Bilad Alrafidain Journal of Humanities and Social Science Vol. 6, No. 1 **ISSN: 2788-6026**
Doi: 10.54720/bajhss/2024.060107 **Pages:68-85**

المواجهة الجنائية للاحتيال الإلكتروني وإجراءات مكافحته

م. د. حميد أسعد نداوي
قسم القانون، كلية بلاد الرافدين الجامعة، ديالى، 32001، العراق
hameed@bauc14.edu.iq

الملخص

تعتبر جرائم الاحتيال الإلكتروني من بين أخطر الجرائم وأكثرها ضرراً على أحوال المواطنين، سواءً كان ذلك على مستوى الأفراد أو فيما يتعلق بأموالهم، ويظهر أنها ظاهرة لا يمكن تجاهلها، حيث يصبح الانخراط في مثل هذه الأنشطة شبه لازم في معظم المجتمعات المعاصرة. يُمكن النظر إلى هذه الجرائم على أنها إحدى الجوانب السلبية للتقدم الاقتصادي والاجتماعي والتحضر الشامل، حيث تعتبر تلك الظاهرة نتيجةً غير مرغوبة لتطور المجتمعات الحديثة، لما يمتلكه المحتالون اليوم من قدرة سلوكية تتمثل بالاستهانة بالقوانين والتعليمات، وتعد جريمة الاحتيال أحد أساليب الإجرام المنظم بسبب ما يقوم به المحتالون من وسائل الغش والتدليس.

الكلمات المفتاحية: القانون، الاحتيال الإلكتروني.

Criminal Confrontation of Online Scam and Measure to Combat It

Lect. Dr. Hameed Asaad Nidawi AL – jewari
Department of Law, Bilad Alrafidain University College, Diyala, 32001, Iraq.
hameed@bauc14.edu.iq

Abstract

Electronic fraud crimes are considered one of the most serious crimes and harmful to the conditions of citizens, whether in their persons or their money, and almost no modern society is devoid of them . These crimes can be viewed as one of the taxes of economic and social progress and urbanization in general that societies pay, due to the behavioral ability that fraudsters possess today . It consists of flouting laws and instructions, and the crime of fraud is one of the methods of organized crime due to the fraudulent and deceptive methods used by fraudsters.

Keywords**:** Law Fraud Electronic.

أولاً: موضوع الدراسة

إن الاكتشافات العلمية التي حدثت في الربع الأخير من القرن العشرين وبداية القرن الحادي والعشرين فتحت آفاقاً جديدة ضخمة أمام تقدم البشرية وتحقيق مستوى أفضل من الحياة، فقد أضحت تقنية المعلومات من أساسيات الحياة وسمة بارزة في هذا العصر، إلا أن الإنسان استغلها وأصبحت أداة لارتكاب الجريمة بدلاً من كونها نعمة تسخر لخدمة البشرية.

فقد بات للإجرام صور مستحدثة حيث تزايدت الجرائم الواقعة في صورة معلوماتية "إلكترونية" حتى أصبحنا أمام صورتين للجريمة أحدهما تقليدية والأخرى إلكترونية، وأوضحت الجرائم المستحدثة تنفذ بلمسة زر إلكتروني واحدة مما يتيح الأمر للجاني أن يجلس ويمارس سلوكه الإجرامي "الإلكتروني" في قارة فيما تتحقق الجريمة في قارة أخرى، فضلاً عن أن العديد من هذه الجرائم لا تجد نصوصاً قانونية تواجهها في العديد من البلدان ولا سيما البلاد العربية ومنها العراق.

تحول الاحتيال عبر الإنترنت إلى ظاهرة جديدة أتاحت لمرتكبيها دخول المنازل والمكاتب واجتياز الحدود والوصول إلى الضحايا بسهولة بالغة خصوصاً مع انتشار الإنترنت كوسيلة مهمة لتقديم الخدمات المالية والمصرفية، فيما يبتكر المحتالون الإلكترونيون وسائل جديدة يومياً للتغرير بضحاياهم والإيقاع بهم وفي الوقت الذي يعمل فيه قراصنة الإنترنت والمحتالون الإلكترونيون المحترفون طوال اليوم لابتكار وسائل جديدة والعثور على ثغرات يمكن من خلالها تنفيذ مهامهم.

في القرن الحادي والعشرين، أصبح الإنترنت بيئةً خصبةً لجرائم الاحتيال، حيث نشاهدها تتكاثر يوماً بعد يوم، مما يسهم في انتشارها وتكاثرها، يعد البحث المشترك عن المال أمراً يسيراً وخالٍ من العناء لكل من المجرم والضحية على حد سواء، حيث لم يعد المجرم بحاجة إلى استخدام الأدوات والآلات التقليدية لارتكاب جريمته. يظهر أن الإنترنت قد أوسع المجال وأصبح جهاز الكمبيوتر الوسيلة الأساسية المستخدمة في هذا السياق."

ومن المؤكد أن الدول المتقدمة، التي تعتمد بشكل كبير على التكنولوجيا المتطورة في إدارة شؤون الحياة، تشهد زيادة في حالات جرائم الاحتيال الإلكتروني بشكل أكبر مقارنة ببقية الدول.

ثانياً: أهمية البحث:

تكمن أهمية البحث في هذه الجريمة لأهميتها الاجتماعية والاقتصادية ولما تعالجه من موضوعات نعيشها في حياتنا اليومية تقريباً فهي كونها من أكثر الجرائم خطورة، تعد من جرائم الحديثة التي تطورت في مجال الحياة سواء كان حضارياً أو اقتصاديا وغيرها للمجتمع وما رافق ذلك من استحداث أساليب جزائية جديدة فتحت المجال أمام ارتكاب الجرائم.

أخذت جريمة الاحتيال الإلكتروني مكانةً مميزةً بين الجرائم التقليدية الأخرى، نظراً للاعتماد على مقومات وأسس تتركز في الأعمال الذهنية والابتكار، بالإضافة إلى القدرات المهارية التي يظهرها المحتالون في تنفيذ أساليبهم، يتلاءم ذلك مع التطورات التقنية الحديثة والتغيرات الاقتصادية والاجتماعية والثقافية والحضارية.

ثالثاً: مشكلة البحث:

يسعى ضحايا هذا الإجرام بأنفسهم إلى شبكة المحتالين، مدفوعين بدافع الطمع وحب الثراء، اللذين يقدمهم الجناة بطرق سريعة وسهلة، يقوم الجناة بعرض أكاذيبهم بشكل ذكي وماهر، مدعومين بمظاهر خارجية برَّاقة، مما يساهم في خلق وهم يجعل هؤلاء الضحايا يثقون فيهم، يؤدي هذا الوهم إلى تسليم الضحايا أموالهم بإرادتهم الحرة، دون إكراه أو ضغط، خاصة من قبل الأشخاص الذين يتمتعون بالطيبة وحسن النيةـ، لذلك كانت الإشكالية الرئيسية التالية:

ماهي جريمة الاحتيال الإلكتروني وما هي حالات وأركان هذه الجريمة؟

ويتفرع عن هذه الإشكالية عدداً من الأسئلة الفرعية التالية:

1- ما مدى حجية الأدلة الإلكترونية في جريمة الاحتيال الإلكتروني؟

2- ما هي إجراءات مكافحة الاحتيال الإلكتروني وما هي عقوبته؟

رابعاً: أهداف البحث:

إن معظم الجرائم المرتكبة بواسطة الوسائل الإلكترونية تعد من الجرائم الخفية حيث يقع العديد منها لصعوبة اكتشاف الفاعل ويبدو أن طبيعة هذه الجرائم تنطوي على قدر كبير من الخداع والاحتيال، وتتسم هذه الجرائم بالتعقيد المتزايد الأمر الذي يعوق عملية الكشف عنها أو حتى ملاحقة مرتكبيها وعقابهم لقدرت الفائقة على إخفائها فضلاً عن أنهم يمكن أن يكونوا من ذوي الخبرة العالية لذلك كان الهدف من هذا البحث:

1- لمعرفة حالات الاحتيال الإلكتروني.

2- لمعرفة أركان جريمة الاحتيال الإلكتروني.

3- لمعرفة إجراءات مكافحة الاحتيال الإلكتروني وعقوبته.

خامساً: نطاق البحث

يقتصر البحث على التشريع العراقي وإجراءات مكافحته والوقاية منه، وموقفه من معالجة المشكلات العلمية والقانونية التي تثيرها موضوع الاحتيال الإلكتروني.

سادساً: منهج البحث:

اعتمدنا في هذا البحث على المنهج التحليلي من خلال تحليل النصوص القانونية المتصلة بالموضوع والوقوف على الأحكام القانونية وتحليلها وبينان المبدأ القانوني الذي تقوم عليه.

سابعاً: خطة البحث:

من أجل معالجة إشكالية البحث، اعتمدنا التقسيم الثنائي، لذا سنتناول هذا البحث من خلال مبحثين نتناول في المبحث الأول حالات وأركان الاحتيال الإلكتروني من خلال مطلبين، نتناول في المطلب الأول حالات الاحتيال الإلكتروني، أما في المطلب الثاني نتناول فيه أركان

جريمة الاحتيال الإلكتروني. أما المبحث الثاني نبحث فيه مدى حجية الأدلة الإلكترونية في الأثبات وسلطة القاضي الجنائي في قبول وتقدير الأدلة. من خلال مطلبين، نتناول في المطلب الأول حجية الدليل الرقمي في إثبات جريمة الاحتيال الإلكتروني، أما في المطلب الثاني نتناول فيه إجراءات مكافحة الاحتيال الإلكتروني وعقوبته.

المبحث الأول

صور وأركان جريمة الاحتيال الإلكتروني

أدت ثورة المعلومات والاتصالات إلى ظهور جريمة الاحتيال الإلكتروني، حيث أحدثت تغييرات جذرية ونوعية في مختلف مجالات الحياة الاقتصادية والقانونية وغيرها. تركت الثورة المعلوماتية خلفها آثاراً سلبية، حيث بدأ البعض في سوء استخدام الأنظمة المعلوماتية بشكل غير قانوني، مما أدى إلى ظهور فضاء الجرائم الإلكترونية المعلوماتية، ولا سيما جريمة الاحتيال الإلكتروني، استجابةً لهذا التحدي المتزايد، اتخذت معظم التشريعات إجراءات قانونية تهدف إلى مكافحة ومواجهة جريمة الاحتيال الإلكتروني، بهدف حماية المواطنين والأعمال من التهديدات الرقمية المتزايدة، ومن ذلك اتفاقية بودابست لمكافحة جرائم الاحتيال الإلكتروني عام2001[1].

