القوانين وعمودها الذي تقوم عليها كل العقوبات، وهو المسؤول عن تلك الأفعال المخالفة إن حدثت، إن صعوبة تحديد المسؤولية ما بين المستخدم نفسه في قصوره أو إهماله، وما بين التقنيات وما بين الخوادم وما بين المجهزين للخدمة سواءً من شركات الاتصالات أو أصحاب المواقع الإلكترونية، وما مدى استعداد الأجهزة الحكومية في استقبال، وحل مثل تلك الجرائم، وهي تزداد باضطراب وتتطور بشكل سريع ويحتاج إلى عمل دؤوب ومستمر.

المبحث الثاني: الجرائم الإلكترونية وجرائم الميتافيرس أنواعها وطبيعتها

Cybercrimes and Metaverse Crimes, Their Types and Nature

لابد ونحن نتحدث عن الجرائم الإلكترونية من تحديد تعريف لهذه الجريمة، ولم أجد تعريفًا لها في قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي(38)، وكذلك في قانون مكافحة جرائم تقنية المعلومات المصري(39)، في حين عرفتها (اتفاقية بودابست) (40) التي انعقدت بدولة المجر أنها " **كافة النشاطات غير القانونية أو غير المشروعة المرتبطة بأجهزة الكمبيوتر وباستخدام الشبكة العنكبوتية**"، وصنفت هذه الجرائم المرتكبة إلى عدة فئات منها الجرائم التي ترتكب ضد سلامة المعلومات وخصوصيتها، والجرائم ذات الصلة بالكمبيوتر، والجرائم المتعلقة بمحتوى الكمبيوتر، والجرائم المتعلقة بالعلامات التجارية والملكية الفكرية (41).

والملاحظ من خلال التعريف السابق أن التعريف يبدو غير دقيق من حيث أن الغير مشروع هو ذاته غير القانوني، وكذلك قد تكون هناك جرائم إلكترونية ولا ترتبط بالشبكة العنكبوتية، ويصاف على التصنيفات هناك جرائم الاعتداء على الرمز في فضاء الميتافيرس، وأيضاً هناك الجرائم الواقعة على الأشخاص من اعتداء لفظي أو ازدراء، أو كراهية أو عنصرية.

ومن المعروف في العرف القانوني أن ترك التعريف يكون غالباً لإفساح المجال للفقه والقضاء لتعريفها بما يتطلب ويواكب التطورات السريعة في هذا المجال، ولعلنا نجد تعريفًا مناسبًا للجريمة الإلكترونية إذا ما قلنا أنها "**كل فعل أو ترك يخالف عليه القانون، حدث عبر الشبكة العنكبوتية أو لم يحدث من خلالها، مستعينًا بأي تقنية كانت من برامج أو أجهزة إلكترونية أو ممغنطة**"، ويضاف لها في التعريف إذا ما تحدثنا عن العالم الافتراضي "وأن يكون مكانها العالم الافتراضي"، إذ وإن تشابهت الجرائم في عالمنا المادي بتلك الجرائم الإلكترونية، إلا أنها تختلف عن تلك التي تحدث في العالم الافتراضي من حيث المكان، فالأخيرة مكانها العالم الافتراضي حصرًا، هذا إذا ما اعتبرنا أن الرموز المشفرة التي تعبر عنا في الميتافيرس بدأ في التصرف من خلال تعلمها الذاتي مستخدمة الذكاء الاصطناعي.

وبوجود هذه الجرائم فرض المشرع لها العقوبات حسب ما ورد في تلك القوانين، ولا بئس من إلقاء نظرة عن تلك الجرائم التي قننت ضمن قانون الجرائم الإلكترونية على عجالة لنعرف الفرق بين تلك الجرائم وبين ما يمكن أن يحدث من جرائم في عالم الميتافيرس ولنرى إذا ما كان قانون الجرائم الالكتروني وحده كافيًا.

يعد مبدأ "**لا عقوبة ولا جريمة إلا بنص**" من المبادئ القانونية العامة، ونحن بصدد تحديد ما هو مجرم من الأفعال في العالم الإلكتروني، لا بد من الرجوع إلى القوانين التي شُرعت لحماية المتعاملين في هذا المجال، ليتبين لنا ما هي تلك الأفعال وما هي عقوبتها، وهل تعد كافية لما هو قادم، وما هو من الممكن أن يحدث في عالم الميتافيرس، لا سيما وأنهما (عالم الإلكترونيات، والميتافيرس) متلازمان إذ لا ميتافيرس بدون عالم الإلكترونيات، وسيكون دليلنا في هذا النطاق جملة من القوانين الأجنبية والعربية ذات الصلة.

وقبل الخوض في بيان تلك الأفعال المجرمة وعقوباتها، وبيان أن للجريمة ظرفًا زمانيًّا ومكانيًّا، لابد من إيراد بعض التعريفات لتتوضح لنا الحدود المكانية في عالم الجرائم الإلكترونية التي على أساسها يكيف الفعل على أنه من نوع تلك الجرائم.

وسيكون في مطلبين:

المطلب الأول: الجرائم الإلكترونية وجرائم الميتافيرس. Cybercrimes and Metaverse Crimes

المطلب الثاني: حماية المستخدم في جرائم الميتافيرس. User Protection in Metaverse Crimes

المطلب الأول: الجرائم الإلكترونية وجرائم الميتافيرس
Cybercrimes and Metaverse Crimes

لا شك أن كل جريمة تستخدم فيه التقنية سواءً كانت مرتبطة بالشبكة العنكبوتية أم لا، تعد جريمة إلكترونية ويتبين ذلك من خلال تعريف المستخدم في قانون مكافحة الشائعات والجرائم الإلكترونية الذي سوف يذكر لاحقًا في تناولنا للجرائم الإلكترونية، والقضايا كثيرة وتملأ أرفف المحاكم، ففي تقرير عن حجم الخسائر الناتج عن الجرائم الإلكترونية المتوقع لسنة 2025 قد يبلغ 10.5 تريليون دولار مقارنة بسنة 2015 الذي بلغ حجم الخسائر فيها إلى 3 تريليون دولار، وتتوقع الشركة أنه تزيد الجرائم بنسبة 15% سنويا(42)، ومع دخول المستخدمين عالم الميتافيرس لن يكون ذلك العالم أكثر آمنًا، ولا بد من تظافر الجهود بين الهيئات الحكومية ومؤسسات المجتمع المدني من خلال نشر التوعية وحث المستخدمين على اتباع الخطوات التي تحقق لهم المزيد من الأمن.

ويسعى علم النفس الجنائي إلى معالجة كل من نظرية الجريمة الإلكترونية وكيفية التعامل معها، حيث تشرع الحكومات القوانين من جهة ومن أخرى من خلال السياسات والإجراءات التي تصدرها الشركات. (43)

وقد عرفها مؤتمر الأمم المتحدة في سنة 2000 م، **"بأنها الجريمة التي يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب، أو في بيئة إلكترونية"**، وعرفها أيضاً خبراء منظمة التعاون الاقتصادي والتنمية الجريمة الإلكترونية **"بأنها كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/أو نقلها، وقد وضع هذا التعريف مجموعة من الخبراء المشار إليهم للنقاش في اجتماع باريس الذي عقد عام 1983"**. (44)

ولدراسة هذا المطلب سيتم تقسيمه إلى فرعين:

الفرع الأول: ماهية الجرائم الإلكترونية. The notion of Cybercrime

الفرع الثاني: طبيعة الجرائم الإلكترونية. The Nature of Cybercrime

الفرع الأول: ماهية الجرائم الإلكترونية
The Notion of Cybercrime

وقبل الخوض في بيان تلك الأفعال المجرمة وعقوباتها، من المناسب ذكر بعض التعريفات ليتوضح لنا أولًا ماهية تلك الجرائم والكيفية التي تمت بها ليتوضح على أساسها ويكيف الفعل على أنه من نوع تلك الجرائم أم لا.

عرف المشرع الإماراتي في قانون مكافحة الشائعات والجرائم الإلكترونية جملة من المصطلحات العلمية التي تضفي على تلك الأفعال الوصف الإلكتروني، فقد عرف الشبكة المعلوماتية في المادة (1) على أنها **"ارتباط بين مجموعتين أو أكثر من البرامج المعلوماتية ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات"**، كما عرف مزود الخدمة على أنه **"كل شخص طبيعي أو اعتباري عام أو خاص يزود المستخدمين بخدمات الوصول بواسطة تقنية المعلومات إلى الشبكة المعلوماتية"**، وفي شمولية عامة لم يستثنِ الوسيط فعرفه في ذات المادة (1) **"كل شخص يقدم أي خدمات وسيط شبكة المعلومات ويشمل: خدمات وسائل التواصل الاجتماعي، ومحرك البحث، وتجميع المحتوى المرسل عبر شبكة المعلومات، ومشاركة**

الفيديو وما في حكمها"، وعرف المستخدم بأنه **"كل شخص طبيعي أو اعتباري يستخدم خدمات تقنية المعلومات أو يستفيد منها بأي صورة"**، وفي هذا التعريف يرى الباحث لو أن المشرع عمم في تعريف المستخدم ليصبح كالتالي **" كل شخص طبيعي أو اعتباري أو من ينوب عنهما بموافقتهما أيًا كانت صفته استخدام خدمات تقنية المعلومات أو يستفيد منها بأي صورة "**، وهذه الإضافة توسع من دائرة تعريف المستخدم لتكون مواكبة لما هو قادم، فقد تكون التكنلوجيا بأي شكل من أشكالها لا سيما في عالم الذكاء الاصطناعي قد تنوب عن المستخدم، وبدأنا نلمس هذا في المواقع الإلكترونية من وجود (chat) على مدار الساعة لتقديم المساعدة، وهو عبارة عن برنامج إلكتروني يتم تعليمه من خلال الذكاء الاصطناعي للبحث عن الأجوبة التي يتلاقها من قبل المستخدمين من خلال ما تم تعليمه من أجوبة محفوظة لديه، ومن الأمثلة الأخرى ذاك الذي يعرف عن نفسه بأنه المساعد الافتراضي عند الاتصال بشركة الاتصالات، وهذا من الأهمية بمكان فقد يعطل أو يقدم معلومة مغلوطة، أو حتى لا يقدمها في الوقت المحدد لها، لذا نجد أن المشرع لم يغفل عن ذلك في تعريفه الروبوت الإلكتروني **"برنامج إلكتروني يتم إنشاؤه أو تعديله لغرض تشغيل المهام المؤتمتة بكفاءة وسرعة"**، ويجد الباحث أن التعريف كان مقتضبًا على غير العادة في تعريف المشرع للمصطلحات، فالكفاءة كلمة غير قطعية الدلالة على معنى محدد إذ تحتمل مراحل متعددة للكفاءة، وكذلك السرعة، فإلى أي حد تكون الكفاءة والسرعة؟، وفي هذا النطاق نجد أنه لابد من تحسين دور حقوق المستهلك في الأيام القادمة، وتفعيل لجان المراقبة وتنوع تلك اللجان، وألا تتخلى الحكومات عن دورها في حماية المجتمعات وتفعيل دور مؤسسات المجتمع المدني في ذلك.

كما عرف المشرع الحساب الإلكتروني في المادة (1) من ذات القانون على أنه **"أي حساب يتم إنشاؤه لدى وسيط شبكة المعلومات لاستخدام خدمات هذا الوسيط"**، وتطرق المشرع إلى المحتوى فعرفه **"المعلومات والبيانات والخدمات الإلكترونية التي يمكن أن توفر قيمة للمتلقي في سياقات محددة"**، وقد يتوضح التعريف عندما عرف المحتوى غير القانوني في ذات المادة على أنه **"المحتوى الذي يكون موضوعه إحدى الجرائم المعاقب عليها قانونًا أو يكون من شأن نشره أو تداوله أو إعادة تداوله داخل الدولة الإضرار بأمن الدولة أو سيادتها أو أيًا من مصالحها أو الصحة العامة أو ضمن السلم العام أو بالعلاقات الودية بين للدولة مع الدول الأخرى أو التأثير في نتائج انتخابات أعضاء المجلس الوطني الاتحادي أو المجالس الاستشارية بإمارات الدولة أو التحريض على مشاعر العداء أو الكراهية بين مجموعة مختلفة من الأشخاص أو انخفاض ثقة العامة في أداء أي واجب أو مهمة أو في ممارسة أي صلاحية من قبل إحدى سلطات الدولة أو أي من مؤسساتها"**.

الفرع الثاني: طبيعة الجرائم الإلكترونية
The Nature of Cybercrime

تختلف الجريمة الإلكترونية عن غيرها من الجرائم كونها تحصل في العالم الافتراضي حيث لا ماديات ولا محسوسات، ولا حدود لها وسنتناول في هذا الفرع طبيعة تلك الجرائم ونصفها بما يلي:

أولًا: جريمة عابرة للحدود لا تعترف بالجغرافيا الطبيعية

جرائم الميتافيرس والجرائم الإلكترونية من سماتها وطبيعتها بأنها من الممكن أن تكون جرائم محلية أو جرائم عابرة للقارات، يستطيع المجرم أن يتحرك بحرية حول العالم وهو في مقره، دون أن يغادره.

ثانيًا: جريمة لا تترك بالضرورة أثرًا ماديًّا

فالاختراق، أو سرقة البيانات، أو أي عمل آخر من أنواع الجرائم الإلكترونية لا يترك آثارًا مادية لجريمته كسلاح الجريمة أو آثار أقدام أو بصمات، أو كل ما تعودنا أن نراه في مسرح الجريمة مما يدل على الفاعل، ويسهل من تعقبه.

ثالثًا: صعوبة اكتشاف الجريمة المعلوماتية

عندما تكون الجريمة من الجرائم الإلكترونية فإنها تتعلق بأمور في أغلبها لا يمكن اكتشافها، فمثلا من منا يعلم وهو يعمل على حاسوبه الشخصي ما إذا كان مخترقًا، وتتم سرقة بياناته ومعلوماته وجميع الملفات التي في حاسوبه أو التجسس عليه وربما رؤيته وهو لا يعلم؟، لا سيما وأن السرقة ليست بالضرورة أن تكون أخذًا للبيانات أو المعلومات، بل يكفي أن يأخذ نسخة منها.

رابعًا: صعوبة إثبات الجريمة الإلكترونية

يصعب تحديد الجريمة الإلكترونية من أوجه كثيرة، فكونها في عالم غير محسوس بأي طريقة من طرق الإحساس البشري العادي بجعل الأمور تزداد تعقيدًا لدى السلطات المختصة من أجل إثباتها وملاحقة مرتكبيها (45)، رغم أن لكل حاسب آلي على الشبكة العنكبوتية عنوانًا يسمى بروتوكول الإنترنت (Internet Protocol) الذي يختصر بـ (IP) (46)، فإنه من الممكن تغييره من خلال الشبكة الافتراضية الخاصة (virtual private network) واختصارها (VPN) (47)، كما أنه قد ينفع الشخص في عدم تعقبه لتجنب الاختراقات والهجمات، إلا أنه من الممكن أن يستخدم في حالات الهجوم على أجهزة أخرى لأنه يصعب تعقب المستخدم لمثل هذه البرامج، وقد ذكره المشرع الإماراتي بمسمى العنوان البروتوكولي للشبكة في قانون مكافحة الشائعات والجرائم الإلكترونية بأنه" **معرف رقم يتم تعيينه لكل وسيلة تقنية معلومات مشاركة في شبكة المعلومات، ويتم استخدامه لأغراض الاتصال**".

خامسًا: تحتاج إلى تقنيين وفنيين متخصصين في علم الحاسوب

كباقي الجرائم في واقعنا المادي وما نحتاجه من خبراء وفنيين في علم الجريمة ليساعدوا المحققين في تلك الجرائم، فإننا نحتاج في الجرائم الإلكترونية إلى متخصصين في عالم الحاسوب والشبكة العنكبوتية، ولعل الصعوبة تكمن ليس في التخصص وحده، بل في المهارات الفردية بين أبناء التخصص الواحد.

يبقى أن نقول إن هناك فرق بين الجرائم الإلكترونية وجرائم الميتافيرس رغم التشابه في طبيعتها، إلا أن جرائم الميتافيرس لها خصوصية أخرى، فمثلا لا يتصور في الجرائم الإلكترونية

التعدي على الجسد، كما هو الحال في جرائم الميتافيرس الذي يتمثل فيه الإنسان بجسد إلكتروني، من الممكن التعدي عليه ولو اختلفت طريقة الإحساس، وقد لا تختلف إذا ما تحدثنا عن المستقبل البعيد قليلًا فقد تكون هناك أجهزة تنقل كامل إحساس الجسد الإلكتروني من خلال أجهزة تقنية.

فيمكن للمتعدي قطع جزء أو تشويهه أو إخفائه أو قتله، وذلك من خلال التلاعب بالرموز (Avatar) بما يحدث الجرائم التي تحدثنا عنها، ولا يتصور مع تلك الأعمال أن يكون قانون العقوبات هو القانون الواجب التطبيق، إذ في الجرائم التي عددناها سابقًا تشترط أن يكون التعدي على جسد إنسان حي.

إلا أن البعض أيضاً يصفها بالجريمة الناعمة لعدم تطلبها قدرات جسدية أو أدوات قتالية، وهذا في حد ذاته لا يعطي المجرم الشعور بالجريمة التي ارتكبها، (48) وهنا يمكن القول إن هذا الإحساس بعدم وجود جريمة يأتي من عدم الإحساس بالنتائج، إذ أن الجاني لا يرى عواقب مادية كالدماء أو شعور الضحية أو حتى أنه لا يعلم بحاله وما حصل له جراء فعلته.

