جريمة الاحتيال عبر شبكة المعلومات الدولية

دراسة مقارنة النظام السعودي والقانون الأردني

د/ وائل محمد نصيرات
أستاذ القانون الجنائي المساعد
أ.د/غادة عبد الرحمن الطريف
أستاذ علم الاجتماع الجنائي
جامعة الأميرة نورة بنت عبد الرحمن

ملخص:

تعد جريمة الاحتيال من الجرائم التي بدأت تزداد خطورتها بسبب التطورات التقنية التي تساعد المحتالين على تنفيذ جرائمهم وتتناول هذه الدراسة عرض مفهوم الاحتيال المعلوماتي وأركانه، وطرق التلاعب في البينات والبرامج الإلكترونية، وبيان أهم وسائل ارتكابها،وعرض العقوبات المقررة في النظام السعودي والقانون الاردني بهدف وضع توصيات يمكن أن تساهم في مكافحة جريمة الاحتيال عبر شبكة المعلومات الدولية.

الكلمات المفتاحية : جرائم الاحتيال / شبكة المعلومات الدولية

Summary:

This study deals with the presentation of the concept of information fraud and its components, the methods of manipulating electronic evidence and software, the most important means of committing it, and the presentation of the penalties prescribed in the Saudi and Jordanian laws with a view to making recommendations Can contribute to combating the crime of fraud through the international information network.
Keywords: Fraud Crimes / International Information Network

المقدمة:

مع شيوع استخدام وسائل تقنية المعلومات وتزايد الاعتماد على نظم المعلومات وشبكات الحاسوب، شاعت طائفة جديدة من الجرائم يطلق عليها "الجرائم المعلوماتية" وعلى رأسها جرائم الاحتيال عبر شبكة المعلومات الدولية التي تستهدف المعلومات وبرامج الحاسوب كالدخول غير المرخص به إلى أنظمة الحاسوب والشبكات والاستيلاء على المعلومات أو إتلافها عبر تقنيات الفايروسات وغيرها من وسائل التدمير المعلوماتي و جرائم قرصنة البرمجيات، وتبرز أهميه دراسة هذه الجرائم باعتبارها أشدو قعاً في التأثير على المجتمع،وفي نفس المجني عليهم من غيرها من الجرائم الواقعة على الأموال.

وتأتي هذه الدراسة محاولة لسد النقص العلمي في الأبحاث الأكاديمية العلمية لموضوع جرائم الاحتيال عبر شبكة المعلومات الدولية نظراً لحداثتها وخطورتها على الأموال العامة والخاصة وتهديدها الأفراد والدول، وتهدد الأنشطة الاقتصادية الفردية والدولية، لذا تتلخص مشكلة الدراسة في التعرف على مفهوم الاحتيال المعلوماتي وأركانه، وطرق التلاعب في البينات والبرامج الإلكترونية، وبيان أهم وسائل ارتكابها،وعرض العقوبات المقررة في النظام السعودي والقانون الأردني بهدف وضع توصيات يمكن أن تساهم في مكافحة جريمة الاحتيال عبر شبكة المعلومات الدولية.

أهمية الدراسة:

- تظهر أهمية الدراسة من خلال بيان ماهية جريمة الاحتيال عبر شبكة المعلومات الدولية "الإنترنت" والتعرف على طرقها وأساليبها للحد من وقوعها ، ونشر الوعي بين أفراد المجتمع .
- الوقوف على الطرق الاحتيالية الحديثة والتي يمكن أن تكون وسيلة لإتمام فعل الاحتيال بالرغم من عدم النص عليها صراحة من ناحية وجهل أفراد المجتمع بها من ناحية أخرى.
- كما تبرز الأهمية من خلال عرض عقوبة جريمة الاحتيال الجريمة في النظام السعودي والقانون الأردني التي تحد من هذه الجرائم وتعديل النصوص القانونية القائمة بما يتلاءم والمستجدات التي تواكب تطور هذه الجريمة.

أهداف الدراسة:

تهدف الدراسة إلى التعرف على جريمةالاحتيال عبر شبكة المعلومات الدوليةوالتلاعب في البينات والبرامج الإلكترونية ووسائل معالجتها، ثم عرض تجربةالمملكة العربية السعودية والمملكة الأردنية في مكافحة جريمة الاحتيال عبر شبكة المعلومات الدولية وذلك من خلال التشريعات الوطنية والمستوى الدولي والمؤسسات المعنية بمكافحة الجرائم المعلوماتية بهدف وضع توصيات يمكن أن تساهم في مكافحة جريمة الاحتيال عبر شبكة المعلومات الدولية.

تساؤلات الدراسة:

تسعى هذه الدراسة للإجابة على التساؤل الرئيس التالي:

ما هيه جريمة الاحتيال عبر شبكة المعلومات الدولية ويتفرع من هذا التساؤل عدد من التساؤلات التالية:

1. ما مفهوم جريمة الاحتيال عبر شبكة المعلومات الدولية؟
2. ما أركان جريمة الاحتيال عبر شبكة المعلومات الدولية ؟
3. ما أساليب ووسائل التلاعب في البيانات والبرامج الإلكترونية بأشكالها المختلفة؟
4. ما هي تجربة المملكة العربية السعودية والمملكة الأردنية في مكافحة جريمة الاحتيال عبر شبكة المعلومات.

مفاهيم الدراسة:

البريد الإلكتروني:هو تلك الوثائق التي يتم تراسلها بواسطة نظام اتصالات بريدي الكتروني يتضمن ملحوظات مختصرة ذات طابع شكلي.

الموقع الإلكتروني: مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد.

المجرم التقني: مجرم سلك تقنية المعلومات سبيلاً لتنفيذ جرائمه الخاصة بشبكة المعلومات (الإنترنت).

الاختراق: الولوج غير المصرح به وبشكل غير مشروع إلى نظام معالجة آلية للبيانات باستخدام الحاسوب.

البيانات: المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، وكلما يمكن تخزينه، ومعالجته، ونقله، وإنشاؤه بواسطة الحاسب الآلي، كالأرقام والحروف والرموز وغيرها.

شبكة الويب العالمية : عبارة عن كم هائل من المستندات المحفوظة في شبكة الحاسوب والتي تتيح لأي شخص الاطلاع على معلومات تخص جهات أخرى أو أشخاص آخرين .

الدخول غير المشروع: دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها.

برامج الحاسب الآلي: مجموعة من الأوامر والبيانات التي تتضمن توجيهات أو تطبيقات حين تشغيلها في الحاسب الآلي، أو شبكات الحاسب الآلي،وتقوم بأداء الوظيفة المطلوبة.

الاحتيال المعلوماتي: التأثير في نظام معلوماتي إلكتروني أو شبكة معلوماتية أو مستند أو سجل إلكتروني أو وسيلة تقنية معلوماتية أو نظام أو جهاز حاسب آلي وذلك عن طريق البرمجة أو الحصول أو الإفصاح أو النقل أو النشر لرقم أو كلمة أو رمز سري أو بيانات سرية أو خاصة أخرى، بقصد الحصول على منفعة دون وجه حق أو الإضرار بالغير.

القانون الإلكتروني: هو مجال جديد نسبياً من مجالات قانون الحاسوب وشبكة المعلومات الدولية "الأنترنت". وما زال قيد التعريف حيث إنه يشمل مناطق جديدة، مثل مسؤوليات موفري خدمة شبكة المعلومات الدولية، ومشغلي نظام لوحة النشرات عن المواد التي تنشر مؤقتاً أو تخزن على الأنظمة الخاصة بهم، والهيكل الخاص بالتجارة الإلكترونية الدولية، فضلاً عن بعض النواحي التقليدية من منظور جديد، مثل حقوق الملكية الفكرية وحقوق الطبع والرقابة.

منهج الدراسة:

تعد هذه الدراسة من الدراسات المكتبية التي تعتمد منهجياً على تحليل وتفسير الأنظمة والنصوص القانونية ذات الصلة بالموضوع وبيان المبدأ القانوني الذي تقوم علية.

محددات الدراسة :

اعتمدت هذه الدراسة على عرض العقوبات المقررة في النظام السعودي والقانون الأردني بهدف وضع توصيات يمكن أن تساهم في مكافحة جريمة الاحتيال عبر شبكة المعلومات الدولية.

الدراسات السابقة:

1.دراسة الدكتور عبد الفتاح بيومي حجازي، بعنوان "جرائم الانترنت والبريد الإلكتروني"، مصر، 2007م تناولت هذه الدراسة موضوع جرائم الانترنت والبريد الإلكتروني من خلال ثلاثة فصول تناولت ماهية جريمة الانترنت وسماتها العامة، وقد هدفت هذه الدراسة إلى بيان جرائم الانترنت والبريد الإلكتروني، وأشارت الدراسة إلى أن هذا النوع من الإجرام المعاصر يثير الكثير من المشكلات في نواحي عديدة أهمها صعوبة إثبات هذه الجرائم. ذلك أن هذا النوع من الجرائم يتسم بالمكر والحيلة والدهاء والغش والاحتيال. حيث يتطلب مكافحة جرائم الانترنت بصفة عامة وضع سياسة جنائية رشيدة تستند على تدريب أجهزة العدالة الجنائية.

للإحداث ويمتد هذا التدريب إلى العاملين في الشرطة والتنفيذ والقضاء. ولأن القوانين السائدة من بلد إلى آخر تختلف بشكل كبير وهذا ينسحب على جرائم الاحتيال عبر البريد الإلكتروني، الحل يكمن في قانون دولي يصدر بصورة اتفاقية دولية، ويمثل الحد الأدنى لمتطلبات كل دولة حتى يتم مواجهة ظاهرة الجريمة في فضاء الانترنت والتي اصبحت عابرة للحدود.

2.دراسة محسن بن سليمان الخليفة، بعنوان (جرائم الحاسب الآلي وعقوبتها في الفقه و النظام) رسالة ماجستير،كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، 1423 ه.تناولت هذه الدراسة موضوع جرائم الحاسب الآلي وعقوبتها في الفقه والنظام من خلال ثلاثة فصول تناولت في الفصل الأول مفهوم الحاسب الآلي، وعالجت في الفصل الثاني موقف الفقه والنظام من جرائم الحاسب الآلي، وفي الفصل الثالث عقوبة جرائم الحاسب الآلي. وهدفت هذه الدراسة إلى بيان موقف الفقه والنظام (المشرع الجزائي)من جرائم الحاسب الآلي والعقوبة المترتبة على ارتكابها. وقد وصلت هذه الدراسة إلى نتائج من أهمها: أن جرائم الحاسب الآلي من الظواهر السلبية وأنها في تصاعد.وأشارت الدراسة إلى وجود نقص في الأنظمة المجرمة لهذه الجرائم في الوطن العربي.وركزت هذه الدراسة بشكل عام على جرائم الحاسب الآلي ولم تركز على جريمة الاحتيال عبر شبكة الأنترنت.

3.دراسة محمد عبيد الكعبي، بعنوان الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت رسالة دكتوراه، جامعة القاهرة، سنة 2015.تناولت هذه الدراسة الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت من خلال ثلاثة فصول تناولت فيها الجرائم الواقعة على الأشخاص وأوصت هذه الدراسة بالدعوة إلى عقد اتفاقيات دولية بشأن الجرائم الإلكترونية التي تقع على الأشخاص أو الأموال وإفراد نصوص قانونية خاصة بهذه الجرائم. وقد ركزت هذه الدراسة بشكل عام على الجرائم التي تقع على الأشخاص والأموال عبر الأنترنت، وبالتالي لم تركز على جريمة الاحتيال عبر الأنترنت ولم تتناول جوانبها ووسائلها وستعمل هذه الدراسة على الاستفادة من الجهود السابقة المتعلقة بالموضوع مع التركيز بشكل أساسي على جريمة الاحتيال عبر شبكة المعلومات الدولية وسوف تتميز الدراسة باحتوائها على محور المقارنات مع باقي الجرائم التي تقع عبر هذه الشبكة وتعرض وسائل ارتكابها من خلال عرض تجربة المملكة العربية السعودية والمملكة الأردنية في مكافحة جريمة الاحتيال عبر شبكة المعلومات الدولية من خلال التشريعات الوطنية والمستوى الدولي والمؤسسات المعنية بمكافحة الجرائم المعلوماتية بهدف وضع توصيات يمكن أن تساهم في مكافحة جريمة الاحتيال عبر شبكة المعلومات الدولية.

المبحث الأول:

مفهوم جريمة الاحتيال عبر شبكة المعلومات الدولية

تعد جريمة الاحتيال عبر شبكة المعلومات الدولية أكثر الجرائم خطورة وضرراً بأحوال الناس سواء في أشخاصهم أو أموالهم ، ولا يكاد يخلو مجتمع معاصر منها، ويمكنا لنظر لهذه الجريمة على أنها إحدى ضرائب التقدم الاقتصادي والاجتماعي والتحضر بنحو عام التي تدفعها المجتمعات (الشوابكة،2004).وقد تباينت هذه جريمة وتعددت، وأساس تباينها تحديد الأفعال المنطوية تحت هذا الوصف.والطبيعة الخاصة التي تتميز بها جريمة الاحتيال التي تقع على العمليات الإلكترونية باستخدام الوسائل الإلكترونية المستحدثة لا تقف عند الطبيعة الخاصة بالأفعال التي تتحقق بها هذه الجريمة، وإنما تمتد هذه الطبيعة لتشمل البعد العالمي أيضاً لهذا النوع من الجرائم، فيستطيع أي شخص في دولة معينة الدخول إلى شبكة الإنترنت العالمية، ويمكنه ارتكاب نشاطه الإجرامي في دولة أخرى أو مجموعة من الدول الأخرى.وفي هذا المبحث نتناول مفهوم جريمة الاحتيال عبر شبكة المعلومات الدوليةضمن مطلبين وذلك على النحو التالي:

المطلب الأول.

تعريف جريمة الاحتيال عبر شبكة المعلومات الدولية.

تعتبر جريمة الاحتيال عبر شبكة المعلومات الدولية من أهم الجرائم المتطورة ،وتختلف صورها وفقًا للتطور الاجتماعي والاقتصادي ،فالجاني في هذه الجريمة يعتمد على مدى قابلية الناس للاقتناع،وفقًا للظروف التي تحيط بهم؛ فيلجأ إلى أساليب ووسائل احتيالية توقعهم فى أخطاء تدفعهم إلى تسليم أموالهم إلى هذا الجاني طواعية واختيارًا دون مقاومة،فهي جريمة لا تتسم بالعنف،وغالبًا ما يكون للمجني عليه دو رفيها؛الأمر الذي يدفعه إلى عدم الإبلاغ عنها(الشوابكة،2004).وفي هذا المطلب نتناول تعريف شبكة المعلومات الدولية وجريمة الاحتيال عبر شبكة المعلومات الدولية ضمن الفروع التالية:

الفرع الأول: تعريف شبكة المعلومات الدولية.

تعرف شبكة المعلومات على أنها عدد من الوحدات المرابطة فيما بينها من خلال وسائل الاتصال المختلفة, تقوم بتبادل المعلومات فيما بينها والاشتراك بالمصادر عبر شبكة المعلوماتية(عبد الجبوري،2014،ص9).

وتعرف الفقرة (4) من المادة (2) من قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015 شبكة المعلوماتية بأنها:" ارتباط بين أكثر من نظام معلومات لإتاحة البيانات والمعلومات والحصول عليها".

كما تعرف الفقرة (3) من المادة (1) من نظام مكافحة جرائم المعلوماتية السعودي الصادر بموجب المرسوم الملكي رقم م/ 17 بتاريخ 1428/3/8هـ الشبكة المعلوماتية بأنها: "ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية ".

من خلال التعريفات السابقة لشبكة المعلومات نجد أن هذه الشبكة هي عبارة عن مجموعة هائلة من المستندات المحفوظة في شبكة الحاسوب تتيح لأي شخص الاطلاع عليها إلا المحظور عليه الاطلاع إلا بالاشتراك أو المصرح له دخول موقع المعلومات.

الفرع الثاني:تعريف جريمة الاحتيال عبر شبكة المعلومات الدولية.

معظم التشريعات العربية لم تورد تعريفًا لجريمة الاحتيال سواء بصورتها التقليدية أو الإلكترونية في قوانينها العقابية وترك الأمر للفقهاء،و هذا مسلك جيد في تقديرنا باعتبار أن صياغة التعريف ليست من مهام المنظم، وإنما من اختصاص الفقهاء.

فقد عرف بعض الفقهاء الاحتيال المعلوماتي بأنه: "التلاعب العمدي بمعلومات وبيانات تمثل قيماً مادية يختزنها نظام الحاسب الآلي، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة، أو أية وسيلة أخرى من شأنها التأثير على الحاسب الآلي، حتى يقوم بعملياته بناءً على هذه البيانات أو الأوامر أو التعليمات، من أجل الحصول على ربح غير مشروع وإلحاق الضرر بالغير" (عبد الجبوري،2014،ص6).

وعرف البعض الآخر الاحتيال المعلوماتي بأنه"الاستعمال غير المصرح به لنظام الحاسب الآلي بنية الحصول على ممتلكات أو خدمات عن طريق الاحتيال"(الرومي، 2003).

ومن خلال التعريفين السابقين يتضح أنا لفعل المرتكب غير المشروع قد يكون باستخدام طرق احتيالية أو تغيير حقيقة لبيانات أو اختلاسها أو تخريب البيانات أو دخول غير مشروع إلى موقع خاص.

وقد يوجه هذا الفعل غير المشروع ضد نظام حاسوبي آخر كتخريب بياناته أوقد يتعلق بنفس النظام الحاسوبي،كاستخدام (كتقديم خدمة وهمية مثلاً).

المطلب الثاني: طبيعة وخصائص وسمات جريمةالاحتيال عبر شبكة المعلومات الدولية.

وفي هذا المطلب نتناول طبيعة وخصائص وسمات جريمة الاحتيال عبر شبكة المعلومات الدولية ضمن الفروع التالية:

الفرع الأول: طبيعة جريمةالاحتيال عبر شبكة المعلومات الدولية.

لا تقف جريمة الاحتيال التي تقع على العمليات الإلكترونية باستخدام الوسائل الإلكترونية المستحدثة عند الطبيعة الخاصة بالأفعال التي تتحقق بها هذه الجريمة ، وإنما تمتد هذه الطبيعة لتشمل أيضاً البعد العالمي لهذا النوع من الجرائم، فإذا كانت شبكة الاتصالات من بعد ذا نطاق عالمي لا يتقيد بحدود دولة معينة فإنه يتصور تبعاً لذلك أن تتميز الجرائم التي تقع عليها أو تقع بسببها بالطبيعة العالمية، فيستطيع أي شخص في دولة معينة الدخول إلى شبكة المعلومات الدولية، ويمكنه ارتكاب نشاطه الإجرامي في دولة أخرى أو مجموعة من الدول الأخرى (**Naserat**, 2016, p. 11).

