مجلة جامعة الملك سعود، م٢٢، الأنظمة والعلوم السياسية (٢)، ص ص ٢٣١- ٢٦٤، الرياض (٢٠١٠م/ ١٤٣١هـ)

الاتجاهات الحديثة في تجريم الاحتيال المعلوماتي

أسامة بن غانم العبيدي
أستاذ القانون المشارك
معهد الإدارة العامة، الرياض

(قدم للنشر في ١٤٣٠/٤/٢٥هـ؛ وقبل للنشر في ١٤٣١/١/١٢هـ)

ملخص. أدى الانتشار المتزايد في استخدام الحاسب الآلي وشبكات الإنترنت إلى زيادة كبيرة في الجرائم المعلوماتية المرتكبة ومنها جرائم الاحتيال المعلوماتي، وهي من الجرائم التي يتزايد انتشارها سنوياً وتشكل تحدياً كبيراً للسلطات في دول العالم المختلفة وتتسبب في خسائر سنوية تقدر ببلايين الدولارات. ويتناول هذا البحث جرائم الاحتيال المعلوماتي من حيث ماهيتها ووسائل ارتكابها وصورها وكيفية تعامل القوانين والتشريعات المقارنة معها. وقد بينا في المبحث التمهيدي من هذا البحث ماهية جرائم النصب (الاحتيال) وماهية الاحتيال المعلوماتي. كما بينا في المبحث الأول من هذا البحث مدى قابلية البيانات والمعلومات للاستيلاء عليها، ومدى صلاحية النقود الإلكترونية لأن تكون محلاً لجرائم الأموال. كما بينا في المبحث الثاني مزايا وعيوب التحويل الإلكتروني للأموال ووسائل ارتكاب جرائم الاحتيال المعلوماتي. أما في المبحث الثالث فقد تطرقنا للاحتيال باستخدام بطاقات الائتمان. أما في المبحث الرابع فقد تناولنا فيه موقف بعض التشريعات المقارنة من جرائم الاحتيال المعلوماتي.

مقدمة

أدى التزايد المستمر في استخدام الحاسب الآلي وشبكة الإنترنت إلى ازدياد كبير في ارتكاب الجرائم المعلوماتية بشكل عام وجرائم الاحتيال المعلوماتي بشكل خاص. واستحوذت جرائم الاحتيال المعلوماتي على النصيب الأكبر من الجرائم المعلوماتية المرتكبة في العالم اليوم بالنظر إلى اعتمادها على استخدام الحاسب الآلي وشبكة الإنترنت وإمكانية ارتكابها من أي مكان في العالم. وسوف نناقش في هذا البحث جرائم الاحتيال المعلوماتي وهي الجرائم المرتكبة باستخدام الحاسب الآلي وشبكة الإنترنت وتعامل القوانين والتشريعات المقارنة مع هذه الجرائم.

الدراسات السابقة

معظم الدراسات السابقة التي تناولت الجرائم المعلوماتية لم تتطرق بشكل محدد لجرائم الاحتيال

المعلوماتي، بل تطرقت لهذه الجرائم بشكل موجز ومختصر. وقد قمنا بذكر عدد من المراجع ذات العلاقة بجرائم المعلوماتية في قائمة المراجع لهذا البحث ويمكن الرجوع إليها عند الحاجة. ويهدف هذا البحث إلى تناول جرائم الاحتيال المعلوماتي بتركيز وتعمق وتحديد ماهيتها، وصورها ووسائلها وطرق مكافحتها وموقف القوانين والتشريعات المقارنة من هذه الجرائم.

هدف البحث وأهميته

يهدف هذا البحث إلى دراسة موضوع جرائم الاحتيال المعلوماتي. وإبراز ماهية جرائم الاحتيال المعلوماتي وصورها ووسائل ارتكابها، وموقف القوانين والتشريعات المقارنة من جرائم الاحتيال المعلوماتي، وصولاً إلى إبراز مدى الحماية الجنائية التي أسبغها النظام السعودي بغية الحد من ارتكاب جرائم الاحتيال المعلوماتي ومكافحتها.

خطة البحث

سوف يقسم هذا البحث إلى:

مبحث تمهدي: ماهية جرائم النصب(الاحتيال) وماهية الاحتيال المعلوماتي.

المبحث الأول: مدى قابلية البيانات والمعلومات والنقود الإلكترونية لأن تكون محلاً لجرائم الأموال.

المبحث الثاني: مزايا وعيوب التحويل الإلكتروني للأموال ووسائل ارتكاب جرائم الاحتيال المعلوماتي

المبحث الثالث: الاحتيال باستخدام بطاقات الائتمان

المبحث الرابع: موقف بعض التشريعات المقارنة من جرائم الاحتيال المعلوماتي

منهج البحث

يعتمد هذا البحث على منهج الدراسة التحليلية للقوانين والأنظمة المقارنة مع الرجوع والاعتماد على المراجع القانونية ذات العلاقة.

مبحث تمهيدي:

ماهية جرائم النصب (الاحتيال)

وماهية الاحتيال المعلوماتي

نظراً لأهمية جرائم النصب (الاحتيال) وتحديد ماهية الاحتيال المعلوماتي سنتناول في المطلب الأول من هذا المبحث تعريف جرائم النصب (الاحتيال)، ثم نتناول ماهية الاحتيال المعلوماتي في المطلب الثاني.

المطلب الأول: ماهية جرائم النصب (الاحتيال)

يمكن تعريف جريمة النصب بأنها " الاستيلاء على مال منقول مملوك للغير بخداع المجنى عليه وحمله على تسليمه " (عفيفي، بدون تاريخ) فالنصب يتكون من فعلين هما الاحتيال والاستيلاء. فالنصب يترتب

عليه وقوع المجنى عليه في غلط ينتج عنه إتيانه تصرفاً مالياً من شأنه تسليم مال إلى المتهم .

وقد نص المشرع المصري على جريمة النصب في المادة (٣٣٦) من قانون العقوبات المعدلة بالقانون رقم (٢٩) لعام ١٩٨٢م والذي نص على أنه "يعاقب بالحبس كل من توصل إلى الاستيلاء على نقود أو عروض أو سندات دين أو سندات مخالصة أو أي متاع منقول وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها، إما باستعمال طرق احتيالية من شأنها إيهام الناس بوجود مشروع كاذب أو واقعة مزورة أو إحداث الأمل بخصوص ربح وهمي أو تسديد المبلغ الذي أخذ بطريق الاحتيال أو إيهامهم بوجود سند دين غير صحيح أو سند مخالصة مزور، وإما بالتصرف في مال ثابت أو منقول ليس ملكاً له وليس له حق التصرف فيه، وإما باتخاذ اسم كاذب أو صفة غير صحيحة(عفيفي، بدون تاريخ) (Short, 1994) . والعقوبة تصل إلى ثلاث سنوات . أما من شرع في نصب ولم يتمه فيعاقب بالحبس مدة لا تتجاوز سنة ويجوز وضع الجاني في حالة العود تحت ملاحظة البوليس سنة على الأقل وسنتين على الأكثر " .

ويتبين لنا من النص السابق أن المشرع المصري لم يعرف جريمة النصب وإنما قام فقط بتحديد طرقه والأشياء التي يرد عليها .

