بحث بعنوان

جرائم الإحتيال المعلوماتي وصعوبة إثباتها

الباحث

علاء ناصر جبريل علي

دارس الدكتوراه في القانون

كلية الحقوق

جامعة أسوان

ملخص الدراسة:

يتسم الإثبات في جرائم الاحتيال المعلوماتي عموماً بالدقة والتعقيد، حيث تحيط به صعوبات كثيرة، حيث أكد خبراء الحاسوب والإنترنت وجود عجز تشريعي يعيق مواجهة هذه الجرائم بشكل فعال، خاصةً في ظل تزايد تعقيدها وتطورها. فبرامج التأمين الإلكتروني والحماية، رغم تنوعها وتقدمها، لم تعد كافية لضمان الأمن والحماية في ظل اتساع نطاق الشبكة العنكبوتية. وتبرز أهمية قواعد الإثبات في هذا السياق، إذ أن الإثبات هو جوهر التقاضي، ويصبح بلا قيمة إذا لم يتمكن من إثبات الواقعة التي يستند إليها. فالدليل هو عماد الحياة القضائية والغاية منها.

وتكمن صعوبة إثبات جرائم الاحتيال المعلوماتي في أنها غالبًا لا تترك أثرًا ماديًا يُسهل كشف الجناة، كما أنها تتطلب حداثة تقنية وتطورًا فنيًا قد لا يتوفر لدى جهات التحقيق التقليدية. وتعتمد هذه الجرائم بشكل أساسي على الذكاء والمهارة في ارتكابها، مما يجعل الاحتفاظ بآثارها الفنية أمرًا بالغ الصعوبة. ومن أبرز التحديات في هذا المجال صعوبة فك تشفير البيانات المخزنة إلكترونيًا أو على الإنترنت، مما يعيق الحصول على أدلة جنائية قاطعة.

إضافة إلى ذلك، فإن الطبيعة العالمية لهذه الجرائم تثير إشكالات تتعلق بتحديد الولاية القضائية المكانية والقانون الوطني الواجب التطبيق، خاصة في الحالات التي ترتكب خارج النطاق الإقليمي للدولة. وهذا يجعل قضية الملاحقة الجنائية لهذه الجرائم أكثر تعقيدًا.

لذلك، يتطلب استكشاف هذا النوع من الجرائم وتتبعها أساليب إلكترونية وفنية متطورة تتناسب مع طبيعتها المعقدة. ويشمل ذلك القدرة على فك تشفير كلمات المرور السرية، وترجمة الإشارات الإلكترونية إلى بيانات قابلة للقراءة، وإثبات الأدلة الرقمية بشكل يمكن الاعتماد عليه في الإجراءات القضائية. كل ذلك يهدف إلى كشف الحقيقة وتمكين الملاحقة الجنائية الفعالة لمرتكبي جرائم الاحتيال المعلوماتي .

الكلمات المفتاحية: الجرائم المعلوماتية– الأدلة الرقمية – الاحتيال المعلوماتي

Abstract:

Proof of cyber fraud crimes is generally characterized by subtlety and complexity, and is fraught with difficulties.

Computer and internet experts have confirmed the existence of a legislative deficiency that hinders effective combating of these crimes, especially given their increasing complexity and sophistication. Cybersecurity and protection programs, despite their diversity and advancements, are no longer sufficient to ensure security and protection in light of the expanding scope of the internet. The importance of the rules of evidence is highlighted in this context, as proof is the essence of litigation and becomes worthless if it cannot prove the underlying fact. Evidence is the foundation and purpose of judicial life.

The difficulty of proving cyber fraud crimes lies in the fact that they often leave no physical trace that would facilitate the identification of perpetrators. They also require technological innovation and technical sophistication that may not be available to traditional investigative bodies. These crimes rely primarily on intelligence and skill in their commission, making it extremely difficult to preserve their technical traces. One of the most prominent challenges in this area is the difficulty of decrypting data stored electronically or online, which hinders the acquisition of conclusive criminal evidence. In addition, the global nature of these crimes raises issues related to determining territorial jurisdiction and applicable national law, especially in cases committed outside the territorial limits of a state. This makes the criminal prosecution of these crimes even more complex. Therefore, detecting and tracking these types of crimes requires advanced electronic and technical methods commensurate with their complex nature. This includes the ability to decrypt passwords, translate electronic signals into readable data, and reliably present digital evidence in judicial proceedings. All of this aims to uncover the truth and enable the effective criminal prosecution of perpetrators of cybercrime.

Keywords: Cybercrimes - Digital Evidence - Cyber Fraud

مشكلة الدراسة:

تتمثل الإشكالية الرئيسية في هذا الموضوع في اختلاف إثبات جرائم الاحتيال المعلوماتي عن الجرائم التقليدية، وذلك من حيث طبيعة البيانات المُدخلة في أجهزة الحاسوب وكيفية إثباتها. فإثبات جرائم الاحتيال المعلوماتي يتطلب التعامل مع كميات هائلة من البيانات الرقمية، بالإضافة إلى تحديد الوسائل الفنية اللازمة لإثباتها، سواء من حيث الأدوات المستخدمة أو الجهات المختصة بالتحقيق. وهنا تبرز مشكلة رئيسية، وهي أن الأجهزة التقليدية غالبًا ما تفتقر إلى الخبرة والتقنيات اللازمة للتعامل مع هذا النوع من الجرائم، مما يعيق عملية التحقيق ويُضعف فاعليتها.

ويُضاف إلى ذلك أن المجرم المعلوماتي يتميز عادةً بدرجة عالية من الذكاء، حيث يستخدم أعلى مستويات المهارة في التعامل مع الحاسوب والأجهزة الإلكترونية الحديثة. بل إن بعض المجرمين ينظرون إلى هذه الأفعال على أنها "فن" أو "هواية" وليس مجرد جريمة، مما يجعل اكتشاف جرائمهم وإثباتها أمرًا بالغ الصعوبة. وتتعدد الصعوبات التي تعترض سبيل إثبات هذه الجرائم، حيث يصعب اكتشافها بسبب سهولة ارتكابها وإخفاء آثارها، كما أن طبيعتها الرقمية تجعلها لا تترك أثرًا خارجيًا يُسهل تتبعه.

هذه الطبيعة الفريدة لهذه الجرائم تثير العديد من التساؤلات، التي يتناولها هذا البحث .

أهداف الدراسة:

يتمثل الهدف الرئيسي للدراسة الحالية في بيان المعوقات التي تواجه الإثبات الجنائي في الجرائم المعلوماتية، ويتفرع من هذا عدة أهدف كالآتي:

١) تحديد الطرق المستخدمة في الاحتيال المعلوماتي والكشف عنها.
١) بيان الصعوبات التي تواجه التحقيق والاثبات الجنائي في الاحتيال المعلوماتي.
٢) بيان سبل مكافحة تلك الجريمة والمؤثرات الطارئة عليها.

تساؤلات الدراسة:

تسعى الدراسة إلى الإجابة على التساؤلات التالية:

أولاً : مدى إمكانية استخدام طرق الإثبات التقليدية في إثبات جرائم الاحتيال المعلوماتي: هل يمكن الاعتماد على الأساليب التقليدية في التحقيق والإثبات، أم أن هذه الجرائم تتطلب أدوات ومنهجيات خاصة؟

ثانياً : حجية الدليل الرقمي في الإثبات الجنائي الإلكتروني: ما هي القيمة القانونية للأدلة الرقمية، وهل يمكن الاعتماد عليها كأدلة قاطعة في المحاكم؟

ثالثاً : معوقات تطبيق قواعد القانون الجنائي من حيث المكان في جرائم الاحتيال المعلوماتي: ما هي التحديات التي تواجه تحديد الولاية القضائية في الجرائم التي تُرتكب عبر الحدود، وما هي شروط قبول الدليل الرقمي كدليل إثبات جنائي؟

رابعاً : سبل مكافحة الاحتيال المعلوماتي وتأثير العولمة عليها: كيف يمكن تطوير آليات فعالة لمكافحة هذه الجرائم في ظل الطبيعة العالمية للإنترنت، وما هو تأثير العولمة على انتشارها وتعقيدها؟

أهمية الدراسة:

تستمد هذه الدراسة أهميتها من الأهمية البالغة لمعرفة المعوقات التي تواجه الإثبات الجنائي في جرائم الاحتيال المعلوماتي، والتي تُعد من القضايا الشائكة التي تثير جدلًا واسعًا بين فقهاء القانون الجنائي. كما أن الموضوع يرتبط ارتباطًا وثيقًا بالتكنولوجيا الحديثة، التي تتطور بوتيرة سريعة، مما يؤدي إلى تطور أساليب ارتكاب هذه الجرائم بشكل متوازٍ. هذا التطور التكنولوجي المستمر يشكل تحديًا كبيرًا أمام القائمين على التحقيق والإثبات، حيث يتطلب منهم مواكبة التقنيات الحديثة وتطوير أدواتهم وأساليبهم لمواجهة هذه الجرائم المتطورة.