لذا سنتناول في هذا المبحث حالات وأركان الاحتيال الإلكتروني من خلال مطلبين، نخصص المطلب الأول لحالات الاحتيال الإلكتروني، ويبحث في المطلب الثاني أركان جريمة الاحتيال الإلكتروني.

المطلب الأول

صور جريمة الاحتيال الإلكتروني

على الرغم من هذه المميزات العديدة التي قدمها "الإنترنت" للعالم هناك من استخدم هذه الخدمة بالصور الخاطئة ولا يخفى أيضاً عن المؤامرات التي تحدث خلف هذه الواجهة التي أدت إلى انتشار كثير من الجرائم والظواهر الغريبة بين متسللي الشبكات والأنظمة المعلوماتية وبين رواد مواقع التواصل الاجتماعي، ومن بين الجرائم الأكثر خطورة وانتشاراً جرائم الاحتيال الإلكتروني التي أصبحت أخطر من جرائم الإرهاب وبطرق وأشكال متنوعة ومدروسة للاحتيال والاستيلاء على أموال الآخرين، ولعل أبرزها ما تم عن طريق مواقع التواصل الاجتماعي خصوصاً فيس" "بوك" و "تويتر" كونه أداة سهلة للتلاعب بالآخرين لسرقة أموالهم وهذا ما أدى إلى وقوع كثير من مستخدمي هذه المواقع فريسة الاحتيال عليهم[2].

وفي ضوء ذلك سنتناول أركان حالات الاحتيال الإلكتروني من خلال فرعين، نبحث في الفرع الأول التسويق الإلكتروني وعروض الوظائف، أما الفرع الثاني نبحث فيه عن الاحتيال عبر التسول الإلكتروني وأسئلة الامتحان.

الفرع الأول

التسويق الإلكتروني وعروض الوظائف

تنجذب شريحة الشباب إلى عروض العمل المنشورة على وسائل التواصل الاجتماعي في القطاعين العام والخاص وذلك لحاجة الخريجين للعمل ورغبتهم في العثور على عمل علماً أن ندرة الوظائف أو زوال الوظيفة الحكومية قياساً مع كثرة الخريجين هذا كله أدى الى امتداد ظاهرة مواقع التوظيف الإلكترونية والشركات الوظائف التي لا سند لها وهي وهمية التي اجتاحت الدول العربية.

والتي يمكن تحديدها ببعض الفقرات والتي تتمثل فيما يلي:

أولاً-الاحتيال عبر التسويق الإلكتروني:

أصبح التسويق عبر وسائل التواصل الاجتماعي ظاهرة هامة تنتشر بشكل واضح في الآونة الأخيرة، نظراً لسهولة الوصول إليها عبر الإنترنت وإمكانية الحصول بسهولة على المواد المرغوبة، بالإضافة إلى ذلك، يشهد هذا النوع من التسويق انخفاضاً في الأسعار ويتيح للمستهلكين الوصول إلى منتجاتهم حتى باب منازلهم. يمكنك الآن بسهولة طلب كتاب، أو جهاز إلكتروني، أو هدية، أو أي شيء آخر من خلال متاجر التسوق الإلكتروني.

ومع تطور هذه الظاهرة، تمتد نطاقات التسويق إلى صفحات خاصة على وسائل التواصل، حيث يتم نشر إعلانات المتاجر والمحلات ومجموعات البيع والشراء، حيث يمكنك أن تتجول كما لو كنت في سوق حقيقي، حيث يعرض كل شخص سلعه وفقاً لمنطقته ونوعية بضائعه.

يبدأ الأفراد بعرض مجموعة واسعة من البضائع، بدءاً من بيع العقارات والأغراض المستعملة، وصولاً إلى المحلات التي تروج لأحدث منتجاتها كوسيلة دعاية، يُنشر أيضاً إعلانات حول مستحضرات التجميل ومنتجات التنحيف، بالإضافة إلى تسويق الأعمال اليدوية وبيعها عبر هذه المنصات، مثل أعمال الخياطة وصناعة قطع البديل، وبالنسبة للأشخاص الذين يتقنون أي مهارة أو حرفة، يمكنهم نشرها في هذه المجموعات للتواصل مع الجمهور وتسويقها بنجاح [1].

يكمن التحدي الرئيسي في المغالطات المتعلقة بالعروض السخية والأسعار الجاذبة، حيث يقع الأفراد في فخ الجذب ويتم استهدافهم من قبل بعض المحتالين، ويتمثل الخطر في أن الأشخاص يمكن أن يدفعوا ثمناً باهظاً مقابل منتجات أو خدمات غير حقيقية، مما يتيح للمحتالين الاستيلاء على أموالهم دون تقديم أي قيمة فعلية [3].

تجتمع هذه الشركات عادة بعدد كبير من المندوبين والمندوبات، حيث يفضل بشكل كبير استقطاب الإناث، ويتم تجنيد المندوبات لمهمة إقناع العملاء، وغالباً ما لا تتفاعل المندوبة مباشرة مع الشركة بل تعمل من خلال مندوبة أخرى، وهكذا تتكون شبكة من التعاملات. كلما اجتمعت المندوبة مع مندوبات إضافيات، زادت نقاطها، ويُفتح بذلك المجال لها لسحب كميات أكبر من المنتجات [4].

تعد المواقع الإلكترونية التجارية وشبكات التواصل الاجتماعي اليوم سوقاً افتراضياً لسلع متنوعة لراغبي البيع والشراء من خلال الحاسوب أو التطبيقات على الهواتف النقالة التي تنتشر بشكل كبير بين أفراد المجتمع باختلاف أعمارهم لشراء منتجات بأسعار أقل من المحال التجارية وفي بعض الأحيان تتوافر لدى تلك المواقع الإلكترونية والأسواق الافتراضية منتجات يصعب الحصول عليها من المحال التجارية المحلية مزايا كثيرة يحصل عليها الفرد من تلك الأسواق الإلكترونية وسلع تصل إلى الزبائن في أماكنهم، تلك المميزات والفوائد التي يحصل عليها الفرد من الأسواق الإلكترونية يقابلها عدد من المخاطر خلال عملية الشراء منها عدم تطابق المميزات الخاصة بالسلعة المدونة في المواقع التجارية أو صلاحية السلعة أو الترويج لبضائع مقلدة وعدم الالتزام بموعد التسليم التي أقرها واطلع عليها المشتري بعناية [5].

للتعرف إلى سبل الوقاية من عمليات الاحتيال التجاري الإلكتروني بسبب استخدام تلك الأسواق سواء من خلال مواقع تجارية إلكترونية أو شبكات التواصل الاجتماعي وطرائق التقدم بشكوى أو بلاغ جراء التعرض لعمليات احتيال تجاري الكرتوني أو الإخلال بتعهدات تقوم بها مواقع إلكترونية محلية أو دولية من مزايا التسوق الإلكتروني التركيز على اختصار الجهد والزمن فكثير من الناس يقضون ساعات طويلة في التردد على الأسواق لشراء احتياجاتهم أو البحث عن الصفات التي يريدونها، وهذا الأمر يوفر عليك كل هذه الجهود ولا أرى لهذا النوع من البيع أية مخاطر إذا كانت المواقع العارضة بعيدة عن الغش واستغفال العميل ولم تخالف الوصفات وهناك مماطلة في مواعيد التسليم وأحياناً لا تأتي السلع بالصفات المعروضة، ويتعذر إرجاعها كون معظم هذه السلع بلا ضمان لو توافر الوقت الكافي للإنسان يكون الشراء من المحال التجارية التقليدية أفضل بكثير من الاستعجال والشراء من هذه المواقع الإلكترونية لكن نظراً إلى كثرة العمل والمسؤوليات نضطر إلى الشراء بهدف كسب الوقت والتفرغ لأمور أخرى أكثر أهمية [6].

ثانياً-الاحتيال عبر عروض الوظائف:

تعتبر عروض الوظائف المعلنة على شبكات التواصل الاجتماعي جاذبة لفئة الشباب، سواء كانت الإعلانات تتعلق بالقطاع الخاص أو القطاع العام، ويعود ذلك إلى احتياج الخريجين الملح إلى فرص عمل، حيث يسعى الشباب لاكتساب تجربة العمل، وذلك في ظل نقص الفرص الوظيفية وقلة الوظائف الحكومية بالمقارنة مع زيادة عدد الخريجين، تلك الظروف قادت إلى انتشار ظاهرة مواقع التوظيف الإلكتروني وشركات الوظائف الوهمية التي اجتاحت الدول العربية.

وبالرغم من غياب المعلومات الكافية حول نشاط هذه المواقع وعدد الموظفين الفعليين، فإن المحتالين يقومون بابتكار أفكار جديدة للاحتيال على الأفراد، ويأتي العديد من حالات الاحتيال في شكل عروض عمل وهمية، حيث يتواصل المحتالون مع الأشخاص للحصول على بياناتهم الشخصية، ويلجأ بعضهم إلى استخدام مواقع التوظيف كوسيلة للاحتيال على الأفراد [7].

لذلك، على كل خريج أو طالب عند شروعه للتقدم إلى وظيفة ما عليه أولاً أن يقرأ جيداً الشروط والرواتب المقدمة من الشركة ومقارنتها بتفاصيل العمل وعندما يرى أن هناك عرضاً مغرياً جداً يعلم أن هناك شيئاً مخبأً خلف هذا العرض [8].

الفرع الثاني

الاحتيال عبر التسول الإلكتروني وأسئلة الامتحان

يعد التسول الإلكتروني ظاهرة حديثة تنطوي على استغلال التكنولوجيا الحديثة للتلاعب بالأموال والاحتيال على الأفراد وينبغي على الجمهور أن يكونوا مدركين لمفهوم التسول الإلكتروني وأساليبه المتعددة حتى يتمكنوا من الوقاية من هذا النوع الجديد من الاحتيال الإلكتروني، كما إن ظاهرة تسرب الأسئلة وخاصة الأسئلة الوزارية عبر مواقع التواصل من الأمور الخطرة على المجتمع وأغلب الأحيان تكون عبارة عن نصب واحتيال يأخذون المال وبالمقابل تكون الأسئلة ليست الأسئلة الوزارية، لذلك يمكن تناولها من خلال الفقرات التالية:

أولاً-الاحتيال عبر التسول الإلكتروني:

مع تطور المجتمع وانتشار استخدام وسائل التواصل الإلكتروني، شهدت ظاهرة التسول تحولًا وتطوراً، حيث أصبحت مؤسسة مستقلة على الإنترنت، وبات بعض الأفراد يمتلكون أسماء ذات شهرة واسعة عبر النطاق الإلكتروني، ليبدؤوا بعد ذلك في عمليات التسول عبر مختلف وسائل التواصل الاجتماعي، بما في ذلك تطبيق واتساب، ومنصات التغريد تويتر، فيسبوك، وغيرها،

باستخدام رسائل متأثرة تستهدف القلوب وتثير الوجدان، ويتلقى المستخدمون هذه الرسائل بشكل يومي من جميع أنحاء العالم، دون أن يكونوا على علم بمدى مصداقية أو زيف تلك النداءات[7].

