Journal Of the Iraqia University (75-4) March (2026)

ISSN(Print): 1813-4521 OnLine ISSN:2663-7502
Journal Of the Iraqia University
available online at
https://iasj.rdd.edu.iq/journals/journal/view/247

التطورات الحديثة في مفهوم المسؤولية الجنائية في الجرائم الإلكترونية

م.د. انمار عبد الوهاب حمدان

الجامعة العراقية / كلية الهندسة / الوحدة القانونية

Recent Developments in the Concept of Criminal Liability in Cybercrimes

anmar.a.hamdan@aliraqia.edu.iq

الملخص:

ان هذا البحث يتناول دراسة المسؤولية الجنائية في الجرائم الإلكترونية باعتبارها من أبرز التحديات القانونية في العصر الرقمي فقد تزايدت الجرائم الالكترونية في ظل التطور التكنولوجي مما جعل المشرعين والقضاء تطوير آليات قانونية وتقنية لإثبات هذه الجرائم وتسهل الوصول لمرتكبيها ومعاقبتهم.كما قد خلص هذا البحث الى ان المسؤولية الجنائية تتحقق عند توافر اركان الجريمة (الركن المادي، الركن المعنوي) وأن الأدلة الرقمية كسجلات الدخول والبريد الإلكتروني اصبحت اداة رئيسية في اثبات الجريمة.كما وقد بين هذا البحث التطور الحاصل في مجال التشريعات الوطنية والدولية مثل تحديث قوانين الجرائم الالكترونية في عدد من الدول وتطوير التعاون الدولي عبر اتفاقية بودابست وتوجيه NIS2 الأوروبي، كما وقد أكد هذا البحث على أهمية التكامل بين التشريع والتقنية والتعاون الدولي لمواجهة الجرائم الالكترونية والحد منها.وفي ختام البحث أوصى بضرورة تحديثات التشريعات بشكل مستمر وتعزيز الوعي القانوني والتكنولوجي للافراد والكيانات إضافة الى ضرورة تطوير آليات الاثبات الرقمي وذلك تزامناً مع تطور أساليب الجريمة الالكترونية.الكلمات المفتاحية: الجرائم الالكترونية – المسؤولية الجنائية – التشريعات الجنائية – وسائل الاثبات الرقمي.

Abstract:

This research examines criminal liability in cybercrimes, as one of the most prominent legal challenges of the digital age. Cybercrimes have increased in light of technological advancements, prompting legislators and the judiciary to develop legal and technical mechanisms to prove these crimes and facilitate the identification and punishment of perpetrators.This research also concluded that criminal liability is established when the elements of the crime are present (the material element, the moral element) and that digital evidence such as login records and email have become a primary tool in proving the crime .This research also demonstrated the developments in national and international legislation, such as updating cybercrime laws in a number of countries and developing international cooperation through the Budapest Convention and the European NIS2 Directive. This research also emphasized the importance of integrating legislation, technology, and international cooperation to combat and reduce cybercrime.At the conclusion of the study, the researcher recommended the need to continuously update legislation, enhance legal and technological awareness among individuals and entities, and develop digital proof mechanisms to keep pace with the development of cybercrime methods .Keywords: Cybercrimes - Criminal Liability - Criminal Legislation - Digital Evidence.

المقدمة

مع تطور الجرائم الالكترونية تزامناً بتطور العصر التكنولوجي الامر الذي أدى الى تطور المسؤولية الجنائية لم تعد المسؤولية مقتصرة على الأفعال التقليدية كالسرقة او الاحتيال المادي بل شملت جرائم جديدة كاختراق الأنظمة وسرقة البيانات، ونشر الفيروسات، والاحتيال الإلكتروني.وكلما تطورت التقنيات جعلت من الصعب تحديد المجرم الحقيقي بسبب إمكانية إخفاء الهوية باستخدام VPN او التشفير او الحسابات الوهمية وهذا بدوره دفع المشرع الى إعادة صياغة قواعد المسؤولية بحيث تشمل حتى المساعدة او المشاركة عن بعد.

اولاً: أهمية البحث:-

ان هذا البحث يطرح التطورات الحاصلة في المسؤولية الجنائية وذلك نظراً لتطور الفضاء السيبراني مما أدى الى ظهور تطور ملحوظ في هذه الجرائم كإخفاء هوية الجاني عبر استخدام تقنيات الـ VPNs كما لم يقتصر ارتكاب هذه الجرائم بالنسبة للأفراد فقط بل امتدت لتشمل الشركات والمؤسسات والهيئات التي أصبحت متواطئة مع هؤلاء المجرمين لتعود لها بمنافع مالية وتجارية، الأمر الذي أدى الى ضرورة تدخل المشرع ووضع حد لهذه الظاهرة من خلال فرض قانون مكافحة الجرائم المعلوماتية او عن طريق عقد اتفاقيات دولية للحصول على التعاون القضائي بين الدول وذلك بسبب ان المجرم المعلوماتي الذي يخترق نظم معلومات داخل الفضاء السيبراني قد يكون في بلد آخر، لذا لابد من وجود تعاون قضائي دولي لردع هؤلاء المجرمين.

ثانياً: إشكالية البحث:-

مع تطور الجريمة الرقمية (الالكترونية) أصبح لابد من تدخل المشرع واتخاذ الدول كافة الإجراءات اللازمة لإعادة التوازن في العالم الرقمي، وبذلك ذهبت الدول لعقد اتفاقيات دولية بمحاولة لإعادة الأمور الى نصابها الصحيح ومع وضع رقابة قضائية وقوانين لازمة لصد هجمات المجرم المعلوماتي تظهر الإشكالية في البحث عن التوازن الرقمي:

-ما هو مفهوم الجرائم الالكترونية؟

-كيف تطورت التشريعات الجنائية الرقمية؟

-هل تطورت التشريعات تزامناً مع تطور أساليب الجريمة الالكترونية؟

-ما هي المسؤولية شالجنائية للفرد المرتكب للجريمة الإلكترونية؟

-هل المسؤولية الجنائية للفرد الطبيعي كمسؤولية الفرد المعنوي (الشركات، المؤسسات، الهيئات)؟

ثالثاً: منهجية البحث:-

في هذا البحث تم تحليل المسؤولية الجنائية في الجرائم الالكترونية للافراد والشركات إضافة الى المقارنة بين التشريعات القانونية التي وضعتها الدول لمكافحة الجرائم الالكترونية حيث تمت المقارنة بين الاتفاقيات الدولية كاتفاقية بودابست، وتوجيه NIS2 للاتحاد الأوروبي، وكذلك النظم القانونية للأمارات والسعودية ومصر والعراق والأردن.