ولا يخرج النصب عن كونه استيلاء على الحيازة الكاملة لمال الغير بوسيلة تتسم بالخداع وينتج عنها تسليم ذلك المال، أو هو تدليس عبارة عن تشويه للحقيقة أو كذب في واقعة يؤثر في عقيدة شخص وتفكيره مما يجعله يعتقد غير الحقيقة (الصغير، ١٩٩٢)، (فايد، ١٩٨٩) .

ويعتبر التشريع الفرنسي الصادر في عام ١٧٩١م أول من تناول جريمة النصب، كما أن التشريع الصادر عام ١٨١٠م قد عاقب على هذه الجريمة باعتبارها جريمة قائمة بذاتها ومستقلة عن جريمة السرقة. وتتفق جريمة النصب مع جريمة السرقة في أن كلاً منهما يقع على محل واحد وهو المال المنقول المملوك للغير، أي الاعتداء على حق الملكية، ولكن جريمة النصب تختلف عن السرقة في أن الجاني في جريمة النصب يأخذ المال برضاء المجنى عليه وإن كان مصحوباً بالخداع من الجاني بعكس الحال في جريمة السرقة والتي لا يكون فيها أي رضاء من المجنى عليه"(فضل، ٢٠٠٧)، (عتيق، ٢٠٠٢) .

كما ينص قانون العقوبات الإماراتي في المادة (٣٣٩) على أنه " يعاقب بالحبس أو بالغرامة كل من توصل إلى الاستيلاء لنفسه أو لغيره على مال منقول أو سند أو توقيع هذا السند أو إلى إلغائه أو إتلافه أو تعديله وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو صفة غير صحيحة متى كان من شأن ذلك خداع المجنى عليه وحمله على التسليم ويعاقب بالعقوبة ذاتها كل من قام بالتصرف في عقار أو منقول يعلم أنه غير مملوك له أو ليس له حق التصرف فيه أو

تصرف في شيء من ذلك مع علمه بسبق تصرفه فيه أو التعاقد عليه وكان من شأن ذلك الإضرار بغيره " .

أركان جريمة النصب :

يتضح لنا من نص المادة (٣٣٦) من قانون العقوبات المصري المعدلة بالقانون رقم (٢٩) لعام ١٩٨٢م أن جريمة النصب تتكون من ركنين :

أولاً: الركن المادي

وحتى يتوافر الركن المادي في هذه الجريمة يجب توافر العناصر الآتية :

١- نشاط إجرامي يباشره الجاني ويتمثل في قيامه بالاحتيال باستخدامه لوسيلة من وسائل الاحتيال المنصوص عليها .

٢- نتيجة إجرامية، أي أن يترتب على ذلك النشاط الإجرامي تسليم المجنى عليه للمال إلى الجاني، مع وجود علاقة سببية بين الأفعال الاحتيالية أو التدليسية وتسليم المال .

والملاحظ على نص المادة (٣٣٦) السابقة أن المشرع المصري لم يحدد ما هية الطرق الاحتيالية أو نوعها أو أسلوبها حتى تعتبر وسيلة من وسائل الاحتيال وهو في ذلك يتوسع في الأفعال التي تعتبر طرقاً احتيالية بغرض الاستيلاء على مال الغير، مع وجوب أن تكون الطرق الاحتيالية محبوكة بشكل يسمح بخداع الشخص العادي، فالقانون لا يعاقب على مجرد الكذب. فمن سلم أمواله طوعاً واختياراً بناء على أقوال كاذبة مخادعة فلا يستطيع أن يلوم إلا نفسه . واشترط المشرع أن يكون الهدف من الكذب هو الإيهام بوجود مشروع كاذب أو واقعة مزورة أو إحداث أمل بحصول ربح وهمي أو تسديد المبلغ الذي أخذ عن طريق الاحتيال أو الإيهام بوجود سند دين غير صحيح أو سند مخالصة مزورة أو معنوية وذلك لتدعيم كذبه .

ثانياً: الركن المعنوي

جريمة النصب من الجرائم العمدية التي تتطلب توافر القصد الجنائي العام والخاص ويتمثل القصد الجنائي العام بتوافر العلم والإرادة، علم الجاني بأن ما يقوم به من فعل هو احتيال من شأنه خداع المجنى عليه وحمله على تسليم المال، واتجاه إرادته إلى ذلك . أما القصد الجنائي الخاص فيتوافر بانصراف نية الجاني إلى الاستيلاء على الحيازة التامة لمال المجنى علي أي أتجاه إرادة الجانبي إلى نيه تملك الشيء وحرمان صاحبه منه، وذلك بتغييره للحيازة من ناقصة إلى حيازة كاملة (فضل، ٢٠٠٧)، (الكعبي، بدون تاريخ) .

المطلب الثاني: ماهية الاحتيال المعلوماتي

يعرف الاحتيال المعلوماتي بأنه " كل تظاهر أو إيحاء يكون صالحاً لإيقاع المجنى عليه في الغلط بطريقة تؤدي إلى الاقتناع المباشر بالمظهر المادي الخارجي، أي أن المجنى عليه في جريمة الاحتيال المعلوماتي هو من جازت عليه حيلة الجاني باستخدام الحاسب الآلي وشبكة الإنترنت، فانخدع بها وسلمه ماله (الشوابكة، ٢٠٠٤) .

ولا يقع الاحتيال المعلوماتي على الشخص الطبيعي فقط، بل أنه يصلح لأن يقع أيضاً على الشخص المعنوي، فالمؤسسات العامة والشركات وكذلك المؤسسات الخاصة هي من الأشخاص الاعتبارية في حكم القانون، وحيث أن الحاسبات الآلية والشبكات الداخلية للمنشأة تعد من فروع المؤسسة أو الشركة فإنها تكون صالحة لأن تكون ضحية للتحايل أو الخداع (قشقوش، ١٩٩٢)، (العريان، ٢٠٠٤)، (العبيدي، ١٤٢٩).

ولكن إذا كان من الممكن الاحتيال على الأشخاص الطبيعية والمعنوية فهل يمكن الاحتيال على الحاسب الآلي وإيقاعه في الغلط ؟ وقد انقسمت الآراء في هذا الشأن.

الاتجاه الأول

يذهب أنصار هذا الاتجاه إلى عدم إمكانية ارتكاب أفعال الاحتيال على الحاسب الآلي ومن ثم عدم إمكانية تطبيق النصوص الخاصة بجريمة الاحتيال في حالة وقوع الجريمة على الحاسب الآلي. إذ يستلزم أنصار هذا الاتجاه لقيام فعل الاحتيال أن يكون المخدوع شخصاً طبيعياً (أي أن يكون إنساناً) ومن ثم لا يمكن خداع الحاسب الآلي بوصفه آلة، ووفقاً لهذا الاتجاه فإن من يمارس وسائل احتيالية في مواجهة نظم المعالجة الآلية للبيانات لتحقيق منفعة مادية أو للحصول على خدمة لا يسأل عن ارتكاب جريمة احتيال وفقاً للمفهوم التقليدي لهذه الجريمة. إذ أن نظام معالجة البيانات حاسوبياً تفتقد إلى خاصية التفكير فهو ينفذ أوامر يتلقاها مسبقاً أو يتلقى أسلوب معالجتها، إضافة إلى أن معطيات الحاسب الآلي هي ذات طبيعة معنوية تفتقر إلى كونها مالاً منقولاً ذا طبيعة مادية، وهو ما يشترطه المشرع عادة في محل جريمة الاحتيال.