لا يعني وجود شخص يتسول أنه بالضرورة فقير أو معدم، وبالمثل، لا يعني وجود متسول أنه يعاني من الأمراض المستعصية، بل يستخدم بعض الأفراد هذه الوسيلة كمصدر للدخل الذي يحقق لهم ربحاً كبيراً دون الحاجة إلى بذل أي جهد بذلك، بفضل عدم كشف هوية المتسول، يصعب التعرف على اسمه الحقيقي، أو عمره، أو وضعه الاجتماعي، هذا يحميه من الإحراج والعار الذي قد يلاحق المتسولين التقليديين.

وقد أظهرت الأبحاث أن بعض المتسولين لديهم صلات مع دعم منظمات إرهابية، وهذا الأمر يعد الأكثر خطورة وأهمية، ولذلك يجب التوقف عن التعاطف مع المتسولين والإبلاغ عنهم إلى الجهات المختصة، حيث أصبحت معظم وسائل التواصل بمثابة بؤر للاحتيال، وعليه يجب أخذ الحيطة والحذر عندما يتعلق الأمر بإرسال أي مبالغ مالية إلى جهات مجهولة [9].

ثانياً-الاحتيال عبر أسئلة الامتحان

في السابق، كانت أساليب الغش في الامتحانات تتمثل في استخدام قصاصات أو كتابة الإجابات على اليد، وكان الطلاب يتبنون العديد من الطرق لتسهيل عملية الغش، ومع مرور الوقت، تغيرت تلك الطرق وأصبحت أكثر سهولة من قبل، والآن يتبنى الطلاب طرقاً مختلفة، حيث لا يرغبون في محاولة دخول والتلاعب بالأسئلة مباشرة، الأمر الفكاهي والمحزن في الوقت ذاته هو أن الطلاب ليس لديهم مشكلة في دفع مال لشراء الأسئلة بأكملها، حيث يمكن للبعض شراء سؤال أو سؤالين بكل سهولة، وعندما يكتشف الطالب الساذج في اليوم التالي أن تلك ليست الأسئلة الحقيقية، يسأل المختص حول بيع الأسئلة، ويتلقى إجابة تفيد بتغيير الأسئلة في اللحظة الأخيرة، مما يجعل الطالب يعيد الكرة مرة أخرى بسذاجة[10].

لشراء الأسئلة النموذجية" أو نماذج الأسئلة المتوقع طرحها في امتحان البكالوريا أضحت تجارة تدرّ أموالاً كبيرة على أصحابها والذين يستغلون تخوّف الطلبة المقبلين على البكالوريا من الأسئلة ويقيسون إقبالهم على أي شيء قد يعطيهم بصيص أمل لمعرفة نوعية الأسئلة فيطرح مجهولون عبر مواقع التواصل الاجتماعي نماذج لأسئلة ويدعون أنها الأسئلة المتوقع طرحها في الامتحان

يتورط كثير من الطلبة المقبلين على امتحان البكالوريا في الاعتماد الكلي على بعض نماذج أسئلة البكالوريا التي يتم تداولها أياما قبل امتحانهم المصيري ويدعي مروجو هذه الأسئلة أنهم تمكنوا من الحصول وبصفة حصرية على الأسئلة المسربة التي ستكون في الامتحان فيقبل عليها الطلبة وبأي ثمن [11].

الخطير أن الطلبة يركزون مراجعتهم على دروس الأسئلة المذكورة في وثيقة الأسئلة النموذجية فقط، مهملين بقية دروسهم لكنهم سرعان ما يتعرضون لخيبة أمل وصدمة عندما توضع أمامهم الأسئلة الحقيقية يوم الامتحان ويجدونها بعيدة كل البعد عما راجعوه وتوقعوه.

المطلب الثاني

أركان جريمة الاحتيال الإلكتروني

إن النشاط أو السلوك المادي في جرائم الإنترنت يتطلب وجود بيئة الإلكترونية واتصال بالإنترنت ويتطلب أيضاً معرفة بداية هذا النشاط والشروع فيه ونتيجته، فمثلاً يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة فيقوم بتحصين الحاسب ببرامج اختراق أو أن يقوم بإعداد هذه البرامج بنفسه وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد داعرة أو مخلة بالآداب العامة وتحميلها على الجهاز المضيف كثيرا ما نسمع عن مصطلح (السيرفر) أو خادم الإنترنت، دون أن نعرف معنى هذا المصطلح التقني أو إلى ماذا يشير.

إلا أنه في الأساس يعد أداة لتوفير المعلومات لأجهزة الكمبيوتر المتصلة به ويمكن من خلاله الوصول إلى البرامج والمواقع وغيرها من المعلومات من الخادم ويعد (السيرفر) بشكل أبسط هو جهاز كمبيوتر ذو قدرات عالية، أبرزها القدرة على الاتصال بالإنترنت بسرعة فائقة ومصدر كهرباء مستمر فضلاً عن وجود أنظمة تبريد عالية لأنه يعمل بشكل متواصل 24 ساعة طوال الوقت

ويجري تخزين بيانات المواقع عليه فهو أساس استضافة مواقع الإنترنت على الشبكة العنكبوتية فيما تتمثل مهمته الرئيسية في إدارة الموارد المعلوماتية الموجودة على الشبكة مثل أجهزة الحاسوب والآلات الطابعة والهواتف وغيره [12].

وفي ضوء ذلك سنتناول أركان جريمة الاحتيال الإلكتروني من خلال فرعين، حيث نبحث في الفرع الأول الركن المادي لجريمة الاحتيال الإلكتروني، أما الفرع الثاني نبحث فيه الركن المعنوي لجريمة الاحتيال الإلكتروني.

الفرع الأول

الركن المادي لجريمة الاحتيال الإلكتروني

يعرف الركن المادي في جريمة الاحتيال الإلكتروني بأنه: " الوسيلة التي يلجأ إليها المحتال بهدف الاستيلاء على ممتلكات، سواء كانت لنفسه أو للآخرين، تكون عادةً عبر استخدام أساليب خادعة وغالبًا ما تتعلق بالتلاعب بالمعلومات أو الوثائق، ولكن تركيزها يكون على المال المنقول، خاصة النقود. تشمل هذه الوسائل عدة أساليب، مثل الاحتيال الإلكتروني، والتلاعب بالبيانات المالية، واستخدام وثائق مزورة، والتحيل عبر الهاتف أو البريد الإلكتروني، من ذلك يتبين أن عناصر الركن المادي هي [13]:

1. السلوك الإجرامي الطريقة الاحتيالية أو اتخاذ اسم كاتب أو صفة غير صحيحة:

إن كل ما يؤدي إلى الخداع يُعتبر طريقة احتيالية، ولذا فإن الكذب، مهما كان مرتباً، يشير إلى احتمال وجود أسلوب احتيالي. ولكن، يجب أن يترافق الكذب بمظاهر خارجية أو أعمال مادية يقوم المحتال بحبكها، بهدف إقناع المجني عليه بصدق الكذب وتحقيق التأثير المرجو. ومع أن جريمة الاحتيال لا تتأكد بمجرد الأقوال والادعاءات الكاذبة، حتى لو كان الجاني يؤكد صحتها بشكل مبالغ فيه، فإن توفر أعمال خارجية يتعين على القانون أن يأخذها في اعتباره. يشمل ذلك استخدام الجاني لوثائق أو مكاتب تبدو صادرة عن شخص آخر، سواء كان له وجود حقيقي أم لا [14].

تتفق جريمة الاحتيال مع جريمة السرقة من ناحية محل الاعتداء وهو أخذ مال منقول مملوك للغير أي إن الهدف من الاعتداء هو الاستيلاء على ملكية الغير وحرمانه منها وحيازتها, أما الفرق بينهما فهو أن الحصول على مال الغير في جريمة الاحتيال أساسه القيام بمناورات الاحتيال والغش الاحتيالية الذي يوهم المجني عليه بما يخالف عليه الحقيقة للوقوع في الفخ أي إن الحصول على المال يتم برضا المجني عليه بعكس السرقة التي تتم عنوة، إلا أنه وإن كان الكذب يشكل عنصراً لازماً للمناورة الاحتيالية فهو غير كافٍ لوحده، بل يجب دعمه بعناصر خارجية إذ إن الكذب المجرد ليس له التأثير الفعال طالما لم تعقبه أو ترافقه أفعال مادية مؤلفة للمناورات الاحتيالية قد يتوافر أيضاً إلى جانب الاحتيال جريمة استعمال أشياء الغير دون وجه حق وذلك إذا كان مستخدم البطاقة قد سرقها أو التقطها أو استولى عليها بطريقة الحيلة والخداع أو كانت بين يديه بمقتضى عقد في عقود الأمانة واستعمالها في غير الغرض المتفق عليه حتى لو استولى عليها لا بقصد تملكها ولكن بقصد الاستخدام غير المسموح به لأن مثل هذا الاستخدام بترتب عليه الأضرار بالحامل الشرعي لتلك البطاقة وهذا الجرم يتحقق في الحالة التي يقوم فيها المدعي عليه بالاستيلاء على أشياء تخص غيره من دون وجه حق فيقوم باستعمالها من دون قيام نية لديه باختلاسه, فضلاً عن ذلك يعد الإنترنت عنصراً أساسياً في الركن المادي لجريمة الاحتيال الإلكتروني [15].

2. النتيجة الجرمية (تسليم المال):

قبل ظهور الإنترنت، كانت جريمة الاحتيال تتعلق بشكل رئيسي بالأموال المنقولة ذات الطبيعة المادية والمحسوسة، في هذا السياق كانت جميع الأموال التي يمكن للجريمة أن تستهدفها تكون قابلة للمس وملموسة. كان تنظيم القوانين والأحكام المتعلقة بجريمة الاحتيال يركز بشكل أساسي على حماية المال المنقول، سواء كان التسليم لهذا المال مادياً أو حكمياً.