رابعاً هيكلية البحث:-

تم تقسيم هذا البحث الى مطلبين حيث تناولنا في الأول منه: مفهوم الجرائم الالكترونية، وفي المطلب الثاني: المسؤولية الجنائية للأفراد في الجرائم الالكترونية.

المطلب الأول مفهوم الجرائم الالكترونية

يقصد بالجرائم الالكترونية هي تلك الأفعال التي ترتكب باستخدام الحاسوب او الشبكات او أنظمة المعلومات بهدف الاعتداء على بيانات او أنظمة وشبكات الغير وقد عرفها قانون الجرائم الالكترونية الأردني لعام ٢٠٢٣ بأنها: ((الأفعال التي تتم باستخدام نظام المعلومات او الشبكة المعلوماتية او أي وسيلة من وسائل تكنولوجيا المعلومات لارتكاب جريمة او المساهمة في ارتكابها))[١].ونظراً الى ان هذه الجرائم تتميز بطابع غير ملموس فهي ترتكب وسط فضاء وهمي وتكون ذات طبيعة عابرة للحدود أي يمكن ان تقع الجريمة في جولة ويكون الجاني او الضحية في دولة أخرى كما وانها ذات طابع سريع بارتكابها وبنفس الوقت ذات مدى واسع أي قد تمتد هذه الجريمة لتصيب مئات وآلاف الأشخاص حول العالم في لحظة واحدة[٢] الامر الذي دعى ضرورة وضع تشريعات تتوافق مع تطور هذه الجرائم التي تتطور بتطور الوسائل التكنولوجية، وكلما تطورت تلك الوسائل ظهرت مشكلة امام القضاء وهي اثبات الجريمة لذا لابد من توافر وسائل حديثة للاثبات، أي ان هذه الجرائم بتطورها لم تؤثر على التشريعات التي تطرأ على مرتكبيها بل امتدت لتشمل تطور واضح في وسائل الاثبات.ولهذا سنقوم بتقسيم هذا المطلب إلى فرعين هما:الفرع الأول: تطور التشريعات الجنائية الالكترونية.الفرع الثاني: تطور وسائل الاثبات الرقمية.

الفرع الأول تطور التشريعات الجنائية الالكترونية

مع توسع استخدام الانترنت في الحياة اليومية ظهرت أشكال جديدة من الأنشطة الإجرامية كالتخريب الرقمي، سرقة البيانات، الاحتيال الالكتروني والتشهير عبر وسائل التواصل هذه الظواهر استدعت تدخل المشرع ليس فقط على الصعيد الوطني بل أيضاً عبر أطر تشريعية دولية وإقليمية حديثة بهدف ضبط هذه الجرائم وتعزيز التعاون القضائي وضمان حماية الحقوق أثناء التحقيق، كما واكد التوجه الأوروبي رقم ٤٦/٩٥ الصادر في ٢٤ أكتوبر ١٩٩٥[٣]على ضرورة حماية الحقوق الأساسية وحريات الأشخاص الطبيعيين وبصفة خاصة الحق في حرية الحياة الخاصة في مجال

معالجة البيانات الشخصية (م ١/١/)[٤]وبهذا اقرت اتفاقية بودابست لمكافحة الجرائم المعلوماتية في عام ٢٠٠١ لتكون أول إطار دولي شامل يتناول تجريم الأفعال الإلكترونية ووضع آليات للتعاون القضائي الإلكتروني[٥]، كما وقد اعتمدت جامعة الدول العربية في عام ٢٠١٠ اتفاقية لمكافحة جرائم تقنية المعلومات وبدأ حيز العمل بها في عام ٢٠١٢ والتي تهدف الى توحيد المفاهيم القانونية العربية حول الجرائم الإلكترونية وتنظيم التعاون القضائي وتبادل الأدلة بين الدول الأعضاء[٦].كما وأصدر الاتحاد الأوروبي توجيه ٤٠/٢٠١٣ لتجريم الهجمات على نظم المعلومات " كالاختراق وتعطيل البيانات" ثم قدم الاتحاد توجيهات NIS لسنة٢٠١٦ و2NIS لسنة ٢٠٢٢ والتي شملت تعزيز أمن الشبكات وفرض حماية البيانات وجعلت الإبلاغ عن الحالات الاجرامية امراً الزامياً للجهات الحيوية[٧]، وفي سنة٢٠٢١ أصدرت هيئة مجلس أوروبا البروتوكول الإضافي الثاني والذي عزز التعاون الدولي في تبادل الأدلة الإلكترونية عن طريق تمكين التواصل المباشر مع مزودي الخدمات والتسجيلات وتسهيل التعاون في الحالات الطارئة مع ضمان حماية الحقوق الإنسانية وخصوصية البيانات ليأتي بعد ذلك في ٢٤ ديسمبر من سنة ٢٠٢٤ حيث اعتمدت الجمعية العامة للأمم المتحدة اتفاقية دولية جديدة لمكافحة الجرائم الإلكترونية والتي تهدف إلى توسيع نطاق التعاون القضائي ورفع قدرات الدول ومنها الدول النامية في مكافحة الجرائم الرقمية حيث تعد هذه الاتفاقية أول معاهدة دولية شاملة من نوعها ضمن ملحقات النظام القضائي الدولي[٨]، والتي رحبت بها منظمة الإنتربول باعتبارها نقطة انعطاف تاريخية في مجابهة الجرائم السيبرانية[٩].اما في مصر حيث صدر قانون يعد من اهم التشريعات العربية الحديثة وهو القانون رقم ١٧٥ لسنة ٢٠١٨ اذ جرم جرائم الاختراق وتعطيل المواقع والمعالجة الرقمية للمحتوى وعزّز حجية الأدلة الإلكترونية مع ضرورة مزودي الخدمة بالتعاون القضائي[١٠]، اما في الامارات فقد جاء المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ وهذا يوفر اطار موسع لتجريم نشر الشائعات والاختراق والتعطيل المتعمد للأنظمة ووسع العقوبات المالية والسالبة للحرية وقد بدأ حيز التنفيذ في سنة ٢٠٢٢[١١].ومن مقارنة تشريعية دقيقة نلاحظ تطوراً افي الأطر القانونيّة حيث بدأ بالاساسيات العامة في بودابست سنة ٢٠٠١ ثم تطور عبر البروتوكول الإضافي في سنة ٢٠١٠ لتوسيع الأدوات التعاونية، ثم شهد تطوراً هيكلياً أوسع مع اتفاقية الأمم المتحدة لسنة ٢٠٢٤ لتشمل التعاون الوقائي وقد مكنت الاتفاقيات الإقليمية مثل الاتحاد الأوروبي والجامعات العربية من مواءمة القوانين بين الدول، واخيراً تجلت الاستجابة الوطنية بمرونة لتحديات الامن الرقمي واحتياجات العدالة الجنائية في تشريعات محدثة كمصر والامارات.