أيضاً تتميز طبيعة هذه الجرائم بأن الذين يرتكبونها هم فئة من المجرمين يتميزون بصفات خاصة فهم أشخاص لديهم السلطة في التعامل مع المعلومات التي يحتويها نظام الحاسب الآلي سواء كان ذلك في مرحلة إدخال البيانات أو

إخراجها أو التعامل معها بعد تخزينها و يستطيعون تحويل التلاعب في هذه البيانات إلى ربح مادي غير مشروع(.(p.170Case. 2000.

كما تحتاج جرائم الاحتيال التي تقع على العمليات الإلكترونية باستخدام الوسائل الإلكترونية إلى تأهيل فني وعلمي خاص يجب توافره في جميع الأشخاص الذين تتصل أيديهم بهذه الجرائم بدءاً من مرحلة التحري وجمع الاستدلالات ومروراً بمرحلة التحقيق الابتدائي وانتهاءً بمرحلة المحاكمة.

فإذا كان هذا النوع من الجرائم يتميز بطبيعة فنية معقدة وقد لا يخلف وراءه آثار تكشف عنه، فإنه يحتاج لكشفه والوصول إلى مرتكبيه إلى خبرة معينة فيمن يتصلون بهذه الجرائم كرجال الشرطة، وأفراد سلطة الادعاء، وقضاء الحكم(سلامة ، 2009م).

الفرع الثاني: خصائص وسمات جريمة الاحتيال عبر شبكة المعلومات الدولية:

أولاً: خصائص جريمة الاحتيال عبر شبكة المعلومات الدولية.

من أهم الخصائص التي تتميز بها جريمةالاحتيال عبر شبكة المعلومات الدولية.

1. البيئة الالكترونية: أهم ما يميز هذه الجريمة وقوعها من خلال البيئة الالكترونية، فهي تتم في بيئة الحاسوب والانترنت عن طريق نبضات الكترونية غير مرئية تنتقل بين أجهزة الحواسيب عبر النظام المعلوماتي، كما أنها تتميز باعتمادها على جوانب الإخفاق والقصور في الشبكات ونظم التحكم الخاصة بتكنولوجيا المعلومات(عرب، 2002م).
2. إلى جانب ذلك فإنها تستغرق في الغالب وقتاً طويلاً لكي يتم اكتشافها، إذ لا يتم ذلك إلا من قبل المصادقة أو من خلال الإبلاغ عنها في حالات قليلة، كما تعتبر من الجرائم البسيطة من الناحية النظرية، والبساطة هنا نعني أنها تتطلب فرداً واحداً –على الأقل – يتمتع بقدر كبير من المعرفة التقنية التي تمكنه من تتبع مسارات القصور في الشبكات ليتمكن من اصطياد فريسته بكل سهولة (منشأوي، 2002).
3. إخفاء الجريمة وسرعة التطور في ارتكابها: تتسم جريمةالاحتيال عبر شبكة المعلومات الدوليةبأنها مخفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة وربما على مرأى من عينيه، حيث يستخدم الجاني قدراته الفنية ومهاراته وكامل خبراته للإيقاع بالمجني عليه وإتمام جريمته بدقة عالية دون أن يلاحظه الضحية، ومن ذلك إرسال الفيروسات المدمرة وسرقة الأموال والبيانات الخاصة أو إتلافها والتجسس وسرقة المكالمات وغيرها(إبراهيم، ٢٠١١م،ص133-134).
4. جريمة عابرة للحدود: أدى ظهور شبكات المعلومات إلى إلغاء كافة الحدود المرئية أو الملموسة والتي كانت تقف في الزمن الماضي أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة وهائلة من المعلومات وسهولة تبادلها بين أنظمة يفصل بينها آلاف الأميال أدت إلى نتيجة مؤداها تأثر أماكن متعددة في دول مختلفة بالجريمة المعلوماتية الواحدة في آن واحد(الصغير، 2001).

ثانياً: سمات جريمة الاحتيال عبر شبكة المعلومات الدولية

يعتبر الحاسب الآلي من أهم أدوات جريمة الاحتيال، وغيرها من الجرائم التي ترتكب على شبكة المعلومات الدولية،وهي سمة وخاصية منفردة عن أي جريمة أخرى ،ذلك أن الحاسب الآلي هو الأداة ا لوحيدة التي تمكن الشخص من الدخول على شبكة المعلومات الدولية وقيامه بتنفيذ جريمته أيا كان(الخن، 2011م،ص68).

ومن سماتها أيضاً أنها حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم كالبنوك والشركات الصناعية وغيرها من الأهداف التي ما تكون غالباً الضحية لتلك الجرائم ، وه وما دعى معظم تلك الأهداف إلى اللجوء إ لى نظم

الأمن الالكتروني في محاولة منها لحماية نفسها من تلك الجرائم أوعلى الأقل لتحد من خسائرها عند وقوعها ضحية لتلك الجرائم. (عبَادي ، 2015، ص17).

كذلك من سماتها أن مرتكب جرائم الاحتيال شخص ذو خبرة فائقة في مجال الحاسب الآلي لاستخدام الحاسب الآلي لارتكاب جريمة على **شبكة المعلومات الدولية** إذ لا بد أن يكون مستخدم هذا الحاسب على دراية فائقة تمكنه من تنفيذ جريمته والعمل على عدم اكتشافها ولذلك نجد أن معظم من يرتكبون تلك الجرائم هم من خبراء الحاسب الآلي وأن الشرطة أول ما تبحث عن خبراء الكمبيوتر عند ارتكاب الجرائم الالكترونية(نصيرات، 2015 م).

ويمكن القول أن مرتكبي الاحتيال المعلوماتي هم أشخاص لديهم السلطة في التعامل مع المعلومات التي يحتويها نظام الحاسب الآلي سواء كان ذلك في مرحلة إدخال البيانات أو إخراجها أو التعامل معها بعد تخزينها ويستطيعون تحويل التلاعب في هذه البيانات إلى ربح مادي غير مشروع.

المطلب الثالث :تمييز جريمةالاحتيال عبر شبكة المعلومات الدولية عن الاحتيال في صورته التقليدية

هناك كثير من القواسم المشتركة بين جريمة شبكة المعلومات الدولية وبين جريمة الاحتيال العادية، فكلاهما يعتمد على وسائل الغش والخداع(الصغير، 2001)، والجريمتين من الجرائم الواقعة على الأموال، وغاية الجاني تتمثل في الاستيلاء على مال الغير بنية تملكه وحرمان صاحبه منه. كما أن الجريمتين تعتمدان بالدرجة الأساس على دهاء وفطنة الجاني المحتال وقدرته على الاستيلاء على مال الغير برضاه وبكامل إرادته وبتمام سلامة قواه العقلية (للمجني عليه المخدوع) (منشأوي، 2002).

ولهذا فكثير من الدول لم تشرع نصوصاً قانونية تجرم وتعاقب مرتكبي جريمة الاحتيال شبكة المعلومات الدولية لأن القضاء الجنائي في هذه الدول وسع من تفسيره للنصوص القانونية الخاصة بجريمة الاحتيال العادية وجعلها تمتد لتشمل هذه الجريمة، وهذا ما أخذت به كافة الدول الانجلوسكسونية كبريطانيا واستراليا وكندا، كما ظهرت اتفاقات على المستوى الإقليمي لمواجهة جرائم الانترنت مثل الاتفاقية الأوروبية حول الجريمة الافتراضية، والقانون العربي الاسترشادي لجرائم المعلومات على المستوى العربي(عبَادي ، 2015، ص17).

أما أوجه الاختلاف بين جريمة الاحتيال عبر شبكة المعلومات الدولية وبين الاحتيال في صورته التقليدية، فمتى استخدم الفاعل إحدى هذه الوسائل فإن سلسلة من التلاعبات قد تتكرر مرات عديدة، وهو ما يطلق عليه في خصوص الجريمة المعلوماتية الأثر الآلي للنشاط الإجرامي(منشاوي، 2002، ص87)، فإمكانية تكرار النتيجة الإجرامية يرجع بصفة خاصة على حقيقة مؤداها أن جريان العمل في نظام الحاسبات الآلية منظم بشكل دقيق للغاية، فمتى اكتشف الجاني ثغرة في النظام فإنه ينفذ منها ويستغلها كيفما شاء، وفي كثير من الأحيان يترتب على النشاط الإجرامي سلسلة من التلاعبات. فعلى سبيل المثال في حالتي التلاعب في البرامج وإجراء تغييرات في بيانات رئيسية كإجمالي المرتب، فإن النشاط الإجرامي يتكرر في كل مرة يتم فيها استخدام البرنامج أو استدعاء البيانات دون أن يكون للفاعل أي دور آخر (عرب، 2002م).

ولمعرفه الجريمة وقتية أو مستمرة فإنه يجب الرجوع إلى طبيعة الفعل الذي يعاقب عليه القانون. فإذا كان مما يقع وينتهي بمجرد ارتكابه كانت الجريمة وقتية أما إذا كان حالة مستمرة فترة من الزمن فتكون الجريمة مستمرة طوال هذه الفترة، والعبرة في الاستمرار هنا هي بتدخل إرادة الجاني في الفعل المعاقب عليه تداخلاً متتابعاً متجدداً (تمام، 2000 م).

كما لا يمكن تصور فكرة التتابع التي تتطلبها فكرة الجريمة متتابعة الأفعال في جريمة الاحتيال عبر شبكة المعلومات، فالنشاط الإجرامي الذي قام به الفاعل لا يعدو أن يكون تلاعباً في بيانٍ واحد أنتج مجموعة من الاعتداءات

على مجموعة من الحقوق ،فبمجرد قيام الفاعل بالتلاعب في البيان المطلوب وإعطائه أمراً إلى الحاسب الآلي بتطبيق البيان الجديد على مجموعة من الأرصدة فإن الأمر كله لا يستغرق سوى فترة قصيرة يتم من خلالها تنفيذ النشاط الإجرامي بأكمله (سرور، 1985، ص 883.)، إلا أن التساؤل الذي يثار هل نحن بصدد جريمة واحدة ام جرائم متعددة تتعدد بتعدد المجني عليهم الذين قد يبلغوا عدداً كبيراً بسبب الطبيعة الآلية للنشاط الإجرامي ؟

لكي نكون بصدد تعدد في الجرائم فإنه ينبغي توافر ثلاثة عناصر : أن يكون الفاعل شخصاً واحداً، وأن يرتكب عدداً من الجرائم، وأخيراً ألا يصدر من أجل أحداها حكم بات.

وتعدد الجرائم نوعان: التعدد الصوري أو المعنوي أو الحكمي للجرائم والتعدد المادي أو الحقيقي للجرائم، ويتحقق التعدد المادي للجرائم إذا تعدد السلوك المرتكب من الجاني وترتب على ذلك تعدد في الوقائع القانونية المتحققة فالعبرة هي بتعدد السلوك مع تعدد النتائج المترتبة بحيث تستقل كل واقعة عن الوقائع الأخرى في العناصر المكونة لها، فلا محل لتعدد الأفعال إلا إذا تعددت هذه العناصر بقدر عدد الأفعال بحيث يكون لكل منها على حدة العناصر المتطلبة لتكوينه. أما التعدد المعنوي للجرائم فيعني أن تتعدد الأوصاف الإجرامية للفعل الواحد أوان يخالف الشخص بسلوكه نصاً تجريمياً أكثر من مرة أو يخالف أكثر من نص تجريمي (فرج، 2008).

وينطبق التعدد المعنوي على عدة حالات : الحالة الأولى – أن يقوم شخص بارتكاب فعل واحد يفضي على نتيجة واحدة تحتمل أكثر من وصف إجرامي. أما الحالة الثانية – أن يرتكب شخص فعل واحد يفضي على نتائج عديدة متنوعة، وأخيراً حالة ارتكاب فعلٍ واحدٍ أفضى إلى نتائج عديدة متماثلة، وبذلك لا تعتبر الجرائم المتعددة معنوياً على اختلاف أشكالها جريمة واحدة، وإنما تتعدد الوقائع الإجرامية على الرغم من وحدة السلوك وهو ما يستلزم طبيعة الحال أن يتعدد الموقف النفسي حيال كل من النتائج المتحققة (حسني، 1988) .

وبتطبيق القواعد السابقة على الاحتيال عبر شبكة المعلومات الدولية، فإنه لا يمكن اعتباره جرائم متعددة تعدداً مادياً إذ أن قوام هذا النوع من الجرائم تعدد الأفعال فضلاً عن تعدد النتائج وهو ما لا يتوافر في حالتنا، إذ النشاط الإجرامي أو الحركة العضوية الصادرة عن الفاعل من أجل الوصول إلى غايته واحدة، كما أنه من ناحية أخرى لا يمكن القول بأن النشاط الإجرامي في هذه الحالة يشكل جريمة واحدة؛ ذلك أننا نرى أن النشاط قد أسفر عن نتائج إجرامية تتعدد بتعدد المجني عليهم حتى لو كانت هذه النتائج متماثلة من حيث التكييف القانوني لكل منها، إذاً نذهب إلى اعتبار الفعل الذي قام به المتهم تتعدد به عدة جرائم الاحتيال عبر شبكة المعلومات الدولية تعدداً معنوياً إذ تنطبق عليه الحالة الثالثة من حالات التعدد المعنوي، فتعدد الجرائم في هذه الحالة يُكتفي فيه بتعدد النتيجة بصرف النظر عن وحدة السلوك أو تعدده، فالتعدد يقتضي تعدداً في النتيجة دون أن يستلزم تعدداً في السلوك.

وإذا كان المشرع الأردني قد حدد حكم التعدد المعنوي وهو الاعتداد بالجريمة التي عقوبتها أشد والحكم بعقوبتها دون غيرها، فإنه يكون الحكم بالعقوبة المقررة للاحتيال عبر شبكة المعلومات الدولية حيث إن جميع النتائج متماثلة، إلا أنه يلاحظ في هذه الحالة أنه ينبغي النص على تشديد العقوبة، فآلية النشاط الإجرامي تجعل من تكرار النتيجة الإجرامية أمراً في غاية السهولة فبحركة واحدة يتمكن الجاني من تحقيق أكثر من نتيجة إجرامية متماثلة(عبَادي، 2015).

المبحث الثاني:

أركان جريمة الاحتيال عبر شبكة المعلومات الدولية.

يتطلب وقوع جريمة الاحتيال عبر شبكة المعلومات الدولية توافر أركانها، فلابد من أن تتبلور الجريمة مادياً وتتخذ شكلاً معيناً وهو الركن المادي للجريمة المتمثل في سلوك الجاني لإحدى وسائل الاحتيال المنصوص عليها في القانون،إلاّ أنّ هذا الركن لا يكفي إسناد المسؤولية إلى شخص معين بل يجب أن يتحقق الركن المعنوي المتمثل بالقصد

الجنائي والذي يرتكز على توفر الإرادة الآثمة لدى الجاني حين ارتكابه للجريمة وعلمه بأن فعلـــه أو امتناعـــه يشـــكل ضرراً أو خطراً على الغير يعاقب عليه القانون، وفي هذا المبحث نتناول أركان جريمة الاحتيال عبر شبكة المعلومـــات الدولية ضمن مطلبين وعلى النحو التالي:

المطلب الأول: الركن المادي في جريمة الاحتيال عبر شبكة المعلومات الدولية

يتطلب الاحتيال ركنًا مادياً قوامه الاستيلاء بالاحتيال على مال الغير،ويتألف هذا الركن من فعل الاحتيال وهـــو استعمال وسيلة من وسائل الاحتيال ،ونتيجة معاقب عليها هي الاستيلاء على مال منقول للغير،وعلاقة سببية بين السلوك والنتيجة.

ويأخذ الركن المادي الخاص بجريمة الاحتيال عبر شبكة المعلومات الدولية، أشكالاً عدة منها البريد الإلكترونـــي الذي تم إرساله أو الأداة الإلكترونية التي يتم الاستعانة بها في ارتكاب جريمة الاحتيال المعلوماتية، أو الأدوات التي تـــم تصميمها، أو تم الاستعانة بها من خلال الاتصال أو الإيقاع بالضحية كما يلزم توفر الأداة التي تم إرسال الرســـالة مـــن خلالها والتي تتمثل في هذه الحالة الجهاز الحاسوبي لإتمام عملية الاحتيال، أو الوصول إلى قواعد بيانات غير مســـموح بالاطلاع عليها، أو استخدامه للوصول إلى معلومات موجودة على جهاز حاسوبي أخر، وكلها أمور كفيلة بـــأن تثبـــت توفر الركن المادي للجريمة(الغزاوي ، 2005م ،ص98) (الصغير، 2001).

الفرع الأول: الفعل الإجرامي

حدد قانون العقوبات الأردني في المادة (336) أفعال الاحتيال التي رأى أنها جديرة بالعقاب، وقـــد وردت هـــذه الأفعال على سبيل الحصر، حيث إن الاستيلاء على مال الغير لا يعد جريمة احتيال إذا لم يقم الفاعل بأحد الأفعال التـــي حصرها المشرع في ثلاثة هي: استعمال طرق احتياليه، التصرف في مال منقـــول أو غيـــر منقـــول مملـــوك للغيـــر، واستخدام اسم كاذب أو صفة غير صحيحة.

أولاً: الكذب.

الكذب هو تغير للحقيقة ينصب على واقعة، أو هو الإخبار بأمر يخالف الواقع. ويستوي لتوافر الاحتيال أن يكون الكذب شفوياً بالقول أو مكتوباً، بل يتصور أن يكون الكذب بالإشارة متى كان لها دلالة معروفة فهمها المجنـــي عليـــه ووقع بناء عليها في الغلط (الشهري، 2016) ومثال ذلك قيام المشعوذ بحركات يفهم منها المجني عليه قدرتـــه علـــى القيام بأمور معينة.

ولا يشترط في الكذب أن يكون كلياً، فقد يكون جزئياً وعندئذ يتعين أن ينصب هذا الكذب على الجانب الجوهري من الواقعة محل الكذب، ويكون كذلك إذا كان الكذب ينصب على أمر هو محل اعتبار لدى المجني عليه، كما في حالـــة أن يذكر الجاني أنه يوجد مشروع يحقق أرباحاً طائلة، فيعتبر قوله كذباً على الرغم من وجود ذلك المشـــروع، ولكـــن الأرباح التي يحققها ليست طائلة، فالكذب في هذه الحالة كان جزئياً ولكنه انصب على واقعة جوهرية ومحل اعتبار لدى المجني عليه بإمداد آخر بمعلومات أو بمعرفة بخصوص واقعة لا تتفق مع الواقع ، فمتى ما قام شـــخص بـــذلك عـــد كاذباً(الشواء،2003م،ص169).