وبالنسبة للجوانب القانونية، كان ركن التسليم في هذا السياق يشمل بشكل أساسي الأموال المنقولة، سواء كانت التسليمات تتم بشكل فعلي أو بوساطة قرارات قانونية. ولكن مع ظهور الإنترنت وتطور التكنولوجيا، أصبحت جرائم الاحتيال تشمل أيضاً العمليات الرقمية والتحايل عبر الشبكة، مما دفع إلى تطوير التشريعات لتأخذ في اعتبارها هذه التحديات الجديدة وتحمي المواطنين من جرائم الاحتيال الإلكتروني.

هذا النقاش يعكس أهمية أن يكون التركيز في جرائم الاحتيال على القانونية والشرعية للتصرفات المرتبطة بالمال، بغض النظر عن مكان وجود المال أو هوية الشخص الذي يحمله، قد تشمل جرائم الاحتيال العديد من السيناريوهات التي تتعامل مع التلاعب والخداع، والتي يجب أن يُعالجها القانون بصرامة لضمان العدالة.

صحيح، يتعامل القانون بشكل عام مع مفهوم المال المنقول في جرائم الاحتيال على أساس أن يكون له قيمة مالية، وهذا يعكس التركيز على حقيقة أن الجريمة تتعلق بالاستيلاء على أموال تمتلك قيمة مالية، بالإضافة إلى ذلك، يظهر تطور في التشريعات حول المفهوم القانوني للمال المنقول، حيث يشمل ذلك السندات والتواقيع التي قد تحمل قيمة اقتصادية. هذا يعكس التكيف مع التطورات في التكنولوجيا وطرق التعامل المالي.

مع ظهور الإنترنت وتطوير الخدمات الرقمية، أصبحت النتائج الجنائية تعتمد أيضًا على التفاعلات والتسليمات التي تتم عبر الشبكة، يُعد تسليم المجني عليه للمحتال تحت تأثير الغلط نتيجة جرمية تعكس كيف يمكن أن يؤثر الخداع والتلاعب الرقمي في قرارات الأفراد ويؤدي إلى ارتكاب جرائم الاحتيال عبر الإنترنت.

صحيح، يمكن أن يكون التسليم في سياق جريمة الاحتيال يُفهم بشكل أكبر كفعل قانوني بدلاً من مناولة مادية يُركز النظر هنا على الإرادة القانونية للمجني عليه، حيث يعتبر التسليم عملًا يتمثل في نقل السيطرة القانونية على المال من ملكية المجني عليه إلى ملكية الجاني.

الجوهر هنا يكمن في إرادة المجني عليه المعيبة أو الخادعة، حيث يتيح للمحتال السيطرة على المال بناءً على توجيه قانوني مشروع. قد يتم تحقيق هذه السيطرة فوراً أو في وقت لاحق بناءً على تفاعلات أو أحداث معينة، وهو ما يبرز التعقيدات القانونية المتعلقة بالتحقق من الإرادة والسيطرة في سياق جرائم الاحتيال [16].

توضح هذه التوجيهات القانونية أن التسليم في سياق جريمة الاحتيال يمكن أن يكون تصرفاً قانونياً يتمثل في تحويل السيطرة القانونية على المال من المجني عليه إلى المحتال. حيث يتم التأكيد على أن الجوانب القانونية للتسليم تعتمد بشكل أساسي على الإرادة المشتركة بين المجني عليه والمحتال.

في حال تحقيق هذا التوافق في الإرادة، يعتبر التسليم تصرفاً مالياً وقانونياً، حتى إذا لم تكن هناك مناولة مادية فورية، يُظهر الأمثلة المقدمة، مثل تسجيل اسم المحتال كدائن في سجل المجني عليه أو حتى حذف دين ثابت، كيف يمكن أن تتنوع صور التسليم وتشمل تصرفات متعددة.

بشكل عام، يبرز هذا السياق الحاجة إلى تفصيل دقيق للظروف الفعلية والتحقق من الإرادة والتفاعلات بين الأطراف لتحديد ما إذا كان قد تم التسليم القانوني أم لا [11].

صحيح، يُبرز هذا البيان أن التسليم في سياق جريمة الاحتيال يمكن أن يحدث من المجني عليه بنفسه أو من طرف آخر، حيث يمكن للمجني عليه أن يسلم المال إلى الجاني بشكل مباشر أو من خلال نائبه أو وكيله وفقاً لأمره.

يتساوى التسليم، سواء كانت حيازة المجني عليه للمال مشروعة أو غير مشروعة، مما يعني أنه حتى في حالة حيازة المجني عليه لمال مسروق أو مكتسب بشكل غير قانوني، يمكن أن يكون التسليم جزءاً من جريمة الاحتيال، يظهر هذا التوجيه القانوني أهمية التحقق من شروط التسليم والتفاعلات بين الأطراف لتحديد القانونية والملاءمة في سياق جريمة الاحتيال.

يُشير هذا إلى أن التسليم في سياق جريمة الاحتيال يُعتبر ذا أهمية بغض النظر عن مشروعية أو غير مشروعية الغرض الذي يسعى المجني عليه لتحقيقه. يُظهر أن المجني عليه قد يسلم المال للمحتال من أجل أغراض مثل تقديم رشوة لموقف معين أو للمشاركة في أنشطة تهريب، وفي تلك الحالات، يُعتبر التسليم جزءًا من جريمة الاحتيال. أن الضرر المتعلق بجريمة الاحتيال لا يقتصر على الضرر المالي المباشر. بل يُفترض أن يحدث ضرر فيما يتعلق بالعدوان على الملكية والتداخل مع الحقوق القانونية، مثل إقامة علاقة جنسية غير مشروعة. هذا يبرز تعقيدات جريمة الاحتيال وكيف يمكن أن يشمل آثارها عدة جوانب في القانون [6].

3.العلاقة السببية:

توضح هذه التوجيهات القانونية أهمية العلاقة السببية في جريمة الاحتيال، حيث يتكون الركن المادي للجريمة من وجود رابطة سببية بين طريقة الاحتيال المستخدمة من قبل الجاني والنتيجة، التي في هذه الحالة تكون تسلم المال.

يُشير البيان إلى أن تسلم المال يعتبر ناتجًا متوقعًا ومنطقيًا للخداع الذي وقع فيه المجني عليه. يبرز أيضًا أهمية وجود رابطة سببية بين السلوك المادي للجاني والنتيجة المحققة بسبب هذا السلوك. في حال عدم وجود نتيجة بسبب السلوك، ينقطع الرابط السببي وقد لا يتم اكتمال مثلث الركن المادي للجريمة.

هذا التوجيه القانوني يعكس أهمية تحديد التسلسل الزمني والعلاقة السببية بين الأفعال والنتائج في سياق جرائم الاحتيال لتحقيق العدالة والقانونية في المسائل الجنائي من ثم إذا انعدمت طريقة الاحتيال ومع ذلك انخداع الشخص الآخر فإن الواقعة لا تعد احتيالاً عندئذٍ تنتفي العلاقة السببية متى ما ثبت أن تسليم المال لم يكن نتيجة للغش والخداع بل كان سبب آخر كالخوف والرهبة من الجاني [17].

وإن التسلسل الزمني في جرائم الاحتيال والتأكيد على أن تسليم المال يجب أن يتبع استخدام الحيلة أو الاحتيال. إذا تم تسليم المال قبل استعمال وسيلة الاحتيال، وكان ذلك قد تم بالترتيب وبرضا المجني عليه، يمكن أن يكون الوضع أقرب إلى جريمة مثل "خيانة الأمانة" بدلاً من جريمة الاحتيال.

وإن استخدام الحيلة والخداع هنا يكون بالنية الخفية لدى الجاني لتملك المال لنفسه أو لشخص آخر، وليس للضغط على المجني عليه لتسليم المال أو نقل حيازته. هذا يبرز أهمية تحديد النية والتفاصيل الدقيقة لتفاعلات الأطراف لتحديد طبيعة الجريمة والمسؤولية القانونية [11].

الفرع الثاني

الركن المعنوي لجريمة الاحتيال الإلكتروني (القصد الجرمي)

الركن المعنوي هو علم الجاني بالفعل الإجرامي أي الحالة النفسية له وكل ما يربط بين ماديات الجريمة وشخص الجاني، وإن جريمة الاحتيال الإلكتروني جريمة عمدية تستلزم توافر القصد الجزائي العام والقصد الجزائي الخاص، حيث يمكن تعريف الركن المعنوي بأنه: "ما يربط ماديات الجريمة وشخصية الجاني من علاقة والتي تعتبر محل الذنب في استحقاق العقاب، ثم يتم توجيه عقاب القانون ولومه".

الركن المعنوي يشير إلى الجانب الأخلاقي أو النية الخفية والدافع الخلفي للفعل الجنائي، وهو جزء أساسي في تحديد الطبيعة الكاملة للجريمة. في جرائم الاحتيال الإلكترونية، يعتبر التوافر الركن المعنوي أمرًا هامًا لتحديد السلوك المرتكب وتكييف العقوبات المناسبة.

بدون الركن المعنوي، يمكن أن يقتصر الأمر على جريمة الدخول أو الولوج غير المشروع دون تحديد الدوافع والأفكار التي دفعت الجاني للقيام بفعله. يساعد التركيز على الركن المعنوي في فهم النية والدوافع والسلوكيات الفعلية التي تميز جريمة الاحتيال الإلكترونية. لذا، تحديد الركن المعنوي يعزز فهم السلوك الجنائي بشكل أفضل ويسهم في تحديد العقوبات اللازمة بشكل أكثر دقة وفاعلية.

صحيح، توضح هذه المقارنة الفارق بين جريمة الدخول غير المشروع وجريمة تجاوز الصلاحيات في سياق نظام المعالجة الآلية للبيانات.

في جريمة الدخول غير المشروع، يقوم الجاني بالدخول إلى نظام معالجة البيانات دون وجود إذن أو صلاحية للقيام بذلك، بينما في جريمة تجاوز الصلاحيات، يكون الفاعل قد حصل على صلاحية للدخول إلى النظام، ولكنه يتجاوز هذه الصلاحية للوصول إلى أقسام أو أنظمة داخلية ليست من حقه الوصول إليها.

هذا التمييز يعكس التفاصيل الدقيقة التي يتعين على المحققين والقضاة فهمها لفهم الطبيعة الدقيقة للجريمة وتحديد المسؤولية بشكل دقيق [18].

وقد عرف المشرع العراقي القصد الجرمي في المادة 33 من قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل بأنه"" القصد الجرمي هو توجيه الفاعل إرادته الى ارتكاب الفعل المكون للجريمة هادفاً إلى نتيجة الجريمة التي وقعت أو أية نتيجة جرميه أخرى" [19].