المطلب الثاني: حماية المستخدم في جرائم الميتافيرس

User Protection in Metaverse Crimes

أراد المشرع بجملة القوانين التي سردها في قانون مكافحة الشائعات والجرائم الإلكترونية وقانون حماية البيانات الشخصية، وما فرضه من عقوبات حماية المستخدم للشبكة العنكبوتية وما يتخفى ورائها من مجرمين يظهرون أو يتظاهرون، وفي حقيقة الأمر فإن معدل الجرائم الإلكترونية في ازدياد مطرد، وقد سبق وأشرنا إلى بعض الإحصاءات بهذا الشأن، ولا يوجد في حقيقة الأمر ما يبعث على التفاؤل، فحجم المبالغ المالية التي يتحصل عليها المتخصصون في هذا النوع من الجرائم فاقت 10 المليار دولارًا، هذا المعلن منها وما أمكن حصره، وإلا فإنَّ كم المبالغ أكبر من ذلك بكثير.

إذا ما الحل؟

لم يتبقَ لنا سوى أمرين: الأمر الأول: هو زيادة الوعي المجتمعي، والأمر الآخر: هو زيادة في الاهتمام من قبل الحكومات بالهيئات المختصة من حيث العدد، وكذلك من حيث تخصص العاملين، ومهارتهم، والاطلاع الدائم من خلال التعاون الدولي المشترك في تعميم الحالات لهؤلاء المتخصصين ليتم دراستها والاستفادة منها، بالإضافة إلى منشورات يومية من قبل جهات الاختصاص حول أهم وأشهر طرق الاحتيال الإلكتروني أو الفايروسات والاختراقات، لأن هذا يزيد من حرص الجمهور ويزيد من ثقافتهم حول هذا النوع من الجرائم، مع تغليظ العقوبات وتسهيل الإجراءات بالنسبة للشكوى إلى حين حصول الحق.

بَقيَ أن نقول إن كل تلك الأفعال تحدث في العالم السيبراني (**Cyber**) الذي عرفه المشرع في المادة (1) بأنه" **كل ما يتعلق بالشبكات المعلوماتية الحاسوبية، وشبكة الإنترنت، والبرامج المعلوماتية المختلفة وكل الخدمات التي تقوم بتنفيذها**".

ولعل من أوائل القوانين في مكافحة الجرائم الإلكترونية قانون مشروع أمريكي متعلق بالاحتيال والانتهاك الحاسوبي (Computer Fraud and Abuse Act) الذي يعبر عنه اختصارا (CFAA) (49)، وتتابعت الدول مع التقدم التكنولوجي وما يصادفها من متطلبات مجتمعاتها بإصدار القوانين تتابعاً، فنجد قانون مكافحة الشائعات والجرائم الإلكترونية في الإمارات العربية المتحدة، وقانون الجرائم الإلكترونية في جمهورية مصر العربية وهكذا باقي الدول.

ولدراسة هذا المطلب سيكون في فرعين:

الفرع الأول: الاختراق. Hacking

الفرع الثاني: الإضرار بأنظمة المعلومات. Damage to information systems

الفرع الأول: الاختراق (Hacking)

وهنا يمكن القول إن الدخول غير المصرح به قد يكون بحالين، الحالة الأولى هي أن يكون الدخول للمصرح لهم ولكن تجاوزوا حدود المصرح لهم به، أو في غير الوقت المحدد لهم حسب معايير العقد أو القانون أو العمل، والحالة الثانية أن يكونوا غير مالكين للتصريح، ولعل من أخطر ذلك الدخول ما يسمى بالرجل المنتصف (Man in the middle) والتي يقوم فيها المخترق باستلام البيانات منك، وتمريرها للطرف الآخر دون علم أي من الطرفين بوجوده، وتكمن خطورة هذه الطريقة في صعوبة اكتشافها أو أحياناً في استحالة اكتشافها، إذ يحصل المخترق على جميع بياناتك ويمكنه أن تنفذ هذه الطريقة بأكثر من وسيلة منها إنشاء شبكة لاسلكية (Wi-fi) تحت مسمى (Free Internet)، وعند الدخول عليها فإن جميع ما تفعله في هذه الشبكة هو في متناول المُخترق (50).

عرفه المشرع الإماراتي في ذات القانون في المادة (1) بأنه "**الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة في نظام معلوماتي أو حاسب آلي أو نظام تشغيل جهاز أو آلة أو مركبة أو شبكة معلوماتية وما في حكمها**"، كما عـرفه قانون مكافحة جـرائـم تقنية المـعلومـات المـصري في المادة (1) بأنـه "**الدخول غير المرخص به، أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة، إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية، وما في حكمها**"، كما عرف قانون الـ (CFAA) في المادة 1030(a)(2) (51) الدخول بنوعيه، فقال:

" **يحظر الوصول عمدا إلى جهاز كمبيوتر دون تصريح أو ما يزيد على ذلك الترخيص والحصول على المعلومات من مؤسسة مالية أو الحكومة الفيدرالية أو أي كمبيوتر محمي**".

وتطرق المشرع الأمريكي إلى ماهية الدخول من حيث الوصول "بدون تصريح" (Access without authorization)، أو الوصول "يتجاوز الوصول المصرح به" (Access

exceeding authorized access) [52]، وكذلك اشترط وجود القصد في الدخول، وليس عن طريق الخطأ، كما توسع في معنى الحصول، وبين أنه ليس فقط الامتلاك المادي بل مجرد النظر إليها أو حتى قرأتها من خلال شاشة الحاسب الآلي [53]، وتناولها المشرع الإماراتي في قانون مكافحة الشائعات والجرائم الإلكترونية في المادة (9) بعنوان الحصول بدون تصريح على رموز وشفرات للغير، مُجَرِّمًا الحصول عليها أيًا كانت تلك الرموز أو الشفرات، كما عرفت الفقرة (7) من المادة الأولى من نظام مكافحة جرائم المعلوماتية السعودي [54] الدخـــول الـغير مـشروع بأنه **"دخول شخص بطريقة متعمدة إلى حاسب آلي أو موقع إلكتروني، أو نظام معلوماتي أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها"**.

وفي لفتة سريعة نجد أن القوانين محل البحث لم تذكر أو تتحدث عن الوقت المسموح بالمكوث، وتحدثت عن التصريح، فقد يكون الشخص مخولًا للدخول ولديه تصريح بذلك، لكنه تجاوز المدة المسموح بها، أو دخل بغير الأوقات المصرح له بالدخول.

الأصل أن كل جريمة تتكون من ركنين الركن المادي والركن المعنوي وإذ تخلف أحدهما اعتبر الفعل غير مجرم كما تطلب القانون لبعض الجرائم قصداً خاصاً. ويقصد بالركن المادي للجريمة كما جاء في المادة (31) من قانون العقوبات الاتحادي وتعديلاته [55] أي نشاط إجرامي بارتكاب فعل أو الامتناع عن فعل متى كان هذا الارتكاب أو الامتناع مجرم قانوناً.

أما الركن المعنوي للجريمة فيقصد به العمد أو الخطأ وفقاً للمادة (38) من قانون العقوبات الاتحادي. والعمد هو اتجاه إرادة الجاني إلى ارتكاب الفعل أو الامتناع متى كانا مجرمين قانونين وذلك لأحداث نتيجة مباشرة أو نتيجة أخرى مجرمة يتوقعها الجاني. [56]

أما الخطأ فيتوفر بوقوع النتيجة الإجرامية بسبب خطأ الفاعل سواء بإهماله أو عدم انتباهه أو عدم احتياطه أو طيشاً أو رعونة أو عدم مراعاة للقوانين واللوائح والأنظمة والأوامر كما في جرائم القتل الخطأ أو الإصابة الخطأ بسبب حوادث السير.

وتكون الجريمة مكتملة في ركنيها المادي والمعنوي، إذ يتمثل الركن المادي في الدخول بدون تصريح أو تجاوز حدود الدخول، أما الركن المعنوي - وفق المشرع الإماراتي والمصري - سواء أكان متعمدًا أم غير متعمد، بخلاف ما بينه نظام مكافحة الجرائم السعودي في الفقرة (7) من المادة الأولى حين قالت "دخول شخص بطريقة متعمدة"، وهنا اختلف الركن المعنوي، إذ أصبح مجرد الدخول سواءً كان بقصد أو دون قصد يعد جريمة، وبهذا كان أقرب إلى ما رآه المشرع الأمريكي، إذ لا يعد الخطأ قصداً، وهو من وجهة نظرنا أقرب إلى الصواب، إلا أن المشرع السعودي لم يتناول تجريم حدود التصريح بالدخول إلى النظام المعلوماتي أو البقاء فيه. [57]

الفرع الثاني: الإضرار بأنظمة المعلومات
(Damage to information systems)

لم يعرف المشرع الإماراتي في قانون مكافحة الشائعات والجرائم الإلكترونية أنظمة المعلومات، وذهب بدلا من ذلك إلى تعريف تقنية المعلومات أو تكنولوجيا المعلومات في المادة (1) بأنها **"كل أشكال التقنية المستخدمة لإنشاء ومعالجة وتخزين وتبادل واستخدام نظم المعلومات الإلكترونية والبرامج المعلوماتية والمواقع الإلكترونية والشبكة المعلوماتية وأي وسيلة من**

وسائل تقنية المعلومات"، كما لم أجد أيضًا في قانون مكافحة جرائم تقنية المعلومات المصري أي تعريف لأنظمة المعلومات، وعرف تقنية المعلومات بأنها **"أي وسيلة أو مجموعة وسائل مترابطة تستخدم لتخزين، واسترجاع، وترتيب، وتنظيم، ومعالجة، وتطوير، وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكيًا أو لا سلكيًا"**.

ولا شك أن هناك فرقًا بين أنظمة المعلومات أو نظم المعلومات (IS) (58) التي يعرفها المتخصصون في هذا المجال بأنها " **دراسة واستخدام النظام لمعالجة البيانات من المدخلات لتوليد المعلومات الضرورية والمفيدة لإدارة العمليات. فهو يساعد في تحليل العمليات المستقلة ويتيح أنشطة العمل المنظمة. ويعتبر عاملاً رئيسياً لتوفير المعرفة الصحيحة لاتخاذ القرار داخل المنظمة** "، وبين تقنية المعلومات (information technology) واختصارها (IT) التي تعرف بأنها **"في الأساس دراسة واستخدام النظام لإنشاء اتصالات أسرع والحفاظ على التخزين الإلكتروني وتوفير الحماية لسجلات الأعمال أو سجلات الشركة. إنه يشير ببساطة إلى أي شيء متعلق بتكنولوجيا الحوسبة مثل البرامج والأجهزة والشبكات وما إلى ذلك** ".

ويتضح من خلال التعريفات أن تقنية المعلومات أو تكنولوجيا المعلومات (IT) تركز على البنية التحتية التكنولوجية والأجهزة والبرامج والشبكات التي تتيح معالجة البيانات والاتصالات. ومن ناحية أخرى، يركز نظام المعلومات الذي يعبر عنه بـ اختصارًا (IS) على الإطار والعمليات والإجراءات التي تمكن من الاستخدام الفعال للبيانات لدعم العمليات التجارية وصنع القرار.

وفرض قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي العقوبات في المادة (4) على الإضرار بأنظمة المعلومات بشكل عام، وفي المادة (5) خصصها للإضرار بأنظمة المعلومات التابعة للدولة أو المرافق الحيوية، والمادة (7) للاعتداء على البيانات والمعلومات الحكومية.

ولا بأس أن نستعرض جميع التعريفات السابقة لنخلص بعدها إلى سؤال يطرح نفسه هو هل تتوافق تلك التعريفات مع ما عرفه المشرع الإماراتي في قانون حماية البينات الشخصية رقم (45) لسنة 2012؟

للإجابة على السؤال (أي سؤال من السؤالين؟) علينا بيان الفرق بين البيانات (Data) والمعلومات (Information)، فالبيانات جزء من المعلومة يحتاج إلى غيره أي بمعنى إلى معالجة، أما المعلومة فهي أجزاء من بيانات تم علاجها لاستخراج معلومة منها، أو مجموعة من (البيانات) والمعلومات أي خليط بين الإثنين يتم معالجتها لإعطائنا معلومة، فمثلا لو أردنا نسبة القضايا الخاصة بالجرائم الالكترونية من إحصائية عدد القضايا التي حكم بها في محاكم دبي، ورجعنا إلى إحصائية تقول أن العدد الإجمالي (1000) قضية وإن عدد قضايا الجرائم الإلكترونية (100) قضية، فكلاهما بالنسبة لنا بيانات، ولمعرفة المعلومة المطلوبة والتي هي نسبة القضايا التي تخص الجرائم الإلكترونية تتم معالجة هذه البيانات بقسمة الرقم الأول على الرقم الثاني وضربها بالنسبة المئوية فيكون الناتج (10%).

كما سنأتي على جملة من الأفعال المجرمة في قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي التي من الممكن أيضا حدوثها في عالم الميتافيرس بالإضافة إلى ما سبق التي من الممكن أن تأخذ حكمها إذا ما كيفت على أنها جرائم إلكترونية، وهذا هو الصحيح من وجهة نظر

الباحث، مع ما يتبعها من حقـوق أدبية أخـــرى تتعلق بالضحية، ولـــو أن البعض ذهب إلى أبعد من ذلك (59).

- الاعتداء على بيانات المنشآت المالية أو التجارية أو الاقتصادية في المادة (8)، وعرف **أي منشأة تكتسب**المشرع المنشآت المالية أو التجارية أو الاقتصادية في المادة (1) بأنها " **وصفها المالي أو التجاري أو الاقتصادي بموجب الترخيص الصادر لها من جهة الاختصاص بالدولة**".
- التحايل على الشبكة المعلوماتية بقصد ارتكاب جريمة كما وردت في المادة (10)، ولعل ورود لفظ " القصد" أجده غريبًا فهل فعل التحايل على الشبكة المعلوماتية إن لم يكن بقصد ارتكاب جريمة لا يعد جريمة؟، والجواب هنا أن التحايل في حد ذاته والدخول على الشبكة المعلوماتية يعد جريمة ولو لم يكن بغرض ارتكاب جريمة، إذ قد يكون التحايل هنا على وجهين:

الأول: أن يكون التحايل من خلال الاختراق الإلكتروني المادة (2).

الثاني: من خلال الحصول على الرموز والشفرات بدون تصريح من صاحب الشأن، المادة (9).

ولعل المشرع أراد أن تكون هناك عقوبتان مختلفتان، الأولى ما جاء بدون قصد ارتكاب جريمة كما ورد في المادتين (2) و(9) والتغليظ عندما يرتبط العفل بالقصد، إذ قد يحصل الفعل ولا يتوفر القصد، فكانت العقوبات أخف كما لاحظنا في المادتين المشار إليها.

- ، وعرف المشرع12)الاعتراض غير المشروع وإفشاء المعلومات، كما ورد في المادة (**مشاهدة أو مراقبة البيانات أو المعلومات أو الحصول**الاعتراض بأنه " **عليها بغرض التنصت أو التعطيل، أو التخزين أو النسخ أو التسجيل أو التحليل أو تغيير المحتوى أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه وذلك لأسباب غير مشروعة ودون وجه حق**".
- فعل التزوير في المستند الإلكتروني كذلك، هو من الجرائم الممكن حدوثها في عالم **سجل أو بيان معلوماتي يتم إنشاؤه أو**الميتافيرس، وقد عرفه المشرع في المادة (1) بأنه " **تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية على وسيط**" وقد جرمه المشرع في المادة (14) سواءً كان التزوير لشخص طبيعي أو معنوي.
- فعل الاعتداء على وسائل الدفع الإلكتروني، جرم هذا الفعل في المادة (15)، فكل من زور أو قلد أو نسخ بطاقة ائتمانية أو بطاقة مدنية أو أي وسيلة من وسائل الدفع الإلكتروني أو استولى على بياناتها أو معلوماتها، وذلك باستخدام وسائل تقنية المعلومات، أو نظام معلوماتي.
- إذا ما استخدمت الأنظمة الإلكترونية في ارتكاب جرائم أو إخفاء أدلة، كما ورد في المادة (16) من ذات القانون التي جرمت كل من حاز، أو أحرز، أو أعد، أو صمم، أو أنتج، أو استورد، أو أتاح، أو استخدم أي برنامج معلوماتي أو وسيلة تقنية معلومات أو أكواد مرور، أو رموز، أو استخدم التشفير بقصد ارتكاب أي جريمة من الجرائم المنصوص عليها في ذات القانون، أو اخفاء أدلتها، أو آثارها، أو الحيلولة دون اكتشافها. وما يلاحظ هنا أن

المشرع اشترط القصد بارتكاب جريمة، فهل لو حازها الشخص الطبيعي أو الاعتباري دون قصد ارتكاب جريمة، يعد جريمة؟ في الأصل هناك برامج يمكن استخدامها لأغراض شخصية ومن الممكن استخدامها كذلك في ذات الوقت لأغراض ارتكاب جرائم أو اخفاء أدلة، فمثلًا من الممكن استخدام برامج التصميم والمونتاج لأغراض شخصية وكذلك من فيمكن)Hackerالممكن أن تستخدمها لأغراض ارتكاب الجرائم، وكذلك برامج الـهكر (استخدامها في لأغراض شخصية، أو لغرض الدخول والتلصص والسرقة، فمجرد الحيازة **تحويل المعلومات**لا يعد جريمة إلا إذا توفر شرط القصد، وقد عرف المشرع التشفير بأنه " **أو نظم أو وسائل تقنية المعلومات إلى نموذج غير قابل للقراءة أو التعرف عليها دون إعادتها إلى هيئتها الأصلية باستخدام كلمة سرية أو أداة التشفير المستخدمة**".