ويشترط في الكذب أن يكون من شأنه الإيقاع في الغلط، وإذا كان الأصل أن يولّد الكذب غلطاً لم يكن موجـــوداً من قبل، ومثاله أن يكون المجني عليه آمناً غير معتد بمخاطر تهدد حياته أو أمواله، فيـــأتي المـــتهم فيـــدعي كـــذباً أن مزرعته مهددة بالحريق، مدخلاً في اعتقاده خطأً صحة ذلك. (نصيرات،2015، ص55)

ثانياً: وسائل الاحتيال

لكي يبلغ الكذب أو تغير الحقيقة مبلغ الاحتيال، الذي يشكل أحد عناصر الركن المادي في جريمة الاحتيال، يجب أن يتخذ صورة من صور ثلاثة نص عليها المنظم الأردني على سبيل الحصر في المادة والمادة(417) من قانون العقوبات الأردني وهي:استعمال الطرق الاحتيالية، والتصرف في مال ثابت أو منقول ليس مملوك للجاني ولا له حق التصرف فيه،استخدام اسم كاذب أوصفة غير صحيحة.

1. الاحتيال باستخدام الطرق الاحتيالية:

لا يكفي الكذب وحده لتقوم به الطرق الاحتيالية، إذ لا بد وأن يدعم هذا الكذب ببعض المظاهر الخارجية التي تؤيده وتعززه، مما يكون من شأنه ان تتولد الثقة لدى المجني عليه بصدق ما يزعمه الجاني، أي يحمل المجني عليه على تصديق ادعاءات الجاني الكاذبة، فينخدع بما يقول ويُقدم على تسليم المال(الصغير، 2001) (عبيد، 1985،ص 447)

والطرق الاحتيالية في واقع الأمر هي عبارة عن مظاهر خارجية يلجأ إليها الجاني لتأييد كذبه وحمل الناس على تصديقه سواء كانت هذه المظاهر أفعالاً صادرة عن الجاني أو عن شخص سواه، أو كانت ظروفاً واقعية هيأها الجاني، أو تهيأت عرضاً، فأحسن استغلالها(الشهري، 2016) .

ونلاحظ أن المشرع الأردني قد نص على المظاهر الخارجية كوسيلة من وسائل الاحتيال دون أن يحدد ماهيتها ودون أن يورد تعريفاً أو بياناً لها بالرغم من تحديده لأغراضها. ويمكن أن تتخذ المظاهر الخارجية إحدى الصور الثلاثة التالية:

أ. **القيام ببعض الأعمال المادية (إعداد الوقائع المادية):** هذه الأعمال المادية التي يقوم بها الجاني يجب أن تكون مستقلة عن الكذب ومدعمة بعناصر خارجية، أما إذا كانت مجرد ترديد للكذب فلا قيمة لها؛ ويشترط في هذه الأفعال أن يكون من شأنها أن تدعم الكذب فتلبسه ثوب الصدق، كذلك يشترط أن يكون الجاني هو الذي حرك الظروف تجاه المجني عليه أو دفع به إليها ليقع تحت تأثيرها(الشواء،2003م).

ب. **الاستعانة بشخص من الغير**، حيث يستعين الجاني في هذه الصورة بتدخل شخص أو أشخاص من الغير لتأييد الكذب أو تأكيده، وذلك لكي يتمكن من الاستيلاء على مال المجني عليه لأن الجاني حين يبدأ برواية أكاذيبه ثم يتدخل شخص آخر لتعزيز تلك الأكاذيب،فإن الشك سوف لن يتولد لدى المجني عليه، خاصة إذا تظاهر الشخص الآخر بأن لا مصلحة له في الأمر وهو حين يؤيد مزاعم الجاني ويؤكد صحتها،إنما يساعد هذا الجاني على بث الطمأنينة في نفس المجني عليه مما يحمله على تسليم ماله(الشواء،2003م).

فقد قضت محكمة التمييز الأردنية بأن :" أول شرط لقيام الطرق الاحتيالية أن تدعم ادعاءات الجاني بأشياء خارجية تساعد على إلباسها ثوب الصدق ويؤدي إلى إدخال الغفلة على المجني عليه وحمله على تسليم ماله سواء أكانت هذه الأشياء الخارجية أفعالاً صادرة عن الجاني أو ظروفاً أجنبية، ومن أبرز صور الظروف الأجنبية تدخل شخص آخر يقرر أو يؤكد أقوال الجاني شريطة أن يكون للجاني يد في تدخل ذلك الشخص ولا فارق بين أن يكون الشخص الآخر سيئ النية أم حسن النية"(تمييز جزاء.(1991) رقم 1991/275، مجلة نقابة المحامين النظامين، سنة، ص224).

ج. **إساءة استغلال صفة الجاني الحقيقية**، حيث يشترط في الصفة التي يتمتع بها الجاني أن تكون حقيقية وليست منتحلة إذ لو كانت هذه الصفة غير صحيحة، لوقع الاحتيال بطريقة انتحال اسم كاذب أن صفة غير صحيحة وهو أمر لا

يؤثر في النتيجة وهي قيام جريمة الاحتيال في كلتا الحالتين. إذا أسفر استعمال أي من الطريقتين عن تسليم المجني عليه المال للجاني (الشواء،2003م)

د.**الاستعانة بأوراق أو مستندا ت مكتوبة منسوبة للغير**، حيث يدخل في عداد الأعمال الخارجية التي ترفع الأكاذيب إلى مصاف الطرق الاحتيالية استعانة الجاني بأوراق أومستندات منسوبة للغير يقدمها للمجنى عليه أويبرزها له كي يحمله على تصديق مزاعمه (الشهري، 2016).

ه. **إحاطة الجاني نفسه بمظاهر خارجية تؤكد مزاعمه**، فقد يحيط الجاني نفسه بمظاهر خارجية ليدعم بها ادعاءاته الكاذبة التي توصله إلى الاستيلاء على مال الغير.

ومن صور السلوك الإجرامي لجريمة الاحتيال عبر شبكة المعلومات الدولية صورة الدخول غير المشروع أو بغير إذن لموقع إلكتروني على شبكة المعلومات، تغيير تصاميم الموقع الإلكتروني (الحربي، 2008م،ص211) وقد عرّف نظام مكافحة جرائم المعلوماتية السعودي الدخول غير المشروع في المادة الأولى منه بقوله "الدخول غير المشروع، دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها".

ولم يشترط النظام السعودي أن يكون النظام محمياً بكلمة السر، بل إن الدخول غير المشروع معاقب عليه حتى ولو لم يُعنَ صاحبُه بوضع كلمة المرور عليه لكي يحميه من تطفل الآخرين.

والنظام السعودي في ذلك يتماشى مع الاتجاه العالمي في هذا المجال حيث يحمي القانون الفرنسي، والقانون الإنجليزي، والقانون الكندي، الحاسب الآلي بدون شرط أن يكون محمياً بكلمة مرور(منشوي، 1434ه).

وعلى الرغم من أن النظام المشار إليه قد جرّم الدخول غير المشروع في نظام حاسب آلي أو موقع إلكتروني أو شبكة، فإنه لم يجرّم مجرد الدخول، بل اشترط أن يكون ذلك الدخول بقصد تحقيق غاية معينة، أي استلزم توافر نية معينة وهو ما نسميه بالقصد الخاص.

ويرجع السبب في تلك الحماية الخاصة إلى أن من يدخل نظام الكمبيوتر غالباً ما يكون قد أخلّ بحرمة المكان دون أن يقوم بدخول مادي في هذا المكان في حالات كثيرة. يضاف إلى ذلك أن نظام الكمبيوتر يتيح التعرف على كمية هائلة من المعلومات بسهولة ويسر وفي وقت قصير، الأمر الذي لا يتوافر في حالة الملفات الورقية التقليدية (قوره، 2006، ص87).

- صورة الدخول غير المشروع بإتلاف الموقع، وتعطيله عن العمل.
- صورة الدخول غير المشروع بتعديل الموقع.
- الدخول غير المشروع للحصول على بيانات، والاستيلاء عليها.

ولكن هذه الأمور تختلف فيما بينها، فالأول وهو الدخول غير المشروع جريمة بحد ذاته ولو لم يتبع هذا الدخول أي تصرف آخر أو إضرار بالموقع.

وأما بقية صور الركن المادي للجريمة (تغيير التصاميم وإتلاف الموقع وتعديله) فلا يلزم تحققها واقعياً.

ثالثاً: التصرففي مال منقول أو غير منقول وهو يعلم أن ليس له صفة للتصرف فيه

عبر المشرع عن هذه الوسيلة في المادة (٣٣٦)من قانون العقوبات الأردني بقوله" وأما بالتصرف في ما ل ثابت أو منقول ليس مملوك له ولاحق التصرف فيه". (يراجع نص المادة لأن الصياغة غير جيدة)

وتقوم هذه الوسيلة مثل وسيلة استعمال الطرق الاحتيالية على الكذب الذى يتمثل في ادعاء الجاني ملكيته للمال موضوع التصرف وحقه في التصرف فيه . ولكن هذه الوسيلة تختلف عن وسيلة استعمال الطرق الاحتيالية في أن

الكذب فيها يكفى لتوافر فعل الاحتيال دون حاجة إلى تدعيمه بمظاهر خارجية أو أعمال مادية كما أنا لمشرع لم يحـــدد لهذه الوسيلة غايات معينة(الصغير، 2001).

وباعتبار جريمة الاحتيال المعلوماتي تلاعب ب البيانات والمعلومات من أجل الحصول على ربح غير مشـــروعاً ومنفعة تقوم بالمال فهذا يعني أن موضوع المال محل ا لاختيار يشمل كل ربح يمكن أن يحصل عليه الفاعل عن طريق الاحتيال وكذلك كل منفعة يمكن أن تقوم بالمال،فالدخول إلى نظام مدفوع الأجر باستخدام شفرة غير صحيحة فضلاً عما يترتب عليه من ضرر يلحق بمستخدم الشفرة الأصلي والذي يمثل في القيمة النقدية المستحقة نظير استخدام النظام،فإنـــه يحقق من ناحية أخرى للمتهم منفعة تقوم بالمال والتي تتمثل في استخدام النظام من دون تحمل النفقات اللازمـــة لهـــذا الاستخدام(منشوي، 1434ه).

فمحل النشاط الإجرامي في هذه الحالة ليس مالاً مادياً له كيان ملموس إلا أنه في إطـــار خصوصـــية الجريمـــة المعلوماتية فهو يصلح لأن يكون محلا للاحتيال المعلومـــاتي ففكـــرة المـــال الملمـــوس تتعـــارض مـــع الجريمـــة المعلوماتي،فهذه الجريمة تقوم في أساسها على المعلومات والبيانات وبرمجتها بصورة آلية،وفي بعض الأحيان في نقود وأعيان كأن يتمكن الجاني من سحب مبالغ نقدية من اجهزة الصرف الآلي عن طريق بطاقة الائتمان بعد التوصل إلـــى الرقم السري الخاص بها أو بتلاعب في بيانات أو برنامج كي يستخرج الحاسب باسمه صكوك أو فواتير بمبالغ غيـــر مستحقة يستولي الجاني عليها(المشهداني، ص132) ،إلا انه في كثير من الحالات الأخرى يتمثل المحل في نقود كتابية كما لو تلاعب ا لجاني في البيانات أو البرامج كي يحول كل أو بعض أرصدة الغير أو فوائدها إلى حســـابه.،وتختلـــف الدول في مدى قابلية الأموال الكتابية لأن تكون محلاً لجريمتي السرقة والاحتيال فبينما تذهب بعض التشريعات إلى عدم إمكانية ذلك التشريع الألماني والياباني،نتيجة تشريعات أخرى إلى عكس ذلك مثل كندا و هولنـــدا وسويســـرا وانجلتـــرا وكثير من الولايات الأمريكية ،وهو ما ذهب إليه القضاء الفرنسي(الشواء،2003م،ص170).

ويثور شأن محل الاحتيال عبر شبكة المعلومات الدولية تساؤل حول إمكانية أن يكون هذا المحل عقاراً؟

بالنسبة للمنظم الأردني جعل العقار(نصت الفقرة 2/من المادة 417 من قانون العقوبات الأردني) ، شأنه في ذلك شأن المنقول، يمكن أن يكون محلاً للنشاط الإجرامي فالعبرة هي بوضع الشيء في متناول يد الجـــاني أو تحـــت أمـــره وليس بتسليم المال بالمناولة، فإذا ما تمكن الجاني على سبيل المثال من التلاعب في البيانات التي تثبت ملكية العقـــار أو التي تحدد ثمنه أو تمكن من إنشاء حقوق عينية على العقار، فنحن نرى إمكانية وقوع الاحتيال في هذه الحالة طالما كان للحاسب الآلي دوره في إتمام النشاط الإجرامي، فإعطاء الحاسب الآلي أمراً يعتمد في تنفيذه علـــى البيانـــات التـــي تـــم التلاعب فيها ويتم بمقتضاه الاحتيال الذي قد يتخذ على سبيل المثال صورة نقل ملكية العقار أو تغيير ثمنـــه أو إنشـــاء حقوق عينية عليه، يقوم به الاحتيال عبر شبكة المعلومات الدولية(القهوجي ، 2002م)

أما بالنسبة للمنظم السعودي فقد فعل صنعاً (هنا عبارة مفقودة) عندمااشترط أن يكون المال منقولاً بصريح نص المادة الرابعة من النظام، فلا تقع الجريمة بالاستيلاء على العقار، ولكنها تقع بالاستيلاء على سندات ملكية هذا العقـــار. غير أنه لا يشترط أن يكون هذا المال مبالغ نقدية، بل يكفي أن يكون سنداً أو حتى تصل إلى وضع توقيع الغير بـــدون وجه حق على سند بدون وجه حق.

رابعاً: الاحتيال باتخاذ اسم كاذب أوصفة غير صحيحة

وهذه الوسيلة نص عليها المشرع الأردني في المادة(٣٦٦)من قانون العقوبات وهى اتخاذ الجاني اســـماً كاذبـــا أوصفةً غير صحيحة متى كان شأن ذلك خداع المجنى عليه وحمله على تسليم ماله.

1. **الاسم الكاذب.**ويقصد بالاسم الكاذب ان تحال الشخص لنفسه اسماً غير اسمه الحقيقي ،سواءً كان الاسم المنتحل لشخص حقيقي موجود أم لشخص وهمي لا وجود له . ويستوى في ذلك أن يكون الاسم المنتحل كاذباً برمته أي مختلفًا اختلافًا كاملاً عن الاسم الحقيقي أ وكان كاذباً في جزء منه أي مختلَف اختلافًا جزئياً عن الاسم الحقيقي.قد قضت محكمة التمييز الأردنية في حكم لها بإدانة المدعى عليه لانتحاله صفة وكيل مالك لأرض حيث قام باستلام قيمة الأرض من المشترين بناءً على كذبه وبيان نص الحكم على النحو التالي: "ثبت بالبينات الواردة في الدعوى أن المحكوم عليه قد ادعى لدى المشتكين بأنه يحمل وكالة ببيع قطعة أرض وأجرى الكشف عليها معهم وأطلعهم على مخططها في البلدية فانخدع المشتكون بأقواله وسلموه عشرين ألف دينار من ثمنها على أن يتم معاملة فراغها باليوم الثاني، وأخذ من المشترين جوازات سفرهم لإعداد معاملة البيع، وبما أن المحكوم عليه انتحل صفة وكيل مالك الأرض وأنه صاحب مكتب عقاري، فيتحقق البند الثالث من المادة 417 من قانون العقوبات فضلاً عن قيامه بالكشف على موقع الأرض وإطلاع المشتكين على مخططها لدى البلدية. هذه الأفعال معززة لكذبه بما يعني أنها تشكل ركناً من أركان جريمة الاحتيال ولم يكن فعله مجرد كذب" (قرار محكمة تمييز جزاء رقم2009/110 (هيئة خماسية) تاريخ 28/4/2009 المنشور على الصفحة 2185 من عدد مجلة نقابة المحامين بتاريخ 1/1/2010).
2. **الصفة غير الصحيحة.**حيث يدخل في دائرة المظاهر الاحتيالية استعانة الجاني بأوراق غير صحية ينسب صدورها إلى جهة مالية مثل الرسائل والعقود والمذكرات والشهادات وقد تكون هذه الأوراق سنداً مزوراً، فيعد محتالاً من يطالب شخص بدين يدعي أنه يستحقه في ذمة مورثهم وتأييداً لادعاءاته يتقدم بسند مزور قلد فيه إمضاء المورث (عبيد، 1985،ص460).

فقد قضت محكمة التمييز الأردنية بأنه (إذا زور المتهم سند صرف اللوازم الذي يعتبر من السندات الرسمية وحصل بموجبه على كمية من البنزين الخاص بأمانة العاصمة والذي لم يكن تحت إرادته أو حفظه حسب استعمال المستند كطريقة احتيالية لحمل الغير على تسليمه البنزين فإن عمله يشكل جريمتين مستقلتين:

1. جريمة التزوير خلاف المادة .265
2. جريمة الاحتيال خلاف لأحكام المادة 417. (تمييز جزاء (2011) رقم 2011/4مجلة نقابة المحامين النظامين الأردنيين، سنة 2010، ص 315)

ثانياً : النتيجة الإجرامية (الاستيلاء على مال يعود للغير).

من أجل قيام جريمة الاحتيال يجب أن تؤدى وسائل الاحتيال التي نص عليها المشرع إلى إيقاع المجني عليه في غلط يحمله على تسليم ماله إلى الجاني طواعية، ويعد هذا التسليم بمثابة النتيجة الإجرامية في جريمة الاحتيال، وبتحققه تصبح الجريمة تامة، فلا يكفي أن يبذل الجاني أحد أساليب الاحتيال بل يجب أن يُسفر هذا الأسلوب عن إيقاع المجني عليه في الغلط، كما يتعين أن يتم تسليم المال إلى الجاني تحت تأثير الغلط الذي وقع فيه، أما إذا تم التسليم بناء على سبب آخر انقطعت العلاقة السببية (سرور، 1985م.).

ولا يختلف الأمر بشكل عام في خصوص جريمة الاحتيال المعلوماتي، فالأساليب التي يستخدمها الفاعل يجب أن تسفر عن نتيجة إجرامية ألا وهي الحصول على ربح مادي غير مشروع، أو بقول آخر الاستيلاء على مال الغير، وذلك بتسلمه من المجني عليه تحت تأثير الغلط الذي أحدثه فعل الاحتيال، أي أن يكون هذا الاستيلاء راجعاً إلى فعل الاحتيال ذاته وإلا انقطعت العلاقة السببية(قوره، 2006، ص87)

وإذا كان من المتفق عليه أن الاحتيال المعلوماتي شأنه في ذلك شان الاحتيال بصفة عامة فينبغي أن يسفر عن تسليم المال محل النشاط الإجرامي وأن يكون هذا التسليم ثمرة للغلط الناشئ عن فعل الاحتيال فإن التساؤل الذي يكون هو -:هل يمكن أن يسلم الحاسب الآلي محل النشاط الإجرامي إلى الفاعل؟.