من خلال التعريف السابق الذي قدمته حول القصد الجرمي والعنصرين الأساسيين (العلم والإرادة) يتفق مع المفاهيم القانونية العامة. في النظام القانوني، يُفهم العلم بأنه الوعي والإدراك من قبل الفاعل بأن تصرفه سيؤدي إلى نتيجة جرمية، والإرادة تعبر عن النية الحرة والمتعمدة للقيام بالفعل المتعلق بالجريمة.

فعندما يتحقق العلم والإرادة، يمكن اعتبار القصد الجرمي متوافرًا، وبالتالي يمكن معاقبة الجاني بناءً على العمد. وبالعمل بهذه النصوص القانونية، يتم إرساء أسس تحديد المسؤولية الجنائية بناءً على النية والإلمام بالعواقب الجنائية للأفعال.

إذا انتفى العلم بأحد هذه العناصر، يُنفى القصد الجنائي، لأنها تمثل العناصر التي تمد النشاط الإجرامي بالوصف القانوني، وبالتالي تميزه عن باقي الوقائع الإجرامية الأخرى. يرتبط العلم اليقيني بشكل وثيق بالواقعة الجنائية التي يقوم بها الجاني، ويُفترض من الجاني أن يكون على دراية بالقانون الذي يُعاقب على كل الجرائم مهما كان نوعها. والإرادة تُعد العنصر الثاني للقصد الجنائي بعد العلم، حيث تُعبّر عن القوة النفسية التي توجه أعضاء الجسم نحو تحقيق غرض غير مشروع. ومع اختيار الإرادة، ينتفي القصد الجنائي. وقد اتجه المشرع العراقي في قانون العقوبات العراقي نحو نظرية العلم والإرادة، وكان ذلك مسلكًا موفقاً وذكياً.

ولا يكتفي إرادة السلوك وحدها بتحقيق القصد في جريمة الاحتيال الإلكتروني، بل يتطلب أيضًا انصراف إرادة الجاني نحو النتيجة الجنائية، والتي تتمثل في الحصول على المال أو الفوائد. ويُعتبر ذلك تفرقة هامة بين القصد الجنائي والخطأ غير العمدي [20] وتكون النتيجة عمدية عندما تُمثل الغاية التي يسعى الجاني إلى تحقيقها بواسطة سلوكه، حيث تُعبِر عن النية التي دفعته للقيام بالفعل الإجرامي لتحقيق تلك الغاية.

والعلم كعنصر في الركن المعنوي للجريمة فإنه غالباً وإن لم يكن دائماً ما يسبق في وجوده على قيام عنصر الإرادة، فالجاني يوجه إرادته دائما إلى خدمة ما يزمع القيام به من فعل، أي أن النية تتوافر لديه في شكل علم بالجريمة والعناصر الأساسية لها، ثم تتولد إليه الإرادة لارتكاب الفعل المكون لهذه الجريمة، فالإرادة تعد هي المحرك لتنفيذ الفعل الذي يعلم بعدم مشروعيته وبأنه يشكل جريمة يعاقب عليها القانون.

المبحث الثاني

مدى حجية الأدلة الإلكترونية في الأثبات وسلطة القاضي الجنائي في قبول وتقدير الأدلة

تتصف جريمة الاحتيال الإلكترونية بكونها من الجرائم الإلكترونية صعبة الاكتشاف والإثبات في آن واحد وذلك لعدم وجود آثار مادية كالتي تشاهد في الجرائم التقليدية مستندات ورقية بصمات أموال أدوات الجريمة فهي جرائم تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الإلكترونية غير المرئية، ونلاحظ افتقار المحقق التقليدي للمهارات اللازمة بالتعامل مع هذا النوع من الجرائم القائمة على الخداع والتضليل وصعوبة إجراء غير مهم التحريات السرية [21].

كما إن المحقق قد يتسبب بدون قصد أو بطريق الخطأ في إتلاف الدليل الإلكتروني أو تدميره كمحوه من الأسطوانة الصلبة مثلاً وقد يتجاهل الدليل الرقمي ظناً من أنه غير مهم أو لا يقوم بمصادرة الجهاز المستخدم في الجريمة [22]. وتزداد المشكلة عند وجود الأدلة في أنظمة حواسيب تقع خارج سلطة التحقيق في دولة ثانية مثلاً الأمر الذي يتطلب الحصول على إذن أو طلب مساعدة قضائية من تلك الدولة. بناءً على ما تقدم سنتناول في هذا المبحث مدى حجية الأدلة الإلكترونية في الأثبات وسلطة القاضي الجنائي في قبول وتقدير الأدلة من خلال مطلبين، نتناول في المطلب الأول طبيعة الدليل الإلكتروني في إثبات جريمة الاحتيال الإلكتروني، بينما نبحث في المطلب الثاني إجراءات مكافحة الاحتيال الإلكتروني وعقوبته.

المطلب الأول

طبيعة الدليل الإلكتروني في إثبات جريمة الاحتيال الإلكتروني

إن الإثبات مشتق من ثبت الشيء ثبوتاً أي دام واستقر وعرف فمادة ثبت تتفيد المعرفة والبيان والدوام والاستقرار، وعلى هذا فالإثبات في اللغة معناه إقامة الحجة على ما وتعددت تعريفات الدليل الرقمي وتباينت بين مُوسع ومضيق لهذا التعريف ويرجع ذلك لموضع العلم الذي ينتمي إليه هذا الدليل فاختلفت التعريفات بين الباحثين في مجال التقنية وبين الباحثين في مجال القانون على النحو التالي:

الدليل الإلكتروني، أو الدليل الرقمي في بعض الأحيان، يمثل مجموعة من المعلومات التي يمكن قبولها من قبل المنطق والعقل. يتم الحصول على هذا الدليل من خلال إجراءات قانونية وعلمية، حيث يتم ترجمة البيانات الحسابية المخزنة في أجهزة الحاسوب وملحقاتها وشبكات الاتصال. يمكن استخدام هذا الدليل في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل مرتبط بجريمة، أو جاني، أو مجني عليه [23]. هو تلك المعلومات التي تم استحصالها من خلال شبكات الاتصال باستخدام إجراءات قانونية وتقنية، حيث يتم تحليلها علمياً وتفسيرها في شكل نصوص مكتوبة أو رسومات أو صور وأشكال وأصوات. يُقدم هذا الدليل للقضاء لإثبات وقوع الجريمة، سواءً كان لتقديم تقرير البراءة أو للإدانة، بعد إجراء التحليل العلمي [24].

لذا سوف نبحث هذا المطلب من خلال فرعين، نتناول في الفرع الأول طبيعة الدليل الإلكتروني في إثبات جريمة الاحتيال الإلكتروني، بينما نتناول في الفرع الثاني مدى سلطة القاضي الجنائي في قبول وتقدير الدليل الإلكتروني.

الفرع الأول

طبيعة الدليل الإلكتروني في إثبات جريمة الاحتيال الإلكتروني

بالطبع، يعد الدليل الإلكتروني هو نوع من الأدلة يتم استخراجه من الوسائل التقنية المتاحة في النظام المعلوماتي، ويختلف هذا الدليل تماماً عن الأدلة المادية التي قد تكون متاحة في مسرح الجريمة، يتميز الدليل الإلكتروني بتوفير تفاصيل دقيقة حول الأنشطة والتفاعلات على الشبكة، ويمكن أن يكون له تأثير كبير في عمليات التحقيق والمحاكمة.

وتعتبر أهمية الإثبات وتحديد طرقه من الأمور التي لا تخفى فهي واضحة وضوح الشمس في رابعة النهار لكونها تجعل صاحب الحق على بينة ومعرفة واطلاع فيما يجب عليه القيام به وبما يلزمه التمسك فيه أو إحضاره عند نشوء الحق ضماناً من الجحود وارتكاب هذا من جهة صاحب الحق المدعى، وأما من جهة المنكر فبدون إثبات ما ينسب إليه فهو برئ منه وأما من جهة القاضي فيكون على بصيرة تامة وعلى يقين كامل لحكمه من خلال نظره في هذه الأدلة وأعمالها وبهذا كله تكتمل المنظومة القضائية وتصل الحقوق إلى أصحابها كاملة غير منقوصة.

صحيح، الإثبات يشكل جزءًا أساسيًا من العدالة وتحقيق الحقوق في أي نظام قانوني. إن قوة الحق أو الالتزام يعتمد بشكل كبير على قدرة الطرف على إثبات ما يدعيه بوجود دليل يثبت صحة مطالباته. في غياب الأدلة أو الإثبات، يمكن أن يكون الحق أو الالتزام غير فعّال أو يفقد قيمته القانونية، ويتجرد الحق من دليله وعجز صاحبه عن إثباته يصبح عند المنازعة فيه والعدم سواء فالإثبات هو قيام الحق وبعبارة أكثر وضوحاً حيث لا إثبات فلا حق [25].

ولا شك أن الدليل الرقمي يُعد من الموضوعات ذات الحداثة التي تنتج عنها إشكالات قانونية في التعامل معه ومما لا جدال فيه أن الدليل الرقمي موضوع فرض نفسه لأنه مصاحب وملازم للتطور التكنولوجي في المعلومات، وبالتالي مسألة الاخذ به وقبوله في الإثبات الجنائي يثير العديد من الإشكاليات التي تحتاج البحث والدراسة والتمحيص للاعتماد عليه كوسيلة من وسائل الإثبات الجنائي.

صحيح، عملية الضبط أو التحريز في سياق النظم الرقمية والكمبيوترية لا تقتصر فقط على تحريز الأجهزة الفعلية (مثل أجهزة الكمبيوتر) بل تتضمن أيضًا التحريز والتحقق من المعلومات والبيانات المخزنة في هذه الأجهزة. يمكن أن يشمل ذلك تحديد البرمجيات والتطبيقات المستخدمة، ومتابعة تدفق البيانات، والبحث عن أدلة رقمية قد تكون ذات صلة بالجريمة أو الحادث المحتمل. يعتبر احترام الخصوصية وحقوق المستخدمين أمرًا حيويًا في عمليات الضبط المعلوماتي. يجب أن تتم هذه العمليات وفقًا للقوانين

واللوائح المعتمدة ومع مراعاة القوانين المتعلقة بحقوق الخصوصية. الجوانب القانونية والأخلاقية لعمليات الضبط وجمع الأدلة الرقمية هي جوانب حيوية في ضمان توجيه العدالة بشكل سليم وتجنب انتهاك حقوق الأفراد [26].