- الجرائم المرتكبة من المسؤول عن الموقع أو الحساب الإلكتروني، المادة (17)، وهي تلك الأفعال التي تصدر من كل من أدار أو أنشأ أو استخدم موقعًا أو حسابًا على شبكة معلوماتية يهدف إلى ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانونًا.
- العبث بالأدلة الرقمية، المادة (18)، الأفعال الصادرة من كل مسؤول عن إدارة موقع أو حسابًا على شبكة معلوماتية أو بريد إلكتروني أو نظام معلوماتي أخفى أو عبث بالأدلة الرقمية لإحدى الجرائم المنصوص عليها بقانون مكافحة الشائعات والجرائم الإلكترونية بقصد إعاقة عمل جهات البحث والتحري والتحقيق أو الجهات المختصة الأخرى.
- نشر بيانات أو معلومات لا تتوافق مع معايير المحتوى الإعلامي، المادة (19) والتي تصدر من كل مسؤول عن إدارة موقع أو حساب إلكتروني إذا ما نشر على أي منها محتوى، أو بيانات، أو معلومات لا تتوافق مع معايير المحتوى الإعلامي الصدار من الجهات المعنية.

المبحث الثالث: المسؤولية القانونية في جرائم الميتافيرس والقانون واجب التطبيق

Legal Responsibility in Metaverse Crimes and the law Must be Applied

يتربص أصحاب النفوس الضعيفة ـــ المجرمون ـــ، باستمرار وإصرار على ما غلب في ظنهم أنها الطرق الأسهل لكسب المال أو الشهرة، من خلال سرقة أموالهم، أو ابتزازهم، أو التعدي على خصوصياتهم، ويتنوع هؤلاء بتنوع ما يبرعون به أو يتدربون عليه، بل وقد يمضون الساعات والأيام الطوال في إتقان ذلك الشر من أجل أن يحصلوا على ما يريدون غير آبيهن لا بخلق ولا قانون.

ويزداد ويتنوع أعداد هؤلاء المجرمين كل ما وجدوا فرصة أو ثغرة، فالتقدم الكيميائي جلب لنا المزيد من المخدرات، والتطور التقني خلق لنا مجرمين من نوع آخر، وهذا ليس عيبًا في العلم والتقدم، فجميع ما ذكر هو سلاح ذو حدين من الممكن أن يستغل بشكل صحيح فيريح المجتمعات، ويمكن أن يقع بأيد آثمة فيكون نقمة على المجتمعات، والباحث ليس متشائمًا أو سوداويًّا، عندما يتحدث عما يمكن حصوله في عالم الميتافيرس، وما سيفتح من أبواب وفرص لما تسول له نفسه إيذاء الآخرين.

إن ما ذكـــر يجعلنـــا أكثر استعدادًا، وأشد حرصًا، ففي فبراير 2022 صدر تقرير عن مركز روسكومنادزور التقني العلمي الروسي (The Scientific Technical Center of Roskomnador)، وهو الـــوكالة الروسية الفدرالية لمراقبة الاتصالات، وقد أعرب هذا التقرير عن قلقه الانخراط في ميتافيرس وتحويلها أسلوبًا تفاعليًا بين البشر، وذكر أنه يبحث فرض قيود جديدة على الواقع الافتراضي، إذ قد يسبب امتلاك مساحات في هذا الواقع حالة من المعاملات غير القانونية عبر الحدود الوطنية (60). ولا شك في أن جميع الجرائم في واقعنا الحقيقي المادي يمكن أن تحصل في عالم الميتافيرس من قتل وسرقة وتحرش، وغيرها من الجرائم (سواءً كانت جنايات أم جنح أم مخالفات)، وهنا يكمن السؤال هل ستكون القوانين المحلية المطبقة في عالمنا الحقيقي المادي لمعالجة تلك الجرائم كافية؟، ويتبعه أيضا ما الفرق بين الجرائم الإلكترونية وتلك الجرائم في العالم الافتراضي؟

وقد تبين لنا سابقًا طبيعة الجرائم الإلكترونية التي هو نواة الميتافيرس، إذ كل جريمة تمر عبر التقنية هي جريمة إلكترونية، وكل جريمة في الميتافيرس هي جريمة إلكترونية ولا شك.

لذا سيكون هذا المطلب على مطلبين:

المطلب الأول: المسؤولية القانونية في جرائم الميتافيرس. Legal Responsibility in Metaverse Crimes

المطلب الثاني: القانون واجب التطبيق في جرائم الميتافيرس.The law Must be Applied in Metaverse Crimes

المطلب الأول: المسؤولية القانونية في جرائم الميتافيرس

Legal Responsibility in Metaverse Crimes

تتفق جرائم الميتافيرس مع الجرائم الإلكترونية بعدة صفات فكلاهما من الجرائم الإلكترونية، وكلاهما عابران للجغرافيا الطبيعية، ويقعان في الفضاء السيبراني، وكلاهما يتخذان من البيانات والمعلومات والتقنية طريقًا لتنفيذ الجريمة، إلا أن الميتافيرس تختلف في طبيعتها عن الجرائم الإلكترونية كونها أقل صعوبة في إيجاد الفاعل في حالات قليلة، ويرجع ذلك إلى أن مرتكب الجريمة في الميتافيرس له شفرة ورمز يمكن تتبعه، وبشكل عام تعتبر الميتافيرس أكثر خطورة وتوسعًا في الاستغلال، فمع بداية الميتافيرس وبداية الملكية الرقمية وتحويلها إلى أصول ورموز غير قابلة للاسترداد يمكن الغير من الاستيلاء على مناطق جغرافية تعود إلى بلدان متعددة واستغلالها بطريقة غير شرعية أو أخلاقية، ولذا حسنًا فعل المشرع الإماراتي بإمارة دبي لإصداره قانون تنظيم الأصول الافتراضية في إمارة دبي رقم (4) لسنة 2022, وقرار مجلس الوزراء رقم (111) لسنة 2022 ، كما تُمَكِنْ الميتافيرس من تسهيل الكثير من الجرائم مثل الاتجار بالبشر، إذ يعد ثالث أكبر تجارة غير شرعية مربحة في العالم، وتشمل منظومة الاتجار بالبشر عمليات تجنيد، ونقل، وإيواء عن طريق أوسع العصابات الاجرامية احترافًا، ويدل مؤشر العبودية العام لمنظمة (Walk Free Foundation) الأسترالية في أغسطس 2018 على أنَّ نحو 40 مليون شخص على مستوى العالم يعيشون تحت وطأة نظام العبودية الحديث(61).

وعندما نتحدث عن الجريمة فلا بد من وجود المسؤول عن تلك الجرائم، فقد تنصب المسؤولية على شخص، أو مجموعة أشخاص، ولعل الجرائم الإلكترونية وجرائم الميتافيرس أغلبها تتوزع في جرائمها المسؤولية على أكثر من شخص سواءً كان طبيعيًا أم اعتباريًا أو من هذا وذلك.

ولدراسة هذا المطلب سنقسمه إلى فرعين:

الفرع الأول: المسؤولية القانونية على المستخدم في جرائم الميتافيرس.

Legal Responsibility on the user for Metaverse Crimes

الفرع الثاني: المسؤولية القانونية لمزود الخدمة والوسيط ومن في حكمهم في جرائم الميتافيرس.

The legal Responsibility of the Service Provider, The Intermediary, and the like in Metaverse Crimes

الفرع الأول: المسؤولية القانونية على المستخدم في جرائم الميتافيرس

Legal Responsibility on the user for Metaverse Crimes

المستخدم لتقنية المعلومات إما أن يكون ملتزمًا بالقوانين أو مخالفًا لها، أو جاهلًا، والجهل بالقانون لا يُعْفَى من المسؤولية، فالجريمة في الميتافيرس إما أن تكون مخالفة للضوابط التي تحافظ على المصلحة العامة كنشر الشائعات وعدم استقاء الأخبار من مصادرها الموثوقة، أو يكون مستخدمًا للتقنية في الميتافيرس بغرض التربح الغير المشروع سواءً كان من خلال الابتزاز أو السرقة أو تجنيد الآخرين لأعمال إرهابية أو المتاجرة بالبشر، أو غيرها من الأعمال التي جرمتها القوانين والاتفاقات الدولية في قوانين مكافحة الجرائم الإلكترونية أو في قوانين حفظ البيانات الشخصية. تنشأ المسؤولية القانونية على المستخدم بمجرد التعامل مع تقنية المعلومات أو نظم المعلومات سواءًا كان من خلال إنشاء حساب إلكتروني (62) خاص على مواقع التواصل الاجتماعي أو أي موقع إلكتروني، أو من خلال الروبوت الإلكتروني(63)، ويدخل في حكم إنشاء الحساب البريد الإلكتروني أو الموقع الإلكتروني المستقل.

وقد ذكرنا سابقًا بعض التعريفات التي أوردها المشرع الإماراتي في القانون رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية، ونورد البعض الآخر لنعرف ما المقصود بكل ما عناه المشرع واعتبره جزءًا من أدوات الجريمة أو ما يمكن أن يستخدم كأداة في هذه الجريمة.

عرف المشرع في القانون المشار إليه أعلاه الحساب الإلكتروني على أنه" **مكان أو مجال افتراضي على الشبكة المعلوماتية يعتمد على برامج ذكية تمكن مستخدميه من إتاحة أو تبادل أو نشر أي محتوى سواءً كان نصي أو صوتي أو مرئي أو بيانات، ويشمل مواقع وشبكات ومنصات التواصل الاجتماعي والصفحات والحسابات الشخصية والمدونات والخدمات الإلكترونية وما في حكمها** ".

يبقى أن نحدد مسؤولية المستخدم ومدى شدة حرصه أو أن يكون الحرص المعتاد، لعل مدى الحرص هنا يحدد بالمفترض معرفته من شخص يستخدم التقنية بالشكل العادي أو باحتراف، كما يحدد بمدى القصد من دونه، فالمشرع الإماراتي يتضح أنه فرق بين حسن النية وبين غيره، ويتضح ذلك من ما أشار إليه المشرع الإماراتي في قانون مكافحة الشائعات والجرائم الإلكترونية في المادة (56) حين قال: " **مع عدم الإخلال بحقوق الغير حسني النية، وفي حالة الإدانة يحكم بمصادرة الأجهزة والبرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها، وبحذف المعلومات أو البيانات** "، فمتى ما ثبتت المسؤولية الجزائية من خلال حجية الأدلة كما أشار المشرع الإماراتي في قانون مكافحة الشائعات والجرائم الإلكترونية في المادة (65) " **يكون للأدلة المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو النظام المعلوماتي أو برامج الحاسوب أو من أي وسيلة لتقنية المعلومات حجية الأدلة الجنائية المادية في الإثبات الجنائي** "، كما ونفى خروج المسؤولية الجزائية في حالات تناولها في ذات القانون في المادة (64) " **في تطبيق أحكام هذا المرسوم بقانون، لا يعد سببًا لانتفاء المسؤولية الجزائية الآتي:**

1. خضوع الشخص لواجب بموجب أي تشريع أو قاعدة قانونية أو عقد أو قاعدة للسلوك المهني تقيد أو تحول دون امتثاله لأي جزء من الأوامر المنصوص عليها في هذا المرسوم

بقانون.

2. قيام الشخص المعني أو وكيله بالتظلم أو الطعن، بحسب الأحوال، على تلك الأوامر وفقًا لنص المادة (63) من هذا المرسوم ".

لم يجز المشرع الإماراتي كما يتبين الدفع عن الجاني بعدم مسؤوليته لكونه خاضعًا لواجب من الواجبات سواءً كان هذا الواجب تشريعًا أو قاعدة قانونية، فضلا عن أن يكون عقدًا أو سوكًا متبعًا في عمل أو أحد قواعده.

وكبادرة أجاز المشرع الإماراتي في ذات القانون المادة (67) الصلح مع المتهم، مالم يصدر حكم نهائي في القضية، ضمن ضوابط حددتها المادة المشار إليها أدناه، بغض النظر عن أطراف الجريمة، أكانوا من الأشخاص الاعتباريين أو المعنويين، أم كان أحد الأطراف معنويًا والآخر اعتباريًا، فجاءت على النحو الآتي "**للمحكمة أو النيابة العامة بحسب الأحوال أن تقبل بالتصالح مع المتهم في الجرائم المنصوص عليها في المواد (13)، (19)، (24)، (25)، (26)، (27)، (28)، (47)، (48)، (49)، (50)، (51)، (52)، (53)، من هذا المرسوم بقانون، وعلى النحو الآتي:**

1. يجوز التصالح قبل إحالة الدعوى الجزائية إلى المحكمة مقابل أداء مبلغ لا يقل عن نصف الحد الأدنى ولا يزيد على نصف الحد الأقصى للغرامة المقررة للجريمة.

2. يجوز التصالح بعد إحالة الدعوى الجزائية إلى المحكمة وحتى قبل صدور حكم نهائي فيها مقابل أداء مبلغ لا يقل عن مثلي الحد الأدنى للغرامة المقررة، ولا يزيد على ثلثي حدها الأقصى.

3. يترتب على التصالح انقضاء الدعوة الجزائية، ولا أثر له على حقوق المضرور من الجريمة إن لها مقتضى."

مما سبق يستشف أنه متى ما أثبتت المسؤولية الجزائية لحقتها المسؤولية المدنية عن الأضرار المتحققة في هذه الجريمة، ولا يسقط الصلح القائم المسؤولية المدنية عن المتهم اتجاه الضحية، وإن ترتب انقضاء الدعوة الجزائية بالصلح.

وأجاز المشرع الإماراتي العفو عن الجريمة في ذات القانون في المادة (61) بشروط أوردها كما يلي"**1. تقضي المحكمة، بناء على طلب من النائب العام، بتخفيف العقوبة أو بالإعفاء منها، عمن أدلى من الجناة إلى السلطات القضائية أو الإدارية بمعلومات تتعلق بأي جريمة من الجرائم المنصوص عليها في هذا المرسوم بقانون، متى أدى ذلك إلى الكشف عن الجريمة ومرتكبيها أو إثباتها عليهم أو القبض على أحدهم،** 2. **وفي الجرائم** الماسة **بأمن الدولة للنائب العام للاتحاد دون غيره أن يطلب من المحكمة المنظورة أمامها الدعوى إعمال حكم الفقرة السابقة في غير الحالات المنصوص عليها فيها، إذا تعلق الطلب بالمصلحة العليا للدولة أو بأي مصلحة وطنية أخرى، فإذا صدر حكم في الدعوى جاز له أن يقدم الطلب إلى المحكمة التي أصدرته قبل التنفيذ أو أثناء التنفيذ**".

كما أورد المشرع الظروف المشددة للعقوبة في المادة (60) من ذات القانون على النجو الآتي:" **في تطبيق أحكام هذا المرسوم بقانون يعد ظرفًا مشددًا:**

1. ارتكاب الجاني لأي جريمة منصوص عليها في هذا المرسوم بقانون بمناسبة أو بسبب تأدية عمله.

2. استخدام الجاني شبكة المعلومات أو أي نظام معلوماتي إلكتروني أو موقع إلكتروني أو وسيلة تقنية معلومات عند ارتكاب أي جريمة لم ينص عليها هذا المرسوم.

3. ارتكاب الجاني أي جريمة منصوص عليها في هذا المرسوم بقانون لحساب أو مصلحة دولة أجنبية أو أي جماعة معادية أو جماعة إرهابية أو تنظيم غير مشروع."

أضاف المشرع إلى ظرف التشديد كما جاء في المادة (5) من الإضرار بالأنظمة المعلوماتية لإحدى مؤسسات الدولة والمرافق الحيوية فجاء نص المادة على النحو الآتي" **يعاقب بالسجن المؤقت والغرامة التي لا تقل عن (500,000) خمسمائة ألف درهم ولا تزيد على (3,000,000) ثلاثة ملايين درهم، كل من تسبب عمدًا في الإضرار أو تدمير أو إيقاف أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، عائدة لمؤسسات الدولة أو أحد المرافق الحيوية. فإذا وقعت الجريمة نتيجة لهجمة إلكترونية أعتبر ذلك ظرفًا مشددًا.**".

ومن الظروف المشددة أيضًا ما جاء في المادة (6) من ذات القانون بند (2) " **2. إذا ما كانت البيانات أو المعلومات المشار إليها في البند (1) من هذه المادة تتعلق بفحوصات أو تشخيص أو علاج أو رعاية أو سجلات طبية أو حسابات مصرفية أو بيانات ومعلومات وسائل الدفع الإلكتروني عد ذلك ظرفًا مشددًا.** **(64)**"

أشار المشرع البرازيلي**(65)** في تعريف البيانات الشخصية في القانون العام لحماية البيانات الشخصية **(LGPD)** المادة (5) الفقرة (الأولى) أن " **البيانات الشخصية: المعلومات المتعلقة بشخص طبيعي محدد أو يمكن تحديد هويته"**.