الاتجاه الثاني

يرى أنصار هذا الاتجاه إمكانية تطبيق النصوص الخاصة بجريمة النصب على الاحتيال المعلوماتي، ومن التشريعات التي أخذت بهذا الرأي تشريعات الدول الأنجلوساكسونية (Anglo Saxon). ففي بريطانيا فإن التغيير الموسع لنصوص قانون السرقة (Theft Act) يتضمن أيضاً التلاعب في البيانات لغرض الحصول على منفعة مادية. فقد نص قانون السرقة الإنجليزي على أنه يعاقب كل من حصل على نحو غير مشروع وبأي وسيلة خداع سواء لنفسه أو للغير على منفعة مادية (الشوا، ١٩٩٨)، (الشوابكه، ٢٠٠٤)، (Savage,2001). وقد أدان القضاء الإنجليزي أحد الأشخاص بارتكاب جريمة الاحتيال حيث كان المتهم المذكور يعمل في أحد البنوك في دولة الكويت وقام بتحويل أموال باستخدام الحاسب الآلي من حسابات بعض الزبائن لحسابه الخاص في بريطانيا، وقد أدانته المحكمة بتهمة الحصول على أموال بطريق الخداع والاحتيال (الشوا، ١٩٩٨)، (الكعبي، بدون تاريخ).

كما يرى الفقه الفرنسي أنه من الممكن وقوع الاحتيال في أنظمة الحاسب الآلي وما تحتويه من بيانات

ومعلومات ومن ثم إيقاعه في الغلط بهدف سلب الأموال باستخدام طرق احتيالية ككذب تدعمه أعمال مادية أو وقائع خارجية متمثلة في تقديم الوثائق أو المعلومات المدخلة إلى الحاسب الآلي أو باستخدام مستندات غير صحيحة يخرجها الحاسب اعتماداً على ما وقع على برامجه أو بياناته المخزنة من تلاعب لغرض الإستيلاء على أموال لا حق له في الحصول عليها (الشوابكة، ٢٠٠٤).

وقد جرم قانون العقوبات الكندي أيضاً في مادتيه (٣٨٧)، (٣٨٨) الاحتيال ويمكن تطبيق هاتين المادتين على حالات الاحتيال المرتكب عن طريق العبث في البيانات المعالجة آلياً. وقد طبق القضاء في كندا ذلك في حكمه الصادر في قضية ريجينا (Regina) والتي تتمثل وقائعها في قيام أحد الأشخاص ببيع وتأجير ألعاب فيديو (Video Games) مقرصنة على نحو غير مشروع وقد أدانت المحكمة الكندية المتهم لتسببه وبنية الغش في إلحاق الضرر بأصحاب الحق في تلك الألعاب رغم عدم وجود خديعة أو كذب أو أي علاقة بين المجنى عليه والمتهم، وبنت المحكمة حكمها على الضرر المؤثر وعلى تعريض المصالح الاقتصادية لأصحاب حقوق التوزيع لخطر الضرر وأن نزع الحيازة على نحو غير مشروع ينطوي بحد ذاته على احتيال (قشقوش، ١٩٩٢)، (عفيفي، بدون تاريخ).

الاتجاه الثالث

وتقوم التشريعات التي تتبنى هذا الاتجاه بتطبيق القوانين المتعلقة بالغش في مجال البريد والاتصالات الهاتفية والبنوك، وتقوم بتطبيقها كذلك على الاتفاق الجنائي بهدف ارتكاب الغش والاحتيال، وأعطت بعض القوانين الفيدرالية الأمريكية مفهوماً موسعاً للمال (Property) بحيث يشمل كل شيء له قيمة وقد بينت أحدى الدراسات الصادرة بالولايات المتحدة الأمريكية حديثاً أن عدداً متزايداً من مستخدمي الهواتف الجوالة وأجهزة الحاسب الآلي المحمول يقومون بإرسال بيانات سرية خاصة بهم لاسلكياً بدون اتخاذ التدابير الأمنية اللازمة لحماية تلك البيانات والمعلومات. وكشف الدراسة التي تم إعدادها من قبل إحدى شركات أمن المعلومات الأمريكية أن هذه التصرفات تعد واحدة من نقاط الضعف في حماية البيانات الخاصة بالمستخدمين سواء للهواتف الجوالة أو الحاسب المحمول، وبينت الدراسة أن نحو ٨٥٪ ممن شملتهم الدراسة بالولايات المتحدة الأمريكية اعترفوا بإرسال بيانات سرية خاصة بهم عن طريق بريد موقع جوجل (Google) أو موقع ياهو (Yahoo) وهو ما يماثل نفس السلوك من المستخدمين في أوروبا واليابان. وأوضحت الدراسة أن اليابانيين كانوا أيضاً غير مدركين لخطورة هذه السلوكيات حيث اعترف ٦٠٪ منهم بتحميل تلك الملفات بينما كان مستخدمو الهواتف الجوالة هناك أكثر حذراً حيث ذكرت الدراسة أن ٤٩٪ منهم فقط قالوا أنهم يحملون الملفات

باستخدام هواتفهم الجوالة. وأشارت الدراسة إلى قيام بعض المؤسسات والشركات بمنع الموظفين لديها من الدخول إلى بعض المواقع غير الآمنة من أجهزة الحاسب التابعة لها . ومع انخفاض الوعي الأمني في تقنية المعلومات تبقى تقنيات وبرامج تأمين المعلومات هي خط الدفاع الأول في مكافحة جرائم المعلوماتية (جريدة الجزيرة، ١٤٢٩) . ويدخل ضمن نطاق هذا التعريف الموسع للمال الأموال المعنوية والبيانات المعالجة آلياً (الشوا، ١٩٩٨)، (الشوابكه، ٢٠٠٤)، كما تعاقب هذه القوانين الفيدرالية على الاستخدام غير المصرح به للحاسب الآلي، بهدف ارتكاب أفعال الغش أو الاستيلاء على الأموال. ويقوم الجاني الذي يقوم بسرقة أموال الناس عادة باستخدام برامج مشابهة لبرامج التجسس أو الفيروسات التي يتم إرسالها عبر البريد الإلكتروني أو عبر مواقع الشات، كما يقوم بعضهم بوضع برامج التجسس في مواقع تحميل الأفلام ثم إرسال وصلة بالبريد عن آخر الأفلام الخلاعية أو الفضائح أو مشاهد مثيرة ... إلخ، وعند ما يتبع المجنى عليه الوصلة يتوجه إلى موقع تحميل الأفلام وهناك يتم تنزيل الملف إلى جهازه، ولا تتطلب صناعة مثل هذه البرامج مجهوداً كبيراً حيث أنها تراقب فقط المواقع التي يزورها المجنى عليه وتقوم بإرسالها بالبريد الإلكتروني، وبعد تفحص المحتال لقائمة المواقع التي تزورها يمكنه البدء بالمرحلة الثانية حيث يرسل إلى المجنى عليه رسالة بان البنك يريد تحديث بياناته قبل أن يتم إيقاف بطاقته الائتمانية وتجميد حساباته، وقد يقوم محتالون آخرون إلى الإيقاع بالضحية بشكل مباشر ودون الحاجة إلى متابعة تحركاته عن طريق القيام بإرسال رسائل بريدية بريئة تظهر وكأنها رسائل دعائية لمواقع مشهورة للبيع على الإنترنت مثل موقع (ebay) الشهير، والبنوك والمؤسسات المالية والتجارية الشهيرة وغيرها، وتحتوي تلك الرسائل على صور جذابة لمنتجات جديدة للموقع الأصلي أو خدمات مجانية ووصلة (Link) للموقع الذي ينشأه المحتال بشكل مماثل للموقع الأصلي وبكل تفاصيله حتى الوصول لمرحلة الدخول بكلمة السر (Password) واستخدام بطاقة الإئتمان لعملية الشراء أو تحديث البيانات (جريدة الرياض، ١٤٢٩) .