وفي سياق الجرائم الإلكترونية، يجب أن تتم عمليات التفتيش والضبط وفقًا للقوانين والأنظمة المعتمدة وباحترام حقوق الأفراد والمؤسسات. الأدلة المستحصلة يجب أن تتمتع بالوضوح والعقلانية والمشروعية لتكون قانونية وقابلة للاعتماد أمام القضاء [27]. والقضايا المتعلقة بقواعد الاختصاص القضائي تشكل تحديًا هامًا في مجال مكافحة الجرائم الإلكترونية، نظراً لأن هذه الجرائم يمكن أن تتسارع عبر الحدود بسهولة، يصبح تحديد الاختصاص القضائي أمرًا معقداً، يمكن أن يتطلب مكافحة هذه الجرائم تعاوناً دولياً فعّالاً لتحديد الجهة التي تتولى محاكمة الجناة وتطبيق القانون.

توجد محاولات لتطوير إطارات قانونية دولية تساعد في التعاون وتبادل المعلومات بين الدول للتعامل مع تلك التحديات. بعض الاتفاقيات والمعاهدات الدولية تهدف إلى تحديد قواعد الاختصاص القضائي وتسهيل تسليم الأدلة الرقمية بين الدول.

سلطة وحرية القاضي في تقدير الأدلة وفحص القضايا الجنائية. إذ يُظهر أن تقدير الدليل متروكٌ لمحكمة الموضوع، وعندما تقتنع بالدليل وتطمئن إليه، فإنه لا يوجد استئناف أو اعتراض على هذا القرار. القاضي يتمتع بسلطة واسعة وحرية كاملة في جمع الأدلة وتقدير قوة هذه الأدلة.

تؤكد هذه المقولة على حق القاضي في الاعتماد على الوسائل التي يجدها مناسبة للكشف عن الحقيقة وفهم تفاصيل الجريمة. السلطة الواسعة للقاضي في معالجة الدعاوى الجنائية تعكس أهمية توفير الحرية الكاملة للقاضي للوصول إلى العدالة. يظهر أيضاً أن القاضي ليس ملزماً باتباع أساليب محددة في قراراته، بل لديه حرية مطلقة في تقدير الوقائع وظروف القضية والاعتماد على الأدلة. يتعين عليه السعي جاهدًا لاكتساب فهم دقيق للحقيقة واتخاذ قرارات قائمة على أساس هذا الفهم.

يعبر هذا النص عن مبدأ أساسي في القانون الجنائي، حيث يُشير إلى أن قواعد الإثبات وضعت لتتناسب مع خصوصيات الجرائم الجنائية. يتعين على هذه القواعد أن تحقق مصلحة الجماعة وتكون عادلة، مما يشمل معاقبة كل جاني وتبرئة كل برئ، يُشير النص أيضًا إلى حق المحكمة في تقدير أدلة الدعوى وتكوين معتقدها. هذا يعني أن محكمة الموضوع (المحكمة التي تقوم بالنظر في القضية في المرحلة الأولية) لديها حق تقدير الأدلة بحرية، وليس من المسموح بالطعن في تقديراتها أمام محكمة التمييز. هذا يعكس مبدأ عدم جواز الطعن في قرارات المحكمة التي تقوم بالنظر في القضية للمرة الأولى، إلا إذا كان هناك خطأ قانوني واضح [28].

تحديات ومشكلات البُعد الإجرائي لمواجهة جرائم الكمبيوتر والإنترنت. يُسلط الضوء على عدة نقاط مهمة:

سرعة الكشف: الحاجة الملحة للكشف السريع عن الجرائم الإلكترونية لتفادي فقدان الدليل، والتحديات التي تواجه هذه العملية، خصوصية التفتيش والضبط: ضرورة ضمان توافق قواعد التفتيش والضبط مع خصوصية الأفراد والتحقق من ملائمتها لهذا النوع من الجرائم، قانونية وحجية الأدلة: أهمية التحقق من توافق الأدلة الرقمية مع القوانين والضوابط، وضرورة تأكيد قانونيتها وحجيتها، وتحديد اختصاص القضاء للتعامل مع جرائم قابلة للانتقال عبر الحدود، وكيفية التعاون بشكل فعال في هذا السياق.

التعاون الدولي: أهمية التعاون الدولي الشامل في التحقيق والملاحقة لمواجهة هذه الجرائم والتغلب على التحديات المرتبطة بالتحقيق خارج الحدود.

شير النص إلى أن تطوير الإجراءات القانونية والتعاون الدولي يعدان ذات أهمية كبيرة لمواجهة جرائم الكمبيوتر والإنترنت على المستويين الوطني والد وهذا كله إنما يذهب بنا إلى ضرورة مواكبة التطورات الإجرائية والحاجة إلى الخصوصية بالإجراء.

وهذا كله مرتبط بشكل عام بالمشروعية الإجرائية التي يجب توافرها وذلك كاستثناء سلبي على حرية القاضي في الاقتناع بالدليل ذلك أن الحرية في تكوين القناعة مقيدة بالمشروعية فلا يجوز للقاضي الحكم إلا بناءً على أدلة مشروعة [27].

بحيث يتطلب إقرار قواعد إجرائية خاصة وتشكيل أجهزة الضبط القضائي المختصة قانونياً وتقنياً بحيث تواكب القدرات المتعاظمة للإجرام الإلكتروني مع توفير كامل الإمكانيات المادية والتدريبية.

الفرع الثاني

مدى سلطة القاضي الجنائي في قبول وتقدير الدليل الإلكتروني

إن وسائل الأثبات الجزائية التي مكن للقاضي أن يستند إليها في تكوين قناعته غير محصورة، وذلك عملاً بالمبدأ القائل بحرية القاضي في تكوين قناعته التي تبنى على ما يرتاح إليه ضميره، واستناداً لما يطلع عليه من قبل أطراف الخصومة أو من خلال جهده الخاص ولكن ليس من معلوماته الشخصية [29].

وفي هذا الاطار يقوم مبدأ قناعة القاضي على استبعاد أي تدخل قانوني في تحديد الأدلة التي يستند إليها القاضي في حكمه وباب الأدلة مفتوح أمامه فهو يتمتع بالحرية المطلقة في تنقيب الأدلة وجمعها وتقديمها ومناقشتها، كما له الحرية في تقديرها فمدلول هذا المبدأ لا يقتصر على تقدير الأدلة المعروضة فقط وإنما يتسع ليشمل حرية الاستعانة بأي دليل يراه القاضي ضرورياً، ويزن قيمته على حدة لتكوين قناعته واستبعاد دليل لا يطمئن إليه والقانون لم يفرض على القاضي في سبيل تكوين قناعته طريقاً معيناً يعتمد عليه في الإثبات، فإنه فرض على القاضي أن يصدر حكمه عن اقتناع يقيني[30]. بصحة ما ينتهي به من وقائع ولا يمكن أن يبني هذا الاقتناع إلا بالوقوف على الحقيقة التي لا يمكن توافرها إلا باليقين التام لا مجرد الظن والاحتمال فإن قناعة القاضي الجزائي تكون مبنية على عنصرين أحدهما شخصي والآخر موضوعي:

فالعنصر الشخصي: يقوم على أدلة مقبولة عقلاً فحرية القاضي في تقدير الأدلة المعروضة مشروطة في أن عملية استنتاج القاضي لحقيقة الواقعة وما ينتج عنها من أدلة يجب أن تكون متناسبة مع مقتضيات العقل والمنطق، وأكدت المادة (212) من قانون أصول المحاكمات الجزائية العراقي على أن "لا يجوز للمحكمة أن تستد في الدعوى في حكمها إلى دليل لم يطرح للمناقشة أو لم يشير إليه في الجلسة ولا إلى ورقة قدمها أحد الخصوم دون أن يمكن باقي الخصوم من الاطلاع عليها، وليس للقاضي أن يحكم في الدعوى بناء على علمه الشخصي."

أما العنصر الموضوعي: هو ما يلجأ إليه القاضي لإصدار حكمه، لأن العنصر الشخصي يبقى عاجزاً لوحده عن بناء قناعة القاضي، مما دفع المشرع إلى إلزام القاضي بضرورة تعليل حكمه بحيث يقتضي تحديد الحجج المبني عليها والمنتجة له سواء من حيث الواقع أو من حيث القانون كما يجب أن يتضمن الحكم أدلة الأثبات وأن تكون متناسبة مع النتيجة التي توصل إليها الحكم.[31]

وأهم مبادئ الاقتناع القضائي تنطلق من صلاحيات القاضي الجزائي المتمثلة في قبول جميع الأدلة التي يقدمها أطراف الدعوى بحيث لا يوجد أدلة يحظر عليها القانون قبولها كما له الحق باستبعاد أي دليل لا يطمئن إليه وله بعد ذلك السلطة التقديرية الكاملة .

وفي استخلاص نتيجة منطقية تتمثل في حكم البراءة أو الإدانة وإن هذا المبدأ أقرت به أغلب التشريعات، وعليه سوف نطلع على موقف التشريع والفقه والقضاء لهذا المبدأ.

والإثبات هو كل ما يؤدى إلى كشف الحقيقة إما في معناه القانوني هو كل ما يؤدى إلى كشف الحقيقة وإقامة الدليل على وجود قاعدة قانونية تترتب آثارها أمام القضاء بالطرق التي حددها القانون وبعد الإثبات من أهم التحديات التي تواجه الأجهزة الأمنية ويزداد صعوبة في جريمة الاحتيال الإلكتروني بصفة عامة، لأن اكتشافها ليس بالسهل بل وحتى عند اكتشاف الجريمة والإبلاغ عنها يتبقى عبء الإثبات والذي يكون به العديد من الصعوبات فجريمة الاحتيال الإلكتروني تتم في بيئة غير تقليدية لأنها تقع في إطار غير ملموس نظراً لأن أركانها تقوم بين بيئة حاسب آلي أو جهاز الكرتوني تقني أو استخدام الإنترنت مما يزيد من الصعوبات التي تواجه رجال الضبط، وذلك لأن العمل في هذه البيئة تكون فيها البيانات والمعلومات عبارة عن نبضات الكرتونية ترسل عبر نظام الكرتوني مما يسهل من محو الأدلة الإلكترونية من قبل الجاني .[27]

يشير إلى أن بعض العناصر يمكن تتبعها بسهولة، حتى بواسطة المستخدمين العاديين، مما يتيح للمجرمين تحديد معلومات المستخدم، كما إن بعض المعلومات قد تكون متاحة لأي شخص يرغب في تتبع تحركات المجرم، سواء كانوا متخصصين أو غير متخصصين، وإن أجهزة المجرمين قد تحتفظ بملفات تسجيل للمواقع التي دخلوها، مما يمكن من تتبع نشاطاتهم، وإن المجرمين المتخصصين يقومون بمحو آثارهم بشكل أفضل، ويتجنبون التتبع باستخدام طرق متقدمة مثل مسح الملفات وإخفاء الهوية، كما إن التتبع يمكن أن يكون تحدياً لاكتشاف المجرمين، خاصةً الذين يعملون بمستوى عالٍ من التخصص.