الفرع الثاني: المسؤولية القانونية لمزود الخدمة والوسيط ومن في حكمهم في جرائم الميتافيرس

The legal Responsibility of the Service Provider, The Intermediary, and the like in Metaverse Crimes

لا تلزم المسؤولية القانونية المستخدم فقط، فمزود الخدمة والوسيط (66) هما في ذات الركب، إذ لو كان المستخدم كما تم افتراضه مستخدمًا عاديًا أو محترفًا تختلف بينهما درجة المسؤولية بحسب خبرتهما المفترضة من خلال طبيعة عملهم أو القصد في ارتكاب الجريمة من عدمه، فإن الوسيط والمزود باعتبارهم شخصيات اعتبارية هم على كفاية ودراية واحتراف عالٍ، إذ من يقوم على هذه الخدمة هم شركات متخصصة ولها من الثقل والعلم في هذا المجال ما يفوق ما يعلمه الناس العاديين ومن هم على سبيل الهواة أو في طريقهم للاحتراف.

لذا لم يغفل المشرع الإماراتي عنهم في قانون مكافحة الشائعات والجرائم الإلكترونية، ففي المادة (58) بين مسؤولية المسؤول عن الإدارة الفعلية للشخص الاعتباري بقوله:" **يعاقب المسؤول عن الإدارة الفعلية للشخص الاعتباري بذات العقوبات المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا المرسوم بقانون إذا ثبت علمه بها، وكان إخلاله بالواجبات التي تفرضها عليه تلك الإرادة قد أسهم في وقوع الجريمة، ويكون الشخص الاعتباري مسؤولًا بالتضامن عن الوفاء بما يحكم به من غرامات أو تعويضات إذا كانت المخالفة قد ارتكبت من أحد العاملين لديه وباسم الشخص الاعتباري ولصالحه.**"

كما أورد المشرع الإماراتي في قانون حماية البيانات الشخصية المادة (1) تعريف المتحكم بأنه " **المنشاة أو الشخص الطبيعي الذي لديه بيانات شخصية، وبحكم نشاطه يقوم بتحديد طريقة وأسلوب ومعايير معالجة هذه البيانات الشخصية والغاية من معالجتها، سواء بمفرده أو بالاشتراك مع أشخاص أو منشآت أخرى.**"، وفرق بينه وبين المعالج الذي عرفه بأنه" **المنشاة أو الشخص الطبيعي الذي يعالج البيانات الشخصية نيابة عن المتحكم، بحيث يقوم بمعالجتها تحت توجيهه ووفقًا لتعليماته.**" وأورد تعريف مسؤول حماية البيانات بأنه " **أي شخص طبيعي أو اعتباري يتم تعينه من قبل المتحكم أو المعالج، يتولى مهام التأكد من مدى امتثال الجهة التي يتبعها بضوابط واشتراطات وإجراءات وقواعد معالجة حماية البيانات الشخصية المنصوص عليها في هذا المرسوم بقانون، والتأكد من سلامة أنظمتها وإجراءاتها من أجل تحقيق الالتزام بأحكامه.**"

ينطبق لفظ "المتحكم" على المنشآت التي من الممكن أن تستخدم البينات والمعلومات بغرض التسويق، أو المتاجرة بشكل أو آخر ببيانات الأشخاص ومعلوماتهم، أو أساء استخدامها بخلاف ما بينته المادة (7) من ذات القانون التي تبين التزامات عامة على المتحكم(67)، والمادة (8) التي وضحت التزامات عامة لتلك المعالجة (68)، والمادة (6) التي حددت شروط الموافقة على معالجة البيانات بعد موافقة صاحب البيانات واستطاعت المتحكم في إثبات تلك الموافقة (69)ضمن ضوابط حددتها المادة (4) من ذات القانون تبين حالات معالجة البيانات الشخصية بدون موافقة

صاحبها [70]، وبما لا يسقط حق المستخدم في حصوله على المعلومات التي تخصه حسب ما وضحته المادة (13) [71]، أو حقه في نقل بياناته الشخصية حسب المادة (14) [72].

أو حقه في تصحيح أو محو بياناته الشخصية على نحو ما أشارت المادة (15) [73]، أو حقه في تقييد معالجة بياناته الشخصية حسب المادة (16) [74]، أو حقه في إيقاف المعالجة كما جاء في المادة (17) [75]. أو حقه في الاعتراض على القرارات التي تنتج عن المعالجة إذا ما كان لها أثر قانوني تبعاً لما بينته المادة (18)[76]، ضمن طرق التواصل مع المتحكم الظاهرة في المادة (19) [77]، هذا كله لا يمنع من أن تكون هناك حالات معالجة للبيانات الشخصية دون موافقة صاحبها، سردها المشرع في المادة (4) من ذات القانون على سبيل المثال لا الحصر، ويفهم ذلك من الفقرة (11) إذ أشار فيها بقوله:" **أية حالات أخرى تحددها اللائحة التنفيذية لهذا المرسوم بقانون**".

كما سمح المشرع نقل البيانات الشخصية عبر الحدود لأغراض المعالجة مشترطًا وجود مستوى من الحماية الملائمة كما بينته المادة (22) [78]، وفي حال عدم وجود مستوى من الحماية كما وضحته المادة المشار إليها آنفًا سمح المشرع نقل البيانات ولكن ضمن ضوابط حددها في المادة (23) [79] الحالات التي يجوز فيها نقل البيانات، كذلك لم يغفل المشرع عن حق صاحب البيانات تقديم شكوى إذا ما وصل إلى علمه أو ظنه بأن هناك مخالفة من المخالفات التي نص عليها قانون حماية البيانات الشخصية الإماراتي كما في المادة (24) [80]، وترك تحديد الجزاءات والمخالفات لمجلس الوزراء واللائحة التنفيذية لهذا القانون كما جاء في المادة (26) [81].

هذا وقد نصت المادة (72) من قانون مكافحة الشائعات والجرائم الإلكترونية أنه ومع عدم الإخلال بعقوبة أشد وردت في قانون العقوبات أو أي قانون آخر، فقد حرص المشرع في هذا النوع من الجرائم على تنفيذ العقوبة الأشد.

المطلب الثاني: القانون واجب التطبيق في جرائم الميتافيرس

The law Must be Applied in Metaverse Crimes

تحدث جرائم الميتافيرس في فضاء سيبراني، تذوب معه حدود المسافات والجغرافيا والخرائط، إذ لا حدود ولا دول ولا تأشيرات سفر، كما سيكون خيارًا للبعض التخفي خلف رموز لا تعبر عن هوية صاحبها الحقيقي إلا من خلال الترميز الذي وإن كان من الممكن تتبعه وإثبات ملكيته، إلا أنه لا يستبعد بحال من الأحوال أن يكون مسروقًا أو حتى متخفيًا كما يخفي البعض عنوانه الإلكتروني (IP) من خلال برامج إلكترونية في متناول الجميع، ولا تحتاج إلا إلى قليل من المعرفة والجهد، فليس من المستبعد أن يستطيع البعض التخفي في عالم الميتافيرس، هذا الأجواء تخلق عند البعض شعورًا بالحرية التي قد تستغل استغلالًا سيئا إذا لم تحددها قوانين وضوابط، لا سيما وأن البشر ليسوا سواء، فهناك من يحكمه الضمير، وهناك من حتى القوانين يتحايل على مخالفتها، وكما قيل فإن الحرية المطلقة مفسدة مطلقة.

سبقت الإشارة إلى صعوبة إثبات الجرائم الإلكترونية، والجهد الذي يبذل لكشفها، وتضيع الكثير من الحقوق في إحقاقها لصعوبة التواصل مع الأجهزة المعنية أو مدى اهتمامها، وبين كثرة القضايا، لا سيما ـ كما تمت الإشارة إليه ـ أننا بصدد زيادة في مضطربة في عدد الجرائم، مع قلة ثقافة ووعي مجتمعي، سببه المجتمع من ناحية، وعدم نشر الوعي بتلك الجرائم من الأجهزة المختصة من ناحية أخرى.

لذا سيتم دراسة هذا المطلب من فرعين:

الفرع الأول: إثبات الجرائم الحاصلة في عالم الميتافيرس. Proof of Crimes Occurring in The World of the Metaverse

الفرع الثاني: القانون الواجب التطبيق على جرائم الميتافيرس. The law Must be Applied to Metaverse Crimes

الفرع الأول: إثبات الجرائم الحاصلة في عالم الميتافيرس
Proof of Crimes Occurring in The World of the Metaverse

مما يميز الجرائم الإلكترونية بشكل عام وجرائم الميتافيرس، صعوبة الإثبات، والإجراءات وتعتمد على براعة الفنيين العاملين في أجهزة الدولة، مقابل براعة من امتهنوا هذه الأسلوب من الجرائم.

من المعلوم أن الإثبات هو عين الحقيقة التي لا يتصور معه خلافها، وفي أول مادة في الباب الأول من قانون الإثبات الاتحادي رقم 10 لسنة 1992 وتعديلاته، تحدث عن الإثبات فيما نصه "**1. على المدعي أن يثبت حقه وللمدعى عليه نفيه،2. ويجب أن تكون الوقائع المراد إثباتها متعلقة بالدعوى ومنتجة فيها، وجائزاً قبولها.3. ولا يجوز للقاضي أن يحكم بعلمه الشخصي.**"

ولا يقبل الإثبات بأشكاله المختلفة إلا وفقًا لما حدده القانون فالإثبات في القضايا المدنية مختلف عنه في القضايا التجارية والجزائية.

ولعل من صعوبات وجود الدليل الإلكتروني كما ذكرنا مهارة العاملين في هذا المجال من أصحاب السلطة القضائية،(82)، وهذا ليس انتقاصًا من شأنهم، فهذه العلوم متجددة بسرعة فائقة، وتكاد لا تتقن شيئًا إلا وجد آخر أحدث منه وتميز عنه، كما أن الدليل الإلكتروني سهل الإتلاف وبوجوه عدة فمن الممكن أن تمحو الدليل بأكثر من طريقة تجعل من المستحيل إعادتها حتى مع وجود التطبيقات المختصة

وهناك تعريفات كثيرة للدليل الجنائي بشكل عام من تلك التعريفات " **معلومة يقبلها المنطق والعقل يتم الحصول عليها بإجراءات قانونية ووسائل فنية ومادية أو قولية ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة أو فعل أو شيء أو شخص له علاقة بجريمة أو جاني أو مجني عليه.**"

أما الدليل الرقمي فقد عرفه البعض بأنه" **الدليل المأخوذ من أجهزة الكمبيوتر، وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون.**" وللدليل الرقمي صور فقد يكون مستخرجًا ورقيًا يتم استخراجه من خلال الطابعات، أو قد يكون على أقراص ليزر (Laser Discs) أو الأقراص الصلبة الممغنطة (Hard Discs). (83)، ونستطيع القول أو نخلص إلى أن الدليل الرقمي يمكن تعريفه بأنه " **كل بيانات أو معلومات حفظت أو عولجت في أي من وسائل التقنية، أو استخرجت منها بأي شكل من الأشكال المسموع أو المرئي، وبأي حالة كانت صورًا أو رسومات أو غيرها، وسواءً شكلت معلومة مفهومة أم لا، ليقام عليه حكم قانوني**".

وتختلف التشريعات القانونية في موقفها من الأدلة الإلكترونية التي تقبل كأساس لإصدار الأحكام القضائية 84، في هذا المجال أرسى المشرع الإماراتي في قانون مكافحة الشائعات والجرائم الإلكترونية مبدأً أساسيًا في حجية الأدلة ذلك حينما أورد في المادة (65) من ذات القانون

ما نصه" **يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو النظام المعلوماتي أو برامج الحاسوب أو من أي وسيلة لتقنية المعلومات حجية الأدلة الجنائية المادية في الإثبات الجنائي**". وذهب المشرع المصري غير بعيد عن ذلك في قانون مكافحة جرائم تقنية المعلومات في المادة (11) إلى تعريف الأدلة "**يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو النظام المعلوماتي أو برامج الحاسوب أو من أي وسيلة لتقنية المعلومات حجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون.**"

ولا يختلف الأمر في قانون الإثبات في المعاملات التجارية (85) رقم (35) لسنة 2022، كما نصت المادة (10) في الفقرة (1) " أن يكون لأي إجراء من إجراءات الإثبات إلكترونياً، ذات حجية الأحكام المقررة في هذا القانون."

لا شك أن هناك صعوبة في التحصيل على الأدلة في عالم الميتافيرس، ويرى البعض أن من معوقات الحصول على الدليل هي قلة خبرة رجال الضبط القضائي أو المحققين في الجرائم الرقمية، أو غياب صفة الفهم والقراءة عن الدليل الإلكتروني، وغياب أو ندرة الآثار المادية، وذلك لسهولة محو الأدلة الإلكترونية أو تدمير الأنظمة الإلكترونية بوقت قصير(86)، إذ يتوجب أن يكون هناك محققون من ذوي الاختصاص وفنيون في الأمن السيبراني، إذ ليس الأمر كما هو عليه في باقي الجرائم الجزائية، فلا دليل ملموس، ولا شهود، ولا أدوات للجريمة ولا مسرح لها، والمشتبه بهم أشباح وأرقام لعناوين الدخول (IP) أو رموز (**Avatar**) كما في الميتافيرس.

الفرع الثاني: القانون الواجب التطبيق على جرائم الميتافيرس
The law Must be Applied to Metaverse Crimes

سيادة الدول تأتي من تطبيق أنظمتها وقوانينها على أراضيها وضمن حدودها، سواءً على مَن يحملون جنسيتها أو من هم على أراضيها بأي صفة كانت، ورغم النظريات(87) الكثيرة إلا أنها لم تعد لتصبح معيارًا عالميًّا يصار إليه لحل التنازع بين قوانين الدول المختلفة، ولذلك اتجه الفقهاء نحو الوضعية الخاصة في حل تنازع القوانين من خلال ما يضعه المشرع الوطني من قواعد للإسناد(88). وفي حالات حصول النزاع يكون عندما يتعدد أطراف النزاع أو مكان وقوع الجريمة أو مباشرتها، والفرق بين الوقوع والمباشرة هنا يتماشى مع ما يحدث من جرائم في الميتافيرس أو الجرائم الإلكترونية، فقد يكون مكان وقوع الجريمة غير مكان مباشرتها، وذلك بأن يقوم شخص ما بخرق أمني سواءً كان لشخص طبيعي أو اعتباري في بلد، وأن يكون هو في بلد آخر، ثم ينتقل إلى بلد ثالث ليباشر عمله منه.

من الجدير بالذكر أن الجرائم الإلكترونية مكانها العالم الافتراضي، فكيف يمكننا القول إن فعلها تم في إقليم الدولة؟، وكيف نحدد ذلك؟، إن الكثير من الجرائم الإلكترونية الخطيرة تتم على إقليم من خارجه، ويمتد أثرها داخل الإقليم، وهنا تكمن صعوبة المعرفة.

فهناك تطبيقات تتيح للمستخدم الدخول من خوادم الويب (Web Server) من بلدان غير البلد الذي يقيم فيه، فمثلاً يمكنه استخدام خوادم الويب في ألمانيا أو أي دولة أخرى وهو يقطن في الإمارات، فيصعب في مثل هذه الحالات تحديد القانون الواجب التطبيق، إذ المجرم في الإمارات على سبيل المثال، ودخل من خلال خوادم لدولة أخرى ليقوم بجريمة في دولة ثالثة، هذه التساؤلات سنحاول الإجابة عليها في هذا الفرع، عمد المشرع الإماراتي إلى تحديد القانون الواجب التطبيق ففي المادة (69) (89) تحدث عن نطاق سريان قانون مكافحة الشائعات والجرائم الإلكترونية، مع عدم الإخلال بما جاء في نطاق سريان قانون الجرائم والعقوبات الإماراتي (90)، من حيث الزمان (91) والمكان(92).

الخاتمة

وخلص البحث إلى ما يلي:

التوصيات:

أن يتم وضع عقوبات تفرق بين الجريمة الصادرة عن الشخص الطبيعي والشخص الاعتباري، إذ إن قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي ساوى بين الأفراد والمنشآت في ذات المخالفات من حيث العقوبة.

زيادة الوعي المجتمعي من خلال الأجهزة المختصة بالأمن السيبراني، والمؤسسات المعنية بهذا الأمر.

وضع برامج توعوية دراسية في مختلف مراحل الدراسة توضح خطورة استخدام الأجهزة الإلكترونية لساعت طويلة، وتشرح كيفية استخدامها بالطرق المثلى.

على الشركات العاملة في مجال تقنية المعلومات، وضع تحذير صحي بخط واضح وأسلوب مفهوم، حول منتجاتها وما ممكن أن تتسبب به من مشاكل صحية إن وجدت، وأن تضع إرشادات الاستخدام بشكل وافي، وعدد ساعات الاستخدام الآمنة..