الدراسات السابقة:

هناك العديد من الدراسات القانونية السابقة التي عالجت نفس موضوع الأطروحة الحالية، ومنها رسائل دكتوراه ورسائل ماجستير منها التالي :

١. **الحماية الجنائية الاجرائية لمواجهة جرائم شبكة المعلومات الدولية، للدكتور أحمد احمد محمد سيد احمد – رسالة دكتوراه – كلية الحقوق – جامعة المنصورة – ٢٠٢٤.**

قسم الباحث دراسته إلى قسمين رئيسين:

القسم الأول: المفهوم العام لشبكة المعلومات الدولية حيث تناول الباحث في القسم الأول مفهوم الشبكة المعلوماتية كما أوضح أنها أداة لتخزين المعرفة ووسيلة لتدفق المعلومات، فإنها أيضاً تُعَدْ أيضًا أداة رفيعة المستوى لارتكاب الجرائم، ففي هذه البيئة الضخمة المزدحمة تضعف قبضة الأمن والمراقبة والتحكم، وتزهر عمليات التجسس على المعلومات المعالجة إلكترونيًا وسرقتها وحيازتها بالاحتيال، حتى أنها تُشكَّل تهديدًا بالغًا لسائر المؤسسات الحكومية التي تعتمد أعمالها على الحاسبات والشبكات الإتصالية، وترتفع مخاطر إساءة استخدام الحاسبات والتلاعب في البرامج وملفات المعلومات المخزنة آليًا بقصد الحصول على أموال أو أصول أو خدمات غير مستحقة، وتتيح حرية نسخ البرامج وتداولها من خلال غير طريق منتجها الأصلي مجالًا واسعًا لدس الفيروسات المعلوماتية التي لا تلبث أن تتفشى وتصيب الأنظمة والشبكات بأنواع ودرجات مختلفة من العطب والضرر، وتأخذ أشكال مختلفة كأهداف لعمليات التخريب والاحتيال المعلوماتي.

والقسم الثاني: وفيه أظهر أن الجاهزية التقنية والتشريعية والأدائية (استراتيجيات حماية المعلومات والإتصالات) لمواجهتها ليست بالمستوى المطلوب إن لم تكن غائبة تمامًا، وبالمقابل فقد أمست جرائم شبكة المعلومات من أخطر الجرائم التي ترتكب في الدول المتقدمة، تحديدًا الأمريكية والأوربية، ولهذا تزايدات خطط مكافحة هذه الجرائم وأنصبت الجهود على دراستها المتعمقة، وخلق آليات قانونية للحماية من أخطارها، وبرز

في هذا المجال المنظمات الدولية والإقليمية، وإدراكًا لقصور القوانين الجنائية بشقيها الموضوعي والإجرائي بما تتضمنه من نصوص التجريم التقليدية كان لابد على الدول من وضع قوانين خاصة في ضوء إتفاقاتها الدولية والإقليمية، أو العمل على تعديل قوانينها الداخلية من أجل ضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم، وأظهر تحليل الجهود الدولية وإتجاهات القانون المقارن بشأن جرائم الإنترنت أن مواجهة هذه الجرائم تكون في قطاعات مختلفة منها مايُعرف بالجرائم ذات المحتوى الاقتصادى، وجرائم الاعتداء على الخصوصية، وجرائم الاعتداء على الملكية الفكرية، وجرائم الأخلاق والآداب العامة، وجرائم المعلوماتية أو التكنولوجية وغيرها، وهذا بدوره أضعف إمكان صياغة نظرية عامة للحماية الجنائية لتقنية المعلومات وشتت الجهود بشأن كُنَّة هذه الظاهرة وصك أدوات ناجحة لمكافحتها ومواجهتها، وهو ما أدى إلى توجه الجهود الآن نحو صياغة نظرية عامة للجرائم المرتكبة عبر الإنترنت.
أنهيت الباحث بحثه باقتراح بعض التعديلات والمقترحات لمواكبة التطور الإجرامي.

١. **الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات – دراسة مقارنة للدكتورة / نبيلة هبة هرم مولاى على – رسالة ماجستير جامعة الإسكندرية ٢٠١٠ .**

بدأت الباحثة بدراسة تعريفياً بجرائم الإنترنت وخصائصها وأركانها والفرق بينها وبين جريمة الحاسب الآلي، بالإضافة إلى أنواع جرائم الإنترنت، ثم استعرضت الباحثة بعد ذلك تكوين الضبطية القضائية في جرائم الإنترنت من ناحية الضبط الإداري ودوره في مكافحة جرائم الإنترنت وأجهزة ضبطية الإنترنت في أغلب دول العالم.

ثم استعرضت الباحثة اختصاصات الضبطية القضائية في مكافحة جرائم الإنترنت في الظروف العادية والاستثنائية. ثم ناقشت التطورات الموضوعية والتكييف القانوني، وضبط الأدلة الرقمية.

أوصت الباحثة بضرورة التنسيق الدولي للسياسات الجنائية من أجل وضع قانون لمكافحة ومتابعة مرتكبي جرائم الإنترنت، وتوضيح فيه إجراءات التشغيل والضبط في العالم الافتراضي، وضرورة إنشاء لجان متخصصة في مجال مكافحة جرائم الإنترنت في الدول العربية والتعاون في هذا المجال، وتبادل الخبرات، وضرورة سن قوانين للإجراءات الجنائية تتماشى مع التطور التكنولوجي الذي تشهده دول العالم، وإنشاء شرطة متخصصة لمكافحة جرائم الإنترنت في الدول العربية.

١. **الجرائم الناشئة عن استخدام الإنترنت (الأحكام الموضوعية) "الجوانب الإجرائية" للدكتور / عمر محمد أبو بكر يونس – رسالة دكتوراه – كلية الحقوق – جامعة القاهرة – ٢٠٠٤.**

بدأ الباحث دراسته بتعريف الإنترنت وأقسامه وخصائصه وتأثيره الاجتماعي والاقتصادي والعلاقة بين القانون والإنترنت والحماية التشريعية للإنترنت. ثم قسم البحث إلى بابين رئيسين:

الباب الأول: تناول فيه الأحكام الموضوعية، حيث تناول الباحث أنواع الجرائم الناتجة عن الإنترنت، وتناول في الباب الثاني: الأحكام الإجرائية في الجريمة الناتجة عن الإنترنت، في الإثبات الابتدائي والمحاكمة، وأيضًا تطرق إلى الأدلة الجنائية في جرائم الإنترنت.

يعد هذا البحث من أوائل الأبحاث التي تناولت موضوع جرائم الإنترنت باستخدامه سواء فيما يتعلق بالشق الموضوعي أو الإجرائي.

منهج الدراسة:

أولًا: تعتمد هذه الدراسة على الأسلوب الاستقرائي والاستنباطي في البحث، حيث يتم الاعتماد بشكل رئيسي على المعلومات المُستقاة مباشرة من الدراسات والأبحاث السابقة، بالإضافة إلى المصادر الأولية والثانوية ذات الصلة، سواء كانت قانونية أو تشريعية، والتي تتناول موضوع جرائم الاحتيال المعلوماتي وإثباتها.

ثانيًا: تتبع الدراسة المنهج الوصفي التحليلي، الذي يعتمد على رصد عناصر الموضوع وتحليلها بشكل دقيق، وذلك بهدف إبراز طبيعة المعوقات التي تواجه الإثبات الجنائي في جرائم المعلوماتية، ومحاولة تقديم رؤية شاملة حول هذه التحديات.