المبحث الأول: مدى قابلية البيانات والمعلومات والنقود الإلكترونية لأن تكون محلاً لجرائم الأموال

سنبين في هذا المبحث مدى قابلية البيانات والمعلومات للاستيلاء عليها في المطلب الأول، ثم سنبحث في المطلب الثاني مدى قابلية النقود الإلكترونية لأن تكون محلاً لجرائم الأموال .

المطلب الأول: مدى قابلية البيانات والمعلومات لأن تكون محلاً لجرائم الأموال

لا يوجد خلاف بخصوص صلاحية البيانات والمعلومات لأن تكون محلاً لجريمة النصب في حال ما إذا احتوتها دعامة مادية، حيث أن الأخيرة هي التي

تكون محلاً أو موضوعاً لهذه الجريمة نظراً لطبيعتها المادية .

ولكن الخلاف يدور حول صلاحية البيانات والمعلومات الحاسوبية لأن تكون محلاً لجريمة النصب إذا كانت مستقلة عن الدعامة المادية التي تحويها حيث اختلفت الآراء في هذا الشأن .

الاتجاه الأول

يرى عدم صلاحية بيانات ومعلومات الحاسب الآلي لأن تكون موضوعاً أو محلاً لجريمة النصب، ويستند أنصار هذا الاتجاه إلى عدم توافر نشاط مادي ملموس يتم به التسليم والاستلام، فلا يترتب عليه أن يحرم المجنى عليه من حيازة هذه البيانات والمعلومات التي تبقى تحت سيطرته، وهذه الأمور لا تتماشى وطبيعة النشاط الإجرامي في هذه الجريمة(الكعبي، بدون تاريخ)، (عفيفي، بدون تاريخ) .

الاتجاه الثاني

يرى صلاحية بيانات ومعلومات الحاسب الآلي لأن تكون موضوعاً أو محلاً لجريمة النصب واستند في هذا الرأي على أن النص القانوني لا يشترط أن يكون هذا المحل مادياً أو معنوياً، وأن هذا النص إنما يورد مجرد أمثلة على المحال التي يمكن أن تكون موضوعاً لهذه الجريمة .

وبهذا نرى بأنه لا يوجد رأي واحد بخصوص صلاحية البيانات والمعلومات المتعلقة بالحاسب لأن تكون محلاً أو موضوعاً لجريمة النصب .

المطلب الثاني: مدى قابلية النقود الإلكترونية لأن تكون محلاً لجرائم الأموال

تظهر أهمية البيانات والمعلومات بشكل جلي وواضح في البيانات والمعلومات المخزنة في الحسابات البنكية حيث تقوم البنوك بقيد الحسابات الخاصة بعملائها على شكل بيانات مخزنة في الحاسب الآلي وبالتالي فإن تلك البيانات والمعلومات قد حلت محل النقود مما دعا الفقه إلى أن يطلق عليها مسمى النقود الإلكترونية أو الكتابية .

وبذلك فإن من الممكن أن يقوم شخص ما بالتلاعب في هذه البيانات والمعلومات وأن يحولها لصالحه باستخدام أساليب وطرق احتيالية، أو أن تتخذ اسم أوصفة غير صحيحة، وهو ما دفع مشرعي الدول المختلفة إلى أن تنص صراحة في قوانينها وتشريعاتها على صلاحية النقود الإلكترونية أو الكتابية لأن تكون محلاً لجرائم الأموال. وحتى الدول التي لم تشر تشريعاتها إلى ذلك صراحة كفرنسا فقد قام القضاء بهذه المهمة بشكل ضمني، حيث قضت محكمة النقض الفرنسية بأن الدفع الذي يتم عن طريق القيد الكتابي يعادل تسليم النقود، وقد استند الفقه الفرنسي على هذا القضاء للقول بإمكانية انطباق وصف الغش المعلوماتي بأشكاله المختلفة على الاحتيال الذي يقترف بالتلاعب في أنظمة المعالجة الإلكترونية للبيانات والمعلومات وتحقق الاستيلاء عن طريق تحويلات تتم بشكل إلكتروني بين أجهزة الحاسب الآلي (الكعبي، بدون تاريخ) . ففي الولايات المتحدة قوانين تعرف المال

بأنه " كل شيء يمثل قيمة، وهذا التعريف يشمل الأموال الإلكترونية أو الكتابية.

أما قانون العقوبات الفرنسي الجديد فقد نص في المادة (٣١٣) منه على انطباق فعل الاحتيال على جميع أفعال التلاعب في عملية البرمجة أو في البيانات المدخلة إلى الحاسب الآلي والمنقولة عبر الإنترنت، والتي قد تؤدي إلى إلغاء رصيد دائن أو إيجاد رصيد دائن بمبالغ غير مستحقة، سواء تم ذلك عن طريق التقاط أمر التحويل بواسطة الجاني وتزييفه عن طريق الأمر بتحويل نفس قيمة المبلغ لحسابه الشخصي، أو بواسطة تلاعبه في عملية البرمجة بهدف تحويل فوائد عائدة لشخص ما إلى حسابه الشخصي، أو عن طريق انتحال الجاني لشخصية شخص آخر وقيامه بالتحويل الإلكتروني للأموال (فضل، ٢٠٠٧)، (Simon , 2004) .

المبحث الثاني: مزايا وعيوب التحويل الإلكتروني للأموال ووسائل ارتكاب جرائم الاحتيال المعلوماتي

المطلب الأول: مزايا وعيوب التحويل الإلكتروني للأموال

التحويل الإلكتروني للأموال يحمل العديد من المزايا والعيوب، وفيما يلي سنعدد المزايا ثم العيوب .

أولاً: مزايا التحويل الإلكتروني للأموال

١- تسهيل حركة البيع والشراء وزيادة حجم المبيعات . فالعديد من العملاء يوجد لديهم الاستعداد لإنفاق أموالهم إذا كانت طريقة السداد هي السحب الإلكتروني من حساباتهم بدلاً من الدفع النقدي .

٢- أن استخدام طريقة التحويل الإلكتروني للأموال أسهم بشكل كبير في التقليل من جرائم السرقات، حيث لا يحتاج الناس إلى حمل مبالغ كبيرة من المال، إلا أنه في المقابل أدى إلى ازدياد في أنماط جديدة من الجرائم ألا وهي الجرائم الإلكترونية .

٣- ساهمت التقنية الحديثة متمثلة في أنظمة الحاسبات الآلية في تقليل النفقات التي تتطلبها الوسائل الحديثة لتحويل الأموال، حيث قلصت من الحاجة إلى استخدام المستندات الورقية وحفظها . وكذلك فإن إمكانية الدخول والإطلاع الفوري التي يتبعها هذا النظام قد قللت بشكل كبير من الحاجة إلى الملفات والمستندات الورقية للبنوك وغيرها من المؤسسات المالية .