الفرع الثاني تطور وسائل الاثبات الرقمية

ومع توسع الجرائم التي تتجاوز الحدود الوطنية تنامى الطلب على أطار قانوني دولي يضمن مساءلة الأفراد ويمنع الإفلات من العقاب، وهذا البعد الدولي أصبح أساسي لتفعيل العدالة الجنائية العالمية من خلال مؤسسات دولية واتفاقيات وتعاون بين الدول للتطورات الحديثة في وسائل الإثبات حيث شهدت السنوات الأخيرة ٢٠٢٠–٢٠٢٥ تحولات عميقة في وسائل الإثبات مدفوعة بالثورة الرقمية والتكنولوجية التي أثرت في كافة المجالات ولاسيما المجال القانوني والقضائي.فقد أصبحت الأدلة الرقمية تحتل موقعاً متقدماً في قاعات المحاكم سواء في القضايا الجنائية او المدنية او التجارية الامر الذي فرض على المشرع والقضاء ضرورة تحديث الأطر القانونية لمواكبة هذا التطور[١٢].ولقد ارتبط هذا التطور بزيادة استخدام التقنيات الحديثة وثيق وتحليل الأدلة والى جانب ذلك ومع تطور الجريمة الالكترونية ظهرت ابعاد جديدة للأدلة الرقمية والتي تتمثل باستخدام وسائل المحاكاة الافتراضية (VR) وتقنيات ثلاثية الأبعاد D3Simulation لعرض مسارح الجرائم أمام المحاكم كما حدث في إحدى قضايا المحكمة الجنائية الدولية عام ٢٠٢٤ حيث مكنت هذه الوسائل القضاة من رؤية مسرح الجريمة الافتراضي بشكل حي وتفاعلي[١٣].وان هذا التطور جعل بعض الدول تشهد تعديلات في قوانين الاثبات فقد ألغت الهند في ٢٠٢٣ قانون الإثبات القديم رقم ١٨٧٢ وأقرت قانون Bharatiya Sakshya Adhiniyam 2023 الذي أعطى حجية أوسع للأدلة الإلكترونية[١٤]، وبالمثل أقر البرلمان الأوزبكي في سنة ٢٠٢٤ قانون خاص بالأدلة الرقمية يعترف رسمياً بالملفات الإلكترونية والمنشورات عبر الإنترنت كوسائل إثبات[١٥].كما ان النقاش الأكاديمي في الفترة بين ٢٠٢٠–٢٠٢٥ ركز على التوازن بين الخصوصية والعدالة في جمع الأدلة حيث قدم باحثون في سنة ٢٠٢٥ نموذج SPADA لتحليل التهديدات المرتبطة بالتحقيقات الرقمية وحيث تعد إطار علمي يضمن احترام الخصوصية أثناء جمع الأدلة الرقمية عبر الحدود[١٦].ومع توسع التحقيقات الجنائية في استخدام بصمات الأجهزة والشبكات لتحديد مصدر الجرائم الرقمية بما في ذلك تحليل أنماط الكتابة Keystroke Dynamics لتحديد هوية المستخدم[١٧]، لم يقتصر الامر على تحليل أنماط الكتابة بل امتد لاستخدام تقنية "Blockchain" لتوثيق المعاملات الرقمية والعقود الذكية في بعض المحاكم الأوروبية والاسيوية لسنة ٢٠٢٢ واعتبرت هذه التقنية سجل موثوق على عدم التلاعب بالبيانات[١٨].ولجمع المعلومات لغرض اثبات الجريمة الالكترونية جاء في القانون الفرنسي المسمى "نظم المعالجة الرقمية والحرية" informatique et Liberté الصادر في ٦ يناير من عام ١٩٧٨ والذي ضمنت مواده بقانون العقوبات الفرنسي حيث يتطلب عند معالجة آلية بيانات اسمية شخصية من قبل اشخاص القانون الخاص اخطار اللجنة القومية

للمعلوماتية والحريات (CNIL) بالإضافة الى الحصول على تصريح سابق اذا كان من يقوم بجمع المعلومات هو احد اشخاص القانون العام او احد اشخاص القانون الخاص العاملين لحساب الدولة[١٩].كما تناول الفقه في الولايات المتحدة الامريكية المشاكل العملية المتعلقة بجرائم الانترنت والإجراءات الجنائية المتعلقة بها واستند في ذلك لاحكام القضاء الأمريكي التي تتطلب مثلاً ان يكون التفتيش لضبط الأشياء الخاصة بالتعبير عن الرأي وفقاً للتعديل الأول للدستور الأمريكي ومنها أجهزة الكمبيوتر[٢٠]، وقد نص المشرع الأمريكي على قانون حماية الخصوصية، وقانون حماية الاتصالات الالكترونية لحماية البيانات الشخصية وبيان الإجراءات المتعلقة بالقبض والتفتيش كل ذلك لحماية الناشرين فنص على العقاب على التنصت او الشروع في التنصت على الاتصالات الالكترونية بالحبس او الغرامة، كما عاقب على فضها واستخدامها نظراً لوجود بيانات تتعلق بمثل هذه الاتصالات على الأجهزة التي تم ضبطها[٢١]