المفاهيم الإجرائية للدراسة:

الإحتيال المعلوماتي :

جريمة الاحتيال المعلوماتي هي فعل يُرتكب باستخدام الوسائل الإلكترونية أو الأنظمة المعلوماتية بهدف الحصول على منفعة مالية أو غير مالية بشكل غير مشروع، وذلك عن طريق الخداع أو التلاعب أو استغلال الثغرات في الأنظمة التقنية. وتُعتبر هذه الجريمة من الجرائم الحديثة التي تواكب التطور التكنولوجي، وتختلف تشريعاتها من دولة إلى أخرى، وتشمل هذه الجرائم مجموعة واسعة من الأفعال، مثل الاختراق، ونشر البرمجيات الخبيثة، وسرقة الهوية، والغش الإلكتروني، وغيرها من الأنشطة التي تُهدد الأمن المعلوماتي للأفراد أو المؤسسات أو الدول.

مدخل

الثورة التكنولوجية وما نجم عنها من ظهور البنوك الالكترونية والتحويل الالكتروني للاموال ضاعف من امكانية ارتكاب الجرائم المعلوماتية وبصفة خاصة الاحتيال المعلوماتي، فالمصارف والمؤسسات المالية في الوقت الراهن يرتكز عملها بشكل اساسي على استخدام الأنظمة المعلوماتية وذلك لاجراء التحويلات المالية والتي تتم يوميا بالطرق الالكترونية وبمبالغ طائلة.

ونتيجة لظهور تقنية نقل الأموال الكترونيا عبر مصارف العالم خلال دقائق ، أصبح بامكان العملاء أصحاب الأرصدة المختلفة في البنوك القيام بهذه العملية من أي مكان في العالم ودون حاجة للذهاب إلى المصرف مباشرة ،ويعد الاحتيال المعلوماتي من اكثر الجرائم المعلوماتية التي ترتكب على نطاق واسع في مختلف

الدول و تسبب خسائر اقتصادية فادحة ، الأمر الذي يشكل قلقا متزايدا لدى المعنين بالامر ، إذ أن هذه الجريمة تهدد ثقة الأفراد بالوسائل التقنية المستحدثة لنقل الأموال .

وتزداد خطورة الاحتيال المعلوماتي اذا ما علمنا أن المعلومات المتعلقة بالنواحي الاقتصادية للجهات المختلفة اصبحت مخزنة في الحواسيب والوصول اليها من أي مكان في العالم يعد أمرا سهلا خاصة مع بروز وسائل الاتصال الحديثة ، وكذلك فإن الاجراءات الأمنية التقنية والتي تحاول الجهات المختلفة أحاطت هذه المعلومات بها ما زالت تعد اجراءات غير كافية حيث أن هناك ثغرات أمنية كثيرة فيها يستغلها المخترقون للوصول إلى مرادهم في تحقيق الكسب غير المشروع.

فالاموال الالكترونية والودائع اصبحت هدفا لمجرمي المعلوماتية من خلال التلاعب بمدخلات النظام المعلوماتي ، بمعنى تغذية الحاسوب ببيانات غير صحيحة أو التلاعب بالبرامج او من خلال تدخلات اخرى في معالجة البيانات ،وللوقوف على جريمة الاحتيال المعلوماتي نلقي الضوء على ماهيته والوسائل التقنية المستخدمة في ارتكابه والمعلومات المستهدفة للاحتيال بإعتبارها الجريمة الأبرز وذلك في فصلين، الأول ماهية الاحتيال المعلوماتي ونبين فيه وسائله وصوره، وفي الفصل الثاني مدى توفر الحماية الجنائية للمعلومات، علي النحو التالي :

الفصل الأول

ماهية الاحتيال المعلوماتى

قبل أن نخوض في ماهية الاحتيال المعلوماتي والاساليب التقنية المستخدمة في ارتكابه لا بد وأن نشير إلى أن عمليات الاحتيال المعلوماتي تشهد تزايدا واضحا في منطقتنا العربية وخاصة في ظل انتشار استخدام الانظمة المعلوماتية .

وتعد دولة الامارات المتحدة من أكثر الدول العربية تعرضا لهذا النمط الاجرامي المستحدث وذلك نظرا لاعتمادها الكبير على اجهزة الحاسوب و على الشبكات المعلوماتية في انجاز اعمالها ، خاصة وأن دولة الامارات العربية قطعت مراحل متقدمة في مجال تطبيق مشروع الحكومة الالكترونية . وقد كشف احد المواقع الالكترونية مؤخرا أن خمسة وخمسون مواطن اماراتي وخلال فترة وجيزة كانوا ضحية لعمليات الاحتيال المعلوماتية. (www . Gn4me . com / etesalat / article . jsp)[١]

وفي مصر ايضا تم القبض على عصابة من الطلبة الجامعيين قاموا بالاستيلاء على حسابات "الفيزا كارت" الخاصة بعملاء احد البنوك وذلك عن طريق عملية احتيال الكتروني (محمد، ٢٠٠٠، ص٧٢-٧٣)[٢]

وفي اليمن تم احباط عملية احتيال الكترونية على احد البنوك اليمنية والتي لو تمت لنجم عنها خسارة اقتصادية فادحة، وبناء على ذلك سوف نتناول ابتداء تعريف الاحتيال المعلوماتي ثم نعرض لأهم الوسائل

التقنية المستخدمة في عملية الاحتيال المعلوماتي وذلك في المبحث الاول ثم نتناول المعلومات المستهدفة الاحتيال المعلوماتى وذلك في المبحث الثاني.

المبحث الأول

الوسائل التقنية المستخدمة فى الاحتيال المعلوماتى

في التالي سنقوم بعرض اهم الاساليب التقنية المستخدمة في ارتكاب جريمة الاحتيال المعلوماتي ونعرض كذلك لبعض الأمثلة العملية التي تم استخدام هذه الأساليب التقنية فيها وذلك لفهم طبيعة عملها بشكل اوضح

أولا : التلاعب في مرحلتي ادخال و اخراج البيانات .

التلاعب بالبيانات المدخلة إلى جهاز الحاسوب يعد من اكثر حالات الاحتيال المعلوماتي حدوثا وذلك نظرا لما يتميز به من سهولة ، وقد ظهر أن ٦٢% من حالات الاحتيال المعلوماتي التي تم اكتشافها في الولايات المتحدة الأمريكية حتى عام ١٩٨٤ تنطوي على تلاعب بالبيانات قبل اواثناء ادخالها إلى جهاز الحاسوب

وتتمثل عملية ادخال المعلومات المزورة في تغذية النظام المعلوماتي بالمعلومات والبيانات المراد معالجتها آليا، وقد تتم عملية الادخال عن طريق الشخص نفسه الذي قام بالتلاعب في المعلومات ، اوعن طريق شخص أخر قد يكون حسن النية. (www . alyaseer . gov . sa / forum / topic . asp . archive) [٣]

ثانيا : التلاعب في البرامج

تتميز هذه الوسيلة بأنها على قدر كبير من التعقيد ، وتحتاج الى خبرة ومعرفة فنية في مجال البرمجة ، كما انها تعتبر من أكثر وسائل الاحتيال المعلوماتي خطورة . ويتم التلاعب في البرامج بصفة عامة عن طريق احدى وسيلتين :

الوسيلة الأولى : تتمثل هذه الوسيلة في تغيير البرامج المطبقة بالفعل داخل المؤسسة المجني عليها ، وذلك بادخال تعديلات غير مرخص بها على البرامج المستخدمة .