٤- تتسم عمليات التحويل الإلكتروني للأموال بالسرعة الكبيرة وعلى النقيض من الوسائل التقليدية من كتابية ونحوها مما يحقق الاستقرار في المعاملات المالية، فالسحب

والإيداع يتم بسرعة كبيرة، وهو ما يجعل الأطراف المختلفة من بنوك وتجار ومستهلكين على علم تام ومعرفة جيدة بمركزهم المالي .

٥- أن نظم التحويل الإلكتروني للأموال تتيح للمستهلكين القدرة على الوصول إلى أموالهم وكافة الخدمات البنكية والمالية بشكل سريع وفي أي وقت ومكان وهو ما لا توفره الطرق التقليدية.

٦- تتيح نظم التحويل الإلكتروني للأموال بسهولة نقل الأموال من دولة إلى أخرى بدون الحاجة إلى نقل تلك الأموال بشكل يدوي تقليدي والذي قد يأخذ أياماً أو أسابيعاً لتحقيقه مع توفير كبير في الجهد والوقت والمال، وكذلك تقليص المخاطر التي قد تترتب على النقل التقليدي لتلك الأموال من سطو عليها أو سرقتها أو ضياعها أو تلفها(قورة، ٢٠٠٥) .

ثانياً: عيوب التحويل الإلكتروني للأموال

١- إن التحويل الإلكتروني للأموال خلق أنماطاً جديدة من الجرائم المستحدثة والتي حلت محل الجرائم التقليدية . وأصبحت المعلومات المتعلقة بهذه التحويلات صيداً ثميناً يسعى إليه المجرمون. ومن أمثلة ذلك أن يجد المجني عليه رسالة في بريده الإلكتروني من البنك الذي يتعامل معه تشير إلى أن البطاقة الائتمانية أو بطاقة الصراف العائدة له قد تم إيقافها نظراً للاشتباه في قيام أحد المحتالين بسحب مبلغ كبير على بطاقته ولهذا فقد تم إيقافها، ولكي يتم تفعيل البطاقة مرة أخرى يجب عليه أن يقوم بزيارة موقع البنك وأن يقوم بتحديث بياناته حتى يتم تفعيل البطاقة مرة أخرى، ويقوم المحتال بإرفاق وصلة بها أرقام كثيرة أحياناً لا يمكن تمييزها أو وصلة يظهر فيها اسم البنك بشكل واضح لكي يعطي ذلك للمجنى عليه الشعور بالثقة والطمأنينة بصحة الرسالة ومصداقيتها مع اختلاف بسيط في التقسيمة الأخيرة بدلاً من Com تصبح Info أو org أو Sw وهكذا وعند الضغط على الوصلة المرفقة تظهر صفحة مماثلة لموقع البنك وعند إدخال الضحية لرقم بطاقته أو رقم المستخدم أو الرقم السري يتم تحويله لصفحة تحديث البيانات لتفعيل البطاقة وعند قيام الضحية بتحديث تلك البيانات يقوم المحتال بسحب أموال الضحية وسرقتها وتحويل المبالغ من حساباتها ليفرغ تلك السحابات بشكل كامل. وقد أدانت الجهات القضائية في أستراليا رجلاً أسترالياً بشكل كامل . وقد أدانت الجهات القضائية

في أستراليا بعد ثبوت تسلسله إلى موقع (eBay) وبنك محلي لسرقة ما يعادل ٣٤ ألف دولار بعد سطوه على حسابات للمستخدمين في موقع المزادات . واتهمت الجهات دوف تينيوبوم (Dove Tebnebaum) بسرقة ٩٠ حساب بيع بموقع (eBay) خلال عام ٢٠٠٧م، وكان ذلك غالباً من خلال تخمين كلمات المرور . وأفاد المحققون في هذه القضية أن الجاني كان يقوم بتتبع المستخدمين من الذين تأتي من عملائهم ملاحظات جيدة عنهم . وكان يتخفى في شخصية مستخدم للموقع لخداع المشترين . وبعد اختراق الحسابات استخدمها الجاني للإعلان عن أجهزة (I Pod) غير موجودة، كما قام الجاني باختراق بيانات أحد البنوك . وتمت إدانة الرجل لقيامه بمحاولة الحصول على المال بطرق غير مشروعة منها الاحتيال ومنها القيام بأعمال غير مشروعة باستخدام الحاسب الآلي . هذا ويواجه تينيبوم عقوبة السجن ١١ عاماً وغرامة قدرها ٩٩٠٠ دولار. وتعتبر مشكلة السطو على الحسابات مشكلة ملحة وخطيرة بين مستخدمي (e Bay) ويقول البعض أن محاولات الاختراق تعود إلى وجود ثغرة أمنية في موقع الشركة، بينما تنفي الشركة ذلك وتقول أن سرقة الحسابات تحدث نتيجة سرقة بيانات تسجيل الدخول نتيجة لضعف كلمات المرور ولمحاولات سرقة كلمات المرور (جريدة الرياض، ١٤٢٩)، (جريدة الجزيرة، ١٤٢٩).

٢- الحاجة الكبيرة إلى الصيانة لهذه النظم، فأي خلل في أنظمة الحاسب الآلي للبنك أو في وسائل الاتصال قد يترتب عليه توقف نقاط البيع عن أداء عملها، وهو ما يعني عجزها عن إتمام عمليات البيع والشراء (المناعسة، ٢٠٠١)، (Jordan , 2001) .

المطلب الثاني: وسائل ارتكاب جرائم الاحتيال المعلوماتي

مع ازدياد اعتماد البنوك على أنظمة التحويل الإلكتروني للأموال (Electronic Funds Transfer) ازدادت جرائم الاحتيال المعلوماتي البنكي بشكل مطرد، كما تنوعت وسائل ارتكابها، ولكن يمكن حصر تلك الوسائل في التالي :

أولاً: التلاعب في البرامج المستخدمة في البنوك

ويقوم الجاني في هذه الجريمة بالتلاعب بالبرنامج الذي يستخدمه البنك، أو اصطناع برنامج وهمي،

ويقوم الجاني باستغلال هذا التعديل بحيث يقوم بنسخ هذا البرنامج إلى عدد كبير من البرامج ويتمكن الجاني من توظيف كسور الفائدة خلال مدة زمنية معينة ثم تضاف مضاعفة إلى حساب الجاني . ومن الأمثلة على هذه الوسيلة الحكم الصادر من محكمة استئناف باريس في ١١أغسطس عام ١٩٨٩م إذ أدانت المحكمة أحد المبرمجين العاملين بأحد البنوك بتهمة النصب لقيامه عن طريق التلاعب في المعلومات داخل نظام الحاسب الآلي بتحويل مبالغ إلى حسابه الخاص وهو ما يعد في نظر المحكمة مكوناً للطرق الاحتيالية التي تقوم بها جريمة النصب . وفي حكم آخر صادر عن محكمة استئناف باريس في ١٣ فبراير عام ١٩٩٠م، ذهبت المحكمة إلى أن قيام المتهم بإدخال بيانات لا وجود لها إلى نظام الحاسب الآلي تسمح بإجراء عمليات تحويل إلكتروني للأموال لحساب شخص آخر بشكل غير مشروع يعد كافياً للقول بقيام جريمة النصب، كما أدانت المحكمة المتهمين الآخرين بتهمة إخفاء أشياء متحصلة من جريمة النصب. كما أدانت محكمة جنح باريس في حكم لها في ٣ فبراير عام ١٩٩٠م المتهمين الذين قاموا بتعديل ومحو المعلومات التي يحتوي عليها نظام الحاسب الآلي من أجل تحويلات غير مشروعة للأموال بتهمة النصب وإدخال أو محو أو تعديل المعلومات المبرمجة آلياً على نحو غير مشروع والمنصوص عليها في المادة (٣٢٣) من قانون العقوبات الفرنسي (الشوا، ١٩٩٨)، (قورة، ٢٠٠٥).