المطلب الثاني المسؤولية الجنائية للأشخاص في الجرائم الالكترونية

ان المسؤولية الجنائية للأفراد في الجرائم الإلكترونية تعني تحمل الشخص العاقل مسؤولية افعاله الجرمية بغض النظر عما اذا كانت اعتداء على بيانات الآخرين او احتيال مالي عبر الإنترنت او ابتزاز الكتروني او اختراق الأنظمة المعلوماتية، وتختلف هذه المسؤولية عن المسؤولية المدنية اذ ترتكز على العقوبة وليس التعويض المالي فقط ، وعليه سنقوم بتقسيم هذا المطلب إلى فرعين وهما كالآتي: الفرع الأول: المسؤولية الجنائية للفاعل الفردي في الجرائم الالكترونية الفرع الثاني: المسؤولية الجنائية للافراد المعنويين في الجرائم الالكتروني.

الفرع الأول المسؤولية الجنائية للفاعل الفردي في الجرائم الالكترونية

كما ذكرنا مسبقاً أن المسؤولية الجنائية تعني تحمل الفرد الطبيعي المسؤولية القانونية عن افعاله الإجرامية التي يرتكبها بالوسائل الرقمية وتتمثل افعاله بالاختراق الالكتروني للأنظمة او الاحتيال المالي عبر الانترنت او الابتزاز الإلكتروني والتشهير ونشر معلومات كاذبة[٢٢].وأن المسؤولية الجنائية للفاعل الفردي تنطوي على ركنين:

أولاً: الركن المادي:يتمثل بالفعل الجرمي الذي قام به الفرد مباشرة كاختراق الأنظمة ووالشبكات الرقمية، نشر فيروسات او برامج خبيثة، او سرقة البيانات والأموال الرقمية.كما وقد يشترط في الركن المادي أن يكون الفعل موثقاً رقمياً كسجلات الدخول او العثور على عنوان IP او قد يعثر على رسائل البريد الالكتروني[٢٣].

ثانياً: الركن المعنوي:يقصد بالركن المعنوي توافر القصد الجنائي أي نية الفاعل في ارتكاب الجريمة أي بمعنى ان يكون على دراية بأن فعله يعتبر جريمة او يسعى لتحقيق مصالح غير مشروعة[٢٤].وفي الجرائم الإلكترونية يعتبر القصد الجنائي جزءاً اساسياً لإثبات المسؤولية خصوصاً في جرائم الاحتيال أو الابتزاز .ومن اشكال الجرائم التي قد يرتكبها الفرد ويتحمل مسؤوليتها:

أولاً: الجرائم المالية والرقمية:تعرف على انها الأفعال الاجرامية التي يقوم بها الفرد بهدف الحصول على منفعة مالية بوسائل رقمية مثل الاحتيال البنكي عبر رسائل البريد الالكتروني او سرقة او اختراق محافظ العملات الرقمية المشفرة، او قد يكون الاحتيال عبر منصات التجارة الإلكترونية او الدفع الإلكتروني.ويتم ذلك عبر الروابط المزيفة، او برمجيات خبيثة Malware مثل Trojans وRansomware، او عن طريق سرقة بيانات الدخول وكلمات المرور Credential Theft.ويتحمل الفاعل المسؤولية مباشرة عن كل فعل قام به بنفسه بين تلك الأفعال التي ذكرت والتي تتراوح عقوبتها بين السجن والغرامات، او قد تكون مشددة إذا ارتكب الفعل عبر شبكات متعددة او اذا كان الفعل مؤثراً على عدد كبير من الضحايا[٢٥].

ثانياً: اختراق الأنظمة والشبكات (الوصول غير المشروع):-

هذا النوع يشمل الوصول إلى أنظمة أو قواعد بيانات فردية او مؤسساتية، بغرض السرقة، التخريب، أو التجسس والتشهير، كمن قد يخترق اختراق أنظمة البنوك أو المؤسسات المالية لغرض السرقة، او كمن يخترق البريد الإلكتروني او خوادم الشركات للحصول على معلومات سرية للتجسس على أنظمة حكومية او صناعية او حتى شخصية عبر الانترنت[٢٦]، ويتم ذلك عبر استغلال الثغرات البرمجية او استخدام أدوات مثل Keyloggers لتسجيل بيانات الدخول، الشبكات الافتراضية الخاصة VPN لإخفاء الهوية.ويحاسب الفرد مباشرة عند ارتكابه هكذا نوع من الجرائم بغض النظر عن هدفه فيما لوكان سرقة او تخريب او تجسس، عندها يكون عقوبته الحبس مدة لا تزيد على سنة او غرامة قدرها لا يزيد عن ٥٠٠ ألف ريال سعودي وفق المادة الثالثة من نظام مكافحة الجرائم المعلوماتية[٢٧].اما في العراق فليس هنالك نص صريح وواضح فيما يخص الجرائم الرقمية او الالكترونية بل يحاسب الفرد لهذه الجرائم بحسب القصد الجنائي الذي يخرج من الفاعل، كأن يكون الاختراق خارجاً عن نية التهديد او استغلال المعلومات او التلاعب فيعاقب وفق المادة ٣٦٩ من قانون العقوبات العراقي بالسجن لمدة اقصاها اربع سنوات (وثمانية عشر سنة اذا اذا كان مرتكب الجريمة دون سن الثامنة عشرة عشر عاماً) على كل من اعتدى على آخر بالقوة او هدده او تلاعب به او انتهك عرضه بأية طريقة كانت،

ذكراً كان او انثى، او بدا مثل هذا الانتهاك[٢٨].وبالمثل، تعاقب المادة ٣٩٦ من قانون العقوبات بالسجن لمدة أقصاها سبع سنوات كل من اعتدى جنسياً على رجل أو امرأة أو شرع في ذلك دون رضاهما، باستخدام القوة أو الخداع أو غيرهما من الوسائل، أما الجرائم المرتكبة ضد المجني عليهم دون سن الثامنة، فتعاقب بالسجن مدة لا تتجاوز عشر سنوات[٢٩].