الوسيلة الثانية : تتمثل هذه الوسيلة في تطبيق برامج اضافية ، وهذه البرامج الاضافية قد يتم كتابتها عن طريق الجناة أنفسهم او قد تكون برامج معدة سلفا تهدف بشكل اساسي إلى تعديل المعلومات في الحواسيب عن طريق اجراء تعديلات مباشرة في ذاكرتها. (الحفناوي،٢٠٠١،ص٤٥٩) [٤]

ثالثا : التلاعب في البيانات التي يتم تحويلها عن بعد

التلاعب في البيانات عن طريق النهاية الطرفية أيا كان موقعها جعل الاحتيال اكثر سهولة من ناحية واكثر صعوبة في اكتشافه من ناحية أخرى ، فيكفي أن يكون الحاسوب متصلا بوحدة التشغيل المركزية عن طريق شبكة الخطوط الهاتفية العادية أو غيرها من وسائل الاتصال حتى يتمكن الفاعل من اتمام عملية الاحتيال من داخل منزله مستخدما لوحدته الطرفية دون الحاجة إلى الدخول إلى المؤسسة المجني عليها

ووفقا لهذه الوسيلة التقنية يمكن للجاني أن يقترف السلوك الاجرامي المكون للركن المادي لجريمته في دولة ما ، وتتحقق النتيجة الاجرامية في دولة أخرى.

رابعاً : استعمال شيفرة غير صحيحة للدخول إلى نظام مدفوع الأجر

تعد هذه الوسيلة صورة من صور الاحتيال المعلوماتي والتي قد يستعين بها الجاني التحقيق كسب غير مشروع. ويعد استعمال شيفرة غير صحيحة من اهم الوسائل للدخول غير المشروع إلى نظام مدفوع الأجر . والمقصود باستعمال شيفرة غير صحيحة هو الدخول إلى الأنظمة المعلوماتية مدفوعة الأجر باستعمال شيفرة مملوكة إلى شخص أخر او باستعمال شيفرة مملوكة للنظام نفسه. فليس المقصود أن تكون هذه الشيفرة غير صحيحة في ذاتها و انما تستمد عدم صحتها من استخدامها من قبل شخص لاحق له في ذلك

المبحث الثانى

المعلومات المستهدفة الاحتيال المعلوماتى

يقول (دولف هيغل) رئيس ادارة شرطة الجرائم الخطيرة في اوروبا: بالنسبة الجرائم الحاسوب والإنترنت ، يبدو اننا قد خسرنا المعركة قبل أن نبدأ القتال .... إذ اننا لا نستطيع مجاراتها

فالحواسيب وما يرتبط بها من شبكات تبدو كبوابة بلا حراس، بل كساحة اجرام تتحدى الأجهزة الأمنية بثغرات قانونية ضخمة ، الأمر الذي اتاح المجال أمام الأفراد والجهات الأخرى للتجول دون رقيب والحصول على المعلومات الأمنية والسرية والتي قد تكون على درجة عالية من الحساسية .(مؤتمر الأمن الكمبيوتر في المملكة المتحدة وتحديدا في العاصمة لندن،٢٠٠٢) [٥]

وللتدليل على خطورة وانتشار عمليات الاحتيال المعلوماتي فلقد خسرت شركة أمريكية للبترول وعلى مدى أشهر المناقصات التي كانت تدخل فيها ، وكانت ترسو هذه المناقصات على شركة أخرى منافسة لها كانت تقدم عروض اسعار تقل فقط بضعة دولارات عن الشركة الأولى،وقد اتضح أن ذلك كان نتيجة لوجود توصيلات سرية على الحاسوب التابع للشركة التي كانت تمني بالخسائر قامت بوضعه الشركة المنافسة لها وذلك للتعرف على عروض الاسعار المقدمة .

ولقد تطورت اساليب التجسس المعلوماتي، كأحد صور الاحتيال المعلوماتي لمواكبة التطور الذي يشهده العالم، خاصة في مجال تكنولوجيا المعلومات والاتصالات . حيث لم يعد التجسس مقتصرا على تجنيد عملاء في الدول الأخرى للحصول على المعلومات العسكرية أو الدفاعية لهذه الدول من قبل دول معادية الها ، او تجنيد هؤلاء العملاء في المؤسسات التجارية والصناعية المختلفة بهدف التوصل إلى اسرار هذه المنشات ، اواللجوء إلى رشوة وابتزاز العاملين في هذه المؤسسات للحصول على المعلومات الحساسة فيها

فالتقنية الرقمية فتحت آفاقا واسعة للقيام بالتجسس في كافة صوره دون حاجة لاختراق الدول والمؤسسات المختلفة من قبل عناصر بشرية ، بل يمكن للجهات الحصول على ما تريد من المعلومات الحساسة والخطيرة

عن بعد،والوسائل التقنية في مجال تكنولوجيا المعلومات والتي تستخدم في التجسس المعلوماتي كثيرة ويصعب حصرها ، إذ انها متطورة باستمرار وهناك سعي وبحث دائم من قبل بعض الجهات والدول للوصول إلى مرحلة متقدمة في مجال صناعتها .

مدى توفر الحماية الجنائية للمعلومات

الاحتيال المعلوماتي هذه الجريمة والتي يزداد معدل ارتكابها يوما بعد يوم وتشكل في ذات الوقت خطرا داهما على المؤسسات المالية وبالتالي على الاقتصاد الوطني،لا بد من مواجهتها تشريعيا وهذا الامر ادركته كثير من الدول فافردت لها نصوص خاصة تراعي طبيعتها والاساليب المستخدمة في ارتكابها.

والسؤال الذي يثور في هذا الصدد هو حول مدى امكانية انطباق النصوص الخاصة بجريمة الاحتيال في قانون العقوبات على جريمة الاحتيال المعلوماتي. وللاجابة عن هذا التساؤل نستعرض وفي (المبحث الأول) الأركان العامة لجريمة الاحتيال في قانون العقوبات، ثم نبحث في مدى انطباق هذه الأركان على جريمة الاحتيال المعلوماتي في (المبحث الثاني) .

المبحث الأول

الاركان العامة لجريمة الاحتيال المعلوماتى فى قانون العقوبات

تناول المشرع المصرى جريمة الاحتيال في الفصل الثاني من الباب الحادي عشر في قانون العقوبات تحت عنوان (في الاحتيال وسائر ضروب الغش) ، وذلك في المواد (٣٣٥-٣٣٦)، وقد نصت المادة (٣٣٦) من قانون العقوبات المصرى على ان كل من حمل الغير على تسليمه مالا منقولا او غير منقول او اسنادا تتضمن تعهدا أو إبراء فاستولى عليها احتيالا:

أ- باستعمال طرق احتيالية من شأنها ايهام المجني عليه بوجود مشروع كاذب او حادث او أمر لا حقيقة له او احداث الامل عند المجني عليه بحصول ربح وهمي او بتسديد المبلغ الذي أخذ بطريق الاحتيال او الايهام بوجود سند دين غير صحيح او سند مخالصة مزور.

ب- التصرف في مال منقول او غير منقول وهو يعلم أنه ليس له صفة للتصرف به .

ت- باتخاذ اسم كاذب او صفة غير صحيحة ،عوقب بالحبس من ثلاثة اشهر إلى ثلاث سنوات وبالغرامة من مائة جنية إلى مائتي جنية.(قانون العقوبات المصري، قانون العقوبات اللبناني، قانون العقوبات الفرنسي) [٦]

اما في الفقه، فقد عرف البعض جريمة الاحتيال على أنها كل تظاهر او ايحاء يكون صالحا لايقاع المجني عليه في الغلط بطريقة تؤدي إلى الاقتناع المباشر بالمظهر المادي الخارجي ، أي أن المجني عليه في جريمة النصب هو من جازت عليه حيله الجاني فانخدع بها وسلمه ماله.(مجلة نقابة المحامين،السنة الرابعة والثلاثين، ص١٣٨٨)[٧]

وقد عرفت محكمة التمييز الاردنية فعل الاحتيال كذلك على انه، فعل الخداع من المحتال ليحمل المجني عليه على تسليمه ماله لكي يستولي عليه ، وهو ما كان ليقبل بهذا التصرف لو عرف الحقيقة

وتعد جريمة الاحتيال من جرائم الأموال والتي يهدف المشرع بتجريمه اياها إلى حماية حق الملكية . حيث يتمثل هذا الاعتداء في نية سلب ثروة الغير كلها أو بعضها ، أي نية تملك المال ، وهي تعني ارادة مباشرة السلطات التي تنطوي عليها حق الملكية.