والواقع أن التسليم هو سلوك صادر عمن خدع بالاحتيال الواقع من الجاني بمقتضاه ينقل إلى الجاني أو إلى غيره المال موضوع الجريمة(هروال،2006م)، وبالنظر إلى بعض الحالات التي تندرج تحت وصف الاحتيال المعلوماتي نجد أن الحاسب الآلي يقوم بفعل التسليم بالمفهوم المادي للكلمة حيث إن التسليم ينطوي على معادلة يدوية كما هو الحال في الاحتيال الذي ينطوي على استعمال غير مشروع لبطاقات الائتمان سواء للوفاء بواسطتها أو لسحب النقود،أما في غير ذلك فإن تسليم المال لا يتم بصورة مادية والتسليم لا يجوز النظر إليه على أنه واقعة مادية تتمثل في مناولة ترد على شيء ينقله المجني عليه من سيطرته إلى حوزة المحتال ولكن يتعين النظر إليه على أنه عمل قانوني عنصره الجوهري إرادة المجنى عليه المعنية بالخداع وليست المناولة سوى المظهر المادي لهذا العمل أوهي على الأقل أثره (قوره، 2006).(إبراهيم، ٢٠١١م،ص133).

فإذا ما أخذنا بهذا المعن للتسليم فإنه لا يثير أي مشكلة في حالات الاحتيال المعلوماتي التي لا تنطوي على تسليم مادي للمال محل النشاط الإجرامي إذ يمكن القول أن تسليم المال يتم في شكل عمليات حسابية يقوم بها الحاسب الآلي بحيث لا يصل المال إلى يد الجاني بصورة مباشرة.

ونخلص من ذلك إلى أن الاحتيال المعلوماتي لا يختلف في هذا الشأن عن الاحتيال في صورته التقليدية،فالتسليم لا يعني في كلتا الحالتين المناولة اليدوية فقط بل يتجاوز ذلك على حالات لاتحقق فيها المناولة،فجوهر التسليم في جريمة الاحتيال أن يكون المجني عليه قد اتجهت إرادته إلى وضع الشيء في متناول يد الجاني أو تحت أمره،وكذلك الأم رفي الاحتيال المعلوماتي ، فالعبرة هنا بوضع المال محل النشاط الإجرامي تحت تصرف الجاني تحت تأثير الأساليب الاحتيالية التي مارسها الأخير.(عثمان،2004،ص543)

ثالثاً : العلاقة السببية .

لتحقيق جريمة الاحتيال يجب أن توجد علاقة سببية بين فعل الاحتيال و الغلط،أي أن يكون وقوع المجني عليه في الغلط ناتجاً عن وسائل الاحتيال التي استخدمها الجاني في تدعيم كذبه،حيثلاتتحقق جريمة الاحتيال إذا كان ما قام به الجاني مجرد كذب دون أن يستخدم إحدى وسائل الاحتيال،وسلم المجني عليه ماله إلى الجاني رغم ذلك، فإن علاقة السببية تنتفي لأنه لايوجد رابطة بين فعل الاحتيال وتسليم المال(هروال،2006م).

وقد يتوافر فعل الاحتيال ولكنه لا يؤدي إلى وقوع المجني عليه في الغلط كما إذا صدر على الجاني كذباً مدعماً بإحدى وسائل الاحتيال ولكن المجني عليه لم يقع في الغلط لكشفه خداع الجاني،وسلمه ماله رغم كشفه لخداعه فإن علاقة السببية تنتفي بين فعل الاحتيال وتسليم المال (أحمد، 1994 م).

. كذلك من يحاول خداع آخر فيكتشف خداعه ولكنه يسلمه المال الذي طلبه على سبيل الإحسان أو للتخلص من إلحاحه لايرتكب جريمة الاحتيال لأن صاحب المال لم يقع في الغلط، مما يترتب عليه انتفاء علاقة السببية بين الفعل وتسليم المال (الخليفة، 1423 ه).

وفي جريمة الاحتيال عبر شبكة المعلومات الدولية تتحقق العلاقة السببية إذا تحققت النتيجة الجرمية المترتبة على ممارسة الجاني للنشاط الإجرامي والمتمثل في التلاعب في البيانات و البرامج وذلك عن طريق الحاسب الإلكتروني، من أجل الحصول على ربح غير مشروع أو فائدة نتيجة ممارسة لهذا النشاط، بحيث يقال بأنه لولا هذا النشاط أو السلوك لما تحققت هذه النتيجة(تمام، 2000 ص 547.).

الفرع الثاني. الشروع في الاحتيال عبر شبكة المعلومات الدولية.

يعاقب المشرع الأردني على الشروع في جريمة الاحتيال، حيث نصت المادة (417) من قانون العقوبات على أنه "يطبق العقاب نفسه على الشروع في ارتكاب أي من الجنح المنصوص عليها في هذه المادة".وهي عوقب بالحبس من ثلاثة أشهر إلى ثلاث سنوات وبالغرامة من مائة دينار إلى مائتي دينار .

أما في المملكة ا لعربية السعودية فلا يوجد نظام معين يعاقب على الاحتيال إلا ما ورد متفرقاً في بعض الأنظمة ومن ذلك ما ورد في المادة الرابعة من نظام مكافحة الجرائم المعلوماتية وما لم يرد فيه نص نظامي فإن على المحكمة أ ن تطبق فيه أحكام الشريعة الإسلامية التي تجعل الاحتيال فعلاً معاقباً عليه ا ستناداً إلى قاعدة تحريم أكل أموال النـــاس بالباطل، وتكون تحديد العقوبة وفقاً لمـــا يتجـــه إليـــه ا لـــرأي فـــي المـــذهب الحنبلـــي المعـــول بـــه فـــي الـــبلاد (عودة،١٩٧٧،ص539.).

ويُعرف الشروع وفقاً للمادة (68) من قانون العقوبات الأردني على أنه البدء في تنفيذ فعل من الأفعال الظـــاهرة المؤدية إلى ارتكاب جناية أو جنحة، فإذا لم يتمكن الفاعل من إتمام الأفعال اللازمة لحصول تلـــك الجنايـــة أو الجنحـــة لحيلولة أسباب لا دخل لإرادته فيها عوقب على الوجه الآتي إلا إذا نص القانون على خلاف ذلك.

ونرى أنه في حالة تجريم الاحتيال عبر شبكة المعلومات الدولية، فإن المشرع يجب أن يتجه إلى العقـــاب علـــى الشروع فيه باعتبار أن الأفعال التي يقوم بها تمثل خطراً على الحق الذي يحميه النظام. .

والشروع نوعان: شروع تام وفيه يحقق الجاني النشاط الإجرامي كاملاً، وعلى الرغم من ذلك لا تتحقق النتيجـــة الإجرامية لأسباب لا دخل لإرادته فيها ويطلق عليه كذلك تعبير الجريمة الخائبة.

أما النوع الثاني: فهو الشروع الناقص حيث لا يكتمل النشاط الإجرامي لسبب أيضاً يخـــرج عـــن إرادة الفاعـــل ويطلق عليه الجريمة الموقوفة(الغزاوي ، 2005م ،ص99).

ونرى أن الشروع بنوعيه يتحقق في جريمة الاحتيال عبر شبكة المعلومات الدولية، فالمنظم السعودي والأردنـــي ذهبا إلى أن وقوع الجريمة يتحقق بالدخول إلى النظام، أما محاولة الدخول إلى النظام بطريق غير مشروع وهو عمـــل "الهاكر" الذي يحاول تخمين كلمة المرور وقد لا ينجح، فإن ذلك مُعاقب عليه بوصف الشروع .

وقد أحسن المنظم السعودي بالنص صراحةً على الشروع في المادة العاشـــرة مـــن نظـــام مكافحـــة الجـــرائم المعلوماتية والتي تنص على أنه "يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظـــام بمـــا لايتجاوز نصف الحد الأعلى للعقوبة المقررة ".

فإذا قام المتهم بمحاولة الاستيلاء على أموال الغير بطريق الاحتيال ولكنه لم يتمكن من ذلك بسبب دقـــة نظـــام الحماية الموضوعة لأجهزة البنك فإنه يُعدُّ مرتكباً للشروع في هذه الجريمة وفقاً لما تقرره المادة العاشـــرة مـــن قـــانون العقوبات الأردني المشار إليه.

كما يلاحظ أن المادة الرابعة من النظام السعودي تعاقب على محاولة الاستيلاء على أي أموال من البنك حتـــى وإن لم يتمم المتهم جريمته بالاستيلاء على المال المقصود، فتنص المادة الرابعة على عقـــاب الوصـــول دون مســـوغ نظامي صحيح إلى بيانات بنكية أو ائتمانية للحصول على أموال .... والعقاب المقرر هو السجن مدة لا تزيد على ثلاثة سنوات والغرامة التي لا تزيد على مليوني ريال أو إحدى هاتين العقوبتين.

المطلب الثاني: الركن المعنوي لجريمة الاحتيال عبر شبكة المعلومات الدولية.

تعتبر جريمة الاحتيال عبر شبكة المعلومات الدولية جريمة عمدية تقوم على القصد الجنائي العام بركنيـــه العلـــم والإرادة، حيث يجب أن تتجه إرادة الجاني إلى فعل الاختراق، أو إلى فعل إعاقة تشغيل النظام، أو إلى فعل الإدخـــال أو المحو والتعديل(الشنوي، ،2008،ص120) . وهذه كلها صور في السلوك الإجرامي في هذه الجريمة، كمـــا يجـــب أن يعلم بأن نشاطه غير مشروع وأنه يعتدي على صاحب الحق في المعطيـــات، أو مـــن لـــه الســـيطرة عليهـــا(قـــوره، 2006م).وجريمة الاحتيال عبر شبكة المعلومات الدولية شأنه في ذلك شأن جريمة الاحتيال بصورتها التقليديـــة وهـــي جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي، فإن لم يثبت توافره لدى الجاني لا تقوم مســـؤوليته مـــن أجل هذه الجريمة.

الفرع الأول : القصد العام.

يتطلب القصد العام في جريمة الاحتيال عبر شبكة المعلومات الدولية أن يعلم المتهم أن التلاعب الذي يحدثه بالمعلومات التي يحتويها علمياً نظام الحاسب الآلي أو أن المعلومات التي يقوم بإدخالها إلى هذا النظام من شأنها أن تجعل الحاسب الآلي يستجيب وفقاً لهذه المعلومات فيقوم بتنفيذ ما يعهد إليه من تعليمات. فيجب أن يتصرف علم الفاعل أولاً إلى أن ما يقوم بإدخاله من معلومات إلى نظام الحاسب الآلي يعدُّ من قبيل التلاعب بهذه المعلومات فمن يعتقد أن التعديل الذي يُلحقُه بالمعلومات داخل نظام الحاسب الآلي ضروري حتى تقوم هذه المعلومات بدورها على نحو صحيح داخل هذا النظام لا يتوافر لديه القصد المتطلب لقيام الجريمة(عياد، 2007). وكذلك من يعتقد أن من حقه إدخال المعلومات إلى نظام الحاسب الآلي كما لو قام الحامل الشرعي للبطاقة باستخدامها على الرغم من إلغائها من قبل الجهة المانحة وهو غير عالم بذلك(الخليفة، 1423 ه).

ويجب أن يعلم الجاني أن المال الذي يستولى عليه مملوك لغيره، ويستوي أن يكون عالماً أنه مملوك للمجني عليه أو لشخص آخر غيره وهو الوضع الغالب في الاحتيال عبر شبكة المعلومات الدولية وبصفة خاصة في الحالات التي ينطوي على تحويل الكتروني غير مشروع للأموال حيث لا يعلم الفاعل في كثير من الأحيان شخصية المجني عليه (مجازي، 2005، ص 190)

الفرع الثاني: القصد الخاص.

يذهب بعض الفقهاء إلى أنه لا يشترط لقيام جريمة النصب توافر القصد الخاص حيث إن الاستيلاء على المال هو نتيجة للاحتيال ولذلك فإن إرادة النتيجة ما هي إلا نية تملك الشيء، فنية التملك – وفقاً لهذا الرأي -لا تمثل غايةً خاصة تخرج عن نطاق العناصر التكوينية للجريمة(عياد، 2007)، (رمضان، 1977).

بينما يذهب جانب كبير من الفقهاء إلى أن نية سلب ثروة الغير أو بعضها، أي نية التملك، تكون القصد الخاص في جريمة النصب (نمور، 1997، ص 213.).

وما يستقر في الوجدان ما ذهب إليه الرأي الأخير الذي ذكره الدكتور محمود نجيب حسني إلى أن الركن المعنوي في جريمة الاحتيال يتخذ صورة القصد الخاص والذي يقوم بينة المتهم أن يباشر على الشيء الذي تسلمه من المجني عليه مظاهر السيطرة التي يخولها حق الملكية (حسني، 1984 ص211 .).

وينطبق ما تقدم على جريمة الاحتيال عبر شبكة المعلومات الدولية، حيث يجب أن تتجه نية المتهم إلى تحقيق ربح غير مشروع له أو للغير، وهو ما تطلبه التوصية الصادرة عن المجلس الأوروبي وعبرت عنه بنية تحقيق ربح غير مشروع للفاعل أو لغيره (مجازي، 2005، ص 190).

ومتى توافر القصد العام والخاص على النحو السالف بيانه فلا عبرة بعد ذلك بالباعث على ارتكاب الجريمة إذ إن الباعث ليس من عناصر القصد، فإذا قام الفاعل بالتلاعب في المعلومات المبرمجة لإجراء تحويل الكتروني للأموال لاستيفاء دين له أول إظهار مهارته في مجال تكنولوجيا الحاسبات الآلية فإن توافر مثل هذه البواعث لا ينفي قصد الاحتيال. (المشهداني، 2001م ،ص122).

المطلب الثالث: عقوبات جريمة الاحتيال الالكتروني وفق النظام السعودي والقانون الأردني.

ففي نظام مكافحة جرائم المعلوماتية السعودي تتمثل عقوبات جرائم الاستيلاء على مالٍ منقولٍ، أو الاستيلاء على سندٍ أو توقيعه وذلك عن طريق الاحتيال، أو اتخاذ اسمٍ كاذب، أو انتحال صفةٍ غير صحيحة المنصوص عليها في المادة الرابعة من نظام مكافحة جرائم المعلوماتية بالسجن والغرامة، أو بواحدة من هاتين العقوبتين، وذلك وفقاً لما يلي:

السجن وقد حددت المادة الحد الأعلى للسجن في الجرائم السابقة، وذلك بما لا يتجاوز ثلاث سنوات.

ولم تضع حداً أدنى، باستثناء ما سيأتي من الظروف المشددة للعقوبة، والتي تجعل الحد الأدنى للسجن نصف المدة، وبالتالي لا تقل مدة السجن في تلك الحالات عن سنة وستة أشهر.

الغرامة والغرامة المقررة في الجرائم السابقة يجب أن لا تتجاوز مبلغ مليوني ريال، ولم تضع حداً أدنى كذلك، إلا في الظروف المشددة، حيث يجب أن لا تقل الغرامة فيها عن النصف وهو مبلغ مليون ريال سعودي.

اما عقوبات المادة الخامسة المتعلقة بجرائم الاعتداء على البيانات الخاصة والشبكات العامة والخدمات الإلكترونية، وتتمثل بالسجن والغرامة، أو بواحدة من هاتين العقوبتين، وذلك وفقاً لما يلي:

السجن وقد حددت المادة الحد الأعلى للسجن في الجرائم السابقة، وذلك بما لا يتجاوز أربع سنوات.

ولم تضع حداً أدنى، باستثناء ما سيأتي من الظروف المشددة للعقوبة، والتي تجعل الحد الأدنى للسجن نصف المدة، وبالتالي لا تقل مدة السجن في تلك الحالات عن سنتين.

الغرامة والغرامة المقررة في الجرائم السابقة يجب أن لا تتجاوز مبلغ ثلاثة ملايين ريال، ولم تضع حداً أدنى كذلك، إلا في الظروف المشددة، حيث يجب أن لا تقل الغرامة فيها عن النصف وهو مليون وخمسمائة ألف ريال سعودي. ويلاحظ من المادة الرابعة انها تجمع بين عقوبات أصلية وعقوبات تكميلية.

من ناحية العقوبات الأصلية قرر النظام عقوبة السجن وقرر عقوبة الغرامة مع السجن جوازية للمحكمة بقوله "أو بإحدى هاتين العقوبتين". فقد خول النظام المحكمة سلطة الحكم بعقوبة السجن أو الغرامة؛ فإن قضت المحكمة بأحدهما كانت عقوبة أصلية، كما أجاز للمحكمة أن تحكم بالغرامة بالإضافة إلى السجن؛ عندئذ تصبح الغرامة عقوبة تكميلية للسجن.

أيضا يلاحظ من المادة الرابعة انها اخذت بالتخيير بين عقوبة الغرامة وعقوبة السجن فوفق المادة الرابعة تقرر عقوبة غليظة لجرائم المعلوماتية أي عقوبة مرتفعة في حدها الأقصى وهو السجن، فإنه يراعى في نفس الوقت أن يكون هناك حدا أدنى منخفض يتمثل في أنه أورد عقوبة الغرامة (دون أن يورد حدا أدنى) بدلاً من عقوبة السجن في كثير من جرائم المعلوماتية. كما أن الحد الأدنى لعقوبة السجن هي يوم واحد، مادامت الجريمة لم يتوافر فيها ظرف مشدد. ويدل ذلك على رغبة المنظم في زيادة السلطة التقديرية للقاضي الجزائي حتى يواجه فروضا عديدة يضيق عنها أي تعداد حصري حيث تتوقف كثير من الجرائم المعلوماتية على تحديد ظروف كل واقعة من حيث أهمية النظام وأهمية المعلومات التي كانت محلا للجريمة، وشخص المتداخل وأسباب التداخل وحجم الضرر الناجم عن تلك الجرائم ومدى تعلقها بأمن الدولة أو بمعلومات هامة.

اما قانون الجرائم الإلكترونية الأردني منح المنظم الأردني للقاضي سلطات تقديرية واسعة في إقرار ما يصل إليه باجتهاده، وإصدار الأحكام بالعقوبات المناسبة بحق الجاني وفقاً لما يراه، ويظهر ذلك جلياً في عدم تحديد العقوبة من قبل المشرع في بعض المواد ومنها المادة (3) التي تنص على انه(يعاقب كل من دخل قصداً إلى الشبكة المعلوماتية أو نظام معلومات باي وسيلة دون تصريح أو بما يخالف أويجاوز التصريح، بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار أو بكلتا هاتين العقوبتين...).