ثالثاً: الجرائم ضد الأفراد عبر الإنترنت:هي الجرائم التي تستهدف افراد معنين بشكل مباشر عبر الوسائل الرقمية وتشمل ابتزاز هذا الفرد عبر نشر معلومات شخصية او صور حساسة، والتهديد بنشر محتوى مضلل يضر بسمعة الضحية ويكون ذلك عبر منصات التواصل الاجتماعي او الرسائل النصية والمكالمات عبر الانترنت او عن طريق أدوات لنشر المحتوى بسرعة مثل برامج البوت او الصفحات المزيفة[٣٠]

رابعاً: الجرائم المتعلقة بالملكية الفكرية الرقمية:هي الجرائم التي ينتهك فيها الفرد الحقوق الملكية الفكرية للأفراد او المؤسسات عبر الوسائل الالكترونية مثل سرقة البرمجيات، او الموسيقى، او الكتب الرقمية، ويكون عن طريق تحميل وبيع برامج كمبيوتر مقرصنة، او نشر محتوى محمي بحقوق الطبع والنشر دون إذن والتلاعب بالترخيص الرقمي للبرمجيات ويتم ذلك عن طريق مواقع التورنت او منصات تبادل الملفات غير القانونية او أدوات فك التشفير والتحايل على حقوق النسخ الرقمية.يعاقب الفرد الذي يرتكب هكذا نوع من الجرائم وفق المادة الرابعة من نظام مكافحة الجرائم المعلوماتية بالسجن مدة لا تزيد على ثلاث سنوات، او الغرامة بمقدار لا يتجاوز مليوني ريال سعودي وقد يحكم القاضي بإحدى هاتين العقوبتين او كلتاهما بحسب طبيعة الجريمة والادلة المقدمة[٣١].اما في العراق فيعاقب الفرد بموجب المادة ٤٥ من قانون حقوق الطبع والنشر[٣٢]، وتشمل التدابير القانونية المتاحة لصاحب حقوق الطبع والنشر بموجب المادة ٤٥ ما يلي:

١- أوامر قضائية تأمر المخالف بالتوقف عن الأنشطة المخالفة

٢- مصادرة الأصل والنسخ والمواد المستخدمة في تصنيع النسخ المخالفة

٣- مصادرة عائدات المخالف.

الفرع الثاني المسؤولية الجنائية للكيان في الجرائم الالكترونية

ان المقصود بالمسؤولية الجنائية للكيان هو مسؤولية الشركات والمؤسسات والهيئات القانونية في الجرائم الإلكترونية أي تتحمل المسؤولية الجنائية للافعال المرتكبة باسمها او لصالحها سواء قام بها أحد الموظفين او الإداريين او ممثل رسمي، والغرض منه هو منع منع استغلال الهيئات القانونية للتغطية على الجرائم الإلكترونية مثل الاحتيال الرقمي والابتزاز الإلكتروني واختراق البيانات او خرق الخصوصية، وتكون المسؤولية تكميلية للمسؤولية الفردية داخل الكيان، أي قد يحاسب الموظف او الموظف والكيان معاً[٣٣].والمسؤولية الجنائية للكيان تكون قائمة على ركنين رئيسيين وهما:

اولاً: الركن المادي:ان الركن المادي يشمل الفعل الإجرامي المرتكب باسم الشخص المعنوي او لصالحه كنشر برمجيات خبيثة باسم الشركة او استخدام قاعدة بيانات العملاء لأغراض غير قانونية واختراق أنظمة طرف ثالث لتحقيق منفعة مالية للشركة[٣٤].وحتى يعتبر هذا الفعل مجرم يجب إثبات ان الفعل قد تم من خلال ممثل قانوني او موظف داخل الكيان وان الاخير حقق منفعة مباشرة او غير مباشرة من الفعل[٣٥].

ثانياً: الركن المعنوي:-ان المقصود بالركن المعنوي هو توفر القصد الجنائي للكيان او السياسة المؤسسية التي تؤدي إلى ارتكاب الجريمة وهذا ممكن ملاحظته في القرارات الإدارية او التعليمات الصادرة عن الإدارة العليا، او عند عدم اتخاذ إجراءات احترازية لمنع الانتهاك الرقمي[٣٦].وان الركن المعنوي يكون متوافراً حتى لو لم يكن لدى الموظف علم كامل بالعواقب القانونية طالما أن الكيان استفاد من الفعل[٣٧].

وكما وان المسؤولية الجنائية للكيان تتحدد وفق شكل الجريمة المرتكبة وكالآتي:

اولاً: الجرائم المالية الرقمية المؤسسية:هي الجرائم التي يرتكبها الكيان بهدف الحصول على منفعة مالية باستخدام الوسائل الرقمية سواء كان ذلك مباشرة او عبر موظفيه ويكون كاختراق الحسابات المالية لشركات أخرى لتحقيق أرباح، او الاحتيال على العملاء باسم المؤسسة مثل الاحتيال عبر منصات الدفع الإلكترونية او سرقة العملات المشفرة او تحويل الأموال الكترونياً بطرق غير قانونية ويكون ذلك عن طريق برامج الاحتيال المالي او البريد الالكتروني الاحتيالي باسم الشركة او عن طريق استغلال الثغرات في الأنظمة المالية الرقمية لشركات المنافسين[٣٨].وان الكيان يتحمل المسؤولية الجنائية المباشرة عن افعال موظفيه او ممثليه وبالأخص إذا حقق الكيان منفعة مباشرة او استفاد من الجريمة وان العقوبات تشمل السجن وفرض غرامات ومصادرات وفرض رقابة قضائية على نشاط الشركة او المؤسسة او الهيئة[٣٩].