النص يبرز التوازن الدقيق بين سهولة تتبع المجرمين وتحديات اكتشاف المجرمين المتقدمين في عالم الجرائم الإلكترونية.[3]

لكن صعوبات كشف هوية صاحب الحساب الوهمي أو المحتال موجودة كذلك في العراق كما يؤكد الخبير بعض الخبراء في هذا المجال أنه: "يتم استعمال IP أي "عنوان رقمي" مشترك لأكثر من مئة شخص وحتى لو تم تحديد العنوان الرقمي لا يمكن معرفة الشخص صاحب الحساب الوهمي أو المحتال وتصبح مهمة كشف هوية هذا الشخص مستحيلة عندما يكون خارج العراق.[3]

وتحاول مختلف الدول والشركات المقدمة لخدمات الإنترنت التغلب على هذه الاختراقات عبر برامج خاصة أحياناً وغير رموز أخرى غير رمز (IP) ومن أهمها Internet service provider (ISP) الذي يقوم بدور مشابه تقريبا لدور (IP) بل وربما أكثر تخصصاً وهذا يتطلب عند محاولة الاستفادة منه لغايات التحري تعاوناً من مزودي الخدمة لأن هذه الرموز تخص مزود الخدمة يتعرف من خلالها على هوية المتصلين عبر خطوطهم .

وزيادة على ذلك يعمل عنوان (IP) بشكل متزامن مع بروتوكول آخر وهو بروتوكول التحكم بالنقل Transmission Control / Protocol (TCP)والذي تكمن وظيفته في تقسيم المعلومات إلى حزم معلوماتية، ويقوم بروتوكول (IP) بعنونة كل حزمة مع إضافة معلومات أخرى ومنه يتم استخدام عنوان (IP) من خلال البحث عن رقم الجهاز وتحديد موقعه الجغرافي بالإضافة إلى إمكانية مراقبة المستخدم من طرف مزود خدمة الإنترنت وتقديم المعلومات التي تفيد في التحقيق بناءً على أن لكل جهاز حاسب آلي يتصل بالإنترنت عنوان (IP) خاص به.

يتحدث النص عن أهمية معرفة مكان الجريمة في حالات الجرائم الإلكترونية، يؤكد على أن المعرفة بمسرح الجريمة تلعب دوراً حيوياً في تحديد وتتبع الجريمة ومرتكبيها. يُشير إلى أن المسرح المعنوي للجريمة المعلوماتية يختلف عن المسرح المادي، حيث يتضح من خلال عنوان الـIP ونوع الجهاز المستخدم. يُبرز أيضًا أن تحديد موقع شخص عبر الشبكة يمكن أن يكون عن طريق ترك آثار معنوية، مثل عنوان الIP الدائم ونوع الجهاز. [28].

المطلب الثاني

إجراءات مكافحة الاحتيال الإلكتروني وعقوبته

إن مكافحة جرائم الاحتيال عملية تستهدف حماية المجتمع من الأنشطة التي يمارسها المحتالون بوسائلهم الخداعية فهم يتعرضون لأموال الأفراد والمؤسسات، ويستحوذون عليها دون وجه حق، وإن أهمية مكافحة هذه الجرائم تتجسد في أن هذه الجرائم ترتكب بأساليب يفترض فيها أنها تقوم على أسس سليمة في التعامل مع الآخرين.

إذ إنها تتعرض إلى حسن النية والثقة المفترضة وإلى العلاقة الإنسانية المطلوبة في تنفيذ الالتزامات فتأتي هذه الجرائم لتقويض دعائم المعاملات بين الأفراد وتشل حركتهم في أدائها مما يحجم أنشطتهم، إضافة إلى تعرضهم للخسارة المالية نتيجة تسليم أموالهم إلى المحتالين دون مقابل وتتضخم أضرارها في العلائق التجارية الدولية والبيوع البحرية والالتزامات الأطراف عندما يكونون في أكثر من دولة. وفي ضوء ذلك سنتناول إجراءات مكافحة الاحتيال الإلكتروني وعقوبته من خلال فرعين، حيث نبحث في الفرع الأول إجراءات مكافحة الاحتيال، أما الفرع الثاني نتناول فيه عقوبة الاحتيال الإلكتروني.

الفرع الأول

إجراءات مكافحة جريمة الاحتيال

إن الأمن الداخلي لأية دولة في العالم لم يعد في الوقت الراهن مرتبطاً بعوامل ومتغيرات داخلية وخصوصاً في ظل كثافة التداخل والترابط بين ما هو داخلي وما هو خارجي في العالم اليوم، إذ لم يعد في مقدور أية دولة في العالم أن تنزل نفسها عن التأثيرات الخارجية سواء الإيجابية أو السلبية، ومن أجل تحقيق الأمن لا بد من مكافحة جريمة الاحتيال الإلكتروني من خلال التحدث عن وسائل تفعيل المكافحة التالية:

1- التقنيات الحديثة: يتم التصدي للجريمة الإلكترونية، وبخاصة الاحتيال الإلكتروني، من قبل القوى الأمنية باستخدام تقنيات وأساليب متقدمة. تشمل هذه الجهود تنظيم دوريات إلكترونية لمراقبة الإنترنت ومنع وتصفية المواقع والإعلانات المشبوهة المتعلقة بالاحتيال والتضليل. تتم هذه الجهود بالتنسيق مع الجهات المختصة. ومع ذلك، تظل مكافحة الجرائم الإلكترونية التي ترتكب خارج حدود الدولة

وتتسع آثارها إلى الداخل تحدياً، حيث تواجه الشرطة صعوبات في عمليات البحث والتحقيق، يتم التغلب على هذه التحديات من خلال التعاون المشترك مع الإنتربول الدولي وأجهزة الأمن في مختلف الدول، بهدف تقليل مخاطر هذه الجرائم [32].

2- دور التشريعات: يعد البريد الإلكتروني المزعج أو غير المرغوب فيه (الأعمال العشوائية) من الأعمال غير المشروعة قانوناً، وتعرض صاحبها للمساءلة القانونية، فمن خلال تحليل عينات عشوائية لرسائل البريد الإلكتروني المزعج أو غير المرغوب فيه (Spam)، تبين أن ثلث هذه الرسائل تحتوي على معلومات غير صحيحة بشكل أو بآخر، وبذلك يمكن اعتبارها نوعاً من الأنواع الاحتيالية. وقد أكدت لجنة التجارة الفيدرالية (trade commission federal) (FTC) على عدم مشروعية البريد الإلكتروني المزعج أو غير المرغوب فيه، وأنه يعد من الناحية القانونية نوعاً من أنواع الاحتيال، سن المشرع في التشريعات المقارنة قوانين لمواجهة هذه الظاهرة عاداً إياها عملاً إجرامياً يتعدى مجرد السلوك غير المشروع لما يسببه من إتلاف برنامج عمل الإنترنت.

3- التدريب التقني: يبدو أن مفهوم الأمن قد تغير تماماً عن مفهومه التقليدي السابق إذ ظهر مصطلح جديد يسمى الأمن الرقمي وأصبح أكثر تجمع لتكنولوجيات الحديثة والكمبيوتر لتعقب المجرمين وحفظ النظام. ومن أهم العوامل التي تنهض بالأنشطة المختلفة في الدولة والأسلوب التدريجي هو الطريقة أو المنهج الذي يستخدمه المدرب لكي ينقل المادة أو الموضوع التدريجي إلى المتدربين وهو الذي يمنح الحياة للبرنامج التدريبي أو يؤدي إلى تجميده أو فشله وهناك العديد من الاعتبارات التي يتوقف عليها اختيار الأسلوب التدريبي يذكر منها [38].

أ- يجب أن تتناسب وسيلة التدريب والمحتوى التعليمي ليكونا ملائمين لكل فئة من الفئات ولكل مستوى منهما.

ب- إن اختيار الوسيلة التدريبية يجب أن يتوقف على قدرة الوسيلة في إحداث التلبية المناسبة للقدر المطلوب في الاحتياجات التدريبية بشكل يعاون المتدرب على التطور والتغير في مواجهة المشكلة.

ج- يجب مراعاة تكلفة الوسيلة مقارنة بالعائد المتوقع أو إمكانيات المنظمة المالية لمخصصات التدريب، وكذلك فترة التدريب، ومراعاة ميول المتدربين واتجاهاتهم.

من أهم الأسباب التدريبية المتبعة، أسلوب المحاضرة أو المناقشة ودراسة الحالة وأسلوب تأدية

الأدوار والمباريات الإدارية وأسلوب تدريب الحساسية، وأسلوب العوامل التدريبية، وإزاء هذا كله، لا بد من تنفيذ العقوبات المقررة لهذه الجريمة.

الفرع الثاني

عقوبة جريمة الاحتيال الإلكتروني في العراق

على الرغم من انتشار استخدام الكمبيوترات في العراق ودخول شبكة الأنترنت وانتشارها وإعطاء الصلاحية للأفراد باستعمالها إلا إن القانون العراقي لم يبحث أثر استخدامها إذ إن نصوص الدستور العراقي والتشريعات الجزائية ليست كافية في توفير الحماية اللازمة في مواجهة الاحتيال المعلوماتي إذ ليس هناك قانون خاص بهذا الشأن، إلا أن هناك مشروع قانون للجرائم الإلكترونية يخص كل من قدم معلومات أو بيانات الكرتونية كاذبة إلى السلطات القضائية أو الإدارية مع علمه بعدم صحتها.

وتنص المادة (456) من تقنين العقوبات العراقي على أنّه " يعاقب بالحبس كل من توصل إلى تسلم أو نقل حيازة مال منقول مملوك للغير لنفسه أو إلى شخص أخر وذلك بإحدى الوسائل التالية باستعمال طرق احتيالية وباتخاذ اسم كاذب أو صفة غير صحيحة أو تقرير أمر كاذب عن واقعة معينة متى كان من شأن ذلك خداع المجني عليه وحمله على التسليم.