على الجهات الرقابية وحقوق المستهلك مراقبة وفحص وتوقيع اتفاقات مع جهات رقابية في دول متقدمة، لمعرفة نتائج الفحوصات والاقتداء بها في حماية المستهلك والمنافسة.
أن تكون الشرائع محل البحث أكثر وضوحا وتفصيلًا في العمد من عدمه، وفي مدة المكوث للمصرح لهم أن تكون بمقدار الوقت المصرح لهم، وأن مجرد الاطلاع بالنظر أو القراءة يعد تعدياً على حقوق الغير في حفظ بياناتهم.
من خلال البحث يستشف تعريف الجريمة الإلكترونية **"كل فعل أو ترك يخالف عليه القانون، حدث عبر الشبكة العنكبوتية أو لم يحدث من خلالها، مستعينًا بأي تقنية كانت من برامج أو أجهزة إلكترونية أو ممغنطة"**.
يرى الباحث لو أن المشرع عمم في تعريف المستخدم ليصبح كالتالي **" كل شخص طبيعي أو اعتباري أو من ينوب عنهما، أو استخدم صلاحيتهما بعلمهم أو بدون علمهم، بموافقتهما، أو دون موافقتهما، أيًا كانت صفته استخدام خدمات تقنية المعلومات أو يستفيد منها بأي صورة "** بدلًا عن **"كل شخص طبيعي أو اعتباري يستخدم خدمات تقنية المعلومات أو يستفيد منها بأي صورة"**.
نخلص إلى أن الدليل الرقمي يمكن تعريفه بأنه **" كل بيانات أو معلومات حفظت أو عولجت في أي من وسائل التقنية، أو استخرجت منها بأي شكل من الأشكال المسموع أو المرئي، وبأي حالة كانت صورًا أو رسومات أو غيرها، وسواءً شكلت معلومة مفهومة أم لا، ليقام عليه حكم قانوني"**.
نستخلص من خلال البحث أن تعريف الميتافيرس **"تقنية تعمل بأدوات مساعدة يظهرون فيها على شكل أبعاد ثلاثية مشفرة أو مرمزة أفتار ()، يختارون بمحضAvatar إرادتهم محل تواجدهم في واقع يفترضونه من بيئتهم الحقيقية أو يستعينون بواقع من تصميم الغير يرغبون التواجد به ليمارسوا مختلف أنشطتهم مع بعضهم البعض بNFT() غير قابلة للاستبدال، ليحققوا مبتغاهم من هذا التجمع سواء أ كان تعليميًّا، أو تجاريًّا، أو ترفيهيًّا، أو اجتماعيًّا، أو بغرض إنجاز الأعمال"**.

قائمة المراجع:

أولا: المراجع العربية:

الكتب والأبحاث والمقالات:

- أمجد خليل حمودة، الوسائل الحديثة لإثبات الجرائم التي ترتكب بواسطة الأجهزة الإلكترونية، مجلة الأزهر- غزة، عدد خاص بمؤتمر كلية الحقوق الخامس المحكم، المجلد 19.
- بوسجرة ليليا، آليات حماية خصوصية البيانات في عصر الميتافيرس: المتداول والضروري، مجلة ألف اللغة والإعلام والمجتمع، المجلد 10 العدد 2 مارس 2023، تأريخ النشر 25/05/2023.
- خالد ممدوح إبراهيم، التنظيم القانوني لتقنية الميتافيرس دراسة مقارنة، دار الفكر الجامعي، بدون طبعة، سنة 2023.
- ربيع محمد يحيى، ميتافيرس الفرص والمخاطر وسيناريوهات المستقبل، مركز الإمارات للدراسات والبحوث الاستراتيجية، الطبعة الأولى، سنة الطبع 2022، ص119.
- زعتر نور الدين، العالم الافتراضي (Metaverse) من منظور سيكولوجي، مجلة العلوم الإنسانية لجامعة أم البواقي، المجلد 9 العدد 2 جوان 2022، تأريخ قبول البحث 10/03/2022.
- سعاد طعبة، تفعيل الآليات القانونية من أجل تحقيق العدالة، مجلة الحقوق والعلوم الإنسانية، المجلد (15)، العدد (03) 2022، تأريخ النشر 08/10/2022.
- سلامة محمد المنصوري، تطبيق مبدأ الاقتناع القضائي على الدليل الإلكتروني، أطروحة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام، جامعة الإمارات العربية المتحدة، 2018.
- عبد السلام محمد المايل وآخرون، الجريمة الإلكترونية في الفضاء الإلكتروني، مجلة آفاق للبحوث والدراسات السياسية، العدد (04)، تأريخ النشر 31/07/2019.
- عبد القادر بن عبد الله الفتوخ، الجريمة في الإنترنت: وطرق الحماية منها، العبيكان للنشر الرياض، بدون طبعة، سنة النشر 2011.
- عبد القادر جدي، الأحكام الشرعية للمعاملات المالية في تكنولوجيا الميتافيرس، مجلة المعيار، مجلد 27 عدد 5 (رث 74)، السنة 2023، تأريخ النشر 15/09/2023، ص4، مصدر مذكور لديه، هاني بن عبد الله الجبير، الفقه الارتيادي نظرات في الفقه المستشرف للمستقبل، مركز نماء للبحوث والدراسات، طبعة 2014.
- عمر عبد العزيز موسى عبد العزيز الدبور، أعمال المؤتمر الدولي الرباع عشر: الجرائم الإلكترونية رقم المؤتمر14، آليات تفعيل الحماية والوقاية من الجرائم الالكترونية: إنشاء ضبطية خاصة بالجرائم الالكترونية، مركز جيل البحث العلمي وجامعة تلمسان- كلية العلوم الاقتصادية- مخبر الحوكمة العمومية والاقتصاد الجامعي، مارس 2017.
- فلاك مراد، آليات الحصول على الأدلة الرقمية كوسائل إثبات في الجرائم الإلكترونية، مجلة الفكر القانوني والسياسي، العدد الخامس، تأريخ النشر 12/06/2019.

- ليليا بو سجرة وآخرون، الميتافيرس وتحدي الحرية والحقيقة قراءة تحليلية في نموذج الحرب الروسية الأوكرانية، مجلة المصداقية مجلد 4 (عدد 1) /2022، تأريخ النشر 26/06/2022.
- مبروك فاطمة، وآخرون، الجرائم المستحدثة ضبط المفهوم وتحديد الأنماط، مجلة الفكر القانوني والسياسي، المجلد السابع العدد الأول 2023، تأريخ النشر 15/05/2023.
- ميرفت محمد حبابية، مكافحة الجريمة الإلكترونية، دار اليازوري العلمية، بدون طبعة، سنة الطبعة 2022.
- ممدوح بن رشيد بن مشرف العنزي، الحماية الجزائية الموضوعية من الدخول غير المشروع لبيانات مستخدمي التطبيقات الإلكترونية: دراسة مقارنة، مجلة جامعة تبوك للعلوم الإنسانية والاجتماعية، المجلد3، العدد 2، تأريخ النشر 2023.
- هدى المراغي، الميتافيرس ومكافحة الجرائم الإلكترونية، بحث منشور في الموقع الإلكتروني لمركز ايجيبيشن انتربرايز للسياسات والدراسات، تأريخ النشر على الموقع الإلكتروني الخاص بالمركز في 12 مارس 2022.
- الدورة السابع والسبعون، البند 69 (ب) من جدول الأعمال المؤقت، تعزيز حقوق الإنسان وحمايتها: مسائل حقوق الإنسان، بما في ذلك النهج البديلة لتحسين التمتع الفعلي بحقوق الإنسان والحريات الأساسية، الحق في الخصوصية، والذي أعيد نشره بتأريخ 19 أيلول/ سبتمبر 2022.

القوانين والتشريعات العربية:

- قانون حماية البيانات الشخصية، رقم (45) لسنة 2021، وأطلق عليه أينما ورد بقانون حماية البيانات الشخصية الإماراتي.
- قانون مكافحة الشائعات والجرائم الإلكترونية، رقم (34) لسنة 2021، وأطلق عليه أينما ورد بقانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي.
- قانون اتحادي رقم (31) لسنة 2021 بإصدار قانون الجرائم والعقوبات وتعديلاته، لدولة الإمارات العربية المتحدة.
- في قانون الإثبات في المعاملات التجارية رقم (35) لسنة 2022، لدولة الإمارات العربية المتحدة.
- قانون حماية البيانات الشخصية، رقم 151 لسنة 2020، وأطلق عليه أينما ورد بقانون حماية البيانات الشخصية المصري.
- قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، وأطلق عليه أينما ورد بقانون مكافحة جرائم تقنية المعلومات المصري.
- نظام حماية البيانات الشخصية، مرسوم ملكي رقم (م/19)، تأريخ الإصدار 09/02/1443 هـ، الموافق 16/09/2021. وأطلق عليه أينما ورد بنظام حماية البيانات الشخصية السعودي.

ثانياً:المراجع الأجنبية

الكتب والأبحاث والمقالات:

- Understanding Blockchain Technology, Simanta Shekhar Sarmah, Computer Science and Engineering 2018, 8(2): 23-29 DOI: 10.5923/j.computer.20180802.02.
- Maria Tzanou, Personal data proyection and legal developments in the European Union, Keele University, UK,,2020 P. 4
- Agnès Rabagny-Lagoa, Fiches de Droit du traitement et de la protection des données personnelles, Editions Ellipses, 2022, p.35
- Peter G. Berris Legislative Attorney, Congressional Research Service2020 21 (،R46536, p15.
- Ahmed Rabaa'I And J.D Jayaraman, Understanding Non-Fungible Tokens (NFTs): Overview, Opportunities, and Challenges, Conference Paper · November 2022, 49th Annual Conference of the Northeast Business and Economics Association in: Portsmouth, New Hampshire, USA.

القوانين والتشريعات الأجنبية:

- Computer Fraud and Abuse Act (CFAA) (18 U.S.C 1030)
- COMMISSION IMPLEMENTING DECISION of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.
- The Clarifying Lawful Overseas Use of Data Act.
- EU Safe Harbor Agreement.
- LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.
- General Data Protection Regulation (GDPR).

المواقع الإلكترونية:

- https://u.ae/ar-AE/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/uae-strategy-for-artificial-intelligence
- https://ai.gov.ae/ar/personal-data-protection-law/
- https://careers.dubaifuture.gov.ae/ar/
- https://news.un.org/ar/story/2021/11/1088372
- https://www.wordreference.com/enar/meta
- https://ar.wikipedia.org
- https://dictionary.cambridge.org/dictionary/english/verse
- https://www.merriam-webster.com/dictionary/verse#dictionary-entry-1
- https://technologyreview.ae
- https://cms.law/en/int/publication/legal-issues-in-the-metaverse/part-1-what-is-the-metaverse
- https://www.researchgate.net
- https://www.merriam-webster.com/dictionary/avatar
- https://www.researchgate.net/publication/361618778_Understanding_NonFungible_Tokens_NFTs_Overview_Opportunities_and_Challenges
- https://www.researchgate.net/publication/336130918_Understanding_Blockchain_Technology
- https://www.dataprivacyframework.gov/s/program-overview
- https://techcrunch.com/2013/07/25/ireland-prism/
- https://www.ohchr.org/ar/documents/thematic-reports/a77196-principles-underpinning-privacy-and-protection-personal-data
- https://www.alarabiya.net/aswaq/special-stories
- https://www.albayan.ae/uae/news/2023-03-04-1.4625756
- https://me.kaspersky.com/resource-center/definitions/what-is-a-vpn
- https://www.wikiwand.com/ar
- https://www.justice.gov/jm/jm-9-48000-computer-fraud
- https://crsreports.congress.gov/product/pdf/R/R46536
- https://www.geeksforgeeks.org/difference-between-information-system-and-information-technology/
- https://www.lefebvre-dalloz.fr
- https://www.dxbpp.gov.ae/NewsPage.aspx?ID=826&Type=5
- https://www.justice.gov/criminal-oia/cloud-act-resources
- https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721
- http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm
- https://gdpr-info.eu/art-1-gdpr/
- https://gdpr.eu/article-68-what-is-the-european-data-protection-board/
- https://egyptianenterprise.com
- https://rm.coe.int/budapest-convention-in-arabic/1680739173

الفهرس

Notes

[←1]

) عبد القادر جدي، الأحكام الشرعية للمعاملات المالية في تكنولوجيا الميتافيرس، مجلة المعيار، مجلد 27 عدد 5 (رث 74)، السنة 2023، تأريخ النشر 15/09/2023، ص4، مصدر مذكور لديه، هاني بن عبد الله الجبير، الفقه الارتيادي نظرات في الفقه المستشرف للمستقبل، مركز نماء للبحوث والدراسات، طبعة 2014، ص18.

[←2]
) مبروك فاطمة، وآخرون، الجرائم المستحدثة ضبط المفهوم وتحديد الأنماط، مجلة الفكر القانوني والسياسي، المجلد السابع العدد الأول 2023، تأريخ النشر 15/05/2023.

[←3]
) ولعل مقولة الشيخ محمد بن راشد حول هذا الموضوع تأتي تأكيدًا لما ذكرته فمقولته الشهيرة لا زالت تلامس مسامعي " يجب علينا ألا ننتظر المستقبل، بل نصنع المستقبل من اليوم".

[←4]

) لمزيد من التفاصيل راجع الموقع الإلكتروني لحكومة الإمارات
https://u.ae/ar-AE/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/government-services-and-digital-transformation/uae-strategy-for-artificial-intelligence

[←5]) لمزيد من التفاصيل راجع الموقع الإلكتروني مكتب وزير دولة للذكاء الاصطناعي والاقتصاد الرقمي وتطبيقات العمل عن بعد

https://ai.gov.ae/ar/personal-data-protection-law/

[←6]

) لمزيد من المعلومات راجع موقع مؤسسة دبي للمستقبل

https://careers.dubaifuture.gov.ae/ar/

[←7]

) لمزيد من المعلومات راجع موقع أخبار الأمم المتحدة

https://news.un.org/ar/story/2021/11/1088372

[←8]

) سنعرف المقصود بالبيانات الشخصية وأنواعها في محله من هذا البحث، حسب ما وردت في مسيرة قانون حماية البيانات الشخصية لدولة الإمارات العربية المتحدة، مرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية، الصادر بتأريخ 20 سبتمبر 2021، والمنشور في الجريدة الرسمية العدد 712 (ملحق 1)، تأريخ النشر 26 سبتمبر، وعمل به اعتبارًا من 2 يناير 2022.

[←9]
) ليليا بو سجرة وآخرون، الميتافيرس وتحدي الحرية والحقيقة قراءة تحليلية في نموذج الحرب الروسية الأوكرانية، مجلة المصداقية مجلد 4 (عدد 1) /2022، تأريخ النشر 26/06/2022، ص4.

[←10]

) وعلى نفس الصيغة السابقة علم الميتافيزيقا وهو علم يدرس ما وراء الطبيعة، لمزيد من التفاصيل راجع الموقع الإلكتروني https://www.wordreference.com/enar/meta

[←11]

) روائي أمريكي ولد عام 1959 معروف بأعماله في الخيال التأملي، مزيد حول الروائي الأمريكي يمكن مراجعة الموقع الإلكتروني:

https://ar.wikipedia.org

[←12]

) تأتي هذه الكلمة في المعاجم الإنجليزية، بمعاني متعددة منها "آية، أو بيت شعر، قصيدة.."، ولم أجدها بمعنى الكون .. لمزيد من المعلومات حول معاني هذه الكلمة يمكن الرجوع إلى التراجم الآتية:

- https://dictionary.cambridge.org/dictionary/english/verse
- https://www.merriam-webster.com/dictionary/verse#dictionary-entry-1

[←13]

) مقال منشور في المجلة الالكترونية شبكة مواقع المجرة (technology review) بقلم عمرو عوض عنوانه " دليلك لفهم الميتافيرس عالم تدخله بدلا من الاكتفاء بمشاهدته، تأريخ النشر 17 نوفمبر 2021، تأريخ الدخول للموقع الإلكتروني 26/08/2023.

https://technologyreview.ae

[←14]

) لمزيد من التفاصيل راجع الموقع الإلكتروني تأريخ الدخول للموقع 17/8/2023
https://cms.law/en/int/publication/legal-issues-in-the-metaverse/part-1-what-is-the-metaverse

[←15]

) لمزيد من التفاصيل يمكنك الرجوع للبحث كاملًا في الموقع الإلكتروني

“The Metaverse is the post-reality universe, a perpetual and persistent multiuser environment merging physical reality with digital virtuality. It is based on the convergence of technologies that enable multisensory interactions with virtual environments, digital objects and people such as virtual reality (VR) and augmented reality (AR). Hence, the Metaverse is an interconnected web of social, networked immersive environments in persistent multiuser platforms. It enables seamless embodied user communication in real-time and dynamic interactions with digital artifacts. Its first iteration was a web of virtual worlds where avatars were able to teleport among them. The contemporary iteration of the Metaverse features social, immersive VR platforms compatible with massive multiplayer online video games, open game worlds and AR collaborative spaces”.

https://www.researchgate.net

تأريخ الدخول للموقع 28/8/2023

[←16]

) كما وضحها قاموس (merriam-webster) تعني باللغة السنسكريتية (وهي لغة قديمة يستخدمها الهنود وبعض دول شرق آسيا) تجسد الآلهة الهندوسية.

"Avatar derives from a Sanskrit word meaning "descent," and when it first appeared in English in the late 18th century, it referred to the descent of a deity to the earth-typically, the incarnation in earthly form of Vishnu or another Hindu deity. It later came to refer to any incarnation in human form, and then to any embodiment (such as that of a concept or philosophy), whether or not in the form of a person. In the age of technology, *avatar* has developed another sense-it can now be used for the image that a person chooses as his or her "embodiment" in an electronic medium."

https://www.merriam-webster.com/dictionary/avatar

تأريخ الدخول للموقع: 01/09/2023

[←17]

) الـ (NFT) اختصار لـ (Non-Fungible Tokens). لمزيد من المعلومات يمكنك الرجوع للبحث المنشور من قبل (Ahmed Rabaa’I And J.D Jayaraman) في نوفمبر 2022، المؤتمر السنوي التاسع والأربعين لجمعية الأعمال والاقتصاد في شمال شرق البلاد في: بورتسموث، نيو هامبشاير، الولايات المتحدة الأمريكية.