فوفق المادة (3) "يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين" ، كما أجاز المشرع إمكانية الجمع بين عقوبتي السجن والغرامة بقوله "أو بهما معاً" في إشارة منه لتشديد العقوبة حال ارتكاب الفعل في حالات خاصة، وفي مواضع أخرى يجدد مقدارها وفق ما ورد في المادة الثانية عشرة .

أما في النظام السعودي فقد اشتمال المادة (4) و (5) كما وضحنا على عقوبات محددة بحد أقصى وفقاً للجرائم المنصوص عليها في طيات النظام، وبالنسبة لجريمة الاحتيال فقد حدد لها النظام السعودي حسب ما ورد في المادة الرابعة منه بألا تزيد مدة حبس الجاني على ثلاث سنوات وبغرامة لا تزيد عن مليوني ريال أو بإحدى هاتين العقوبتين.

المبحث الثالث:

أساليب الاحتيال المعلوماتي في التلاعب بالبينات والبرامج الإلكترونية بأشكالها المختلفة

تعتبر جريمة الاحتيال المعلوماتي من الجرائم المستحدثة المرتبطة بأجهزة الكمبيوتر إذ يمثل الاعتداء على البيانات والبرامج الإلكترونية مجالاً خصباً لارتكاب هذه الجريمة نظراً للتطور التكنولوجي السريع في هذا المجال إذ يتم الاعتداء على أنظمة المعلومات من اختراق أو تعديل أو تبديل أو حذف أو تعطيل أو من خلال المساس بالبرامج الإلكترونية والتلاعب بها وتقليدها من أجل الحصول على ربح غير مشروع(عبد الشافي. 1999،ص156).وفي هذا المبحث نتناول أساليب التلاعب في البينات والبرامج الإلكترونية بأشكالها المختلفة ضمن المطالب التالية:

المطلب الأول:

التلاعب في المدخلات والبيانات المخزونة

إن أكثر حالات الاحتيال المعلوماتي تنطوي على تلاعب في المعلومات والبيانات التي يتم إدخالها إلى النظام، وفي هذا المطلب نتناول مفهوم المدخلات والبيانات المخزونة والتلاعب بها في مرحلة إدخال المعلومات ضمن الفروع التالية:

الفرع الأول: مفهوم المدخلات والبيانات المخزونة.

و تتمثل عملية الإدخال في تغذية الحاسب الآلي ونظامه بالمعلومات والبيانات المراد معالجتها آليا أو بتعليمات لازمة لعملية المعالجة وقد تتم عملية الإدخال عن طريق من قام بالتلاعب في المعلومات أو عن طريق شخص آخر والذي يكون حسن ا لنية في بعض الأحيان. (Sussmann, M. A. 1999 pp. 89),

أما البيانات المخزونة فهي عبارة عن معلومات أ وأوامر أو رسائل أو أصوات،أو صور التي أعدت أو سبق إعدادها لاستخدامها في الحاسب الآلي(حجازي، 2007)..

وقد عرفت الفقرة (4) من المادة (الأولى) من نظام مكافحة جرائم المعلوماتية السعودي (البيانات) بأنها:

(المعلومات، أو الأوامر، أو الرسائل، أو الأصوات ، أو الصور التي تعد أو التي سبق إعدادها،لاستخدامها في الحاسب الآلي، كالأرقام والحروف والرموز وغيرها) .وعرفت الفقرة(2) من ذات النظام(النظام المعلوماتي) بأنه:(مجموعة برامج و أدوات معدة لمعالجة البيانات و إدارتها ، و تشمل الحاسبات الآلية).

وعرف المنظم الأردني المعلومات في المادة (الثانية) من قانون المعاملات الإلكترونية رقم 85 لسنة 2001 بأنه: (النظام الإلكتروني المستخدم لإنشاء رسائل المعلومات أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو تجهيزها على أي وجه آخر .(وعرف المعلومات بانها: (البيانات والنصوص والصور والأشكال والأصوات والرموز وقواعد البيانات وبرامج الحاسوب وما شابه ذلك).

كما أشار قانون جرائم أنظمة المعلومات رقم (30) لسنة (2010) في المادة(الثانية)إلى البيانات وعرفها بأنها (الأرقام والحروف والرموز والأشكال والأصوات والصور التي ليس لها دلالة بذاتها).

ومن خلال التعريفات السابقة نرى أن المنظم السعودي والأردني أوردا تعريفاً للمعلومات بحيث ميزا بين المعلومات والبيانات على اعتبار أن المعلومة هي محل الاعتداء إذ إن البيانات تكون مجردة وبعد إدخالها ومعالجتها آلياً بالحاسب الآلي تصبح معلومات وتكون محلاً للاعتداء عليها.

ومن أبرز مميزات نظام مكافحة جرائم المعلوماتية السعودي أنه توسَّع في إدخال مجموعة كبيرة من الأمور التي تدخل في مفهوم "البيانات"، بحيث تشمل كما سبق: كل ما يُعد أو ما سبق إعداده أو ما يمكن تخزينه أو معالجته أو نقله أو إنشاؤه، بحيث يستخدم في الحاسب الآلي، أو يستخدم الحاسب الآلي في إنشائه،ولذا فإن النظام يعالج بهذا التوسع ما يستجد مستقبلاً من البيانات والمعلومات التي تدخل في عموم هذا التعريف الموسَّع لمصطلح "البيانات".

الفرع الثاني:التلاعب في المدخلات والبيانات في مرحلة إدخال المعلومات.

تتنوع وسائل التلاعب بالبيانات في هذه المرحلة سواء تم ذلك أثناء عملية الإدخال أو في مرحلة إعداد المعلومات للإدخال، ويمكن حصرها بالوسائل التالية:

الوسيلة الأولى: تغير البيانات والمعلومات المراد إدخالها دون أي حذف لها:

تتمثل هذه الوسيلة في تغير المعلومات والبيانات المراد إدخالها إلى النظام دون أن يتضمن ذلك حذفاً لجزء منها أو أجزاء منها(حجازي، 2007) ، وقد ذهب القضاء الفرنسي إلى أن إدخال معلومة بعد إجراء تعديل عليها أو ويعني بذلك إدخ المعلومة غير صحيحة إلى نظام الحاسب الآلي بنية الحصول من وراء ذلك على ربح غير مشروع للجاني أو لغيره فإن ذلك يعد من قبيل الطرق الاحتيالية(الحربي، 2008)

وقد يكون هذا التغير للإدخال كلياً، أي يشمل المعلومات بأكملها أو جزئياً بتعديل بجزء دون الآخر، أو إضافة جزء جديد لها ليس فيها، أو استبدال معلومة بأخرى. ويؤدي كل ما سبق إلى تغير معنى المعلومة بحيث تصبح غير معبرة عن حقيقتها الأساسية التي كانت موجودة بها قبل إجراء التعديل(قوره، 2006، ص87)، (الكعبي،2015).

وحسب الدراسة المسحية التي أجرتها الخطة الوطنية لتقنية المعلومات في السعودية على عينة عشوائية تتجاوز 700 شخص في المملكة، اتضح أن 17% من أفراد العينة يقومون بمحاولات اختراق مواقع وأجهزة الأفراد والمؤسسات لتغير البيانات والمعلومات المراد إدخالها، وهذه النسبة عالية بكل المقاييس. وبعد انتشار الإنترنت، زادت الاعتداءات بشكل كبير وذلك بسبب سهولة الحصول على برامج الاختراق وعناوين البريد الإلكتروني وغيرها(مشروع الخطة الوطنية لتقنية المعلومات، الرياض، ذو الحجة 1423هـ).

الوسيلة الثانية: تغير البيانات عن طريق اتلافٍ أو حذف أو التعديل.

تقع جريمة الإتلاف في نطاق المعلومات بالاعتداء على الوظائف الطبيعية للحاسوب وذلك بالتعدي على البرامج والبيانات المخزنة والمتبادلة بين الحاسوب وشبكاته الداخلية (المحلية) أو العالمية (الإنترنت) ويكون ذلك بطريق التلاعب بالبيانات سواء بإدخال معلومات مصطنعة أو بإتلاف المعلومات بمحوها أو تعديلها أو تغيير نتائجها أو بطريق التشويش على النظام المعلوماتي بما يؤدي إلى إعاقة سير النظام الآلي بصوره المختلفة (الغزوي، 2005م).

ويكون الإتلاف العمدي للبرامج والبيانات بمحوها كلية أو تدميرها إلكترونيا أو تشويهها على نحو فيه إتلاف بما يجعلها غير صالحة للاستعمال(الكعبي، 2015).وقد تطرق المنظم السعودي إلى الإتلاف العمدي فيالمادة الخامسة من نظام مكافحة جرائم المعلوماتية السعودي :(يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية: الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.) (عبد الجبوري،2014،ص66).

كما تناول المنظم الأردني الإتلاف العمدي للبرامج في الفقرة (ب) من المادة (3) من قانون جرائم أنظمة المعلومات فقد نص على أنه :(إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع الكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (200)مائتي دينار ولا تزيد على(1000) ألف دينار أو بكلتا هاتين العقوبتين.

وفق النصيين السعودي والأردني يتم الاكتفاء بالعقاب على الدخول غير المشروع إذا كان غرض الجاني هو العبث بالمعلومات داخل الكمبيوتر وذلك بالتغيير أو بالحذف.

وبتأمل ما ورد في المادة الخامسة من نظام مكافحة جرائم المعلوماتية السعودي نجد أن هناك ثغرة في هذا التجريم، إذ كان من الأولى أن يعاقب النظام على التغيير أو الحذف في حد ذاته، بالإضافة إلى الدخول بغرض التغيير أو الحذف. أما ما أوردته المادة الخامسة من العقاب على "إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها" ، فإن ما ورد فيها بشأن العقاب على البيانات جاء خاصاً بالشبكة المعلوماتية والبرامج أو البيانات الموجودة بها، أما إذا تعلق الأمر ببيانات لا توجد في شبكة معلوماتية، فإن النص يقف قاصراً عن العقاب عليها(Saqeer, J. A. 2001 p.25.).

الوسيلة الثالثة: التلاعب في المعلومات بحيث لا تؤدي وظيفتها.

يتم الاعتداء على المعلومات مما يحول دون أدائها لوظائفها من خلال إخفاء المعلومات أوإدخالها في موقع آخر غير المكان المخصص لها، مع بقاء المعلومة صحيحة ولا يتم التلاعب بها أوتغيرها (Saqeer, J. A. 2001 p.18.).

وفي هذه الحالة يسعى الجاني لإخفاء بعض المعلومات المتعلقة به أو بوضعه المادي أوإخفاء معلومات متعلقة بالمؤسسات من أجل جذب الاستثمار والحصول على الأموال من خلال إخفاء بعض المعلومات المتعلقة بوضعها المالي الحقيقي مما تساعد على تنفيذ الجاني لنشاطه الإجرامي (Sussmann, M. A. 1999 pp. 89),.

ثانياً: التلاعب في البيانات في مرحلة الإخراج.

تفترض هذه الحالة دخول المعلومات إلى جهاز الكمبيوتر صحيحة حتى يتصور التلاعب بها وتغير حقيقتها في مرحلة الإخراج سواء بتغير المعلومة أو تعديلها أو حذف جزء منها فالعبرة في إخفاء حقيقة الجريمة لإتمام جريمة الاحتيال أو إخفاء أي أثر لها(الغزوي، 2005م).

المطلب الثاني :التلاعب بالبرامج الإلكترونية للنظام المعلوماتي

يلاحظ أنه في كثير من حالات الاحتيال المعلوماتي التي تتم عن طريق التلاعب في المدخلات أو التلاعب في البيانات في مرحلة الإخراج،إن درجة المعرفة بتقنية المعلومات المتطلبة في الفاعلين قليلة جداً وذلك على عكس الحال فيما يتعلق بالتلاعب في البرامج إذ يتميز بقدر كبير من التعقيد وهو ما يحدد بدوره فئة الجناة الذي نيقومون بهذا التلاعب، ومن ناحية أخرى يُعدُّ هذا النوع من التلاعب من أصعب الوسائل من حيث إمكانية اكتشافه كما أنهمن أكثر الوسائل خطورة (العريان، 2004م).

ويتم التلاعب في بالبرامج الإلكترونية بصفة عامة عن طريق إحدى الوسائل التالية:

الوسيلة الأولى: التلاعب ببرنامج التشغيل.

يتم الاعتداء على برامج التشغيل من خلال تزويد البرنامج بمجموعة من التعليمات الإضافية من أجل الوصول إلى كلمة السر أو الشفرة أو مفتاح الربط بكل يسر وسهولة ويتم تعديل البرامج من خلال ممرات وفجوات خالية في البرنامج يمكن الوصول من خلالها إلى كافة التعليمات التي يحتويها، ومن ثم الوصول إلى الشفرة والتعليمات أو عن طريق البرامج الوهمية أو الناقصة (Smith,RussellG,2001,pp15) وسوف نتناول وسائل الاعتداء على البرامج التشغيلية على النحو التالي:

1-تغيير البرامج المطبقة.

تتمثل الوسيلة الأولى في تغيير البرامج المطبقة بالفعل داخل المؤسسة المجني عليها وذلك بإدخال تعديلات غير مرخص بها على البرامج المستخدمة فكثير من البرامج بعد إعدادها واختيارها قد تمر ببعض التعديلات لتصويب أخطاء اكتشف تبعد العمل بها وهو ما يتيح في هذه الحالة إدخال تغيرات من شأنها أنت ساعد الجاني على إتمام جريمته وكذلك إخفائها كما قد يتم إجراء هذا التعديل عن طريق استخدام البرامج الخبيثة(الفيروسات)(حجازي، 2007).

2_ تطبيق برنامج إضافية

تتمثل هذه الوسيلة في تطبيق برامج إضافية يتمك شفها عن طريق الجناة أن فسهم أو قد تكون برنامج معدة سلفاً تهدف بشكل أساسي إلى تعديل المعلومات في الحاسبات الآلية عن طريق إجراء تعديلات مباشرة في ذاكرة الحاسب كما قد يتم الاستعانة ببعض البرامج المعدة للاستخدام في أوقات الأزمات لتخطي الإجراءات الأمنية الموضوعية(قايد، 2007).

ولتوضيح هذه الوسيلة من وسائل الاحتيال الالكتروني سنعرض الحالة التالية:

تتلخص وقائع هذه الحالة في قيام مبرمج يعمل بأحد مكاتب الخدمات تمت الاستعانة به بواسطة إحدى الشركات المختصة ببرمجة نظم المعالجات الآلية بالبنوك و أثناء قيامه بكتابة البرنامج الخاص بالبنك الذي يتعامل معه قام بكتابة هذا البرنامج بحيث يتجاهل السحب بما يجوز الرصيد الخاص به ولم يتم اكتشاف هذا التلاعب إلا حينما تعرض نظام الحاسب الآليب البنك للعطل،وتم التعامل مع الحسابات بطريقة يدوية وكان التجاوز في ذلك الوقت يبلغ١٣٥٧،٣٣دولار ومن المثير للدهشة أنه بعد أنتم القبض عليه ومحاكمته أسفرت المحاكمة عن حكم بالإدانة مع إيقاف التنفيذ ثم الاستعانة بهمرة أخرى من قبيل هذه الشركة نظرا لكفاءته الكبيرة في مجال كتابة البرامج(Naserat, 2016, p. 18).

3_ تصميم وإعداد البرامج الوهمية:

تتمثل هذه الوسيلة بإعداد برنامج كامل يتم صناعته وإعداده وتنسيقه من أجل ارتكاب جريمة الاحتيال عبر شبكة المعلومات الدولية (المهيني، 2001م). وفي حالة استخدام هذا البرنامج من قبل مبرمجيه فإنه يقوم بتعطيل عمل البرنامج الأصلي ويدخل البرنامج الوهمي مكانة ويتم التعامل معه من قبل الغير على اعتباره برنامجاً أصلياً لتشغيل نظم المعلومات وبالتالي يستطيع المحتالون الحصول على الأموال المملوكة للغير (الغزوي، 2005م).

ولتجنب هذه البرامج توجد علامتان تحذيريتان شائعتان للرسالة الوهمية هما عدم وجود شعار الشركة، أو طلب للحصول على معلومات عن بطاقة الائتمان إذا كنت تستخدم بالفعل برنامجاً مشهوراً وبارز لمكافحة الفيروسات، (الملط، 2006م، ص174).

الوسيلة الثانية: التلاعب في المكونات المادية للحاسب.

لا تقتصر الأساليب المستخدمة للاحتيال عبر شبكة المعلومات الدولية على التلاعب في البرامج المسئولة عن تشغيل نظام الحاسب الآلي، وإنما قد تمتد أيضاً إلى العناصر الميكانيكية التي تسيطر على الحاسب الآلي، أو إلى الدوائر المختلفة التي يتألف منها النظام، ولا شك أن مثل هذا التلاعب يتطلب درجة كبيرة من العلم بتقنية الحاسب الآلي وهو ما يؤدي بدوره إلى الحالات التي تستخدم فيها مثل هذه الوسيلة للاحتيال، والتي تستخدم فيها هذه الوسيلة (عبدالله، 2007، ص 96).

الوسيلة الثالثة: التلاعب في البيانات التي يتم تحويلها عن بعد.

إن التزايد الكبير في استخدام نظم معالجة البيانات عن بعد في السنوات الأخيرة كان له تأثير كبير في تطوير الوسائل المختلفة المستخدمة للاحتيال في مجال تكنولوجيا المعلومات فالتلاعب في البيانات عن بعد عن طريق النهاية الطرفية أياًكان موقعها جعل الاحتيال أكثر سهولة من ناحية و أكثر صعوبة في اكتشافه من ناحية أخرى،في كفي أن يكون الحاسب الآلي متصلاً بوحدة التشغيل المركزية عن طريق شبكة الخطوط الهاتفية العادية أو غيرها من وسائل الاتصال حتى يتمكن الفاعل من إتمام عملية الاحتيال من داخل منزله

مستخدماً لوحدته الطرفية مند و نحاجة إلى الدخول إلى المؤسسة المجنى عليها(قايد، 2007). (مقابلة ،2008م)،بل إن وسائل الاتصالات الدولية على هذا النحو تساهم أيضاً في خلق الجريمة المعلوماتية متعدية الحدود إذ يرتكب النشاط الإجرامي في دولة لتحقق النتيجة الإجرامية في دولة أخرى(هروال،2006م).