ثانياً: اختراق الأنظمة والشبكات:ان المقصود به هو الوصول غير المشروع الى أنظمة معلومات او خوادم او قواعد بيانات كيان آخر قد يكون شركة او مؤسسة او هيئة بغض النظر عن الأغراض والتي قد تكون تجارية او صناعية لتحقيق منفعة اقتصادية[٤٠]، ويكون بهدف التجسس الصناعي

على شركات منافسة للحصول على اسرار تجارية او اختراق نظم معلومات حكومية لأغراض تجارية او استراتيجية او قد يكون نشر برمجيات خبيثة عبر أنظمة الشركة لأغراض التلاعب بالبيانات، ويتم ذلك باستغلال الثغرات البرمجية او عن طريق تسجيل الضغط على لوحة المفاتيح وشبكات VPN لاخفاء هوية الكيان اثناء ارتكاب الجريمة[٤١].وان الكيان يتحمل المسؤولية الجنائية الصادرة عن موظفيه او الممثل الرسمي او الوكلاء وقد تشمل العقوبة غرامات مالية كبيرة ويمنع النشاط التجاري لهذا الكيان او قد تحظر التعاملات الرقمية مؤقتاً وسحب الترخيص ومنع الكيان من الدخول بمناقصات او عقود حكومية اذا كان الفعل يصب في مصلحة الشركة[٤٢]، كما قد في موقع العدالة ان العقوبات قد تصل الى حل الشركة وحظر مزاولة الأنشطة المهنية والرقابة القضائية واغلاق الفروع واستبعادها من الأسواق العامة ومصادرة الأصول ونشر الحكم وكل هذا قدي يصل الى خمس سنوات[٤٣].

ثالثاً: الجرائم ضد الافراد:هي الجرائم التي تستهدف بيانات العملاء او الموظفين او أي طرف آخر بطريقة غير قانونية بهدف الاضرار او الاستفادة المالية[٤٤]، ويتم ذلك ببيع بيانات العملاء الشخصية او مشاركة المعلومات الحساسة الخاصة بالعملاء بدون موافقة او قد تصل حتى الى الابتزاز الإلكتروني للموظفين او العملاء باستخدام تلك المعلومات حساسة ويكون باستخدام البريد الإلكتروني الخاص بالشركة او عبر تطبيقات الرسائل وقواعد البيانات المخترقة وان الكيان يتحمل المسؤولية المباشرة عن كل فعل ارتكبته اجهزته او ممثليه وان العقوبات ستشمل السجن وغرامة الشركة وفرض مراقبة على السياسات الداخلية للامن الرقمي إضافة الى طلب تعويض من الشركة للضحايا[٤٥].

خامساً: الجرائم المتعلقة بالأمن المعلوماتي:هي مجموعة أفعال يتخذها موظفوا او ممثلوا او وكلاء الكيان أفعال تهدف إلى إلحاق الضرر بالبنية التحتية الرقمية أو تعطيل الخدمات الإلكترونية التابعة للجهات الأخرى ويكون ذلك كما ذكر في السابق من خلال نشر الفيروسات او البرمجيات الخبيثة لتعطيل الخدمات الرقمية شن هجمات DDoS ضد منافسين او مؤسسات حكومية وايضاً استخدام التجسس الصناعي او التخريب الإلكتروني باسم الشركة او استخدام أدوات متقدمة لشلّ الخدمات الرقمية للشركة الأخرى واستغلال الثغرات التقنية[٤٦].وايضاً الشركة تتحمل المسؤولية الكاملة خاصة لو تضررت المصالح العامة او البنية التحتية الحيوية وبهذا فأنها تخضع للعقوبات والتي تتمثل في السجن للشخص المعنوي او فرض غرامات كبيرة وحظر النشاط التجاري الرقمي، ونظراً بأن العراق لا يمتلك تشريع فيما يخص الجرائم الرقمية لذا قد يحاسب الكيان وفق للمادة ٤٣٠ من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل حيث يعاقب بالسجن او الحبس كل من هدد آخر بارتكاب جريمة او أقدم على ارتكابها، مما يشمل الأفعال التي قد تضر بالمصالح العامة او البنية التحتية الحيوية وفيما لو ثبت تورط الشركة في هذا الفعل الذي ضر بالمصالح العامة على حساب منفعة الشركة قد تصدر المحكمة عقوبات تتراوح بين الغرامات والسجن[٤٧].المسؤولية الجنائية للأشخاص المعنويين في الجرائم الإلكترونية تكمل المسؤولية الفردية للموظفين أو المدراء، وتهدف إلى منع استغلال الهيئات القانونية لارتكاب الجرائم. تشمل الأركان المادية والمعنوية، وتعتمد على الأدلة الرقمية والسياسات الداخلية لإثبات القصد والمنفعة.

الخاتمة

تم بحمد الله من إتمام هذا البحث بالمستوى المطلوب يمكننا القول ان المسؤولية الجنائية في الجرائم الالكترونية تمثل احد اهم مجالات القانون الحديث نظراً لتوسع استخدام التكنولوجيا وتطورها مما أدى الى تطور أساليب ارتكاب الجرائم الالكترونية وتنوعها مما أدى الى ضرورة وضع تشريعات تدين مرتكبي هذه الجرائم، ومن خلال هذا البحث تم التوصل الى:

أولاً: النتائج:-

١- ان التشريعات القانونية تطورت تدريجياً منذ ٢٠٠١ ومازلت ليومنا هذا في تطور.

٢- ان الكيان (الشركات، المؤسسات، الهيئات) تتحمل المسؤولية الجنائية خاصة اذا كان احد موظفيها او ممثليها الرميين او وكلائها قاموا بإرتكاب الجريمة لصالح مصلحة الشركة، كما وأن هذا الكيان قد يخرج من المسؤولية الجنائية اذا كان احد موظفيها او ممثليها الرسميين او وكلائها قاموا بإرتكاب الجريمة لأغراض شخصية.

٣- تبين من هذا البحث ان اثبات الجريمة الالكترونية يعتمد على ضرورة توافر الركن المادي والركن المعنوي.

٤- اظهر هذا البحث ان التشريعات الوطنية والدولية عززت القدرة على محاسبة الفاعلين.