"Understanding Non-Fungible Tokens (NFTs): Overview, Opportunities, and Challenges" https://www.researchgate.net/publication/361618778_Understanding_NonFungible_Tokens_NFTs_Overview_Opportunities_and_Challenges

تأريخ الدخول للموقع 28/8/2023

[←18]

) أنظر ربيع محمد يحيى، ميتافيرس الفرص والمخاطر وسيناريوهات المستقبل، مركز الإمارات للدراسات والبحوث الاستراتيجية، الطبعة الأولى، سنة الطبع 2022، ص119.

[←19]

)لمزيد من المعلومات يمكنك الرجوع إلى البحث:

Understanding Blockchain Technology, Simanta Shekhar Sarmah, Computer Science and Engineering 2018, 8(2): 23-29 DOI: 10.5923/j.computer.20180802.02.
https://www.researchgate.net/publication/336130918_Understanding_Blockchain_Technology
تأريخ الدخول للموقع: 08/09/2023

[←20]

راجع)

- Agnès Rabagny-Lagoa, Fiches de Droit du traitement et de la protection des données personnelles, Editions Ellipses, 2022, p.35

[←21]

(The Clarifying Lawful Overseas Use of Data Act) تأتي اختصار لـ)

"The Clarifying Lawful Overseas Use of Data Act is a United States federal law enacted in 2018 by the passing of the Consolidated Appropriations Act, 2018, PL 115–141, Division V."

انظر الموقع الإلكتروني

https://www.justice.gov/criminal-oia/cloud-act-resources

[←22]

) مرجع سابق، ليليا بو سجرة وآخرون، الميتافيرس وتحدي الحرية والحقيقة قراءة تحليلية في نموذج الحرب الروسية الأوكرانية.

[←23]

) زعتر نور الدين، العالم الافتراضي (Metaverse) من منظور سيكولوجي، مجلة العلوم الإنسانية لجامعة أم البواقي، المجلد 9 العدد 2 جوان 2022، تأريخ قبول البحث 10/03/2022، ص1023.

[←24]

) أنظر الخبر في الموقع الإلكتروني

https://www.skynewsarabia.com/business

[←25]
) الجريدة الرسمية العدد (712) ملحق (1) في 26 سبتمبر 2021، والصادر بتأريخ 20 سبتمبر، قانون حماية البيانات الشخصية، رقم (45) لسنة 2021، وسيطلق عليه أينما ورد بقانون حماية البيانات الشخصية الإماراتي.

[←26]
) الجريدة الرسمية العدد (28) مكرر (هـ) في 15 يوليه سنة 2020، قانون حماية البيانات الشخصية، رقم 151 لسنة 2020، وسيطلق عليه أينما ورد بقانون حماية البيانات الشخصية المصري.

[←27]

) نظام حماية البيانات الشخصية، مرسوم ملكي رقم (م/19)، تأريخ الإصدار 09/02/1443 هـ، الموافق 16/09/2021، والمنشور بتأريخ 17/02/1443 هـ، الموافق 24/09/2021.

[←28]

) راجع الموقعين الإلكترونيين ستجد نص اللائحة كاملاً،

- https://gdpr-info.eu/art-1-gdpr/
- https://gdpr.eu/article-68-what-is-the-european-data-protection-board/

[←29]

) أنظر الموقع الإلكتروني

https://www.dataprivacyframework.gov/s/program-overview

[←30]

) أنظر الموقع الإلكتروني

https://techcrunch.com/2013/07/25/ireland-prism/
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

[←31]

) عرفه المشرع في قانون حفظ البيانات المصري بنفس التعريف في الفصل الأول مادة (1).

[←32]

) البيانات الحيوية البيومترية، انفرد المشرع الإماراتي بهذا التعبير عن غيره في قانون حفظ البيانات الشخصية الإماراتي. ويعرفها أنها "التعرف الآلي على الأفراد استنادًا إلى سماتهم البيولوجية والسلوكية". هذا يعني أن البيانات البيومترية بمثابة توقيعات بشرية فريدة يمكن قياسها، وقد تشمل بصمات الأصابع ومسح قزحية العين أو طريقة الفرد في فعل شيء ما (مثل الطريقة التي يسير أو يكتب بها). وهي إحدى أكثر الوسائل الموثوقة لإثبات الهوية المتاحة في حوزتنا، فمن الصعب للغاية تزييفها.

[←33]

) راجع لائحة الاتحاد الأوربي (GDPR) على الموقع الإلكتروني

1. "personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”

https://gdpr.eu/article-4-definitions/

[←34]

) بوسجرة ليليا، آليات حماية خصوصية البيانات في عصر الميتافيرس: المتداول والضروري، مجلة ألف اللغة والإعلام والمجتمع، المجلد 10 العدد 2 مارس 2023، تأريخ النشر 25/05/2023، ص352.

[←35]

) للمزيد راجع ما نشر في الدورة السابع والسبعون، البند 69 (ب) من جدول الأعمال المؤقت، تعزيز حقوق الإنسان وحمايتها: مسائل حقوق الإنسان، بما في ذلك النهج البديلة لتحسين التمتع الفعلي بحقوق الإنسان والحريات الأساسية، الحق في الخصوصية، والذي أعيد نشره بتأريخ 19 أيلول/ سبتمبر 2022، راجع الموقع الإلكتروني https://www.ohchr.org/ar/documents/thematic-reports/a77196-principles-underpinning-privacy-and-protection-personal-data

[←36]

) راجع الموقع الإلكتروني

https://www.lefebvre-dalloz.fr

“Le RGPD est applicable depuis le 25 mai 2018 dans l’ensemble de l’Union européenne. Il vise à protéger les libertés et droit fondamentaux des personnes physiques et, en particulier, leur droit à la protection de leurs données personnelles, mais aussi à garantir la libre circulation de ces données au sein de l’Union (art. 1er). Le RGPD a élargi le champ d’application tant matériel que territorial des règles relatives à la protection des données personnelles (art. 2 et 3). Il définit 26 notions dont certaines font leur apparition, alors que d’autres ne sont pas nouvelles, mais reçoivent une acception différente (art. 4). Ses articles 5 à 11 regroupent les principes généraux, tandis que ses articles 85 à 91 consacrent des dispositions spécifiques à certains traitements ou données.”

[←37]

) **البيانات أو المعلومات:** مجموعة منظمة أو غير منظمة من المعطيات، أو الوقائع أو المفاهيم أو التعليمات أو المشاهدات أو القياسات تكون على شكل أرقام أو أحرف أو كلمات أو رموز أو صور أو فيديوهات، أو إشارات، أو أصوات أو خرائط أو أي شكل آخر، يتم تفسيرها أو تبادلها أو معالجتها، عن طريق الأفراد أو الحواسيب، والتي ينتج بعد معالجتها أو تداولها ما يطلق عليه مصطلح معلومات. **البيانات والمعلومات الحكومية:** البيانات أو المعلومات الحكومية غير المتاحة للكافة، والخاصة أو العائدة إلى إحدى مؤسسات الدولة. **البيانات والمعلومات الشخصية:** المعلومات أو البيانات الخاصة بالأشخاص الطبيعيين متى كانت مرتبطة بحياتهم الخاصة أو تحدد هويتهم أو يمكن من خلال ربط هذه المعلومات والبيانات بطريقة مباشرة أو غير مباشرة تحديد ومعرفة هوية الشخص. **المعلومات والبيانات السرية:** أي معلومات أو بيانات غير مصرح للغير بالاطلاع عليها أو بإفشائها إلا بإذن مسبق ممن يملك هذا الإذن.

[←38]

) أينما ورد هذا اللفظ فالمقصود به هو المرسوم الاتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية، الجريدة الرسمية 712 ملحق، تأريخ النشر 26 سبتمبر 2021.

[←39]

) أينما ورد هذا اللفظ فالمقصود به هو قانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية العدد 32 مكرر (ج) في أغسطس سنة 2018.

[←40]

) أنظر الموقع الإلكتروني

https://rm.coe.int/budapest-convention-in-arabic/1680739173

[←41]

) هدى المراغي، الميتافيرس ومكافحة الجرائم الإلكترونية، بحث منشور في الموقع الإلكتروني لمركز ايجيبيشن انتربرايز للسياسات والدراسات، تأريخ النشر على الموقع الإلكتروني الخاص بالمركز في 12 مارس 2022، ص3.
https://egyptianenterprise.com/

[←42]

) أنظر المواقع الإلكترونية

https://www.alarabiya.net/aswaq/special-stories
https://www.albayan.ae/uae/news/2023-03-04-1.4625756

[←43]

راجع)

Grainne Kirwan and Andrew Power, The Psychology of Cyber Crime, Institue of Art, Design and Tecnology, Ierland, 2012, P. 1.

“The core of the Psychology of Cybercrime seeks to address both the theory of crime and the question of forensic psychology's contribution to the understanding of cybercrime. Specific examples of online crime such as hacking, malware, identity theft, child pornography and cyberbullying are dealt with in some detail in later chapters. This chapter seeks to first define the nature of online crime or cybercrime and look at the ways in which society is responding to it. The nature of the response is multi-faceted. Governments attempt to respond with law, corporations with policies and procedures, suppliers with terms and conditions, users with peer pressure, technologists with code”

[←44]

) راجع عبدالسلام محمد المايل وآخرون، الجريمة الإلكترونية في الفضاء الإلكتروني، مجلة آفاق للبحوث والدراسات السياسية، العدد (04)، تأريخ النشر 31/07/2019، ص246.

[←45]

) عمر عبد العزيز موسى عبد العزيز الدبور، أعمال المؤتمر الدولي الرباع عشر: الجرائم الإلكترونية رقم المؤتمر14، آليات تفعيل الحماية والوقاية من الجرائم الالكترونية: إنشاء ضبطية خاصة بالجرائم الالكترونية، مركز جيل البحث العلمي وجامعة تلمسان- كلية العلوم الاقتصادية- مخبر الحوكمة العمومية والاقتصاد الجامعي، مارس 2017، ص222.

[←46]

) ويعرف (Internet Protocol) ويختصر بـ (IP) على أنه " هو عنوان فريد يعرّف جهاز على الإنترنت أو شبكة محلية. ويرمز الاختصار (IP) إلى عبارة "بروتوكول الإنترنت"، وهو عبارة عن مجموعة من القواعد التي تحكم تنسيق البيانات المرسلة عبر الإنترنت أو الشبكة المحلية، ويكون شكله على النحو الآتي: (176.205.113.139)، لمزيد من المعلومات راجع الموقع الإلكترون:

https://me.kaspersky.com/resource-center/definitions/what-is-an-ip-address

[←47]

)ويعرف " virtual private network" ويختصر بـ (VPN) "الشبكة الافتراضية الخاصة" وتقدم وصفا لكيفية إنشاء اتصال شبكي محمي عند استخدام الشبكات العامة. تقوم شبكات VPN بتشفير حركة البيانات الخاصة بك على الإنترنت وإخفاء هويتك الإلكترونية، مما يجعل تتبع أنشطتك عبر الإنترنت وسرقة بياناتك أمرًا في غاية الصعوبة بالنسبة للغير، حيث يتم التشفير في الوقت الفعلي، ولمزيد من المعلومات راجع الموقع الإلكتروني.

https://me.kaspersky.com/resource-center/definitions/what-is-a-vpn

[←48]

) سعاد طعبة، تفعيل الآليات القانونية من أجل تحقيق العدالة، مجلة الحقوق والعلوم الإنسانية، المجلد (15)، العدد (03) 2022، تأريخ النشر 08/10/2022.

[←49]

) الذي صدر في عام 1986م وهو القانون (18 U.S.C 1030) والذي مر بعدة مراحل من التعديلات خلال الأعوام 1989، 1994، 1996، 2001، 2002، 2008، بموجب قانون إنفاذ واستعادة الهوية الشخصية.

https://www.wikiwand.com/ar

تأريخ الدخول للموقع 11/09/2023

[←50]

) عبد القادر بن عبد الله الفتوخ، الجريمة في الإنترنت: وطرق الحماية منها، العبيكان للنشر، الطبعة بدون طبعة، سنة النشر 2011، ص39.

[←51]

(راجع البحث المنشور من قبل (Peter G. Berris Legislative Attorney) في الموقع الإلكتروني (Congressional Research Service) بتأريخ 21 سبتمبر 2020، R46536. ص15

‘Prohibits intentionally accessing a computer without authorization or in excess of authorization and obtaining information from a financial institution, the federal government, or a protected computer’.

https://crsreports.congress.gov/product/pdf/R/R46536

تأريخ الدخول للموقع 11/09/2023

[←52]

) راجع الموقع الإلكتروني فب التعريفات التالية:

- **Access "without authorization":** Section 1030 describes a number of offenses that occur when a defendant accesses a protected computer "without authorization." See 18 U.S.C. §§ 1030(a)(1), (a)(2), (a)(3), (a)(4), and (a)(5)(B)-(C). The Department will not charge defendants for accessing "without authorization" under these paragraphs unless when, at the time of the defendant's conduct, (1) the defendant was not authorized to access the protected computer under any circumstances by any person or entity with the authority to grant such authorization; (2) the defendant knew of the facts that made the defendant's access without authorization; and (3) prosecution would serve the Department's goals for CFAA enforcement, as described below in B.3.
- **Access "exceeding authorized access"**: Three paragraphs of section 1030 describe offenses involving conduct that "exceeds authorized access," sometimes also phrased "exceeding authorized access." See 18 U.S.C. §§ 1030(a)(1), (a)(2), and (a)(4). The Department will not charge defendants with "exceeding authorized access" or "exceeds authorized access" under these paragraphs unless, at the time of the defendant's conduct, (1) a protected computer is divided into areas, such as files, folders, user accounts, or databases; (2) that division is established in a computational sense, that is, through computer code or configuration, rather than through contracts, terms of service agreements, or employee policies; (3) a defendant is authorized to access some areas, but unconditionally prohibited from accessing other areas of the computer; (4) the defendant accessed an area of the computer to which his authorized access did not extend; (5) the defendant knew of the facts that made his access unauthorized; and (6) prosecution would serve the Department's goals for CFAA enforcement, as described below in B.3.

https://www.justice.gov/jm/jm-9-48000-computer-fraud

تأريخ دخول الموقع: 13/09/2023

[←53]

(مصدر سابق تم الإشارة إليه ص12 (Peter G. Berris Legislative Attorney) ص9.

(Obtaining Information by Unauthorized Computer Access, 18 U.S.C. § 1030(a)(2) Section 1030(a)(2)90 generally prohibits accessing a computer without authorization or in excess of authorization and obtaining information in certain circumstances. Although at first glance it could appear that to "obtain information" might refer specifically to misappropriation or theft of information, the concept is much broader.91 Indeed, as interpreted by courts, "obtaining information" includes "mere observation of the data" such as looking at or reading information on a screen.92 Perhaps unsurprisingly then, the government has invoked § 1030(a)(2) in a variety of prosecutions).

[←54]

) نظام مكافحة جرائم المعلوماتية، الصادر بالمرسوم الملكي (رقم م/17) بتأريخ 08/03/1428هـ، الموافق 27/03/2007، تأريخ النشر 27/03/2007.

[←55]

) الجريدة الرسمية 712 ملحق، في 26 سبتمبر 2021م، قانون اتحادي رقم (31) لسنة 2021 بإصدار قانون الجرائم والعقوبات وتعديلاته.

[←56]

) راجع الموقع الإلكتروني

https://www.dxbpp.gov.ae/NewsPage.aspx?ID=826&Type=5

[←57]

) ممدوح بن رشيد بن مشرف العنزي، الحماية الجزائية الموضوعية من الدخول غير المشروع لبيانات مستخدمي التطبيقات الإلكترونية: دراسة مقارنة، مجلة جامعة تبوك للعلوم الإنسانية والاجتماعية، المجلد3، العدد 2، تأريخ النشر 2023، ص191.

[←58]

) راجع الموقع الإلكتروني تأريخ دخول الموقع 12/09/2023، اختصار لمصطلح (INFORMATIPN SYSTEM).

- **Information System:** Information System, as name suggests, is study and use of system to process data from input to generate information that is essential and useful for managing operations. It helps in analyzing independent processes and enables organized work activities. It is considered key factor to provide correct knowledge for decision-making within an organization.
- **Information Technology:** Information Technology, as name suggests, is basically study and use of system to establish faster communication, maintain electronic storage and provide protection to business's records or company records. It simply refers to anything related to computing technology like software, hardware, networking, etc.
- IT focuses on the technology infrastructure, hardware, software, and networks that enable data processing and communication. IS, on the other hand, focuses on the framework, processes, and procedures that enable the effective use of data to support business processes and decision-making.

https://www.geeksforgeeks.org/difference-between-information-system-and-information-technology/

تأريخ دخول الموقع: 13/09/2023

[←59]
) راجع خالد ممدوح إبراهيم، التنظيم القانوني لتقنية الميتافيرس دراسة مقارنة، دار الفكر الجامعي، بدون طبعة، سنة2023، ص144 وما بعدها.

[←60]

) ربيع محمد يحي، ميتافيرس الفرص والمخاطر وسيناريوهات المستقبل، مركز الإمارات للدراسات والبحوث الاستراتيجية، بدون طبعة، 2022، ص179.

[←61]

) ربيع محمد يحيى، ميتافيرس الفرص والمخاطر وسيناريوهات المستقبل، مصدر سابق، ص190.

[←62]

) تم تعريفه في الفرع الأول من المطلب الأول في المبحث الثاني من هذا البحث.