ويمكن القولب أن التلاعب بواسطة وسائل الاتصالات أو التلاعب عن بعد هو الوسيلة الأكثر شيوعاً في التجسس المعلوماتي، أما فيما يتعلق بجريمة الاحتيال المعلوماتي فإن هذه الوسيلة تعدُّ أكثر ملاءمة للتمويل الالكتروني غير المشروع للأموال وهو احد أهم صور جريمة الاحتيال المعلوماتي(منشأوي، 2002)..

ومن أشهر الحالات التيتم فيها الاحتيال عن طريق التلاعب في البيانات عن بعد تلك الحالة الشهيرة التي استخدم فيها التلاعب في البيانات عن بعد في مجال التحويل الالكتروني للأموال تلك التي قام بها أحد الخبراء في الحسابات ويدعى(Stanly Mank Rifkin) عام١٩٧٨م في أحد البنوك بل وسان جلوس بالولايات المتحدة الأمريكية وهو (Bank Security Pacific) فقد قام المتهم بملاحظة كيفية إجراء عمليات التحويل الالكتروني والشفرة المستخدمة لذلك وذلك بفضل ما كان يتمتع به من حرية الحركة داخل البنك بصفة خاصة لتمكنه من دخول حجرة الأسلاك البرقية المركزية للبنك بحكم عمله خبيرا به وعن طريق هاتف خارج البنك استطاع أن يتصل بشبكة المعلومات الخاصة بالبنك وباستخدام الشفرة التي حصل عليها ولمعرفته بمختلف الإجراءات الأمنية التي تحمي النظام بالبنك و نقاط الضعف بها قام بتحويل عدة مبالغ وصل مجموعها إلى عشرة ملايين دولار أمريكي من حسابات البنك إلى حساب له فينيو يوركث مقام بتحويل معظمها إلى أحد البنوك السويسرية التي تعمل وسيطا رسميا للحكومة السوفيتية(سابقا) في تجارة الألماس ثم قام بشراء ما يقارب ثمانية ملايين دولار من الأحجار الكريمة(Smith, RussellG ,2001 ,pp23) .وربما بسبب الانخفاض النسبي في قيمة هذه التحويلات في محيط التعاملات البنكية في هذا المجال فإن الجريمة لميتم اكتشافها الا بعد ثمانية أيام من ارتكابها.

الوسيلة الرابعة: استعمال شفرة غير صحيحة للدخول إلى نظام مدفوع:

يعد استعمال شفرة غير صحيحة من أهم الوسائل للدخول غير المشروع إلى نظام مدفوع الأجر وهو ما يعدُّ بدوره صورة منصور الاحتيال المعلوماتي، والمقصود باستعمال شفرة غير صحيحة هو الدخول إلى النظم مدفوعة الأجر باستعمال شفرة مملوكة إلى شخص آخر أو باستعمال شفرة مملوكة للنظام نفسه–إذا تمكن الفاعل من الحصول عليها قبل بيعها–فليس المقصود إذاً أنت كون هذه الشفرة غير صحيحة في ذاتها وانما تستمد عدم صحتها من استخدامها من قبيل شخص لاحق له في ذلك، ولقد أثارت هذه الوسيلة الكثير من الجدل وبصفة خاصة في المملكة المتحدة بعد صدور الحكم الشهير في قضية (RV Gold) والذي كان له أبعد الأثر في صدور القانون الخاص بإساءة استخدام الحاسبات الآلية في المملكة المتحدة عام١٩٩٠م (Smith ,RussellG ,2001 ,pp34).

تتلخص وقائع القضية في تمكن المدعو(Gold) وشريكه SCHIFREEمن الحصول على الشفرة الخاصة التي أصدرتها هيئة الاتصالات البريطانية لأحد مهندسيها حتى يتمكن من استخدام نظام المعلومات الالكتروني الخاص بها (Prestel System) وهو نظام يوفر للمشتركين فيه قاعدة عريضة من البيانات والمعلومات نظير رسميد فعل لدخول إلى النظام بصفة عامة بالإضافة إلى ما يحمله المشترك من مقابل نقدي يختلف باختلافكم وصيغة المعلومات المطلوبة وباستخدام الشفرة الخاصة بالمهندس تمكن المتهمان من الدخول إلى النظام والحصول على الخدمة المطلوبة دون تحمل أين فقات وبعد مرور فترة من الوقت بدأ تهيئة الاتصالات ترتاب في نشاطGold)وبعد مراقبة هاتفه الخاص والرجوع إلى الحاسب الآلي(لبرستل) ثم الكشف عن نشاط(Gold).(Smith,RussellG ,2001 ,pp34).

المطلب الثالث:الاحتيال المعلوماتي من خلال التحويل الإلكتروني للأموال

الفرع الأول: التحويل الإلكتروني للأموال.

نظام التحويل الإلكتروني للأموال هو عملية منح الصلاحية لبنك ما للقيام بحركات التحويلات المالية الدائنة والمدينة إلكترونياً من حساب بنكي إلى حساب بنكي آخر(إبراهيم، ٢٠١١م).

ويعرف أيضاً بأنه تفريغ حساب شخص يسمى الآمر وبناء على طلب منه من مبلغ نقدي معين، وقيد هذا المبلغ في الجانب الدائن لحساب آخر قد يكون باسم الآمر نفسه أو باسم شخص آخر هو المستفيد(أبو الوفا ، 2003م).

ويمكن تعريف نظام التحويل الإلكتروني للأموال كما جاء في القانون الفيدرالي في الولايات المتحدة الأمريكية بأنه كل تحويل خاص بالأموال يبدأ من خلال نهاية طرفيه إلكترونية أو حاسب آلي أو شريط مغناطيسي عن طريق إعطاء الأوامر أو التعليمات لمؤسسة مالية لإجراء عملية سحب أو إيداع لأحد الأرصدة (عبد الله، 2007م،ص69).

الفرع الثاني: طرق التلاعب في نظم التحويل الالكتروني للأموال.

إن التلاعب في نظم التحويل الالكتروني للأموال قد يتم بأي وسيلة من وسائل الاحتيال المعلوماتي، فقدي تم التلاعب في البيانات في مرحلة إدخالها أو في البرامج أو في المكونات المادية للحاسب كما قد يتم التلاعب في البيانات أثناء تحويلها عن بعد بحيث يكون الغرض من هذا التلاعب تنفيذ تحويل غير مشروع للأموال،ومن أهم طرق التلاعب في نظم التحويل الالكتروني للأموال(العريان، 2004م).

1- اختراق الأجهزة الرئيسة للشركات المالية المختلفة والدخول إليها من خلال تخطي جدران الحماية كما هو الحال بالنسبة لاختراق البرامج الخاصة بالبريد الإلكتروني وانتحال شخصية ما لخداع الأنظمة المستخدمة بواسطة بيانات هذه الشخصية وتحويل أرصدة حساب إلى حساب آخر(منصور،2006).

2- التلاعب في المكونات المادية لأنظمة التحويل الإلكترونية للأموال عن طريق استخدام خطوط الاتصال أو السجلات الخاصة بنظم التحويل للاحتيال على البنوك والمؤسسات المالية (فورة ،ص 513).

3- الاعتداء على الإجراءات الداخلية لنظم المعلومات من داخل المؤسسة وهي ما تتم بواسطة موظفي المؤسسات المالية الذين يقومون بتحويل الحسابات لأرصدة جديدة أو وهمية يتم إنشاءها لتحويل هذه الأموال إليها وقد تحدث الجريمة من خارج المؤسسة المجني عليها عن طريق وسائل الاختراق السابقة الذكر.

4- الاحتيال باستخدام طرق احتيالية للاستيلاء على الشيكات الإلكترونية عن طريق تحويل بيانات الشيكات الكتابية إلى بيانات إلكترونية بحيث يتم تحويل الشيكات بناء على البيانات الإلكترونية بدلاً من حركة الشيكات التقليدية وتحويلها إلى حساب آخر غير الحساب المطلوب تحويل الشيكات إليه للدخول في حساباته (الزبيدي،2007م، ص 22).

ويقع في مسؤولية المؤسسة المالية عن التحويل الإلكتروني للأموال الالتزام بالحفاظ على السرية المصرفية عن طريق اتخاذ الإجراءات الكفيلة لذلك(عبد الجبوري،2014،ص96). وهذا ما نصت عليه المادة 26/ب من قانون المعاملات الإلكترونية الأردني الذي فرض على المؤسسات المالية المختلفة التقيد بأحكام قانون البنك المركزي الأردني وقانون البنوك والأنظمة والتعليمات المعمول بها وقد يقوم البنك بتحويل الأموال إلكترونياً إلى حساب آخر غير حساب العميل عن طريق الخطأ والإهمال مما يرتب عليه مسؤولية إبطال القيد بإجراء عكسي لاسترداد المبلغ أما إذا سحبته المستفيد فعلى المصرف المطالبة باسترداد المبلغ أما إذا تم القيد في حساب آخر بناء على خطأ من العميل فهو الذي يتحمل مسؤولية خطأه.

ويقع على المصرف مسؤولية عدم التأخير في تنفيذ أوامر التحويل وقد يسأل جزائياً إذا تم التحويل بمقدار مبلغ معين وتم زيادة هذا المبلغ.

فإذا تبين وجود تواطؤ مع الغير من أجل الاعتداء على مال العميل وتحويله إلى حساب المستفيد الآخر فإنه يُسأل عن جريمة احتيال وتقع على عاتق العميل مسؤولية عقدية وفقاً لنص م (27، 28) من قانون المعاملات الإلكترونية الأردني عليه الالتزام بها في حدود العمليات المصرفية أي عليه اتخاذ الحيطة والحذر والحفاظ على الرقم السري ويقع في مسؤوليته إبلاغ المؤسسة المالية عن إمكانية دخول الغير إلى حسابه أو فقدان بطاقته أو احتمال معرفة الغير لرمز التعريف المتعلق به والطلب منها وقف العمل بوسيلة التحويل الإلكترونية وبالتالي لا يعتبر مسؤولاً عن أي قيد غير مشروع في حسابه.

ويسأل العميل عن جريمة الاحتيال إذا ما تم الاتفاق مع غيره من أجل إجراء تحويلات مالية من حسابه إلى حساب المستفيد الآخر ومن ثم الرجوع على البنك والمطالبة باسترداد قيمة التحويل المالي.

المبحث الرابع

تجربة المملكة العربية السعودية والأردن في مكافحة جريمة الاحتيال عبر شبكة المعلومات الدولية

نتناول في هذا المبحث تجربة السعودية والأردن في مكافحة جريمة الاحتيال عبر شبكة المعلومات الدولية ضمن مطلبان يتنول كل منهما التشريعات الوطنية لمواجهة الاحتيال عبر شبكة المعلومات الدولية، ثم جهود الدولتان على المستوى الدولي لمواجهة هذه الجريمة وأخيراًنتناول المؤسسات المعنية بالمكافحة الاحتيال المعلوماتي.

المطلب الأول:

تجربة المملكة العربية السعودي في مكافحة جريمة الاحتيال عبر شبكة المعلومات الدولية.

في هذا المطلب نتناولالأنظمة الوطنية في الفرع الأول: تجربة السعودي لمكافحة جريمة الاحتيال على المستوى الدولي في الفرع الثاني،المؤسسات السعودية المعنية بمكافحة الجرائم المعلوماتية في الفرع الثالث.

الفرع الأول: الأنظمة والقرارات الوطنية.

أولاً : **الأنظمةالوطنية:**

تعتبر المملكة العربية السعوديأول دولة عربية سنّت أنظمة خاصة بمكافحة الجريمة الإلكترونية،فقد صدرت "قواعد ترخيص مقدمي خدمة الإنترنت" عام 1999 عن مدينة عبد العزيز للعلوم التقنية، ثم تلاها صدور نظام للاختراق الإلكتروني عام 10/20/ 1423هـ، حدد من خلاله الكثير من المصطلحات التشريعية حيث أوضح ماهية جريمة الاختراق، ومصادرها، وإجراءات الحد منها، وحدد مسؤوليات عناصر الارتباط بالشبكة المستفيد، مقدم الخدمة، وحدة الإنترنت .وفي عامفي عام7/ 1428/3هـ الموافق 2007/3/26م صدر نظام مكافحة جرائم المعلوماتية السعودي.

وحددت مواد النظام الجرائم المعلوماتية وعقوباتها التي تنوعت بين السجن لمدد مختلفة والغرامات المالية بحسب نوع وطبيعة كل جريمة من الجرائم المعلوماتية واختصاصات كل من "هيئة الاتصالات وتقنية المعلومات" و"النيابة العامة" في المساندة اللازمة للأجهزة الأمنية لتحقيق أهداف وغايات هذا النظام.

ويحدد النظام مجموعةً من الأهداف ومن أهمها حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية، كما يهدف إلى حماية المصلحة العامة والأخلاق والآداب العامة وكذلك حماية الاقتصاد الوطني، أيضاً منع إساءة الاستخدام والاحتيال في التعاملات والتوقيعات الإلكترونية".

وفي عام1429هـ الموافق 2008م صدر عن مؤسسة النقد العربي السعودي دليل مكافحة الاختلاس والاحتيال المالي وإرشادات الرقابة وبموجبة أصدرت المؤسسة عددًا من التعاميم بشأن الاحتيال تنولت موضوعات ومن أهمها : استراتيجية مكافحة الاحتيال وسياسة الرقابة ،إبلاغ سلطات الأمن بأعمال الاحتيال. إرشادات لمكافحة الابتزاز المالي والاحتيال، وحدة التحقيق بشأن الاحتيال، أمن أنظمة المعلومات، وغيرها من الموضوعات التي تتعلق بمكافحة الاختلاس والاحتيال المالي.

كما أقرت وزارة الداخلية السعودية لائحة الجرائم الكبرى الموجبة للتوقيف في المملكة العربية السعودية، وشملت 20 جريمة ومنها الجرائم المعاقب عليها بسجنٍ يزيد حده الأعلى عن سنتين الواردة في نظام مكافحة جرائم المعلوماتية.

الفرع الثاني: المستوى الدولي.

أولاً : الاتفاقيات الدولية:

وقعت المملكة العديد من الاتفاقيات الخاصة بمكافحة جرائم تقنية المعلومات كما التزمت بتنفيذ القرارات الدولية الصادرة عن مجلس الأمن في هذا الشأن، وصادقت على عدد من الاتفاقيات والمعاهدات الدولية ذات العلاقة منها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات حيث أقر مجلس الوزراء في جلسته التي عقدها يوم الإثنين 24 جمادى لأول 1433ه الموافقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ويأتي هذا الإقرار بعد أن وافق مجلس الشورى على مصادقة الاتفاقية، حيث بين الأمين العام للمجلس أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تأتي ضمن الجهود العربية الحثيثة التي تقوم بها جامعة الدول العربية لحشد التدابير الأمنية اللازمة تجاه مكافحة الجرائم في شتى أشكالها وصورها ومنها جرائم تقنية المعلومات عبر إيجاد الأسس النظامية والبيئة القانونية، منوهاً إلى أن الاتفاقية تعزز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات.

منأهم المؤتمرات التي شاركت بها المملكة:

- **المؤتمر السعودي الدولي الثالث لتقنية المعلومات – الأمن الإلكتروني(KACSTIT) .** حيث نظمته مدينة الملك عبد العزيز للعلوم والتقنية (KACST)في الفترة من 20 إلى 21 جمادى الثانية 1437هـ ، وذلك بقاعة المؤتمرات الكائنة بمدينة الملك عبد العزيز للعلوم والتقنية.
- المؤتمر الدولي للأمن الإلكتروني الذي نظمه المركز الوطني للأمن الإلكتروني بمقر نادي ضباط قوى الأمن بمدينة الرياض خلال الفترة من 20-21 ربيع الثاني 1437هـ - 23 يناير 2016م.
- المؤتمر الدولي الأول لمكافحة الجريمة المعلوماتية من 19-21 ربيع الثاني 1436هـ جامعة الإمام محمد بن سعود الإسلامية ،الرياض، المملكة العربية السعودية.

الفرع الثالث: المؤسسات السعودية المعنية بمكافحة الجرائم المعلوماتية.

أ. **اختصاص الجهات الأمنية.**أناط نظام مكافحة الجرائم المعلوماتية بالجهات الأمنية في المملكة مهمة ضبط الجرائم المعلوماتية، وأسند للنيابة العامة دور التحقيق في هذه الجرائم والادعاء فيها بالحق العام، وجعل لهيئة الاتصالات وتقنية المعلومات تقديم الدعم والمساعدة الفنية للجهات الأمنية، وكذا جهات التحقيق وأثناء المحاكمة.

- **مراكز الشرطة.**تتجه مراكز الشرطة في السعودية لمواجهة ملف جرائم الاحتيال الإلكترونية واستقبال البلاغات المتعلقة بقضايا عدة من بينها بث المواد الإباحية على الإنترنت والاختراقات الإلكترونية بغرض الابتزاز المادي أو الشخصي، إضافةً إلى رسائل التهديد واستخدامات والتحويلات البنكية المشبوهة.

- النيابة العامة.بعد إجراءات الضبط الابتدائي والاستدلالي للجريمة الإلكترونية، يتم التحقيق فيها من قبل الجهة المختصة (النيابة العامة)، بالتعاون في هذا المجال مع هيئة الاتصالات وتقنية المعلومات، فيما يتعلق بتبصير المحققين والمدعين بجوانب الجريمة الإلكترونية وكيفية الاستدلال عليها وضبطها والتحقيق فيها واستخراج الأدلة من مسرح الحدث وأداة الجريمة.

و بعد التحقيق واستخلاص الأدلة تنظر جهة التحقيق في مدى التوصل إلى إدانة المتهم من عدمه، وذلك بتكييف الجريمة الإلكترونية حسب نصوص النظام وقواعد الشرع. فإذا ما توصلت إلى إدانته، أصدرت قرار اتهام بحيث يتولى المدعي العام إحالة الدعوى إلى المحكمة المختصة، وهي بحسب التنظيم القضائي (نظام القضاء) الجديد الصادر بالمرسوم الملكي رقم 78 وتاريخ 1428/9/19هـ، فإن الاختصاص ينعقد للمحاكم الجزائية وفق اختصاصها المبين في نظام القضاء.

1. الاختصاص التقني.

تتمثل بهيئة الاتصالات وتقنية المعلومات.حيث أطلقت هيئة الاتصالات وتقنية المعلومات، عام 1435هـ، حملتها التوعوية للتعريف (بنظام مكافحة جرائم المعلوماتية) بهدف رفع مستوى الوعي بسبل مكافحة الجرائم المعلوماتية، وبيان حقوق المستخدمين وفق ما كفله النظام لهم، مع التوعية بسبل الوقاية من خطر الوقوع ضحايا لأي نوع من هذه الجرائم.