٥- ان الجرائم الالكترونية متنوعة وتتخذ عدة اشكال ولكل شكل له مسؤولية جنائية تختلف عن الشكل الآخر.

ثانياً:- التوصيات:-

١- ضرورة استخدام احدث التقنيات لتحليل الأدلة الالكترونية كسجلات الدخول ورسائل البريد الالكتروني وتحليل الأنشطة على الشبكة.

٢- ضرورة تعزيز الاطار التشريعي لمواكبة التطورات التقنية لما بعد سنة ٢٠٢٥ بما يشمل الجرائم المالية الرقمية واختراق الأنظمة وجرائم ضد الافراد.

٣- الزام الشركات والمؤسسات بوضع سياسات واضحة للأمن الرقمي وتدريب الموظفين للامتثال لها.

٤- الدعوة الى تعزيز التعاون الدولي وتبادل المعلومات والخبرات في التحقيق وملاحقة المجرمين المعلوماتيين العابرين للحدود.

٥- دعم الدراسات العلمية وتشجيعها حول الجرائم الالكترونية حلول وقائية وتقنية فعالة.

المصادر والمراجع

اولاً: المصادر العربية:-

١. د. أسامة احمد المناعسة، شرح قانون الجرائم الالكترونية، دراسة مقارنة وفقاً لاحداث التعديلات، ٢٠٢٥.

٢. د. عطية عبد السلام الفيتوري، الحماية الجنائية للبيانات الشخصية للمستهلك في عقود التجارة الالكترونية في القانون الليبي، كلية القانون، جامعة عمر المختار.

٣. د. محمود السيد عبد المعطى، الانترنت وبعض الجوانب القانونية، دار النهضة العربية، القاهرة، ١٩٩٨.

٤. د. مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة، ٢٠٠.

٥. د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الالكتروني، دار النهضة العربية، القاهرة، ٢٠١٢.

٦. أنواع الجرائم الالكترونية وعقوبتها https://manielaw-sa.com وقت وتاريخ الدخول ٢٠٢٥/٦/٦ الساعة ٢:٠٧م

ثانياً: المواقع الالكترونية:

١. تشريعات الجرائم الالكترونية في العراق.https://www.tamimi.com وقت وتاريخ الدخول ٢٠٢٥/٥/٨ الساعة ٣:٠٠م

٢. تنظيم التجارة الالكترونية في العراق https://iraqilawyersnetwork.com وقت وتاريخ الدخول ٢٠٢٥/١/٩ الساعة ١١:٠٧م

٣. جامعة الدول العربية، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ٢٠١٠.

٤. جريمة الابتزاز الالكتروني واساسها القانوني دراسة مقارنةhttps://share.google/hCOLpOZeYoNSFCuvd وقت وتاريخ الدخول ٢٠٢٥/٣/٥ الساعة ١:٠١م

٥. الركن المعنوي للجرائم الالكترونية – حماة الحق https://jordan-lawyer.comوقت وتاريخ الدخول ٢٠٢٥/٧/٧ الساعة ١٢:٠٠م

٦. قانون الجرائم الإلكترونية الأردني لسنة ٢٠٢٣. https://en.wikipedia.org وقت وتاريخ الدخول ٢٠٢٥/٩/١ الساعة ١:٢٢ص

٧. قرار بقانون رقم (١٠) لسنة ٢٠١٨ بشأن الجرائم الإلكترونية – الأردن، المادة (٣) التي تُجرّم الدخول غير المشروع إلى أي نظام معلومات.

٨. المرسوم الاتحادي رقم ٣٤ لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية – الإمارات.

٩. المسؤولية الجزائية لممثل الشخص الاعتباري. https://www.advokatorium.com/index.php/ar/arabic/alqawanin-waltaeliqat/almaswuwliat-aljinayiyat-limumathil-alsharikat-fi-almahkama وقت الدخول ٢٠٢٥/٣/١١ الساعة ٢:١٠م

١٠. المسؤولية الجنائية للاشخاص المعنوية عن الجرائم.https://share.google/TcxZmnuKyreXupuQU وقت الدخول ٢٠٢٥/٦/٢ الساعة ٤:٠٠م

١١. المسؤولية الجنائية للشركات.https://www.menafayq.com/corporate-criminal-liability وقت الدخول ٢٠٢٥/٦/٩ الساعة ٦:٠٠م

١٢. الهجوم الموزَّع لحجب الخدمة: ماذا يعني؟ ما هي أنواعه؟ وما السّبل الكفيلة بالوقاية منه؟https://nordvpn.com/ar/blog/ddos-attack-meaning وقت الدخول ٢٠٢٥/٦/١ الساعة ٨:٤٠م

ثالثاً: المصادر الأجنبية:-

1- Brenner, S.W., Cybercrime and the Law, 2022.

2- Christidis, K. & Devetsikiotis, M. Blockchains and Smart Contracts for Digital Evidence, IEEE Access, 2022.

3- Council of Europe, Convention on Cybercrime (Budapest, 2001)

Directive 2013/40/EU on attacks against information systems ؛4- Directive (EU) 2022/2555 (NIS2).

5- Equifax data breach 2017. https://en.wikipedia.org/wiki/2017_Equifax_data 1/4/2025 3:30pm
6- Gottschalk, P., Corporate Cybercrime and Liability, 2022.
7- Client-side Vulnerabilities in Commercial VPN. https://arxiv.org/abs/1912.04669 6/4/2025 8:30pm
8- Corporate Liability in the United Arab Emirates. https://www.globalcompliancenews.com/wcc/corporate-liability-handbook/corporate-liability-in-the-united-arab-emirates 2/2/2025 4:50pm
9- Kaur, Manpreet & Singh, Harjit. Digital Fingerprinting Techniques in Cyber Forensics, 2022, Journal of Cybersecurity Studies.
10- Kun.uz, Digital Evidence Law in Uzbekistan, 2024.
11- Raciti et al., SPADA: A Privacy Threat Model for Digital Forensics, 2025, arXiv.
12- Shukla, The Admissibility of Digital Evidence: Challenges and Future Implications, 2023.
13- TaxGuru – Cyber Attacks and Corporate Law, 2023.
14- Veterinaria.org, Bharatiya Sakshya Adhiniyam 2023.
15- Wall, D., Cybercrime: The Transformation of Crime in the Information Age, 2021.
16- Wired, ICC Investigation and Digital Media Evidence, 2024.
17- Xavier linants de bellefonds – alain hallande: partique du droit de informatique, ene edition, delnas, 1998, p.240.