وبالاضافة إلى حماية حق الملكية ، يحمي المشرع بتجريمة الاحتيال مصلحة اخرى وهي حرية الارادة وسلامتها . وتتمثل حمايته لسلامة الارادة في تجريمه اسلوب الاحتيال الذي يلجأ إليه الجاني ، فيوقع المجني عليه في الغلط فيسلمه محل الجريمة تحت سطوة هذا الغلط ، فارادة المجني عليه حين سلم المال كانت ارادة غير سليمة.(تجدر الإشارة إلى أن العقار – وهو من الأموال الغير منقولة – لا يكون محلا لجريمة الاحتيال الا بطريقة غير مباشرة وذلك من خلال الاستيلاء باحدى وسائل الاحتيال على عقد بيعة او رهنه او على سند رتب للجاني حق ارتفاق عليه ، فعملية الاستيلاء الفعلي على عقار وحيازته تامة غير ممكنة من قبل أي شخص)[٨]

ويتبين لنا من خلال استعراض نص المادة (٣٣٦) من قانون العقوبات المصرى انه لا بد من توافر ثلاثة اركان لقيام جريمة الاحتيال وهي:

- محل الجريمة
- الركن المادي
- الركن المعنوي

وفيما يتعلق بالركن الأول وهو محل جريمة الاحتيال ، فلا بد أن يكون مالا ذا طبيعة مادية ،ولا يمكن أن يكون محل جريمة الاحتيال الانسان اوالمنفعة حتى ولو كان بالامكان تقييم الاخيرة ماديا.

اما بالنسبة لطبيعة المال محل جريمة الاحتيال فيمكن أن يكون مالا منقول او غير منقول، او إسناد تتضمن تعهد او ابراء او اوراق تجارية ، وذلك بخلاف بعض التشريعات الأخرى والتي اخرجت من دائرة الاحتيال الاموال غير المنقولة كالعقارات كما هو الحال في قانون العقوبات المصري ولا بد أن يكون هذا المال مملوكا للغير وليس للجاني الحق او السلطة للتصرف فيه

اما الركن المادي لجريمة الاحتيال فيقوم على ثلاثة عناصر اساسية هي :

العنصر الأول : نشاط ايجابي يقوم به الجاني ويتمثل هذا النشاط في استخدام الفاعل لوسيلة من الوسائل الاحتيالية والتي حددها المشرع في المادة (٣٣٦) من قانون العقوبات على سبيل الحصر ، وهذه الوسائل تتمثل في :

١. استعمال طرق احتيالية من شانها إيهام المجني عليه بوجود مشروع كاذب او حادث او امر لا حقيقة له او احداث الامل عند المجني عليه بحصول ربح وهمي او تسديد المبلغ الذي أخذ بطريق الاحتيال او الايهام بوجود سند دين غير صحيح او سند مخالصة مزور. ولم يقم المشرع الجزائي الأردني بوضع تعريف قانوني للطرق الاحتيالية ؛ وعلة ذلك أن هذه الطرق من الصعب حصرها وشمولها في تعريف جامع مانع ، إذ أنها تتطور وتنمو وتواكب المستجدات العلمية والتقنية.

وقد سعى الفقه إلى وضع تعريف لهذه الطرق الاحتيالية ، فتم تعريفها على انها،كل كذب مصحوب بوقائع خارجية او افعال مادية يكون من شأنها توليد الاعتقاد لدى المجني عليه بصدق هذا الكذب الأمر الذي يدفعه إلى تسليم ما يراد منه تسليمه طواعية واختيارا .

وبناء على ما تقدم ، فلا بد أن يكون هناك كذب قد صدر عن الجاني وان يكون من شأن هذا الكذب تغيير الحقيقة ، ولا بد من أن يرافق هذا الكذب مظهر خارجي يؤكد ويدعم الكذب وتتمثل هذه المظاهر الخارجية بالاستعانة بالغير او بالإستعانة بأوراق غير صحيحة أو القيام بأعمال مادية أو استغلال الصفة او الثقة .

٢. الوسيلة الثانية من الوسائل الاحتيالية هي تصرف الفاعل في مال منقول او غير منقول هو يعلم أنه ليس له صفة للتصرف به .

٣. اما الوسيلة الثالثة فهي اتخاذ الفاعل اسم كاذب او صفة غير صحيحة.

العنصر الثاني: حصول النتيجة الاجرامية هي العنصر الثاني للركن المادي في جريمة الاحتيال وتتمثل هذه النتيجة في تسليم المال من المجني عليه إلى الجاني ، فحتى تقوم جريمة الاحتيال لابد ان تؤدي الوسائل الاحتيالية التي نص عليها المشرع إلى ايقاع المجني عليه في غلط يحمله على تسليم ماله إلى الجاني طواعية.

ولا بد أن تكون ارادة المجني عليه لحظة التسليم معيبة ، أي انه سلم المال نتيجة الغلط الذي وقع فيه . ولا بد كذلك من أن يكون الشخص الذي قام بالتسليم او امر به هو ذات الشخص الذي وقع نتيجة الاحتيال في الغلط ، كما يجب أن يكون هدف الجاني لحظة استلام المال هو الاستيلاء عليه، و اخيرا يجب أن يكون التسليم لاحقا لاستخدام الأسلوب الاحتيالي لا سابق عليه .

العنصر الثالث: وجود علاقة سببية تربط بين النشاط الايجابي الذي قام به الفاعل والنتيجة الإجرامية،حيث أن النتيجة الإجرامية والمتمثلة بتسليم المجني عليه المال للجاني لا بد أن تكون محصلة للاسلوب الاحتيالي الذي استخدمه الفاعل وادى إلى وقوع المجني عليه في الغلط مما حدا به إلى تسليم المال ، اما اذا تم التسليم بناء على سبب أخر انقطعت علاقة السببية.

اما الركن الثالث والاخير في جريمة الاحتيال فهو الركن المعنوي المتمثل في القصد الجرمي العام والقائم على عنصري العلم والارادة،علم الجاني بكافة عناصر جريمة الاحتيال كما حددها المشرع ، وفي ذات الوقت

اتجاه ارادته إلى اقتراف النشاط الايجابي وهو استخدام احدى الوسائل الاحتيالية التي وردت في المادة ٣٣٦ على سبيل الحصر واتجاه ارادة الجاني ايضا إلى تحقيق النتيجة الجرمية.

والى جانب القصد العام لا بد أن يتوافر لدى الجاني القصد الخاص والمتمثل في نية تملك مال الغير.

مدى أمكانية انطباق نصوص جريمة الاحتيال فى قانون العقوبات على الاحتيال المعلوماتى.

تثير مسألة مدى امكانية انطباق نصوص جريمة الاحتيال التقليدية على التحايل المعلوماتي الجدل حول العديد من المسائل والنقاط التي تستدعي البحث و الدراسة . فالتحايل المعلوماتي جريمة على درجة من التعقيد سواء من حيث طبيعة المحل الذي ترد عليه او من حيث الوسائل التي ترتكب من خلالها.

ولا بد ابتداء من دراسة مدى امكانية ممارسة الافعال الاحتيالية على الحاسوب والنظام المعلوماتي المرتبط به ، بمعنى أخر مدى صلاحية الحاسوب لأن يكون مجنيا عليه،وكذلك لا بد أن نسلط الضوء على مدى اعتبار تسليم الأموال الكتابية او البنكية عن طريق عملية القيد الكتابي تسليما ماديا تتحقق من خلاله النتيجة الاجرامية لجريمة الاحتيال، واخيرا لا بد من تناول مدى امكانية اعتبار الوسائل الاحتيالية التي يلجأ إليها الجاني لارتكاب الاحتيال المعلوماتي من قبيل الطرق الاحتيالية التي نص عليها المشرع الجزائي الأردني في المادة (٣٣٦) من قانون العقوبات المصرى.

اولا : مدى امكانية الاحتيال على الحاسوب والنظام المعلوماتي المرتبط به

اذا كان الاحتيال في صورته التقليدية ينطوي على اتصال بين الجاني وبين شخص أخر يمارس الجاني حياله نشاطه الإجرامي ، فإن الاحتيال المعلوماتي يقوم على اتصال بين الفاعل ونظام الحاسوب فقط ، ويبدو ذلك واضحا في حالة التحويل الالكتروني غير المشروع اللاموال الكترونيا دون تدخل لأي عنصر بشري .