وتهدف الحملة إلى لفت انتباه مستخدمي خدمات الاتصالات وتقنية المعلومات في المجتمع السعودي إلى خطورة الجرائم الاحتيال المعلوماتية، والتحذير من التساهل أو الإهمال أثناء التعامل مع المعلومات، مع إيضاح لمهمات الجهات المعنية بمكافحة الجرائم المعلوماتية، بالإضافة إلى إيضاح للمسؤوليات والعقوبات المترتبة على مرتكب الجرائم المعلوماتية، وكذلك التعريف بسبل التقاضي، وآليات الشكوى لمن يقعون ضحايا لمثل هذا النوع من الجرائم.

وتتضمن الحملة إيضاحاً لأنواع الجرائم المعلوماتية وآليات التعامل معها، والتي من أبرزها:انتحال الشخصية – التشهير –الابتزاز –تسريب الخطابات السرية ونشرها –تحميل البرامج غير الموثوقة –اختراق المواقع الإلكترونية، الاحتيال عبر الإنترنت.

المطلب الثاني:

تجربة الأردن في مكافحة جريمة الاحتيال عبر شبكة المعلومات الدولية.

في هذا المطلب نتناولالتشريعات الوطنية في الفرع الأول: وتجربة الأردن لمكافحة جريمة الاحتيال على المستوى الدولي في الفرع الثاني،والمؤسسات الأردنية المعنية بمكافحة الجرائم المعلوماتية في الفرع الثالث.

الفرع الأول: التشريعات الوطنية .

لقد تولى المشرع الأردني تنظيم المعاملات الإلكترونية بمجموعة من القوانين المتخصصة ومنها:-

أ- **قانون المعاملات الإلكترونية رقم (85) لسنة (2001) والذي بدأ العمل به في 2001/3/1** ، بموجب هذا القانون نجد أن المشرع قد جرم الاعتداء الذي يتم عبر الوسائل الإلكترونية بصورة تخالف أحكام هذا القانون ، فقد جرم الاحتيال المعلوماتي والذي يتم عبر إنشاء أو نشر أو تقديم شهادة توثيق لغرض احتيالي أول أي غرض غير مشروع .

ب- **قانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015م** والذي تولى بيان المقصود بالبيانات والمعلومات الإلكترونية و أوجه المخالفات التي تشكل جرائم إلكترونية ومنها جريمة الاحتيال **عبر شبكة المعلومات الدولية.**

ت- قانون الاتصالات رقم (13) لسنة (1995) ويعتبر من أوائل التشريعات التي تنولت ملاحقة مرتكبي الجرائم المعلوماتية في الأردن ، وذلك بموجب أحكام المادة (71) منه والتي جرمت كل من قام بنشر أو إشاعة مضمون أي اتصال بواسطة شبكة اتصال عامة أو خاصة .

ثانياً: المستوى الدولي.

لم تدخر الأردن جهداً في مدّ أو اصر التعاون مع العالم أيضاً لغايات مكافحة الجريمة العابرة للحدود، ذلك أنه إذا ما أيقنا أن جريمة الاحتيال المعلوماتية تعتبر من الجرائم التي يمكن ارتكابها عن بعد وتكون عابرة للحدود، فإنه لابدَّ من وجود تواصل عالمي لملاحقة مرتكبيها والحدُّ من خطورتهم، فقد تم عقد مجموعة من المؤتمرات في الأردن لغاية مناقشة آثار الجريمة المعلوماتية وطرح التوصيات والأفكار حوله.

فقد صادقت المملكة على جميع الاتفاقيات العربية المتعلقة بالتعاون الأمني والقانوني والقضائي وأهمها اتفاقية الرياض للتعاون القضائي، هذا بالإضافة إلى أن الأردن يرتبط بالعديد من الاتفاقيات الثنائية المتعلقة بالتعاون القانوني والقضائي مع العديد من الدول العربية.

ويعتبر الأردن بحكم موقع هو علاقاته المتميزة مع كافة الدول العربية مبادر في تعزيز مختلف أوجه التعاون والتنسيق الأمني والقضائي بالطرق الرسمية وشبه الرسمية من خلال إدارة الشرطة العربية والدولية التي ترتبط بالأمانة العامة بوزراء الداخلية العرب من خلال شعب الاتصال والمكاتب المتخصصة(الحسينوي، 2009، ص 72) ،كما أن هناكت عون وثيق بين قادة الأجهزة الأمنية المتخصصة وضباط الارتباط الأمنيين في العديد من السفارات العربية، وهنا كاتصالات ودية مباشرة تصب في مصلحة التعاون و التنسيق في مكافحة الجريمة وملاحقة مرتكبيها عبر الحدود.

ثالثاً: الإجراءات التنفيذية:

ت طبيقا للإجراءات التنفيذية التي وضعت، وبغية الكشف عن كافة أشكال الجريمة والاحتيال المعلوماتي قامت حكومة المملكة الأردنية الهاشمية بإنشاء العديد من المراكز و الأقسام التي تهدف إلى تحقيق استراتيجياتها الأمنية ومن أهمها:

1. **المركز الوطني لتكنولوجيا المعلومات.**أنشئ في سنة٢٠٠٣ بموجب قانون توظيف موارد تكنولوجيا المعلومات الوطنية بهدف تقديم الدعم للقطاعين العام والخاص في مجال المعلومات والنصوص والإحصاءات الرسمية في شبكة المعلومات الوطنية، والتي يتم من خلالها توفير أحدث وأشمل المعلومات والمعارف الاقتصادية والاجتماعية والتكنولوجية، ويحتوي على١٧شبكة معلوماتية تضم قطاعات مختلفة مثل الصحة والتعليم والسياحة وغيرها وفي عام٢٠١٢م أصدر المركز" الاستراتيجية الوطنية لضمان أمن المعلومات والأمن السيبراني "والتي تتضمن الاستراتيجية الأردنية لضمان أمن نظم المعلومات التحتية والحيوية للمعلومات لتواكب التطورات في مجال الاتصالات، وإيجاد بيئة آمنة وموثوقة لكافة أشكال الأعمال الإلكترونية ومستلزماتها في الأردن،وتوفير بنية تحتية تكنولوجية قوية، وقد دعت الوثيقة إلى تضافر الجهود الحكومية والخاصة لإنجاح الأهداف التي وضعت من أجلها

2. **قسم مكافحة جرائم الحاسوب والانترنت** :أنشئ هذا القسم عام١٩٩٨م وهو يتبع لإدارة المختبرات والأدلة الجرمية، وتناطبه مكافحة وضبط الجرائم التي تقع باستخدام الكمبيوتر والانترنت واتخاذ الإجراءات القانونية حيالها وذلك بالاشتراك والتنسي قمع الأجهزة المعنية، وتوفير قاعدة بيانات ومعلومات حول هذه الجرائم ومرتكبيها، وتتبع البريد الإلكتروني وال(IP address) وتحديد مصدر الجهاز الذي تم من خلاله ارتكاب عمل جرمي معين مثل التهديد والاستغلال عن طريق الانترنت أو سرقة كلمات المرور أو الاحتيال عبر الانترنت أو اختراق المواقع الإلكترونية.

3. شعبة الجرائم الإلكترونية إدارة البحث الجنائي/مديرية الأمن العام.نظراً للتطور المتسارع في تكنولوجيا المعلومات والاتصالات والإنترنت(49) فقد تم إنشاء قسم الإسناد والتحقيق الفني في بداية عام ٢٠٠٨م في شعبة المتابعة

والتحقيق الخاصة، ويُعنى هذا القسم بالتحقيق بجرائم تكنولوجيا المعلومات والاتصالات والإنترنت(سرقة محتويات الخوادم الرئيسية للشركات والمؤسسات، سرقة حسابات البنوك عبر الانترنت، جرائم التهديد والابتزاز، جرائم القرصنة، ومختلف جرائم تكنولوجيا المعلومات) كما يعمل القسم على تقديم الدعم الفني والتقني لجميع شعب وأقسام إدارة البحث الجنائي، كما يعمل هذا القسم في الحد من القرصنة الإلكترونية على حسابات البنوك والاحتيال عبر الهواتف الخلوية.
وقد شاركت مديرية الأمن العام عام٢٠١٢م في العديد من المؤتمرات و ورش العمل الدولية المتعلقة بمكافحة الجرائم الإلكترونية مثل :تحري الجرائم الإلكترونية واستخدام الأدلة الإلكترونية في مالطا، والجرائم السيبرانيه في بيروت، مؤتمر السلامة والأمن في الفضاء المعلوماتي في عمان و الجرائم الإلكترونية في كوريا الجنوبية.

4. **وحدة مكافحة الجرائم الإلكترونية**: حيث أطلقت مديرية الأمن العام مؤخرا صفحة على موقع التواصل الاجتماعي لتوعية المواطنين من خطر الوقوع كضحايا للجرائم الإلكترونية. والصفحة الوليدة تحمل اسم "وحدة مكافحة الجرائم الإلكترونية" (الحلبي، 2011، ص 107.).

5. **الدعم الفني والتقني لجميع شعب وأقسام إدارة البحث الجنائي.** من واجبات قسم الإسناد والتحقيق الفني في مواجهة الجرائم المستحدثة، التحقيق في الجرائم الواقعة من خلال شبكة الانترنت وتشمل:

- جرائم الاحتيال الإلكتروني.
- جرائم الدفع الإلكتروني وتشمل العملة الرقمية وخدمات الدفع الإلكتروني ومحتويات البطاقات الرقمية.
- جرائم الاحتيال المالي عبر الانترنت والمقامرة الإلكترونية.
- مراقبة تكنولوجيا المعلومات للمنظمات الإجرامية وتطورها.

6. **إدارة العلاقات العامة والتوجيه المعنوي**: حيث تقوم الإدارة من خلال البرامج المتخصصة بتوعية الجمهور عبر وسائل الأعلام المختلفة بالأساليب والوسائل الاحتيالية وتحذير المواطنين من أن يقعوا ضحايا لهذا النوع من الجرائم، وكما سيتم افتتاح محطة إذاعية خاصة بالأمن العام تتولى مهمة إذاعة الأخبار المتعلقة بالأمن العام وتوعية وإرشاد المواطنين والاستماع إلى آرائهم وملاحظاتهم .

خاتمة:

قدمنا في هذه الدراسة الإطار العام لجريمة الاحتيال عبر شبكة المعلومات الدولية .من خلال عدة مباحث ،يتناول المبحث الاول مفهوم جريمة الاحتيال عبر شبكة المعلومات الدولية ، من خلال تعريف جريمة الاحتيال عبر شبكة المعلومات الدولية، وبينا طبيعة وخصائص وسمات جريمة الاحتيال عبر شبكة المعلومات الدولية. أما في المبحث الثاني تناول أركان جريمة الاحتيال عبر شبكة المعلومات الدولية من خلال الركن المادي للجريمة المتمثل في سلوك الجاني والنتيجة الجرمية والعلاقة السببية ثم تناولنا والركن المعنوي ومن خلال القصد العام والخاص . أما في المبحث الثالث عالج أساليب الاحتيال المعلوماتي في التلاعب بالبينات والبرامج الإلكترونية بأشكالها المختلفة، فقد بينا التلاعب في المدخلات والبيانات المخزونة والاختراق والتلاعب في البيانات، والمعلومات المخزونة والتلاعب بالبرامج الإلكترونية للنظام المعلوماتي مستندين على نصوص نظام مكافحة الجرائم الالكترونية السعودي وقانون جرائم انظمة المعلومات الاردني .أما في المبحث الرابع ناقشن تجارب الدول المقارنة في مكافحة جريمة الاحتيال عبر شبكة المعلومات الدولية من خلال تجارب المملكة العربية السعودية و المملكة الأردنية في مكافحة جريمة الاحتيال عبر شبكة المعلومات الدولية وذلك من خلال التشريعات الوطنية والمستوى الدولي المؤسسات المعنية بمكافحة الجرائم المعلوماتية .

نتائج الدراسة:

من خلال دراسة موضوع جريمة الاحتيال عبر شبكة المعلومات الدوليةفقد توصلنا إلى عدة نتائج، نرى أهميتها وضرورة إبرازها والعمل على تحقيقها، وهذه النتائج تتمثل فيما يلي:

أولاً: تعتبر شبكة المعلومات العالمية أهم ظاهرة اتصالية في العصر الحديث. هذه الظروف الاتصالية الجديدة باتت تسهيلات، وإمكانات خدمات الحاسبات وتطبيقات الإنترنت مطية سهلة في مجال التوظيف السلبي لها مسببة هاجساً أمنياً عالمياً، يتردد صداه في أغلب المجتمعات. ومع وجود الإنترنت تجوزت الجريمة في حجمها، وأنماطها الكثير من محددات الجريمة التي صاحبت وسائل الإعلام التقليدية مثل السرقة والاحتيال والتزوير والاختلاس والتجسس عبر شبكات المعلومات والحاسبات وملحقاتها المتجددة كل يوم.

ثانيًا: ساعدت الشبكة العالمية كثيراً من المجرمين على التخفي وراءها لممارسة أفعالهم الجرمية مما صعب كثيراً عمليات الملاحقة والمتابعة لهم، وجمع الأدلة ضدهم التي تمكن الجهات القضائية من تطبيق العقوبات ضدهم معتبراً أن الجرائم ذات الخطر غالباً ما تتم عبر الانترنت التي كانت وما تزال مصدراً لهذه الجرائم التي تهدد الأمن بصور شتى.

ثالثًا: تقع جريمة الاحتيالعبر شبكة المعلومات ضمن فئات متعددة، تحكمها بعض الأسس والمعايير لعدة معطيات أبرزها جرائم تتعلق بمعطيات الحاسوب، كإتلاف وتشويه البيانات والمعلومات وبرامج الحاسوب، والتحوير والتلاعب بالمعلومات المخزنة داخل نظم الحاسوب واستخدامها، كتزوير المستندات المعالجة آليا واستخدامها وجرائم تتعلق بالشخصيات أو البيانات المتصلة بالحياة الخاصة، وتشمل جرائم الاعتداء على المعطيات السرية أو المحمية، وجرائم ترتبط بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه (جرائم قرصنة البرمجيات)، وأشهرها الاعتداء على العلامة التجارية وبراءة الاختراع وانتحال شخصية أخرى بطريقة غير شرعية على الإنترنت.

رابعاً: إن القانون الجنائي التقليدي لا يكفي من حيث المبدأ لمواجهة هذا الشكل الجديد من الإجرام المتمثل فيالاحتيال عبر شبكة المعلومات الدولية ، لذلك تم التدخل تشريعياً عن طريق تعديل النصوص القانونية النافذة أو إصدار بعض التشريعات الجنائية الخاصة التي تهدف إلى فرض الحماية القانونية الجنائية للمعلوماتية،ويلاحظ أن الدول العربية لم تطور تشريعاتها العقابية لمواجهة الجرائم المعلوماتية كما حدث في الدول المتقدمة باستثناء بعض الدول حيث طورت المملكة العربية السعودية والأردن تشريعاتها وأنظمتها متمثلة بإصدار قوانين لمواجهة الجرائم المعلوماتية.

خامساً: أبرز معالم التجربة السعودية والأردنية في مجال مكافحةالاحتيال عبر شبكة المعلومات الدوليةتتمثل في:

- إصدار نظام مكافحة جرائم المعلوماتية السعودي الصادر بموجب المرسوم ملكي السعودي رقم م/ 17 بتاريخ 8/ 3/ 1428هـ
- سنقانون الجرائم الإلكترونية الأردني رقم 27 لسنة 2015 الذي دخل حيز النفاذ في الأردن بتاريخ 2015/6/1، المنشور على الصفحة 5631 من عدد الجريدة الرسمية رقم 5343 بتاريخ 2015/6/1م
- ومن أبرز **المؤسسات السعودية والأردنية المعنية بمكافحة الجرائم المعلوماتية**إنشاء قسم خاص للجرائم الإلكترونية في مديرية الأمن العام، وتوقيع اتفاقيات للحد من الجرائم الإلكترونية، وإطلاق مشروع تطوير قدرات التعامل مع الجرائم الإلكترونية، بالإضافة لتنظيم ورش العمل التدريبية، وإنشاء مركز وطني للاستجابة لحوادث الكمبيوتر، وإنشاء برامج للدراسات العليا تُعنى بهذا المجال، وإنشاء مركز لمكافحة الجرائم الإلكترونية.

سادساً: الاختراقات الإلكترونية أصبحت ظاهرة تشكل مستوى عالياً من الخطورة والقلق، وانتشرت حالات الاختراق بشكل غير مسبوق حتى تعرضت لكثير من الشخصيات المعروفة والمواقع الفكرية والعلمية والاقتصادية.

سابعاً: على الرغم من حملات التوعية المتعلقة وبمختلف الوسائل الإعلامية حول هذا النوع من جرائم الاحتيال، إلا أن العديد من الضحايا ما زالوا يقعون في شرك عصابات الاحتيال الإلكتروني طمعاً في الحصول على الملايين المزعومة من الدولارات الأمريكية.

إنعدم وجود تشريع جنائي عربي موحد يجرم صور جرائم الكومبيوتر بأنواعها بحيث يضع لكل صورة منها العقوبة التي تتناسب مع خطورتها، فوجود مثل هذا القانون الاسترشادي الذي يسهل على البلاد العربية ويمهد الطريق لها لوضع تشريع جنائي خاص بالجرائم الإلكترونية أو تلك الجرائم التي تتخذ من الإنترنت طريقة لاستخدامها.

التوصيات:

نخلص من هذه الدراسة إلى حقيقة أن جريمة الاحتيال عبر شبكة المعلومات الدولية، عمل أو سلوك غير شرعي ينتظر فرصة فنية للوثوب على الضحية، أو ثغرة قانونية للإفلات من طائلة العقاب، أو حتى إجراء إداري غير مدروس للتغلغل في شبكة الإدارة المستهدفة، وتحقيق غايات تخدم مرتكبه.

ومن خلال منطلقات وأهداف الدراسة، ومن خلاصة ما توصلت إليه يمكن تصنيف جملة من التوصيات التي قد تساهم في مكافحة جريمة الاحتيال عبر شبكة المعلومات الدولية وتندرج هذه التوصيات تحت المحور الآتية:

أولاً: في مجال التشريعات والأنظمة.

1. إعطاء جرائم التقنية حقها من الأهمية في مؤسسات التشريع الوطنية، وإدراجها ضمن التشريعات الوطنية المختلفة.
2. إدراك أن جريمة الاحتيال عبر شبكة المعلومات ذات بعد دولي تتطلب الانخراط في اتفاقيات دولية، والاهتمام بالتعاون الدولي في مجال المكافحة.
3. مبدأ الوقاية في جريمة الاحتيال عبر شبكة المعلومات خير من العلاج، وبشكل خاص فيما يختص بالتشريعات، والتدريب.
4. تعديل بعض التشريعات الحالية بما يتلاءم مع طبيعة جرائم الإنترنت، والتقنية، وتثقيف العاملين في الجهات ذات العلاقة بهذه التعديلات، وشرحها لهم بشكل واضح.
5. إيضاح الحكم الشرعي الإسلامي تجاه جرائم الحاسب، والإنترنت، ونشرها ضمن برامج التوعية العامة.