ثانياً: التلاعب في البيانات

وهنا يقوم الجاني بالتلاعب بالبيانات إما أثناء إدخالها أو بتعديلها بعد الإدخال أو إضافة بيانات غير صحيحة إلى الحاسب الآلي . ومن الأمثلة على هذه الوسيلة الحكم الذي أصدرته محكمة جنح باريس في ١٣ يناير عام ١٩٨٢م بحق المتهم بتهمة الشروع في النصب لقيامه بإدخال بيانات غير صحيحة إلى نظام الحاسب الآلي لإجراء ١٣٩ أمر تحويل تقدر قيمتها بحوالي ٢١ مليون فرنك فرنسي، إلا أن تلك التحويلات لم تتم لأسباب خارجة عن إرادة الجاني، وقد ذهبت المحكمة إلى أن التحويل الإلكتروني للأموال يعادل التسليم الذي تتطلبه جريمة النصب وأن إدخال بيانات غير صحيحة إلى نظام الحاسب الآلي يعد استخداماً لطرق احتيالية الهدف منها الإقناع بوجود رصيد وهمي يسمح بإجراء عمليات التحويل . كما أيدت محكمة الاستئناف الحكم السابق (الشوا، ١٩٩٨)، (عبابنه، ٢٠٠٥)، (Mason, 2007) .

ثالثاً: التلاعب في المعطيات

وهنا تتم هذه الجريمة بفك الجاني لرموز التشفير الخاصة بالمؤسسة أو البنك ثم تحويل الأموال لحسابه الشخصي . ومن الأمثلة على ذلك ما قام به أحد الجناة والذي كان يعمل مستشاراً في أحد البنوك الأمريكية، وكان قد تعرف على رموز التشفير الخاصة بالبنك الذي يعمل به ثم قام بالاتصال ببنك آخر معرفاً نفسه كمدير

فرع واستخدم الرموز لتحويل الأموال وبكميات تقل عن مليون دولار إلى أحد البنوك في مدينة نيويورك، ثم طلب من بنك نيويورك تحويل المبلغ والذي كان قد زاد عن ١٠ ملايين دولار إلى حسابه بأحد البنوك السويسرية، ثم قام بالسفر إلى سويسرا حيث اشترى بالمبلغ ماساً، وعاد إلى الولايات المتحدة الأمريكية حيث تم القبض عليه بتهمة التحويل غير المشروع للأموال. أما في المملكة العربية السعودية فقد بدأت لجنة التوعية المصرفية المنبثقة عن البنوك السعودية بث مليون رسالة نصية قصيرة توعوية وتثقيفية لعملاء البنوك كأحد الأدوات التوعوية التي تبثها البنوك في إطار المرحلة الأولى للحملة التي دشنت أخيراً لحماية عملائها من عمليات وأضرار الاحتيال المالي والمصرفي بالتعاون مع مؤسسة النقد العربي السعودي. وتتصف طبيعة الرسائل النصية القصيرة (SMS) الموجهة لعملاء البنوك بالوضوح والمباشرة بالطرح بما يتلاءم وشرائح المجتمع المختلفة حرصاً على تعميم الفائدة ورفع مستوى الوعي في المجتمع. وأوضح خالد أبوعبيد رئيس لجنة التوعية المصرفية وهي الجهة التي تتولى إدارة وتنفيذ الحملة التوعوية بأن هذه الرسائل تحمل مضامين مختلفة ومتنوعة كضرورة معرفة العميل أن البنوك لا يمكن لها أن تطلب أية بيانات شخصية عبر الرسائل الإلكترونية نهائياً. وأن التأكد من عناوين المواقع الإلكترونية للبنوك والجهات المصرفية والمالية من الأمور الواجب التأكد منها من قبل العميل، إضافة إلى وجوب عدم إعطاء أو إفشاء المعلومات المصرفية عبر الهاتف ما لم يكن العميل نفسه من يتصل بالبنك. ولفت خالد أبوعبيد إلى أن الرسائل القصيرة (SMS) تحمل في مضمونها فكرة مهمة تتلخص في المحافظة على البيانات المصرفية. وثمّن أبوعبيد مستوى التجاوب من العملاء مع نداءات البنوك لحماية مدخراتهم وأموالهم من الاحتيال وزيادة وعي العملاء لحماية أنفسهم من الوقوع ضحية أعمال الاحتيال المالي. إذ أن جهل العملاء وقلة وعيهم وإهمالهم هي أساس تفشي عمليات الاحتيال محلياً وإقليمياً ودولياً. وتأتي حملة البنوك السعودية التوعوية ضمن سلسلة متواصلة من الإجراءات المكثفة التي تبذلها البنوك العاملة في المملكة في سبيل توفير الحماية الكاملة لعملائها، لضمان مستويات أعلى من الحصانة لمدخراتهم وحقوقهم من أية محاولات المساس بها، أو اختراقها بطرق غير مشروعة. وتشمل مجموعة أدوات الاحتيال المالي والمصرفي وسائل الاحتيال الإلكتروني والمكالمات الهاتفية ورسائل الجوال وعمليات التزوير وعمليات التحويل غير المشروعة، وإساءة استخدام بطاقات السحب الآلي أو بطاقات الائتمان، وعمليات تزييف العملة والاختلاس والسرقة والعروض المالية الوهمية وغسل الأموال (جريدة الاقتصادية، ١٤٣٠).