[←63]

)تم تعريفه في الفرع الأول من المطلب الأول في المبحث الثاني من هذا البحث.

[←64]

) البند (1) من ذات المادة " يعاقب بالحبس مدة لا تقل عن (6) أشهر والغرامة التي لا تقل (20,000) عشرين ألف درهم ولا تزيد على (100,000) مائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من حصل أو استحوذ أو عدل أو أتلف أو أفشى أو سرب أو ألغى أو حذف أو نسخ أو نشر أو أعاد نشر بغير تصريح بيانات ومعلومات شخصية إلكترونية، باستخدام تقنية المعلومات أو وسيلة تقنية معلومات.

[←65]

) القانون رقم 13.709/2018، والمعدل بالقانون رقم 13853 لسنة 2019، و LGPD هي اختصار لـ (Lei Geral de Proteção de DadoKK، وقد تم تطبيق هذا القانون في 16 أغسطس 2020، نص المادة (5) فقرة (الأولى)

“Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;…”

راجع الموقع الإلكتروني

http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

[←66]

) تم تعريف مزود الخدمة، والوسيط في الفرع الأول من المطلب الأول في المبحث الثاني من هذا البحث.

[←67]

) نص المادة (7) من قانون حماية البيانات الشخصية رقم (45) لسنة 2021، جاء فيها:

يجب على المتحكم الالتزام بما يأتي:

. اتخاذ الإجراءات والتدابير التقنية والتنظيمية الملائمة لتطبيق المعايير القياسية اللازمة لحماية وتأمين البيانات الشخصية حفاظاً على سريتها وخصوصيتها، وضمان عدم اختراقها أو إتلافها أو تغييرها أو العبث بها. مع مراعاة طبيعة ونطاق واغراض المعالجة واحتمالية وجود مخاطر على سرية وخصوصية البيانات الشخصية لصاحب البيانات.

. تطبيق التدابير الملائمة سواء أثناء تحديد وسائل المعالجة أو أثناء المعالجة نفسها، وذلك بهدف الامتثال لأحكام هذا المرسوم بقانون بما فيها الضوابط المنصوص عليها في المادة 5 منه، وتشمل هذه التدابير آلية إخفاء البيانات.

. تطبيق التدابير التقنية والتنظيمية الملائمة بالنسبة للاعتداءات التلقائية، للتأكد من اقتصار معالجة البيانات الشخصية على الغرض المحدد لها، ويطبق هذا الالتزام على حجم ونوع البيانات الشخصية التي يتم جمعها، ونوه المعالجة التي سيتم إجراؤها عليها، وفترة تخزين هذه البيانات، ومدة إمكانية الوصول إليها.

. مسك سجل خاص للبيانات، على أن يتضمن هذا السجل بيانات كل من المتحكم ومسؤول حماية البيانات وبيان وصف فئات البيانات الشخصية لديه، وبيانات الأشخاص المصرح لهم بالوصول إلى البيانات الشخصية، والمدد الزمنية للمعالجة وقيودها ونطاقها، وآلية محو البيانات الشخصية أو تعديلها أو معالجتها لديه، والغرض من المعالجة، وأي بيانات متعلقة بحركة ومعالجة تلك البيانات عبر الحدود، وبيان الإجراءات التقنية والتنظيمية الخاصة بأمن المعلومات وعمليات المعالجة. على أن يقوم المتحكم بتوفير هذا السجل للمكتب متى ما طلب منه ذلك.

. تعيين المعالج الذي بتوفر لديه ضمانات كافية لتطبيق التدابير التقنية والتنظيمية على نحو يضمن استيفاء المعالجة لمتطلبات وقواعد وضوابط المعالجة المنصوص عليها في هذا المرسوم بقانون ولائحته التنفيذية والقرارات الصادرة تنفيذاً له.

. تزويد المكتب، وبناءً على قرار الجهة القضائية المختصة، بأي معلومات يطلبها تنفيذاً لاختصاصاته الواردة في هذا المرسوم بقانون ولائحته التنفيذية.

. أي التزامات أخرى تحددها اللائحة التنفيذية لهذا المرسوم بقانون.

[←68]

) نص المادة (8) من قانون حماية البيانات الشخصية رقم (45) لسنة 2021، جاء فيها:
يجب على المعالج الالتزام بما يأتي:
. إجراء المعالجة وتنفيذها وفقاً لتعليمات المحتكم، والعقود والاتفاقات المبرمة بينهما التي تحدد على وجه الخصوص نطاق المعالجة وموضوعها وغرضها وطبيعتها ونوع البيانات الشخصية، وفئات أصحاب البيانات.
. تطبيق الإجراءات والتدابير التقنية والتنظيمية الملائمة لحماية البيانات الشخصية في مرحلة التصميم، سواء أثناء تحديد وسائل المعالجة أو اثناء المعالجة نفسها، علة أن يراعى فيها تكلفة تطبيق هذه الإجراءات والتدابير وطبيعة المعالجة ونطاقها وأغراضها.
. إجراء المعالجة وفق الغرض والمدة المحددة لها، وفي حال تجاوزت المعالجة المدة المحددة يجب عليه أن يخطر المتحكم بذلك ليأذن له بتمديد هذه المدة أو يصدر إليه التوجيهات المناسبة.
. محو البيانات بعد انقضاء مدة المعالجة أو تسليمها للمتحكم.
. عدم القيام بأي عمل من سانه الافصاح عن البيانات الشخصية أو نتائج المعالجة إلا في الأحوال المصرح بها قانوناَ.
. حماية وتأمين عملية المعالجة وتأمين الوسائط والأجهزة الإلكترونية المستخدمة في المعالجة وما عليها من بيانات شخصية.
. مسك سجل خاص للبيانات الشخصية التي تتم معالجتها نيابة عن المتحكم، على أن يتضمن هذا السجل بيانات كل من المتحكم والمعالج ومسؤول حماية البيانات وبيان وصف فئات البيانات الشخصية لديه، وبيانات الأشخاص المصرح لهم بالوصول إلى البيانات الشخصية، والمدد الزمنية للمعالجة وقيودها ونطاقها، وآلية محو البيانات الشخصية أو تعديلها أو معالجتها لديه، والغرض من المعالجة، وأي بيانات متعلقة بحركة ومعالجة تلك البيانات عبر الحدود، وبيان الإجراءات التقنية والتنظيمية الخاصة بأمن المعلومات وعمليات المعالجة. على أن يقوم المعالج بتوفير هذا السجل للمكتب متى ما طلب منه ذلك.
. توفير كافة الوسائل لإثبات التزامه بتطبيق أحكام هذا المرسوم بقانون عند طلب المتحكم أو المكتب ذلك.
. إجراء المعالجة وتنفيذها طبقاً للقواعد والاشتراطات والضوابط المحددة بهذا المرسوم بقانون ولائحته التنفيذية أو التي يصدر بموجبها تعليمات من الكتب.
. في حال اشتراك أكثر من معالج في عملية المعالجة، يجب أن تنفذ المعالجة وفقاً لعقد أو اتفاق مكتوب يحدد بموجبه بشكل واضح التزاماتهم ومسؤولياتهم وأدوارهم حول عملية المعالجة، وإلا اعتبروا مسؤولين بالتضامن عن الالتزامات والمسؤوليات الواردة في هذه المرسوم بقانون ولائحته التنفيذية.
. تحديد اللائحة التنفيذية لهذا المرسوم بقانون الإجراءات والضوابط والشروط والمعايير الفنية والقياسية المتعلقة بهذه الالتزامات.

[←69]

) نص المادة (6) من قانون حماية البيانات الشخصية رقم (45) لسنة 2021، جاء فيها:
. يشترط للاعتداء بموافقة صاحب البيانات على معالجتها ما يلي:
. أن يكون المتحكم قادراً على إثبات موافقة صاحب البيانات في حال كانت المعالجة مبنية على موافقة صاحب البيانات لمعالجة بياناته الشخصية.
. أن تكون الموافقة معدة بطريقة واضحة وبسيطة وغير مبهمة وسهلة الوصول إليها سواء كانت كتابية أو إلكترونية.
. أن تتضمن الموافقة ما يفيد حق صاحب البيانات بالعدول عنها، وأن يكون إجراء العدول بطريقة سهلة.
. يجوز لصاحب البيانات العدول في أي وقت عن موافقته على معالجة بياناته الشخصية، ولا يؤثر هذا العدول على قانونية ومشروعية المعالجة المبنية على الموافقة التي أعطيت قبل العدول عنها.

[←70]

) نص المادة (4) من قانون حماية البيانات الشخصية رقم (45) لسنة 2021، جاء فيها:
يحظر معالجة البيانات الشخصية دون موافقة صاحبها، وتستثنى أي من الحالات التالية من هذا الحظر وتعتبر المعالجة حينها مشروعة:
. أن تكون المعالجة ضرورية لحماية المصلحة العامة.
. أن تكون المعالجة مرتبطة بالبيانات الشخصية التي أصبحت متاحة ومعاومة للكافة بفعل صاحل البيانات.
. أن تكون المعالجة ضرورية لإقامة أي من إجراءات المطالبة بالحقوق والدعاوى القانونية أو الدفاع عنها أو تتعلق بالإجراءات القضائية أو الأمنية.
. أن تكون المعالجة ضرورية لأغراض الطب المعني أو الوقائي من أجل تقييم قدرة الموظفين على العمل، أو الشخص الطبي أو تقديم الرعاية الصحية أو الاجتماعية أو العلاج أو خدمات التأمين الصحي أو إدارة أنظمة وخدمات الرعاية الصحية أو الاجتماعية وفقاً للتشريعات السارية في الدولة.
. أن تكون المعالجة ضرورية لحماية الصحة العامة، وتشمل الحماية من الامراض السارية والأوبئة أو لأغراض ضمان سلامة وجودة الرعاية الصحية والأدوية والعقاقير والأجهزة الطبية وفقاً للتشريعات السارية في الدولة.
. أن تكون المعالجة ضرورية لأغراض أرشيفية أو دراسات علمية وتاريخية وإحصائية وفقاً للتشريعات السارية في الدولة.
. أن تكون المعالجة ضرورية لحماية مصالح صاحب البيانات.
. أن تكون المعالجة ضرورية الأغراض قيام المتحكم أو صاحب البيانات بالتزاماته ومباشرة حقوقه المقررة قانوناً في كجال التوظيف أو الضمان الاجتماعي أو القوانين المعنية بالحماية الاجتماعية وذلك بالقدر الذي يسمح به في تلك القوانين.
. أن تكون المعالجة ضرورية لتنفيذ عقد يكون صاحب البيانات طرفاً فيه أو لاتخاذ إجراءات بناءً على طلب صاحب البيانات بهدف إبرام عقد أو تعديله أو إنهائه.
. أن تكون المعالجة ضرورية لتنفيذ التزامات محددة في قوانين أخرى في الدولة على المحتكم.
. اية حالات أخرى تحددها اللائحة التنفيذية لهذا المرسوم بقانون.

[←71]

) نص المادة (13) من قانون حماية البيانات الشخصية رقم (45) لسنة 2021، جاء فيها:
. يحق لصاحب البيانات وبناءً على طلب يقدمه إلى المتحكم ومن دون أي مقابل الحصول على المعلومات الآتية:
. أنواع البيانات الشخصية التابعة له التي يتم معالجتها.
. أغراض المعالجة.
. القرارات المتخذة بناءً على المعالجة المؤتمنة بما فيها التنميط.
د. القطاعات أو المنشآت المستهدفة التي سيتم مشاركة بياناته الشخصية معهم من داخل وخارج الدولة.
ه. ضوابط ومعايير مدد تخزين وحفظ بياناته الشخصية.
و. إجراءات تصحيح أو محو أو تقييد المعالجة والاعتراض على بياناته الشخصية.
ز. تدابير الحماية الخاصة بالمعالجة عبر الحدود التي تتم وفقاً للمادتين 22 و23 من هذا المرسوم بقانون.
ح. الإجراءات التي ستتخذ في حال اختراق أو انتهاك بياناته الشخصية، خاصة أن كان الاختراق أو الانتهاك له خطر مباشر وجسيم على خصوصية وسرية بيانته الشخصية.
ط. كيفية تقديم الشكاوى للمكتب.
2. في جميع الاحوال، يجب على المتحكم، وقبل البدء بالمعالجة، تزويد صاحب البيانات بالمعلومات المنصوص غليها في الفقرات (ب) و(د) و(ز) من البند (1) من هذه المادة.
3. يجوز للمتحكم رفض طلب صاحب البيانات في الحصول على المعلومات الواردة في البند (1) من هذه المادة، وفي حال تبين له ما يأتي:
أ. أن الطلب لا يتعلق بالمعلومات المشار إليها في البند (1) من هذه المادة أو كان متكرراً بشكل مبالغ به.
ب. أن الطلب يتعارض مع الإجراءات القضائية أو التحقيقات التي تجريها الجهات المختصة.
ج. أن الطلب قد يؤثر سلباً على جهود المتحكم في حماية أمن المعلومات.
د. أم الطلب يمس بخصوصية وسرية البيانات الشخصية للغير.

[←72]

) نص المادة (14) من قانون حماية البيانات الشخصية رقم (45) لسنة 2021، جاء فيها:

. يحق لصاحب البيانات الحصول على البيانات الشخصية الخاصة به التي تم تزويدها للمتحكم لمعالجتها، وذلك بشكل منظم وقابل للقراءة آلياً متى ما كانت المعالجة مبنية على موافقة صاحب البيانات، أو ضرورية لتنفيذ التزام عقدي، ومنفذة بوسائل مؤتمنة.

. يحق لصاحب البيانات طلب نقل بياناته الشخصية لمتحكم آخر متى ما كان ذلك ممكناً من الناحية التقنية.

[←73]

) نص المادة (15) من قانون حماية البيانات الشخصية رقم (45) لسنة 2021، جاء فيها:

. يحق لصاحب البيانات طلب تصحيح بياناته الشخصية غير الدقيقة، أو استكمالها لدى المتحكم دون تأخير غير مبرر.

. دون الاخلال بالتشريعات السارية في الدولة وما تتطلبه المصلحة العامة، يحق لصاحب البيانات طلب محو بياناته الشخصية الخاصة لدى المتحكم في أي من الحالات الآتية:

. لم تعد بياناته الشخصية ضرورية للأغراض التي جمعت أو عولجت من أجلها.

. عدول صاحب البيانات عن الموافقة التي بنيت عليها المعالجة.

ج. اعتراض صاحب البيانات على المعالجة، أو غياب الاسباب المشروعة للمتحكم في الاستمرار بالمعالجة.

د. أن معالجة بياناته الشخصية تمت بالمحافظة لأحكتم هذا المرسوم بقانون والتشريعات السارية، وأن عملية المحو ضرورية للامتثال للتشريعات والمعايير المعتمدة المعمول بها في هذا الشأن.

3. استثناء مما ورد في البند (2) من هذه المادة لا يحق لصاحب البيانات طلب محو بياناته الشخصية لدى المتحكم في الحالات الآتية:

أ. في حال كان الطلب يتعلق بمحو بياناته الشخصية المتعلقة بالصحة العامة لدى المنشآت الخاصة.

ب. إذا كان الطلب يؤثر على إجراءات التحقيق والمطالبة بالحقوق والدعاوى القانونية أو الدفاع عنها لدى المتحكم.

ج. إذا كان الطلب يتعارض مع تشريعات أخرى يخضع لها المتحكم.

د. أي حالات أخرى تحددها اللائحة التنفيذية لهذا المرسوم بقانون.

[←74]

) نص المادة (16) من قانون حماية البيانات الشخصية رقم (45) لسنة 2021، جاء فيها:
. يحق لصاحب البيانات إلزام المتحكم بتقييد وإيقاف المعالجة في أي من الحالات الآتية:
. اعتراض صاحب البيانات على دقة بياناته الشخصية، وفي هذه الحالة يتم تقييد المعالجة لفترة محددة تسمح للمتحكم التحقيق من دقتها.
. اعتراض صاحب البيانات على معالجة بياناته الشخصية بالمخالفة للأغراض المتفق عليها.
. أن تكون المعالجة قد تمت بالمخالفة لأحكام هذا المرسوم بقانون والتشريعات السارية.
. يحق لصاحب البيانات الطلب من المتحكم الاستمرار بالاحتفاظ ببياناته الشخصية لما بعد انتهاء أغراض المعالجة، كون هذه البيانات ضرورية لاستكمال إجراءات متعلقة بالمطالبة بالحقوق والدعاوى القضائية أو الدفاع عنها.
. على الرغم مما ورد في البند (1) من هذه المادة، للمتحكم المضي في معالجة البيانات الشخصية لصاحب البيانات دون موافقته في أي من الحالات الآتية:
. إذا كانت المعالجة مقتصرة على تخزين البيانات الشخصية.
. إذا كانت المعالجة ضرورية لإقامة أي من إجراءات المطالبة بالحقوق والدعاوى القانونية أو الدفاع عنها أو تتعلق بالإجراءات القضائية.
ج. إذا كانت المعالجة ضرورية لحماية حقوق الغير وفقاً للتشريعات السارية.
د. إذا كانت المعالجة ضرورية لحماية المصلحة العامة.
4. وفي جميع الاحوال، يجب على المتحكم في حال قام برفع التقييد المنصوص عليه في هذه المادة، أن يخطر صاحب البيانات بذلك.