وقد اثارت مسألة الاحتيال على الحاسوب بوصفه مجرد آلة جدلا فقهيا ، وكانت الأراء منقسمة في اتجاهين **الاتجاه الأول** : يذهب إلى أن الحاسوب هو مجرد وسيط للتحايل وان الطبيعة المعلوماتية لجرائم الحاسوب لا تضيف جديدا في مجال الاحتيال التقليدي الا مجرد الوسيلة المستخدمة.(قشقوش، ١٩٩٢، ص١٥٢)[٩]

فالاحتيال على الحاسوب لسلب مال الغير ، تتحقق به الطرق الاحتيالية باعتبار أن ما يتم هو اكاذيب تدعمها وقائع خارجية تتمثل في المعلومات والبيانات التي يتم ادخالها إلى الحاسوب ،وذلك على اعتبار أن هناك دائما شخص طبيعي يقف وراء النظام المعلوماتي ، الأمر الذي يمكن القول معه انه هو الذي خدع بالطرق الاحتيالية التي لجأ اليها الجاني.

ويشير جانب من الفقه الفرنسي المؤيد لهذا الاتجاه إلى أن المشرع انحصر تفكيره عند صياغة القانون في العلاقات القائمة بين البشر ، ولم يعتقد يوما بأن هذه العلاقات ستتطور لتصبح بين الآلة والإنسان ، وهذه المسألة ليست بذات قيمة وفقا لهذا الرأي (الشوا، ١٩٩٤، ص١٢٤) [١٠]

كما يدعم هذا الجانب من الفقه وجهة نظره بما قضت به محكمة النقض الفرنسية بتطبيق عقوبة جريمة الاحتيال على شخص دخل بسيارته إلى أماكن انتظار السيارات ، وبدلا من وضع النقود الأصلية المطلوبة في عداد اماكن الانتظار قام بوضع قطعة معدنية عديمة القيمة فيه وترتب على ذلك تشغيل الماكينة وتحريك العقارب . حيث اسست المحكمة حكمها على ان وضع قطعة معدنية عديمة القيمة في العداد يعد من قبيل الطرق الاحتيالية.

ووفقا لهذا الاتجاه فإنه يمكن تطبيق النصوص التقليدية في قانون العقوبات على جريمة التحايل المعلوماتي.

الاتجاه الثاني:يرى هذا الاتجاه انه لا يمكن القول بصلاحية نظام الحاسوب لوقوع فعل الاحتيال عليه وبالتالي لا يمكن اعتباره مجنيا عليه ، إذ أنه مجرد آلة ،كما أن النصوص القانونية التقليدية التي وضعت لمواجهة جريمة الاحتيال تفترض بأن الطرق الاحتيالية لا بد أن تقع بين شخصين طبيعيين ، فالادعاء الكاذب يفترض علاقة مباشرة بينهما ، مما يسوغ القول بأن الطرق الاحتيالية نطاقها العلاقات الانسانية وليس مجرد اجهزة آلية صماء (الشوا، ١٩٩٤، ص١٢٥) [١١]

ووفقا لهذا الاتجاه فلا بد من استحداث نصوص عقابية تجرم الاحتيال المعلوماتي وذلك بما يتلائم مع طبيعة هذه الجريمة المستحدثة ، وهو الاتجاه الذي نذهب معه إذ أن محاولة مد نصوص القانون لتشمل جريمة الاحتيال المعلوماتي يصطدم مع مبدأ شرعية الجريمة والعقوبة.

بالنسبة إلى موقف التشريعات المختلفة من امكانية ممارسة الاحتيال على نظام الحاسوب وبالتالي ايقاعه في الغلط كانت هناك ثلاثة اتجاهات :

الاتجاه الأول : وفقا لهذا الاتجاه التشريعي لا يمكن خداع نظام الحاسوب بوصفه مجرد آلة، حيث لا بد أن يكون الفاعل قد خدع انسان مثله ، وبالتالي لا يمكن تطبيق النص القانوني الخاص بجريمة الاحتيال التقليدية على جريمة التحاليل المعلوماتي وهذا ما يذهب إليه المشرع المصرى في المادة (٣٣٦) من قانون العقوبات حيث استعمل المشرع لفظ (الغي) ، بقوله في مطلع المادة (كل من حمل الغير على تسليمه ...) فالمشرع يفترض أن المجني عليه انسان يتمتع بالشعور والارادة وقادر على التفكير وليس مجرد آلة .

وهذا ما ذهب إليه ايضا كل من المشرع الفرنسى والألماني والدانماركي والإيطالي(عفيفي، ٢٠٠٥، ص١٥١) [١٢]

الاتجاه الثاني: تمثله تشريعات الدول الأنجلوسكسونية ويرجع السبب في امكانية تصور وقوع الاحتيال على الحاسوب وايقاعه في الغلط وفقا لهذه التشريعات ليس بسبب وجود نص صريح يقر بذلك، و انما بسبب النصوص الواردة فيها والمتعلقة بجريمة الاحتيال والتي تتسم بالعموم والشمول ، بحيث يمكن الاستناد إلى هذه

السمة احيانا لتطبيق احكام تلك النصوص على فعل الاحتيال الواقع على الحاسوب(الشوا، ١٩٩٤، ص١٢٥) [١٣]

الاتجاه الثالث: يمثله التشريع الأمريكي، حيث اتجهت بعض الولايات الأمريكية إلى تعديل النص الخاص بالاحتيال في قانون العقوبات ليشمل الاحتيال على الآلة ، كما هو الحال بولاية الاسكا . ثانيا : مدى اعتبار تسليم الأموال الكتابية(البنكية) عن طريق عملية القيد الكتابي تسليما ماديا تتحقق من خلاله النتيجة الجرمية لجريمة الاحتيال .

المقصود بالنقود الالكترونية (البنكية أو الكتابية)، تلك النقود التي يتم تداولها عن طريق نظم المعالجة الآلية للمعلومات ، وبصفة خاصة في ظل نظم التحويل الالكترونية للاموال والتي تعتمد على نظام (Online) بصورة متكاملة حيث يتم نقل الأموال من خلاله بشكل فوري(الشوا، ١٩٩٤، ص١٣١)[١٤]

وتقتضي جريمة الاحتيال التقليدية أن يقوم الجاني بحيازة المال محل الجريمة حيازة مادية وهي تستلزم كذلك أن يكون الاستيلاء ماديا من قبل هذا الجاني على المال .

ويرى جانب من الفقه أن الاستيلاء الناشئ عن الاحتيال على نظام الحاسوب لا يرتب ادنى مشكلة اذا كان محل الاستيلاء نقودا ، كأن يتم التلاعب في البيانات المدخلة او المخزنة في الحاسوب او برامجه بواسطة شخص ما كي يستخرج الحاسوب باسمه أو باسم شركائه شيكات او مبالغ غير مستحقة يستولي عليها الجاني ماديا او يتقاسمها مع شركائه.

الا أن المشكلة تثور في حالة ما إذا كان محل الاستيلاء في التحايل المعلوماتي هو النقود البنكية او الالكترونية عن طريق ما يعرف بالقيد الكتابي ، فهل يعتبر هذا الاستيلاء استيلاء ماديا ومحققا للنتيجة الاجرامية لجريمة الاحتيال؟

تجدر الإشارة إلى أن القيد الكتابي يتم بالتلاعب في البرامج والبيانات الأمر الذي يترتب عليه تحويل بعض أوكل الأرصدة المالية او فوائدها من حساب اصحابها الشرعيين إلى حساب المتلاعب(قندح، ٢٠٠٤، ص١٢) [١٥]

ويرى البعض أن العبرة في الاحتيال المعلوماتي هو بقيام الحاسوب بوضع المال محل النشاط الاجرامي تحت تصرف الجاني تحت تأثير الأساليب الاحتيالية التي مارسها الأخير ، ولا يشترط أن يتم التسليم او الاستيلاء بطريقة مادية وذلك بالمناولة اليدويةوبالتالي فان التحويل الالكتروني غير المشروع للاموال عن طريق عملية القيد الكتابي لا يتعارض مع مفهوم التسليم في جريمة الاحتيال التقليدية.