المبحث الثالث: الاحتيال باستخدام بطاقات الائتمان

أفرز التطور التقني العديد من بطاقات الائتمان، لا لسحب النقود من البنوك فقط، بل لتسديد أثمان المشتريات، أو لتوفير خدمة الاتصال الهاتفي، أو لغيرها من الخدمات، وقد أحدثت هذه البطاقات ثورة حقيقية في أعمال الدفع والتسديد لتلك الخدمات. ومن أهم هذه البطاقات تلك الخاصة بالائتمان والتي عرفت بأنها " بطاقة مستطيلة من البلاستيك، تحمل اسم المؤسسة المصدرة لها وشعارها وتوقيع حاملها، أو رقمها واسم حاملها ورقم حسابه، وتاريخ انتهاء صلاحيتها، ويستطيع بواسطتها أن يحصل من التجار (المتعاملين بها) على ما يحتاجه من سلع وخدمات دون أن يضطر إلى الوفاء بثمنها فوراً وإنما يكتفي بتقديمها للتجار لتدوين بياناتها (يدوياً أو إلكترونياً) ومن ثم خصم قيمتها من الجهة المصدرة لها (قورة، ٢٠٠٥)، وبذلك فإن بطاقة الائتمان تختلف عن بطاقة الصرف الآلي والتي يقدمها البنك لعملائه ليكون باستطاعتهم سحب مبالغ مالية من أجهزة الصرف الآلي للنقود (Automatic Teller Machines) التابعة للبنك والموزعة في أماكن متعددة ودون التقيد بأوقات عمل البنك (رضوان، ١٤٢٩). ونظراً للانتشار الكبير لهذه البطاقات، فقد أدى ذلك إلى ازدياد إساءة استخدام هذه البطاقة للحصول على المنفعة المالية غير المشروعة سواء كان ذلك من قبل حاملها الشرعي أو من الغير، وقد أتاحت التقنية الحديثة لمجرمي الحاسب الآلي والإنترنت إمكانية الحصول على أرقام البطاقات الائتمانية باستخدام برامج تشغيل، تتيح إمكانية الحصول على أرقام بطاقات بنك معين بواسطة تزويد الحاسب بالرقم الخاص بالبنك واستخدامها بشكل غير مشروع في القيام بعمليات شراء سلع أو الحصول على خدمات عبر شبكة الإنترنت، بحيث يتم خصم قيمة هذه السلع والخدمات من المالكين الحقيقيين لهذه البطاقات (الصغير، ١٩٩٩)، (الشوابكة، ٢٠٠٤). وسنتناول الحالتين فيما يلي :

المطلب الأول: الاحتيال باستخدام بطاقة الائتمان من قبل حاملها الشرعي

وترتكب هذه الجريمة من قبل حامل البطاقة الشرعي الذي صدرت باسمه عبر شبكة الإنترنت عن طريق دفع ثمن السلع والخدمات المعروضة عبر شبكة الإنترنت إما بإساءة استخدام بيانات البطاقة أثناء مدة صلاحيتها، أو باستخدامها بعد انتهاء مدة صلاحيتها أو إلغاؤها، وذلك كما يلي :

١- إساءة استخدام البطاقة خلال فترة صلاحيتها

وترتكب هذه الجريمة باستخدام البطاقة من قبل صاحبها عبر شبكة الإنترنت عن طريق دفع قيمة السلع والخدمات المقدمة على الشبكة، رغم علمه بأن رصيده

بالبنك لا يغطي قيمة تلك السلع والخدمات، أو أن يقوم بإجراء تحويل إلكتروني من رصيد لآخر بشكل يتجاوز رصيده في البنك مصدر البطاقة . وقد اختلف القضاء الفرنسي في مسألة اعتبار هذا الفعل جريمة حيث ذهبت بعض الأحكام الصادرة من المحاكم الفرنسية إلى اعتبار الفعل جريمة سرقة، بينما ذهبت أحكام أخرى إلى اعتبار هذا الفعل من قبيل جرائم النصب (المناعسة، ٢٠٠١)، (الشوابكة، ٢٠٠٤)، وعلى خلاف هذه الأحكام قضت محكمة استئناف (Angers) في حكم صادر لها إلى أن استيلاء مالك البطاقة على مبالغ مالية تتجاوز رصيده بوضعها في أحد أجهزة الصرف الآلي المخصصة لذلك لا تشكل جريمة يعاقب عليها القانون، وقد أيدت محكمة النقض الفرنسية هذا الحكم في سنة ١٩٨٢م، حيث جاء في حيثيات حكمها بأنه " نظراً لأن محكمة الاستئناف ومن أجل الحكم ببراءة المتهم أثبتت أنه لكي يتمكن المتهم من إجراء السحب غير المشروع فقد استخدم البطاقة بوصفه مالكها، وبناء على ذلك فقد بررت محكمة الاستئناف حكمها، إلا أنه في الواقع فإن الوقائع المنسوبة للمتهم تنطوي على عدم ملاحظة التزام تعاقدي، ولا تندرج تحت أي نص جنائي " (الشوا، ١٩٩٨).

كما اختلف الفقه أيضاً في شأن تكييف الواقعة، فعارض أغلب الفقه اعتبار قيام مالك البطاقة بسحب مبلغ يزيد عن مجموع رصيده لدى البنك أو بمقدار الائتمان الممنوح له، احتيالاً استناداً إلى أن جهاز الصرف الآلي مبرمج من قبل البنك على السماح لمالك البطاقة بالسحب من عدمه، فإذا سمح الجهاز بتسليم النقود فمعنى ذلك أن البنك نفسه قد سمح بذلك وبالتالي لا يكون هناك أي احتيال من قبل مالك البطاقة على البنك (رضوان، ٢٠٠٨)، (الصغير، ١٩٩٢) .

فمن الصعوبة بمكان إطلاق وصف السرقة على الفعل، والقول بأن مالك البطاقة قد اختلس المبالغ المالية التي حصل عليها باستخدام بطاقته دون رضاء وموافقة البنك . فالبنك يحدد بشكل مسبق وآلي كيفية الاستجابة لما يطلبه مالك البطاقة، ويتم ذلك بموافقة البنك . أما المبالغ الزائدة التي تتم عن طريق الخطأ فهنا يحق للبنك أن يطالب بردها .

٢- إساءة استخدام البطاقة بعد انتهاء فترة صلاحيتها أو إلغاؤها

أولاً: الاستخدام غير المشروع للبطاقة الملغاة من قبل البنك: قد يقوم البنك في حالات معينة بإلغاء البطاقة الائتمانية، أو يوقف العمل بها ويطلب من العميل رد هذه البطاقة، فإذا ما قام البنك بإلغاءها وأخطر العميل بذلك فإنه يجب على العميل أن يعيد تلك البطاقة إلى البنك، فإذا امتنع العميل عن ردها فإن استخدامه لتلك البطاقة في سحب الأموال يشكل ارتكاباً لفعل الاختلاس تقوم به جريمة خيانة الأمانة (الشوا، ١٩٩٨)، (الشوابكة، ٢٠٠٤).

ثانياً: الاستخدام غير المشروع للبطاقة منتهية الصلاحية: لكل بطاقة ائتمانية مدة صلاحية معينة، وبعد انقضاء هذه المدة يجب على مالكها ردها إلى البنك أو تجديدها، ولكن قد يحدث أن يمتنع مالك البطاقة عن إعادتها إلى البنك ويستمر في استخدامها. وقد ذهب الفقه إلى أن المالك الشرعي لهذه البطاقة لا يرتكب جريمة نصب إذا ما قام بالوفاء للتاجر بموجب بطاقة منتهية الصلاحية، لأن الكذب الصادر عن مالك البطاقة ينص فقط على مدى صلاحية البطاقة لا على الإقناع بوجود ائتمان وهمي، وهو ما يستطيع التاجر كشفه عن طريق الاطلاع على تاريخ صلاحية البطاقة، ويرى هذا الفقه أن المسئولية هنا تقع على التاجر، فيتحمل الضرر وحده إذا ما قبل الوفاء باستخدام بطاقة منتهية الصلاحية.

المطلب الثاني: الاحتيال باستخدام بطاقة الائتمان من قبل الغير

قد يحدث الاستعمال غير المشروع لبطاقة مفقودة أو مسروقة من قبل الغير أما لسحب نقود أو للوفاء بواسطتها لدى المحلات والتجار.