[←75]

) نص المادة (17) من قانون حماية البيانات الشخصية رقم (45) لسنة 2021، جاء فيها:
يحق لصاحب البيانات الاعتراض على معالجة بياناته الشخصية وإيقاف المعالجة في أي من الحالات الآتية:
. إذا كانت المعالجة لأغراض التسويق المباشر بما في ذلك التنميط ذات العلاقة بالتسويق المباشر.
. إذا كانت المعالجة لأغراض إجراء المسوح الإحصائية، إلا إذا كانت المعالجة لازمة لتحقيق المصلحة العامة.
. إذا كانت المعالجة بالمخالفة لأحكتم المادة (5) من هذا المرسوم.

[←76]

) نص المادة (18) من قانون حماية البيانات الشخصية رقم (45) لسنة 2021، جاء فيها:

. يحق لصاحب البيانات الاعتراض على القرارات التي تصدر عن المعالجة المؤتمتة وتكون لها تبعات قانونية أو تؤثر بشكل جسيم على صاحب البيانات، بما فيها التنميط.

. على الرغم مما ورد في البند (1) من هذه المادة، لا يجوز لصاحب البيانات الاعتراض على القرارات التي تصدر عن المعالجة المؤتمتة في الحالات الآتية:

. إذا كانت المعالجة المؤتمتة ضمن شروط التعاقد بين صاحب البيانات والمتحكم.

. إذا كانت المعالجة المؤتمتة ضرورية وفق تشريعات أخرى نافذة في الدولة.

ج. إذا تمت الموافقة المسبقة من صاحب البيانات على المعالجة المؤتمتة وفق الشروط المحددة في المادة (6) من هذا المرسوم بقانون.

3. يجب على المتحكم تطبيق إجراءات وتدابير مناسبة لحماية خصوصية وسرية البيانات الشخصية لصاحب البيانات في الحالات المشار إليها في البند (2) من هذه المادة، وعجم الإضرار والمساس بحقوقه.

4. يتعين على المتحكم إدخال العنصر البشري في مراجعة قرارات المعالجة المؤتمتة بناءً على طلب صاحب البيانات.

[←77]

) نص المادة (19) من قانون حماية البيانات الشخصية رقم (45) لسنة 2021، جاء فيها:
على المتحكم توفير طرق وآليات مناسبة وواضحة لتمكين صاحب البيانات من التواصل معه وطلب ممارسة أي من حقوقه المنصوص عليها في هذا المرسوم بقانون.

[←78]

) نص المادة (22) من قانون حماية البيانات الشخصية رقم (45) لسنة 2021، جاء فيها:
يجوز نقل البيانات الشخصية إلى خارج الدولة في الأحوال الآتية المعتمدة من المكتب:
. أن تكون للدولة أو الإقليم الذي سيتم نقل البيانات الشخصية إليها تشريعات خاصة بحماية البيانات الشخصية فيها، تتضمن أهم الأحكام والتدابير والضوابط والاشتراطات والقواعد الخاصة بحماية خصوصية وسرية البيانات الشخصية لصاحب البيانات، وقدرته على ممارسة حقوقه، وأحكام تتعلق بفرض التدابير المناسبة على المتحكم أو المعالج من خلال جهة رقابية أو قضائية.
. تنضم الدولة إلى الاتفاقيات الثنائية أو متعددة الأطراف المتعلقة بحماية البيانات الشخصية مع الدول التي سيتم نقل البيانات الشخصية إليها.

[←79]

) نص المادة (23) من قانون حماية البيانات الشخصية رقم (45) لسنة 2021، جاء فيها:
. استثناء مما ورد في المادة (22) من هذا المرسوم بقانون، يجوز نقل البيانات الشخصية الى خارج الدولة في الحالات التالية:
أ- في الدول التي لا يتوفر فيها قانون لحماية البيانات، يجوز للمنشآت العاملة في الدولة وفي تلك الدول أن تنقل البيانات بموجب عقد أو اتفاقية يلزم المنشأة في تلك الدول بتطبيق الاحكام والتدابير والضوابط والاشتراطات الواردة في هذا المرسوم بقانون شاملاً أحكاماً تتعلق بفرض التدابير المناسبة على المتحكم أو المعالج من خلال جهة رقابية أو قضائية معينة في تلك الدولة وتحدد في العقد.
ب - الموافقة الصريحة من صاحب البيانات على نقل بياناته الشخصية خارج الدولة بما لا يتعارض مع المصلحة العامة والامنية للدولة.
ج. إذا كان انقل ضروري لتنفيذ التزامات وإثبات الحقوق أمام الجهات القضائية أو ممارستها أو الدفاع عنها.
د. إذا كان النقل ضروري لإبرام أو تنفيذ عقد مبرم بين المتحكم وصاحب البيانات، أو بين المتحكم والغير لتحقيق مصلحة صاحب البيانات.
ه. إذا كان النقل ضروري تنفيذاً لإجراء متعلق بتعاون قضائي دولي.
و. إذا كان النقل ضروري لحماية المصلحة العامة.
2. تحدد اللائحة التنفيذية لهذا المرسوم بقانون الضوابط والاشتراطات للحالات المشار إليها في البند (1) من هذه المادة، والتي يجب أن تتوفر في حالات نقل البيانات الشخصية إلى خارج الدولة.

[←80]

) نص المادة (24) من قانون حماية البيانات الشخصية رقم (45) لسنة 2021، جاء فيها:

. لصاحب البيانات أن يتقد إلى المكتب بشكوى، إذا كان لديه ما يحمله على الاعتقاد بوقوع أي مخالفة لأحكام هذا المرسوم بقانون، او بأن المتحكم أو المعالج يقوم بمعالجة بياناته الشخصية. بالمخالفة لأحكامه وفقاً للإجراءات والقواعد التي يحددها المكتب في هذا الشأن.

. يتولى المكتب استلام الشكاوى المقدمة من صاحب البيانات وفقاً للبند (1) من هذه المادة، والتحقق منها بالتنسيق مع المتحكم والمعالج.

. للمكتب توقيع الجزاءات الإدارية المشار إليها في المادة (26) من هذا المرسوم بقانون في حال ثبوت المتحكم أو المعالج لأحكامه أو مخالفة القرارات الصادرة تنفيذاً له.

[←81]

) نص المادة (26) من قانون حماية البيانات الشخصية رقم (45) لسنة 2021، جاء فيها:
يصدر مجلس الوزراء – بناءً على اقتراح مدير عام المكتب – قراراً بتحديد الأفعال التي تشكل مخالفة لأحكام هذا المرسوم بقانون ولائحته التنفيذية، والجزاءات الإدارية التي يتم توقيعها.

[←82]

) أمجد خليل حمودة، الوسائل الحديثة لإثبات الجرائم التي ترتكب بواسطة الأجهزة الإلكترونية، مجلة الأزهر- غزة، عدد خاص بمؤتمر كلية الحقوق الخامس المحكم، المجلد 19، ص120.

[←83]

) راجع فلاك مراد، آليات الحصول على الأدلة الرقمية كوسائل إثبات في الجرائم الإلكترونية، مجلة الفكر القانوني والسياسي، العدد الخامس، تأريخ النشر 12/06/2019، ص207.

[←84]
) ميرفت محمد حبابية، مكافحة الجريمة الإلكترونية، دار اليازوري العلمية، بدون طبعة، سنة الطبعة 2022، ص 236.

[←85]

) الجريدة الرسمية العدد 737، في 10 أكتوبر 2022، وعمل به في 2 يناير 2022.

[←86]

) سلامة محمد المنصوري، تطبيق مبدأ الاقتناع القضائي على الدليل الإلكتروني، أطروحة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام، جامعة الإمارات العربية المتحدة، 2018.

[←87]

) حسن الهداوي، تنازع القوانين المبادئ العامة والحلول الوضعية في القانون الأردني دراسة مقارنة، مكتبة الثقافة للنشر والتوزيع، الأردن – عمان، الطبعة الثانية، 1997، ص36، وما بعدها.

[←88]

) حسن الهداوي، مرجع سابق، ص49.

[←89]

) نص المادة (69) من حيث سريان القانون "مع عدم الإخلال بأحكام قانون العقوبات المشار إليه، تسري أحكام هذا المرسوم بقانون على كل من ارتكب إحدى الجرائم الواردة به خارج الدولة في الأحوال الآتية:

1 .إذا كان محلها نظام معلوماتي إلكتروني أو شبكة معلوماتية أو موقع إلكتروني أو وسيلة تقنية معلومات خاصة أو عائدة لإحدى مؤسسات الدولة.

2 .إذا تم الإعداد للجريمة أو التخطيط أو التوجيه أو الإشراف عليها أو تمويلها في الدولة.

3 .إذا كان من شأن الجريمة المساس بأمن الدولة في الداخل أو الخارج أو بأي من مصالحها أو إلحاق الضرر بأي من مواطنيها أو المقيمين فيها.

4 .إذا وجد مرتكب الجريمة في الدولة، بعد ارتكابها ولم يتم تسليمه".

[←90]
) قانون رقم 36 لسنة 2022، الجريدة الرسمية العدد 737 (ملحق) 10 أكتوبر 2022، ويطلق عليه أينما ورد في هذا البحث بقانون الجرائم والعقوبات الإماراتي.

[←91]

) الفصل الأول من قانون الجرائم والعقوبات الإماراتي، سريان القانون من حيث الزمان المواد من (13) إلى (16):

المادة (13)

عاقب على الجريمة طبقا للقانون النافذ وقت ارتكابها، والعبرة في تحديده بالوقت الذي، تمت فيه أفعال تنفيذها دون النظر إلى وقت تحقق نتيجتها.

المادة (14)

إذا صدر بعد وقوع الجريمة وقبل الفصل فيها بحكم بات قانون أصلح للمتهم فهو الذي يطبق دون غيره. وإذا صدر بعد صيرورة الحكم باتا قانون يجعل الفعل أو الترك الذي حكم على المتهم من أجله غير معاقب عليه يوقف تنفيذ الحكم وتنتهي آثاره الجزائية ما لم ينص القانون الجديد على خلاف ذلك. فإذا كان القانون الجديد مخففاً للعقوبة فقط، فإنه يجوز للمحكمة التي أصدرت الحكم البات – بناء على طلب النيابة العامة أو المحكوم عليه – إعادة النظر في العقوبة المحكوم بها في ضوء أحكام القانون الجديد.

المادة (15)

استثناء من أحكام المادة السابقة إذا صدر قانون بتجريم فعل أو ترك أو بتشديد العقوبة المقررة له وكان ذلك مؤقتا بفترة محددة أو كانت قد دعت لصدوره ظروف استثنائية طارئة فإن انتهاء الفترة المحددة لسريانه أو زوال الظروف الاستثنائية الطارئة لا يمنع من إقامة الدعوى الجزائية على ما وقع من جرائم خلالها ولا يحول دون تنفيذ العقوبة التي يكون قد حكم بها على أساس ذلك القانون.

المادة (16)

يسري القانون الجديد على ما وقع قبل نفاذه من الجرائم المستمرة أو المتتابعة أو جرائم العادة التي يستمر على ارتكابها في ظله. وإذا عدل القانون الجديد الأحكام الخاصة بالعود أو تعدد الجرائم أو العقوبات فإنه يسري على كل جريمة تخضع المتهم لأحكام التعدد أو يصبح بمقتضاها في حالة عود ولو كانت الجرائم الأخرى قد وقعت قبل نفاذه.

[←92]
) الفصل الثاني من قانون الجرائم والعقوبات الإماراتي، سريان القانون من حيث المكان والأشخاص المواد من (17) إلى (26):

المادة (17)

تسري أحكام هذا القانون على كل من يرتكب جريمة في إقليم الدولة، ويشمل إقليم الدولة أراضيها وكل مكان يخضع لسيادتها بما في ذلك المياه الإقليمية والفضاء الجوي الذي يعلوها.

وتعتبر الجريمة مرتكبة في إقليم الدولة إذا وقع فيها فعل من الأفعال المكونة لها أو إذا تحققت فيها نتيجتها أو كان يراد أن تتحقق فيها.

المادة (18)

تسري أحكام هذا القانون على الجرائم التي ترتكب على ظهر السفن والطائرات الحربية التي تحمل علم الدولة أينما وجدت. وينطبق الحكم المتقدم على السفن والطائرات غير الحربية التي تملكها الدولة أو تديرها لأغراض غير تجارية وكذلك السفن والطائرات التجارية التي تحمل علم الدولة.

المادة (19)

مع عدم الإخلال بالاتفاقيات والمعاهدات التي تكون الدولة طرفاً فيها، لا تسري أحكام هذا القانون على الجرائم التي ترتكب على ظهر السفن الأجنبية في إحدى موانئ الدولة أو في بحرها الإقليمي إلا في إحدى الحالات الآتية:

1. إذا امتدت آثار الجريمة إلى الدولة.
2. إذا كانت الجريمة بطبيعتها تمس أمن الدولة أو تعكر السلم فيها أو تخل بالآداب العامة أو حسن النظام في موانيها أو بحرها الإقليمي.
3. إذا طلب ربان السفينة أو قنصل الدولة التي تحمل علمها المعونة من السلطات المحلية.
4. إذا كان الجاني أو المجني عليه من مواطني الدولة.
5. إذا كانت السفينة تحمل مواد أو أشياء محظور تداولها أو حيازتها أو الاتجار فيها دولياً. وبالنسبة إلى الجرائم التي ترتكب على ظهر الطائرات الأجنبية أو إقليم الدولة الجوي فلا تسري عليها أحكام هذا القانون إلا إذا حطت الطائرة في إحدى مطاراتها بعد ارتكاب الجريمة، أو كانت الجريمة بطبيعتها تعكر السلم في الدولة أو تخل بنظامها العام أو إذا شكلت الجريمة مخالفة للوائح والأحكام المنظمة لحركة الملاحة في الدولة، أو طلب ربان الطائرة المعونة من السلطات المحلية أو كان الجاني أو المجني عليه من مواطني الدولة.

المادة (20)

يسري هذا القانون على كل من ارتكب فعلاً خارج الدولة يجعله فاعلاً أو شريكاً في جريمة وقعت كلها أو بعضها داخل الدولة.

المادة (21)

يسري هذا القانون على كل من ارتكب فعلاً خارج الدولة يجعله فاعلاً أو شريكاً في جريمة من الجرائم الآتية:

1. جريمة ماسة بأمن الدولة الخارجي أو الداخلي أو ضد نظامها الدستوري أو سنداتها المالية المأذون بإصدارها قانوناً أو طوابعها أو جريمة تزوير أو تقليد محرراتها أو أختامها الرسمية.
2. جريمة تزوير أو تقليد أو تزييف عملة الدولة أو ترويجها أو حيازتها بقصد ترويجها سواء تمت تلك الأفعال داخل الدولة أو خارجها.
3. جريمة تزوير أو تقليد أو تزييف عملة ورقية أو مسكوكات معدنية متداولة قانوناً في الدولة أو ترويج تلك العملات والمسكوكات فيها أو حيازتها بقصد ترويجها.
4. جريمة القتل العمد التي تقع على أحد مواطني الدولة.

المادة (22)

يسري هذا القانون على من وجد في الدولة بعد أن ارتكب في الخارج بوصفه فاعلاً أو شريكاً جريمة تخريب أو تعطيل وسائل الاتصال الدولية أو جرائم الاتجار في المخدرات أو النساء أو الصغار أو الرقيق أو جرائم القرصنة والإرهاب الدولي أو جرائم غسل الأموال.

المادة (23) كل مواطن ارتكب وهو خارج الدولة فعلا يعد جريمة بمقتضى أحكام هذا القانون سواء بوصفه فاعلاً أو شريكاً يعاقب طبقاً لأحكامه إذا عاد إلى البلاد وكان ذلك الفعل معاقباً عليه بمقتضى قانون البلد الذي وقع فيه. ويسري هذا الحكم على من يكتسب جنسية الدولة بعد ارتكاب الفعل، وفي تطبيق هذه المادة يعتبر من لا جنسية له في حكم المواطن إذا كان مقيما في الدولة إقامة معتادة.

المادة (24) لا تقام الدعوى الجزائية على مرتكب جريمة في الخارج إلا من النائب العام، ولا يجوز إقامتها على من يثبت أن المحاكم الأجنبية أصدرت حكماً نهائياً ببراءته أو إدانته واستوفى العقوبة أو كانت الدعوى الجزائية أو العقوبة المحكوم بها سقطت عنه قانوناً أو حفظت السلطات المختصة بتلك الدولة التحقيق. ويرجع في تقدير نهائية الحكم وسقوط الدعوى أو العقوبة أو حفظ التحقيق إلى قانون البلد الذي صدر فيه الحكم. فإذا كانت العقوبة المحكوم بها لم تنفذ كاملة وجب استيفاء مدتها، أما إذا كان الحكم بالبراءة صادراً في جريمة مما نص عليه في المادتين (21) و (22) وكان مبنياً على أن قانون ذلك البلد لا يعاقب عليها جازت إقامة الدعوى الجزائية عليه أمام محاكم الدولة. وتكون المحكمة الاتحادية المختصة الكائنة بمقر عاصمة الاتحاد هي المختصة بنظر الدعوى.

المادة (25) تحسب للمحكوم عليه عند تنفيذ العقوبة المدة التي قضاها في الحجز أو الحبس الاحتياطي أو المراقبة الإلكترونية أو تنفيذ العقوبة في الخارج عن الجريمة التي حكم عليه من أجلها.

المادة (26) لا يسري هذا القانون على الأشخاص المتمتعين بحصانة مقررة بمقتضى الاتفاقيات الدولية أو القانون الدولي أو القانون الداخلي، وذلك في إقليم دولة الإمارات العربية المتحدة.