يعاقب بنفس العقوبة كل من يقوم بالوسائل المذكورة سابقًا، سواء كان بحمل شخص آخر على تسليم أو نقل حيازة سند موجود لديه، أو تصرف في مال أو إبراء أو أي سند آخر يمكن استخدامه لإثبات حقوق الملكية أو حقوق عينية أخرى. كما يُعاقب كل من يقوم بأي من الوسائل المشار إليها أعلاه، سواء كان بحمل شخص آخر على توقيع مثل هذا السند، أو إلغائه، أو إتلافه، أو تعديله، كما صدر قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم (78) لعام 2012 [33]. حيث قام هذا القانون بتوفير الشكل القانوني للقيام باستعمال الوسائل الإلكترونية في أجراء المعاملات الإلكترونية.

ومن حيث المواجهة التشريعية لهذه الجرائم صدر قانون منع إساءة أجهزة الاتصالات في إقليم كوردستان رقم (6) لعام 2008[34]. حيث قام المشرع في الإقليم بالإشارة إلى أنه في حال أدت هذه الأفعال المجرمة إلى ارتكاب جريمة فيعد هذا المتسبب فيها شريكاً، كما يعاقب بالعقوبة ذاتها

التي تقرر للجاني.

الخاتمة

نعم، صحيح أن العالم يشهد حالياً ثورة معلوماتية هائلة نتيجة اندماج تكنولوجيا المعلومات والاتصالات. هذا التطور قاد إلى تحولات كبيرة في مختلف جوانب الحياة، بدءًا من التواصل الاجتماعي وانتهاءً بالأعمال التجارية والطب والتعليم، ونتيجة لبروز التطور التقني المتمثل في ظهور الكومبيوتر وشبكة الإنترنت فقد وجدت أشكال جديدة للجريمة لم تكن معروفة سابقاً إزاء ذلك تصدت العديد من التشريعات الجزائية في قسم من دول العالم إلى هذا النوع من الجرائم سواء أكان ذلك في نطاق قانون العقوبات أم في تشريعات خاصة.

صحيح، الجريمة هي ظاهرة اجتماعية معقدة تتأثر بعوامل متعددة وتتفاعل معها. يمكن أن تكون الجريمة ناتجة عن عوامل داخلية متعلقة بالفرد نفسه، مثل الخلفية الاجتماعية، والظروف الاقتصادية، والتعليم، والصحة النفسية. في حين تلعب العوامل الخارجية، مثل الظروف الاقتصادية والاجتماعية، والبيئة، دورًا أيضًا في تشكيل الظاهرة الجرمية.

وإن تطور التكنولوجيا وظهور التحديات الجديدة تتطلب تحديث وتعديل التشريعات لمواكبة التطورات في عالم الجريمة، وخاصةً في مجال جرائم الاحتيال الإلكتروني. إصدار قوانين جديدة أو تعديل القوانين القائمة يمكن أن يوفر إطاراً قانونياً أكثر فعالية لمكافحة هذا النوع من الجرائم وحماية المعلومات الشخصية والأصول الرقمية.

يشمل التدخل التشريعي في بعض الأحيان تعديل تصنيف الجرائم وتحديد العقوبات المناسبة، بالإضافة إلى توفير تعريفات واضحة للجرائم الإلكترونية. يمكن أيضًا أن يتضمن القانون تحديد الإجراءات القانونية والتقنية التي يمكن اتخاذها لتحقيق العدالة في حالات الجريمة الإلكترونية.

وعلى الرغم من حملات التوعية المتعلقة بمختلف الوسائل الإعلامية حول هذا النوع من جرائم الاحتيال إلا إن العديد من الضحايا مازالوا يقعون في شرك عصابات الاحتيال الإلكتروني طمعاً بالحصول على المكتسبات وإن عدم وجود تشريع جزائي موحد يجرم هذا النوع من الجرائم سوف يؤدي إلى المزيد من وقوع الأشخاص ضحايا هذا النوع من الجرائم. ويمكن إجمال النتائج والتوصيات التي تم التوصل إليها من خلال المبحث على النحو الاتي:

أولاً: الاستنتاجات

1 _ يظهر تزايد حالات الاحتيال الإلكتروني في العراق أهمية ضرورة تحديث وتعزيز التشريعات المتعلقة بمكافحة هذه الجريمة، ويجب أن تكون القوانين قادرة على مواكبة التطورات التكنولوجية وتوفير أساس قانوني قوي لمحاربة الجرائم الإلكترونية.

2_توفير تدريب للكوادر القانونية والتنفيذية حيث يجب تعزيز التدريب للمحققين والقضاة والمدعين العامين لتعزيز فهمهم للجوانب التقنية والقانونية المتعلقة بالجرائم الإلكترونية.

3- حداثة "قانون الجرائم الإلكترونية" وصعوبة متابعة تطور أساليب ارتكابها وغياب أساليب التحقيق وندرة مساحات التوعية والتثقيف حول هذه الجرائم لقطاع مستخدمي الإنترنت.

4_ يجب تعزيز التعاون مع الجهات الدولية لمكافحة الجرائم الإلكترونية، حيث يعبر الاحتيال الإلكتروني عن تهديد دولي يتطلب جهود مشتركة.

ثانياً: المقترحات

1- تعديل القوانين لتشديد العقوبات على مرتكبي جرائم الاحتيال الإلكتروني بما يتناسب مع خطورة الجرائم، إضافةً إلى فرض عقوبات مالية وجنائية تكون رادعة وتتناسب مع حجم الأضرار الناتجة عن الاحتيال.

2- إصدار قوانين تتعلق بالتجارة الإلكترونية وحماية المعلومات الشخصية على جميع وسائل التواصل الاجتماعي.

3- نظراً لكون جرائم الأنترنت قد بدأت تدخل العراق وان قانون العقوبات العراقي لم يتطرق اليها مما يجعل مرتكبيها في منأى من العقاب، لذا ينبغي أن يعالجها المشرع في فصل خاص في قانون العقوبات باسم جرائم الحاسوب والأنترنت يتضمن النصوص القانونية اللازمة لحماية مواقع الأنترنت ونقل البيانات والمعلومات عبر شبكة الأنترنت وذلك بمعاقبة كل فعل غير مشروع من قبل المستخدمين سواء أكانوا أشخاص طبيعية أو معنوية أو مقدمي خدمات الأنترنت.

4_ يمكن تحقيق تحسين في رصد ومكافحة الجرائم الإلكترونية من خلال تعزيز التعاون مع شركات تقديم الخدمات الإلكترونية وتشجيعها على تعزيز الأمان في خدماته

قائمة المصادر والمراجع

أولاً: الكتب

[1] فاروق محمد الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الأنترنت، الدار الجامعية للنشر، بيروت، 2008.
[2] أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2005.
[3] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، القاهرة، 2009.
[4] هيثم حمود الشلبي، إدارة مخاطر الاحتيال في قطاع الاتصالات، الطبعة الأولى، دار صفاء للنشر والتوزيع، عمان، الأردن، 2009.
[5] نائلة عادل محمد فريد قورة، جرائم الحاسوب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2005.
[6] جميل عبد الباقي الصغير، الأنترنت والقانون الجنائي، دار الفكر العربي، مصر، 2009.
[7] نهلا عبد القادر المومني، الجرائم المعلوماتية، ط1، دار الثقافة للنشر والتوزيع، عمان، 2008.
[8] أسامة أحمد المناعسة، جلال الزعبي، صايل فاضل الهواوشة، جرائم الحاسب الالي والأنترنت، دراسة تحليلية مقارنة، دار وائل للنشر، عمان، 2010.
[9] علي محمد جعفر، قانون العقوبات القسم الخاص، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، 2006.
[10] . سمير عالية، القانون الجزائي للأعمال، الطبعة الثانية، منشورات الحلبي الحقوقية، بيروت، 2018.
[11] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، 2007.
[12] عباس العبودي، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها، الطبعة الأولى، مطبعة الوئام للحاسبات والطباعة والنشر، بابل، 2009.
[13] عمار عباس الحسيني، التحقيق الجنائي والوسائل الحديثة في كشف الجريمة، منشورات الحلبي الحقوقية، بيروت، 2013.
[14] علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنيت، عالم الكتب الحديث، الأردن، 2004.
[15] حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، منشورات الحلبي الحقوقية، بيروت،
[16] 2014.
[17] محمد عبد الرؤوف الخن، جريمة الاحتيال عبر الإنترنت، منشورات الحلبي الحقوقية، بيروت، 2015.
[18] رمزي رياض عوض، سلطة القاضي في تقدير الأدلة، دار النهضة العربية، مصر، 2010.
[19] . عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، مصر، 2012.
[20] نص المادة 33 من قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل.
[21] فخري عبد الرزاق الحديثي، شرح قانون العقوبات – القسم العام، دار الثقافة للنشر والتوزيع، عمان، 2010.
[22] يوسف حسن يوسف، الجرائم الدولية للإنترنت، ط 1، المركز القومي للإصدارات القانونية، القاهرة،2011، ص 21.

[23] خالد ممدوح إبراهيم، التقاضي الإلكتروني، ط1، دار الفكر الجامعي، القاهرة، 2002.
[24] . مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، الملتقى المصري للأبداع والتنمية، مصر، 2001.
[25] محمد الأمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف للعلوم الأمنية، الرياض، 2002.
[26] عبد الثبور عبد القوى، الجريمة الإلكترونية، دار العلوم للنشر، القاهرة، 2010.
[27] يونس عرب، جرائم الكومبيوتر والأنترنت، اتحاد المصارف العربية، 2001.
[28] أحمد ضياء الدين محمد، مشروعية الدليل في المواد الجنائية، دار النهضة العربية، مصر، 2010.
[29] أحمد محمد البوشي، الابتزاز الإلكتروني مفهوم جديد في جرائم التهديد المعلوماتية، دار النهضة العربية، مصر، 2022.
[30] محمد زكي أبو عامر، الأثبات في المواد الجنائية، دار الجامعة الجديدة، الإسكندرية, 2005.
[31] سمير عالية، الموسوعة الحديثة للاجتهادات الجزائية العليا في قانون العقوبات والأصول الجزائية، المجلد الأول، منشورات الحلبي الحقوقية، بيروت, 2017.
[32] كامل السعيد، أصول المحاكمات الجزائية، دار الثقافة، عمان, 2005.
[33] . محمد سامي قاسم، جريمة الاحتيال عبر البريد الإلكتروني، رسالة ماجستير في القانون العام مقدمة للجامعة الإسلامية في لبنان, 2019.
[34] قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي رقم (78) لسنة (2012).
[35] نص المادة (4)، من قانون منع إساءة استعمال أجهزة الاتصالات في إقليم كوردستان العراق رقم 6 لسنة 2008.