وهذا ما يميل إليه جانب من الفقه المصري وكذلك الفقه الفرنسي، وهو الأمر الذي اكده كذلك القضاء الفرنسي ، حيث سوت محكمة النقض الفرنسية في بعض احكامها بين تسليم النقود وبين الدفع الذي يتم عن طريق القيد الكتابي . فلقد ابتكرت المحكمة نظرية جديدة تعرف بإسم نظرية " التسليم المعادل " والتي وضعت

لمواجهة حالات الاحتيال الواقعة على ضريبة المبيعات وعلى عداد موقف السيارات وعلى الهواتف ، وبعد ذلك اخذ الفقه بهذه النظرية حتى يلاحق بها كافة اشكال النصب باستخدام النظام المعلوماتي. (الشوا، ١٩٩٤، ص١٣٢)[١٦]

فالمحكمة عدلت عن المفهوم التقليدي لفكرة التسليم واعتبرت أن مجرد القيد الكتابي يعادل التسليم ، وجاء في الحكم الذي تبنت من خلاله المحكمة هذه النظرية، (.... وبالنظر إلى أن السند المثبت للانقضاء عن طريق الخصم من الدين المستحق لخزانة الدولة قد اصطنع من قبل الخاضع للضريبة ، فهذا لا ينفي احد العناصر المادية لجريمة النصب ، ويظل الحال كذلك ، حتى ولو لم يكن هناك تسليم لنقود طالما أن الدفع تم عن طريق العملة الكتابية التي تعادل تسليم النقود ...).(الشوا،١٩٩٤، ص١٣٣) [١٧]

اما بالنسبة لموقف تشريعات الدول المختلفة من هذه المسألة ، فلقد تباينت:

أولا : اتجهت بعض الدول إلى الاعتراف للاموال الكتابية او البنكية بصفة الأموال التي تصلح الان تكون محلا لجرائم السرقة والاحتيال وخيانة الأمانة بالرغم من طابعها غير الملموس، ومن هذه الدول الولايات المتحدة الأمريكية(عفيفي، ٢٠٠٥، ص١٥٥) [١٨]

ثانيا : اتجهت دول أخرى إلى عدم اعتبار النقود البنكية أو الكتابية من قبيل الاموال المادية ، بل ينظر اليها باعتبارها ديون لا تصلح محلا لجرائم الاحتيال او السرقة ، كما هو الحال في التشريع الألماني والياباني .

ثالثا : دول اخرى التزمت قوانين العقوبات فيها الصمت فيما يتعلق بهذه المسألة كما هو الحال في معظم تشريعات الدول العربية .

ثالثا: اما بالنسبة للتساؤل الثالث حول مدى امكانية اعتبار الوسائل التقنية المستخدمة في جريمة التحايل المعلوماتي من قبيل الطرق الاحتيالية التي نصت عليها المادة (٣٣٦١٧) من قانون العقوبات؟

فلقد ذهب البعض– كما اسلفنا الذكر – إلى أن خداع نظام الحاسوب لسلب مال الغير تتحقق به الطرق الاحتيالية ككذب تدعمه اعمال مادية أو وقائع خارجية تتمثل في المعلومات او البرامج التي يتم ادخالها إلى النظام المعلوماتي حتى تتم عملية التلاعب .(الشوا، ١٩٩٤، ص١٢٧) [١٩]

ولكن حتى وان سلمنا باعتبار الوسائل التقنية المستخدمة في الاحتيال المعلوماتي من قبيل الطرق الاحتيالية ، فإن ذلك لا يجعل تطبيق نص المادة (٣٣٦) عقوبات على جريمة التحاليل المعلوماتي امرا ممكنا، لأن الطرق الاحتيالية يجب أن تكون ابتداء في اطار العلاقات الإنسانية أي يجب أن تكون في مواجهة انسان آخر وليس آلة وذلك وفقا للمفهوم التقليدي لجريمة الاحتيال

ومما سبق يتضح لنا أن المشرع المصرى في قانون العقوبات وكنتيجة منطقية لعجز النصوص التقليدية عن مواكبة التطور التقني الذي ابرز إلى الوجود مجموعة من الجرائم المستحدثة وعلى رأسها جريمة الاحتيال

المعلوماتي، لا بد وان يقوم بالنص صراحة على تجريم هذا الفعل او ان يقوم بتعديل النصوص القائمة بحيث تشمل في اطارها هذه الجريمة.

وتجدر الاشارة إلى أن المشرع في قانون المعاملات الالكترونية رقم ٨٥ لسنة ٢٠٠١ اشار في المادة (٣٥) منه على ان (يعاقب كل من يقوم بإنشاء أو نشر أو تقديم شهادة توثيق الغرض احتيالي او لأي غرض غير مشروع بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنتين او بغرامة لا تقل عن (٣٠٠٠) جنية ولا تزيد على (١٠٠٠٠) جنية او بكلتا هاتين العقوبتين) ،وهذه المادة تقوم على تجريم كل الافعال الاحتيالية والتي تتم باستخدام شهادة التوثيق،والمقصود بشهادة التوثيق حسب نص المادة الثانية من ذات القانون ،(الشهادة التي تصدر عن جهة مختصة مرخصة أومعتمدة لاثبات نسبة توقيع الكتروني إلى شخص معين استنادا إلى إجراءات توثيق معتمدة.

وتنص المادة (٣٨) من ذات القانون على أن (يعاقب كل من يرتكب فعلا يشكل جريمة بموجب التشريعات النافذة بواسطة استخدام الوسائل الإلكترونية بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة او بغرامة لا تقل عن (٣٠٠٠) جنية ولا تزيد على (١٠٠٠٠) جنية او بكلتا هاتين العقوبتين ، ويعاقب بالعقوبة الأشد إذا كانت العقوبات المقررة في تلك التشريعات تزيد على العقوبة المقررة في هذا القانون.

ولقد وسع هذا النص من نطاق التجريم ليشمل الجرائم التقليدية الواردة في التشريعات النافذة اذا ما ارتكبت باستخدام الوسائل الالكترونية ، دون أن يراعي هذا النص العوائق التي تواجه تطبيق النصوص العقابية التقليدية كطبيعة المال المعلوماتي المعنوي وطبيعة فعل الاخذ في جريمة السرقة مثلا وغير ذلك من الأمور .

وتوصيات البحث:

، البحث إلى جملة من النتائج والتوصيات هي:

حيث أدي التحويل الإلكتروني الهائل في كافة المجالات إلى زيادة كبيرة في الجرائم المعلوماتية والاحتيال المعلوماتي بصفة خاصة، والتي أصبحت تشكل تهديدًا خطيرًا على الأمن الاقتصادي والمؤسسات المالية والأفراد على حد سواء. وقد تم تسليط الضوء على عدة جوانب رئيسية تتعلق بجريمة الاحتيال المعلوماتي، بما في ذلك:

زيادة معدلات الجريمة: شهدت المنطقة العربية، وخاصة دول مثل الإمارات ومصر واليمن، زيادة ملحوظة في حالات الاحتيال المعلوماتي، مما أدى إلى خسائر اقتصادية فادحة وتراجع في ثقة الأفراد بالأنظمة الإلكترونية.

تطور أساليب الاحتيال: تتنوع أساليب الاحتيال المعلوماتي وتتطور باستمرار مع تطور التكنولوجيا، حيث تشمل التلاعب في البيانات المدخلة، التلاعب في البرامج، واستخدام الشيفرات غير الصحيحة للدخول إلى الأنظمة المالية.

تأثيرات اقتصادية وأمنية: الجرائم المعلوماتية لا تؤثر فقط على الأفراد والمؤسسات المالية، بل تمتد تأثيراتها إلى الأمن القومي للدول، خاصة مع تزايد الاعتماد على الأنظمة المعلوماتية في المجالات العسكرية والاقتصادية.

قصور التشريعات الحالية: على الرغم من الجهود المبذولة، إلا أن التشريعات الحالية في العديد من الدول لا تزال غير كافية لمواجهة التحديات التي تفرضها الجرائم المعلوماتية، مما يتطلب تحديثًا مستمرًا للقوانين لمواكبة التطورات التكنولوجية.