ثانياً: في مجال الإجراءات الفنية والإدارية.

ضرورة توحيد الجهود لمكافحة جريمة الاحتيال عبر شبكة المعلومات التي تتطلب توحيد الجهود بجميع الوسائل وعلى جميع المستويات لمكافحتها بمختلف الوسائل ومن أهمها على المستوى الإقليمي هو اللقاءات التي تجمع المهتمين بهذا الجانب سواء من الأكاديميين أو المحققين أو القضاة أو العاملين في مجال البحث والتحري عن مرتكبيها أو من هم من المهتمين بوضع النظم والقوانين التي تساعد على مكافحتها لأن من شأن هذه التجمعات المساعدة على الاستفادة من الخبرات في مواجهة هذه الجرائم.

ثالثاً: في المجال الدولي.

1. ضرورة إنشاء وحدات إنذار مبكر للإبلاغ عن أية عمليات اختراق تتعرض لها أي منظومة من المنظومات العربية الإلكترونية.
2. عقد الندوات والمؤتمرات لمواجهة خطورة جريمة الاحتيال عبر شبكة المعلومات الدولية على الاقتصاد القومي،فضلاً عن الأفراد.

3. التوصية بإنشاء إدارات تخصصة بكل دولة مشاركة لمتابعة ودراسة الظواهر السلبية التي تثبت على الشبكة العالمية للمعلومات ووضع التصورات المستقبلية لها ومدى إمكانية تأثيرها على مستخدمي الشبكة،ومقترحات معالجتها وموجاتها.
4. توثيق الدولي والإقليمي بين الهيئات والمؤسسات المختلفة لنشر الوعي لدى مسؤولي ومستخدمي المعلومات وتعريفهم بالأخطار والتهديدات التي يمكن أن تتعرض لها تلك النظم و كيفية حمايتها،مع ضرورة العمل على إيجاد إجماع عالمي حول نوعية السلوك الذي يشكل جرائم المعلومات.
5. تفعيل الدور الوقائي الذي يسبق وقوع جريمة الاحتيال المعلوماتي،وذلك من خلال تفعيل دَور المؤسسات التوعويَّة(المسجد، الأسرة، دُور التعليم، أجهزة الإعلام)،وذلك بالتوعية بخطورة هذه الجرائم على الأسرة والمجتمع، والسعي في تقوية الوازع الديني.
6. ضرورة إيجاد تعون قضائي وأمني عربي يتفق مع طبيعة جريمة الاحتيال عبر شبكة المعلومات ويخفف من غلو الفوارق بين القوانين والتشريعات الجنائية العقابية وذلك بعقد وإبرام اتفاقيات ومعاهدات خاصة يراعى فيها هذا النوع من الجرائم الإلكترونية العابرة للحدود
7. الدعوة إلى ضرورة وجود تعون دولي ليس فقط في مجال المساعدات القضائية المتبادلة أو في مجال تسليم المجرمين فحسب...، وإنما أيضا في مجال تكوين رجال العدالة، خاصة فيما يتعلق بالجانب التقني والوسائل المستحدثة في التحقيق، فتدريب الكوادر البشرية ليس بنفس المستوى في جميع الدول وإنما يختلف تبعاً لتقدم الدولة من عدمه، ولو أمعنا النظر في بعض التشريعات الدولية أو الإقليمية لوجدنا أنها دعت وبصريح النص إلى ضرورة وجود بين الدول في مجال التدريب ونقل الخبرات فيما بينه.
8. تنسيق وتوحيد الجهود بين الجهات المختلفة في الدولة: التشريعيّة والقضائيّة والضبطية والفنية، وذلك من أجل سد منافذ جريمة الاحتيال المعلوماتية قدر المستطاع ، والعمل على ضبطها بالطرق القانونية والفنيّة .
9. أنشاء منظمة عربية لتنسيق الجهود في مجال مكافحة الجريمة الإلكترونية.

رابعاً: في مجال البحث و التعليم والتدريب

1. تشجيع البحث في دراسة جريمة الاحتيال عبر شبكة المعلومات الدولية وتقييم فعالية التدابير المتخذة لمكافحتها؛حيث يمكن لهذا البحث أن يسهم في إنشاء قاعدة من المعلومات تصلح أساسًا لانطلاق البرامج الوقائية
2. إضافة مادة جريمة الاحتيال المعلومات يضمن مناهج الدراسات القضائية ومناهج الدراسة في الكليات والمعاهد الأمنية وكلية الدراسات العليا،وذلك باستحداث تدريس" مادة تأمين نظم المعلومات على شبكة الإنترنت "والأساليب الإجرامية التي يتبعها قراصنة الحاسب الآلي لاختراقها، نظراً لما تمثله جريمة النصب المعلوماتي من خطر على الاقتصاد القومي.
3. حث الجامعات والمراكز البحثية لدراسة جريمة الاحتيال المعلوماتي، ومحولة إنشاء دراسة متخصصة في المجالات الفنية والقانونية المتعلقة بمكافحة تلك الجريمة.
4. إجراء تدريبا تم تخصصة في جرائم الاحتيال المعلوماتية للقضاة والمحامين وأفراد الضابطة العدلية للاطلاع على أساليب ارتكابها،وكيفية ضبطها وقائياً أو علاجاً.
5. إنشاء مركز وطني استشاري وتوجيهي للتوعية بمخاطر جرائم المعلومات والاستفادة من بعض كوادر "الهاكرز" وإعادة توجيههم والاستفادة منهم في القرصنة البيضاء.

6. ضرورة نشر الوعي بين المواطنين حول خطورة هذه الجرائم وسبل الوقاية منها. وتفعيل دور مؤسسات المجتمع المحلي في مجال التوعية المجتمعية.

قائمة المصادر والمراجع

أولاً:المعاجم

1. مجمع اللغة العربية. (١٤٢٦هـ، ٢٠٠٥م). المعجم الوسيط، القاهرة، مكتبة الشروق الدولية، ط ٤.
2. ابن منظور. (١٩٩٧م). لسان العرب،المجلد التاسع دار المعارف، بيروت، ط١، لبنان.
3. المعجم الوسيط،المجلد الثاني، (1998)، إصدار مجمع اللغة العربية، القاهرة، ط3.

ثانياً: المصادر.

1. نظام مكافحة جرائم المعلوماتية السعودي الصادر بالمرسوم ملكي رقم/ 17 بتاريخ 3/8/ 1428هـ .
2. **نظام للاختراق الإلكتروني عام**10/20/ 1423هـ.
3. **قانون الجرائم الإلكترونية** الأردني رقم 27 لسنة 2015.
4. **قانون المعاملات الإلكترونية** رقم (85) لسنة (2001) والذي بدأ العمل به في 2001/3/1.
5. **قانون الجرائم الإلكترونية الأردني رقم** 27 لسنة 2015.

رابعاً: المراجع الفقهية

1. إبراهيم، حسني عبد السميع (٢٠١١) **الجرائم المستحدثة عن طريق الانترنت**، القاهرة، ، دار النهضة العربية.
2. إسماعيل، محمد عبد الشافي. (1999 م).**الإعلانات التجارية الخادعة ومدى الحماية التي يكلفها المشرع الجنائي للمستهلك**،القاهرة، دار النهضة العربية،ط1.
3. بيومي، عبد الفتاح. (2007).**التجارة عبر الإنترنت، الإسكندرية**، دار الفكر الجامعي.
4. تمام، أحمد حسام طه (2000م). **الجرائم الناشئة عن استخدام الحاسب الآلي**،القاهرة، دار النهضة العربية.
5. **الجنبيهي منير محمد.(** 2006).**جرائم الانترنت والحاسب الآلي ووسائل مكافحتها**، دار الفكر الجامعي، الاسكندرية.
6. حجازي، عبد الفتاح بيومي. (2002).**النظام القانوني لحماية التجارة الإلكترونية**،بالإسكندرية، دار الفكر الجامعي، ج2.
7. الحربي، عبد الرحمن. (2008).**حراب الوقاية من الاحتيال المنظم وتجريمه**، (النسخة الإلكترونية)، المجلة الأفق،15، (5) ،13-18.
8. حسني،محمود نجيب. (1988م). **جرائم الاعتداء على الأموال في قانون العقوبات اللبناني**،بيروت،دار النهضة العربية
9. حسني، محمود نجيب. (ب ت).**شرح قانون العقوبات، القسم الخاص**، القاهرة، دار النهضة العربية.
10. الحسينوي، علي جبار. (، 2009).**جرائم الحاسوب والانترنت**، عمان، دار اليازوري للنشر والتوزيع.
11. الحلبي، خالد عياد.(2011).**إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت**، عمان، دار الثقافة.
12. الخن، محمد طارق،**جريمة الاحتيال عبر الانترنت**،منشورات الحلبي الحقوقية، مصر، الطبعة الأولى، 2011.
13. الرومي، محمد أمين. (2003). **جرائم الكومبيوتر والانترنت**، القاهرة، دار المطبوعات الجامعية، مصر.
14. الزبيدي، محمد عوض (2007م)، **التعاقد الإلكتروني وعمليات البنوك الإلكترونية**، عمان، دار الياقوت للنشر.
15. سرور، أحمد فتحي. (1985).**الوسيط في قانون العقوبات، القسم الخاص**، القاهرة، دار النهضة العربية.
16. الشنوي، محمد. (2008).**جرائم النصب المستحدثة**، القاهرة، دار الكتب القانونية.
17. الشهري، فايز بن عبدالله.(2016).**بحث بعنوان التحديات الأمينة المصاحبة لوسائل الاتصال الجديدة، (النسخة الإلكترونية).**
18. الشواء،محمدساميثورة.(2003م)المعلوماتوانعكاساتهاعلىقانونالعقوبات،القاهرة،دارالنهضة العربية.
19. الشوابكة، محمد امين. (2004). **جرائم الحاسوب والانترنت**، عمان، دار الثقافة للنشر والتوزيع، الأردن، ط1.

20. الصغير، جميل عبد الباقي. (2001).**الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت،** القاهرة، دار النهضة العربية.
21. عبد الله، عبد الكريم عبد الله.(2007)**جرائم المعلوماتية والانترنت،** منشورات الحلبي، الطبعة الأولى.
22. عبيد، روؤف.(1985م) جرام الاعتداء على الأشخاص والأموال، دار الفكر العربي، القاهرة.
23. عثمان، آمالعبد الرحيم.(2004).شرح قانون العقوبات القسم الخاص،دار النهضة العربية.
24. عرب، يونس. (2002).**موسوعة القانون وتقنية المعلومات، جرائم الكمبيوتر والإنترنت،** الجزء الأول، اتحاد المصارف العربية.
25. عودة،عبدالقادر. (١٩٧٧).**التشريع الجنائي الإسلامي مقارناً بالقانون الوضعي،** (3)، بيروت ،دار التراث
26. عياد، سامي علي حامد.(2007).**الجريمة المعلوماتية واجرام الانترنت،** الاسكندرية، دار الفكر الجامعي.
27. الغزوي ، سمير إبراهيم جميل(2005م) **المسؤولية الجنائية الناشئة عن استخدام الانترنت** ، رسالة ماجستير مقدمة إلى كلية القانون ، جامعة بغداد .
28. فرج،أمير. (2008).**الجرائم المعلوماتية على شبكة الانترنت،** دار المطبوعات الجامعية، الاسكندرية، مصر،ط1.
29. قايد، أسامة .(2007)، **الحماية الجنائية للحياة الخاصة وبنوك المعلومات،** القاهرة ، دار النهضة العربية.
30. قوره، نائلة عارف. (2006).**جرائم الحاسب الآلي الاقتصادية،** بيروت، منشورات الحلبي الحقوقية البنان ط1.
31. مجازي، عبد الفتاح بيومي.(2005م)**جرائم الكمبيوتر والانترنت** ،مصر ، دار الكتب القانونية، 2005.
32. المشهداني،محمد أحمد. (2001م).**شرح قانون العقوبات القسم الخاص في القانون الوضعي و الشريعة الإسلامية** . عمان، دار الثقافة للنشر والتوزيع.
33. الملط، أحمد خليفة. (2006). **الجرائم المعلوماتية،** دار الفكر الجامعي، الإسكندرية.
34. منشاوي ، محمد عبد الله.(٢٠٠٢).جرائم الانترنيت من منظور شرعي وقانوني ، مكة المكرمة .
35. منشوي، محمد عبد الله(1434ه)، جرائم الانترنيت من منظور شرعي وقانوني، الرياض،مكتبة ابن رشد.
36. منصور،محمد حسين. (2006م). **المسؤولية الإلكترونية،** الإسكندرية، منشأة المعارف.

خامساً: المراجع الاجنبية

1.Case,Eoghan Digital Evidence and Computer Crime, Academic Press, 1st edition, 2000

سادساً: الرسائل العلمية.

1. حجازي، عبد الفتاح بيومي. (2007). **مكافحة جرائم الكمبيوتر والانترنت، رسالة ماجستيررسالة دكتوراه منشورة ، كلية الحقوق، جامعة القاهرة.**
2. عبَادي ، ماجد عمر.(2015م).**الاحتيال عبر البريد الالكتروني**.رسالة ماجستير مقدمة إلى كلية القانون في جامعة النجاح.
3. العريان، حمد علي (2004م) الجرائم المعلوماتية ، رسالة دكتوراه، كلية الحقوق، جامعة الإسكندرية، دار الجامعة الجديـــدة للنشر .
4. الخليفة، محسن بن سليمان.(1423 ه). **جرائم الحاسب الآلي وعقوبتها في الفقه و النظام** ، رسالة ماجســـتير منشـــورة ،كلية الدراسات العليا،جامعة نايف العربية للعلوم الأمنية.
5. هروال، نيله (2006م)، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات ،رسالة ماجستير في القانون دراسة مقارنة كلية الحقوق، جامعة الإسكندرية، دار الفكر الجامعي.
6. الكعبي، محمد عبيد(2015)، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت رسالة دكتوراه، جامعة القاهرة.
7. الغزاوي ، سمير إبراهيم جميل .(٢٠٠٥).المسؤولية الجنائية الناشئة عن استخدام الانترنيت ، رسالة ماجستير مقدمة الى كلية القانون ، جامعة بغداد .
8. عبد الجبوري، سامر سلمان.(2014).جريمة الاحتيال الالكتروني، رسالة ماجستير مقدمة الى كلية الحقوق ، جامعة البحرين.

سابعاً: الأبحاث العلمية.

1. أحمد، عبد الفضيل محمد.(1994 م) جريمة الخداع التجاري في نظام مكافحة الغش التجاري السعودي ،بحث منشور **مجلة الحقوق** , جامعة الكويت , 18 , (4).
2. الزقرد، أحمد السعيد.(1995 م) الحماية القانونية من الخداع الإعلاني في القانون الكويتي المقارن ، بحث منشور، **مجلة الحقوق** ، جامعة الكويت ، السنة 19 ، العدد 4 ، ص 149،150 ..
3. الزومان ، عبدالعزيز بن حمد.(2010). شبكة الإنترنت وكيفية الارتباط بها (النسخة الإلكترونية) ،بحث منشور **المجلة العالمية المطورة**،15،(3) ،13-17.
4. مقابلة، يوسف عقل،(2008) ، الحماية الجزائية لأموال الغير من إساءة استخدام بطاقة الائتمان، بحث منشور في مجلة البحوث الأمنية، جامعة نايف العربية للعلوم الأمنية، المجلد16 ، العدد، 38.
5. المهيني، صالح المسند .(2001م). جرائم الحاسب الآلي : الخطر الحقيقي في عصر المعلومات بحث منشور .**المجلة العربية للدراسات الأمنية والتدريب**، الرياض، أكاديمية نايف للعلوم الأمنية ،عدد 29،ص24-40.
6. نصيرات ،وائل محمد(2016).جريمة الذم والقدح وطرق اثباتها عبر شبكة المعلومات في القانون الأردني والنظام السعودي بحث منشور ،**مجلة الدراسات الأمنية**،جامعة نايف للعلوم الأمنية، الرياض، 30.

1. **Naserat, Wae'l Mohammed**,[2016],The Experience of the Kingdom of Jordan in Combating the Crime of Money Laundering,Journal of Law, Policy and Globalization,Vol.56,
2. Sussmann, M. A. 1999, 'The Critical Challenges from International High-Tech and Computer Related,Crime at the Millennium', Duke Journal of Comparative and International Law, vol. 9, no. 2,

ثامناً: الندوات والمؤتمرات

3. الزبيدي، زهير. (1988.).التعريف بجرائم التهريب في الوطن العربي، أبحاث الندوة العلمية السادسة، الرياض، دار النشر بالمركز العربي للدراسات الأمنية والتدريب. ص: 18.
4. نصيرات وائل. (**من 19-21 ربيع الثاني 1436هـ**). بحث بعنوان الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجها، قدم إلىالمؤتمر الدولي الول لمكافحة الجريمة المعلوماتية بجامعة الإمام محمد بن سعود الإسلامية، الرياض، المملكة العربية السعودية.
5. العريفي، عبدالله.(21-28 شعبان 1437 هـ). أمن المعلومات.. حماية مقدرات الوطن «المعلوماتية» تتطلب استراتيجية موحّدة، جريدة الرياض العدد 17162، 3 رمضان 1436 هـ-20 يونيو 2015م -
6. أبو الوفا، محمد إبراهيم، (من 3-6 يوليو 2003)المسؤولية الجنائية عند الاستخدام غير المشروع لبطاقات الائتمان في القانون المقارن والفقه الإسلامي، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية المتحدة، ، ص 2070.
7. سلامة، سعد احمد.(2010/6/4). الوقاية من جرائم الاحتيال،حلقة علمية قدمت2010/6/4. جامعة نايف للعلوم الأمنية.
8. النويران، ثامر علي عافت. (10-12 /2015).المداخلة الجرائم الالكترونية وطرق الحد منها تجربة الأردن" ورقة بحثية قدمت إلى المؤتمر الدولي الدول لمكافحة الجرائم المعلوماتية المملكة العربية السعودية/ الرياض من بتنظيم من جامعة الإمام محمد بن سعود الإسلامية.

تاسعاً: المواقع الالكترونية

www.cisco.com
www.ipsos.com
www.norton.com/AntiVirus
www.almoslim.net/node/16321
: info@mcit.gov.sa
me.kaspersky.com/about
http://www.ahmnews.com/
aleqte@aleqt.com