هوامش البحث

[١] قانون الجرائم الإلكترونية الأردني لسنة ٢٠٢٣.https://en.wikipedia.org

[٢] د. أسامة احمد المناعسة، شرح قانون الجرائم الالكترونية، دراسة مقارنة وفقاً لاحداث التعديلات، ٢٠٢٥.

[٣] د. مدحت عبدالحليم رمضان، الحماية الجنائية للتجارة الالكتروني، دار النهضة العربية، القاهرة، ٢٠١٢، ص ٧٩–٨٠ وما بعدها.

[٤] د. عطية عبدالسلام الفيتوري، الحماية الجنائية للبيانات الشخصية للمستهلك في عقود التجارة الالكترونية في القانون الليبي، كلية القانون، جامعة عمر المختار.

[٥] Council of Europe, Convention on Cybercrime (Budapest, 2001)

[٦] جامعة الدول العربية، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ٢٠١٠.

[٧] Directive (EU) 2022/2555 (NIS2 ؛Directive 2013/40/EU on attacks against information systems

[٨] United Nations, Convention against Cybercrime (٢٠٢٤)

[٩] https://www.interpol.int

[١٠] الجريدة الرسمية المصرية، قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

[١١] المرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١.

[١٢] Shukla, The Admissibility of Digital Evidence: Challenges and Future Implications, 2023

[١٣] Wired, ICC Investigation and Digital Media Evidence, 2024

[١٤] Veterinaria.org, Bharatiya Sakshya Adhiniyam 2023

[١٥] Kun.uz, Digital Evidence Law in Uzbekistan, 2024

[١٦] Raciti et al., SPADA: A Privacy Threat Model for Digital Forensics, 2025, arXiv

[١٧] Kaur, Manpreet & Singh, Harjit. Digital Fingerprinting Techniques in Cyber Forensics, 2022, Journal of Cybersecurity Studies

[١٨] Christidis, K. & Devetsikiotis, M. Blockchains and Smart Contracts for Digital Evidence, IEEE Access, 2022

[١٩] Xavier linants de bellefonds – alain hallande: partique du droit de informatique, ene edition, delnas, 1998, p.240.

[٢٠] د. مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة، ٢٠٠، ص٧٣.

[٢١] د. محمود السيد عبد المعطى، الانترنت وبعض الجوانب القانونية، دار النهضة العربية، القاهرة، ١٩٩٨، ص ٩٤.

[٢٢] Wall, D., Cybercrime: The Transformation of Crime in the Information Age, 2021

[٢٣] Brenner, S.W., Cybercrime and the Law, 2022

[٢٤] https://jordan-lawyer.com الركن المعنوي للجرائم الالكترونية – حماة الحق.

[٢٥] https://manielaw-sa.com أنواع الجرائم الالكترونية وعقوبتها.

[٢٦] https://manielaw-sa.com المصدر السابق، جرائم الوصول غير المشروع.

[٢٧] https://manielaw-sa.com أنواع الجرائم الالكترونية وعقوباتها.

[٢٨] https://www.tamimi.com تشريعات الجرائم الالكترونية في العراق.

[٢٩] https://www.tamimi.com تشريعات الجرائم الالكترونية في العراق.

[٣٠] Brenner, S.W., Cybercrime and the Law, 2022

[٣١] https://manielaw-sa.com أنواع الجريمة الالكترونية وعقوباتها.

[٣٢] https://www.tamimi.com تشريعات الجرائم الالكترونية في العراق.

[٣٣] Gottschalk, P., Corporate Cybercrime and Liability, 2022

[٣٤] https://share.google/TcxZmnuKyreXupuQU المسؤولية الجنائية للاشخاص المعنوية عن الجرائم.

[٣٥] https://share.google/TcxZmnuKyreXupuQU المسؤولية الجنائية للاشخاص المعنوية عن الجرائم.

[٣٦] https://share.google/hCOLpOZeYoNSFCuvd جريمة الابتزاز الالكتروني واساسها القانوني دراسة مقارنة.

[٣٧] https://share.google/hCOLpOZeYoNSFCuvd جريمة الابتزاز الالكتروني واساسها القانوني دراسة مقارنة.

[٣٨] المرسوم الاتحادي رقم ٣٤ لسنة ٢٠٢١ بشأن مكافحة الشائعات والجرائم الإلكترونية – الإمارات.

[٣٩] https://www.globalcompliancenews.com/wcc/corporate-liability-handbook/corporate-liability-in-the-united-arab-emirates Corporate Liability in the United Arab Emirates

[٤٠] قرار بقانون رقم (١٠) لسنة ٢٠١٨ بشأن الجرائم الإلكترونية – الأردن، المادة (٣) التي تُجرّم الدخول غير المشروع إلى أي نظام معلومات.

[٤١] Client-side Vulnerabilities in Commercial VPNs https://arxiv.org/abs/1912.04669

[٤٢] https://www.menafayq.com/corporate-criminal-liability المسؤولية الجنائية للشركات.

[٤٣] https://www.advokatorium.com/index.php/ar/arabic/alqawanin-waltaeliqat/almaswuwliat-aljinayiyat-limumathil-alsharikat-fi-almahkama المسؤولية الجزائية لممثل الشخص الاعتباري.

[٤٤] TaxGuru – Cyber Attacks and Corporate Law, 2023

[٤٥] Equifax data breach 2017 https://en.wikipedia.org/wiki/2017_Equifax_data_breach

[٤٦] https://nordvpn.com/ar/blog/ddos-attack-meaning الهجوم الموزَّع لحجب الخدمة: ماذا يعني؟ ما هي أنواعه؟ وما السّبل الكفيلة بالوقاية منه؟

[٤٧] https://iraqilawyersnetwork.com تنظيم التجارة الالكترونية في العراق.