الحاجة إلى تعزيز الأمن المعلوماتي: هناك حاجة ماسة لتعزيز الإجراءات الأمنية التقنية، بما في ذلك استخدام تقنيات التشفير المتقدمة، أنظمة التحقق الثنائي، والقياسات الحيوية، لحماية البيانات والمعاملات الإلكترونية.

دور التوعية والتدريب: زيادة الوعي العام حول مخاطر الاحتيال المعلوماتي وتوفير التدريب المستمر للموظفين في المؤسسات المالية يعدان من العوامل الرئيسية في الحد من هذه الجرائم.

التعاون الدولي: تعزيز التعاون بين الدول ومؤسسات إنفاذ القانون على المستوى الدولي يعد أمرًا ضروريًا لمكافحة

توصيات البحث:

<u>تعزيز التشريعات والقوانين:</u>

تحديث التشريعات: يجب على الدول تحديث قوانينها لتشمل جرائم الاحتيال المعلوماتي بشكل صريح، مع تحديد عقوبات رادعة تتناسب مع خطورة هذه الجرائم.

التعاون الدولي: تعزيز التعاون بين الدول لمكافحة الجرائم المعلوماتية عبر الحدود، بما في ذلك تبادل المعلومات والخبرات وإنشاء أطر قانونية دولية.

تحسين الإجراءات الأمنية:

تطوير أنظمة الحماية: يجب على المؤسسات المالية تطوير أنظمة أمنية متقدمة لتأمين البيانات والمعاملات الإلكترونية، مثل استخدام تقنيات التشفير المتقدمة والتحقق الثنائي.

التدقيق الأمني: إجراء تدقيق أمني دوري لاكتشاف الثغرات الأمنية ومعالجتها بشكل فوري.

<u>زيادة الوعي العام والتدريب:</u>

التوعية بالمخاطر: تنظيم حملات توعية للمواطنين حول مخاطر الاحتيال المعلوماتي وكيفية تجنبها، بما في ذلك عدم مشاركة المعلومات الشخصية والحساسة عبر الإنترنت.

التدريب المستمر: توفير برامج تدريبية للموظفين في المؤسسات المالية حول أفضل الممارسات الأمنية وكيفية التعامل مع محاولات الاحتيال.

تعزيز التكنولوجيا وأنظمتها:

استخدام الذكاء الاصطناعي: استخدام تقنيات الذكاء الاصطناعي والتعلم الآلي لاكتشاف الأنشطة المشبوهة ومنعها قبل حدوثها.

تطوير أنظمة التحقق: تطوير أنظمة تحقق متقدمة مثل القياسات الحيوية (بصمات الأصابع، التعرف على الوجه) لزيادة مستوى الأمان.

إنشاء مراكز متخصصة:

مراكز مكافحة الجرائم المعلوماتية: إنشاء مراكز متخصصة لمكافحة الجرائم المعلوماتية، تعمل على جمع المعلومات وتحليلها وتنسيق الجهود بين الجهات المعنية، وتوفير خطوط مساعدة للإبلاغ عن حالات الاحتيال المعلوماتي وتقديم الدعم الفوري للضحايا.

تعزيز الشفافية:

تشجيع المؤسسات المالية على الإبلاغ عن حوادث الاحتيال المعلوماتي بشكل فوري وشفاف لاتخاذ الإجراءات اللازمة، وإصدار تقارير دورية عن حالة الأمن المعلوماتي والإجراءات المتخذة لتحسينه.

البحث والتطوير:

دعم الأبحاث: تمويل ودعم الأبحاث العلمية التي تهدف إلى تطوير تقنيات جديدة لمكافحة الجرائم المعلوماتية.

تبادل المعرفة: تشجيع تبادل المعرفة والخبرات بين الباحثين والمختصين في مجال الأمن المعلوماتي.

تعزيز التعاون بين القطاعين العام والخاص:

شراكات استراتيجية: إنشاء شراكات بين القطاعين العام والخاص لتطوير حلول أمنية مشتركة ومكافحة الجرائم.

المراجع

(١) انظر الموقع الالكتروني ، www . Gn4me . com / etesalat / article . jsp

(٢) انظر الموقع الالكتروني السابق. وهناك حالات احتيال معلوماتية مختلفة تم ارتكابها في دول مختلفة من العالم ، مشار لها عند محمد ، عادل عبد الجواد، (٢٠٠٠). اجرام الانترنت . مجلة الأمن والحياة . العدد (٢٢١). ص٧٢، ٧٣.

(٣) انظر الموقع الالكتروني ، www . alyaseer . gov . sa / forum / topic . asp . archive

(٤) الحفناوي، فاروق. (٢٠٠١). موسوعة قانون الكمبيوتر ونظم المعلومات (ط١). دار الكتاب الحديث ، ص ٤٥٩

(٥) مناسبة هذا الحديث عقد مؤتمر الأمن الكمبيوتر في المملكة المتحدة وتحديدا في العاصمة لندن عام ٢٠٠٢ . انظر، الموقع الالكتروني،www.annabaa.org/nbsnews/14134.htm.

(٦) عرف المشرع المصري جريمة الاحتيال او النصب وهي التسمية الواردة في قانون العقوبات المصري وذلك في المادة ٣٣٦ من قانون العقوبات المصري. وكذلك الحال بالنسبة للمشرع اللبناني في المادة (٦٥٥) من قانون العقوبات اللبناني، وايضا هذا هو الحال عند المشرع الفرنسي والذي لم يعرف جريمة الاحتيال عند نصه عليها في المادة ٤٠٥ من قانون العقوبات الفرنسي

(٧) تمييز جزاء رقم ٨٥ / ١٣٤ ، مجلة نقابة المحامين، العددين التاسع والعاشر ، السنة الرابعة والثلاثين . ص ١٣٨٨.

(٨) تجدر الإشارة إلى أن (العقار – وهو من الأموال الغير منقولة – لا يكون محلا لجريمة الاحتيال الا بطريقة غير مباشرة وذلك من خلال الاستيلاء باحدى وسائل الاحتيال على عقد بيعة او رهنه او على سند رتب للجاني حق ارتفاق عليه ، فعملية الاستيلاء الفعلي على عقار وحيازته تامة غير ممكنة من قبل أي شخص)

(٩) قشقوش، هدي. (١٩٩٢). جرائم الحاسب الإلكتروني في التشريع المقارن (ط١). دار النهضة العربية، ص ١٥٢.

(١٠) الشوا، محمد سامي. (١٩٩٤). ثورة المعلومات وانعكاساتها على قانون العقوبات. دار النهضة العربية للنشر ، ص ١٢٤.

(١١) الشوا ، ثورة المعلومات ، مرجع سابق، ص ١٢٥يترتب عليه تشغيل الماكينة وتحريك عقارب العداد، مما أوهم المراقب المالي بان الجاني قد دفع أجرة الانتظار في الموقف .

(١٢) عفيفي، مصطفى كامل. (٢٠٠٥). جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون. منشأة المعارف، ص ١٥١.

(١٣) الشوا ، ثورة المعلومات ... مرجع سابق ، ص ١٢٥.

(١٤) الشوا ، ثورة المعلومات ... مرجع سابق ، ص ١٣١.

(١٥) قندح ،٢٠٠٤، الجرائم المرتكبة بواسطة المعلوماتية. ورقة عمل مقدمة لمؤتمر القانون والحاسوب المنعقد في جامعة اليرموك، إربد، ص ١٢.

(١٦) الشوا ، ثورة المعلومات ... مرجع سابق ، ص ١٣٢.

(١٧) مشار لهذا الحكم عند ، الشوا ، ص ١٣٣.

(١٨) عفيفي ، مرجع سابق ، ص ١٥٥

(١٩)صدرت عدة قوانين في الولايات المتحدة الأمريكية عرفت المال على انه (كل شيء ينطوي على قيمة) وهذا التعريف يشمل كافة الأموال سواء أكانت مادية أم معنوية بما في ذلك البيانات المعالجة والأموال البنكية . انظر ، الشوا ، ثورة المعلومات ... مرجع سابق ، ص١٢٧