والجاني الذي يستعمل بطاقة مسروقة أو مفقودة لسحب الأموال من أجهزة الصرف الآلية يعد مرتكباً لجريمة نصب. ويمكن أيضاً نسبة جريمة السرقة إلى الجاني باعتباره سارقاً للبطاقة ذاتها.ومضاهاة التوقيع المدون على البطاقة مع التوقيع المدون على فاتورة البيع يشكل صعوبة كبيرة. فتقديم البطاقة إلى التاجر للوفاء بواسطتها كافٍ لتحقق جريمة النصب (عبابنه، ٢٠٠٥). وقد يتم استعمال البطاقة للوفاء بواسطتها لدى التجار، وهنا لا يحتاج الجاني إلى معرفة الرقم السري للبطاقة، بل يحتاج فقط إلى التوقيع على فاتورة البيع، ويساهم في تسهيل استعمال البطاقة بشكل كبير صعوبة تحقق التاجر أو البائع من شخصية حامل البطاقة. وقد ذكرت دارسة أجريت من قبل شركة سيمانتيك (Semantic) وهي إحدى شركات أمن البرمجيات ومكافحة قرصنة المعلومات أن القراصنة المتخصصين في سرقة بيانات البطاقات الإئتمانية لديهم قدرت إنفاق إتمانية في حدود ٥ بلايين دولار. وتوصلت شركة سمانتيك إلى هذا الرقم خلال إعداد دراسة عند الاقتصاد السري على شبكة الإنترنت خلال عام ٢٠٠٨م. ووفق البحث فإن أرقام البطاقات الائتمانية هي أكثر السلع بيعاً بين القراصنة، حيث تشكل ٣١٪ من السلع المعروضة للبيع في هذا الاقتصاد السري. وجاء في المرتبة الثانية طبقاً لما جاء على موقع (BBC) على شبكة الإنترنت البيانات البنكية التي تشكل ٢٠٪ من السلع التي تعرض في قنوات المحادثة الخاصة بالقراصنة. وقد تم التوصل إلى رقم ٥ بليون دولار عبر مضاعفة متوسط حجم المال الذي تمت سرقته من بطاقة ائتمانية ما، في عدد الناس الذين عرضت عليهم أرقام البطاقة، كما أفادت الدراسة أنه لو سحب قراصنة البطاقات الائتمانية كل الحسابات

البنكية المعروضة تفاصيلها للبيع فإنهم قد يحصلوا على ١,٧ بليون دولار . وقد وجد أن أرقام البطاقات الائتمانية شائعة للغاية لدى قراصنة المعلومات وذلك لأن من السهل الحصول عليها واستخدامها في جرائم الاحتيال . وذكرت الدراسة أيضاً أن أسعار بيانات بطاقات الائتمان تباينت من منطقة إلى أخرى . فالبطاقات الأمريكية تعد الأرخص حيث تشكل ما نسبته ٧٤٪ من البطاقة المعروضة للبيع بين القراصنة . أما البطاقات الصادرة في أوروبا أو الشرق الأوسط فهي أغلى وذلك لندرتها . وقد وجدت الدراسة أن أكثر الجماعات الإجرامية تنظيماً في هذا المجال هي عصابات أوروبا الشرقية، حيث لديهم القدرة على إنتاج بطاقات مزورة بأعداد كبيرة (جريدة الجزيرة، ١٤٣٠). وتتحقق جريمة النصب هنا باتخاذ الجاني صفة غير صحيحة لإيهام التاجر بأنه المالك الشرعي للبطاقة وأنه يملك الرصيد الذي تمثله البطاقة، ويمكن أيضاً القول بأن الجاني قد اتخذ اسماً كاذباً وانتحل شخصية المالك الحقيقي للبطاقة (الصغير، ١٩٩٢) . كما أن توقيعه على فاتورة البيع وتزويره لتوقيع المالك الحقيقي للبطاقة يجعله مرتكباً لجريمة تزوير في المحررات الخاصة وهي جريمة تعاقب عليها القوانين المختلفة وقد أورد تقرير صادر عن شركة سمانتيك (Semantic) السالفة الذكر وهي من الشركات المتخصصة بأمن تقنية المعلومات أن معلومات البطاقات الائتمانية معرضة للسرقة بشكل تزايد ومن ثم البيع بثمن بخس لا يتجاوز ٥,١٥ سنت أمريكي، ولا تقتصر الجرائم الإلكترونية على الاستفادة من البطاقات الائتمانية فحسب، بل حتى الحسابات المصرفية معرضة للاختراق وبيع معلومات، لكن أسعارها أعلى من نظيرتها البطاقات الائتمانية . وذكر التقرير أن الاقتصاد السري على الإنترنت بلغ مرحلة عالية من النمو " تجعله سوقاً تجارية فاعلة على مستوى العالم، يتم فيها بانتظام بيع وشراء البضائع والخدمات المسروقة أو المرتبطة بأعمال الاحتيال، حيث تقدر قيمة البضائع والخدمات المسروقة أو المرتبطة بأعمال الاحتيال فيه بملايين الدولارات، وحسب التقرير فقد جاءت معلومات بطاقات الائتمان في المرتبة الأولى بين أصناف البضائع والخدمات المعروضة في الاقتصاد السري، بنسبة بلغت ٣١ في المائة من إجمالي المعروض . ومع كون بطاقات الائتمان المسروقة تباع بمبلغ ضئيل لا يتجاوز ٥,١٥ إلى ٢,٥ دولاراً للبطاقة الواحدة، إلا أن متوسط الحد الائتماني للبطاقات المسروقة بلغ أكثر من ٤ آلاف دولار . ووفقاً للحسابات التي أجرتها شركة سيمانتيك، فإن القيمة التقديرية لجميع بطاقات الائتمان المعلن عنها خلال فترة التقرير وهي شهر نوفمبر من عام ٢٠٠٨م كانت ٥,٣ بليون دولار.ويعود ذلك إلى سهولة الحصول على معلومات بطاقات الائتمان عبر الإنترنت، فهي يسيرة الاستخدام في التسوق عبر الإنترنت، وغالباً ما يصعب على التجار أو الجهات المصدرة لهذه البطاقات اكتشاف عمليات الاحتيال قبل انتهاء المحتالين من القيام

بعملياتهم وتسلم بضائعهم . إضافة إلى أن معلومات بطاقات الائتمان تباع عادة للمحتالين بالجملة، ع تقديم حسومات جيدة(جريدة الشرق الأوسط، ٢٠٠٨) .

المبحث الرابع: موقف بعض التشريعات المقارنة من جرائم الاحتيال المعلوماتي

سنتناول في هذا المبحث موقف التشريعات في بعض الدول الغربية من جرائم الاحتيال المعلوماتي إضافة إلى موقف التشريعات في بعض الدول العربية بالنسبة لجرائم الاحتيال المعلوماتي .

المطلب الأول: موقف تشريعات بعض الدول الغربية

أولاً: الولايات المتحدة الأمريكية

يعاقب القانون الفدرالي الأمريكي " كل من يقوم بالدخول عمداً إلى حاسب آلي مشمول بالحماية (Protected Computer) دون أن يكون مصرحاً له بذلك أو أن يكون متجاوزاً لحدود التصريح الممنوح له إذا ما كان الغرض والأثر المترتب على هذا الدخول هو الحصول على شيء ذي قيمة بواسطة الاحتيال " [١]. ويتبين لنا من النص السابق بأن تجريم الاحتيال المعلوماتي مشروط بأن يكون الدخول إلى نظام الحاسب الآلي غير مصرح به، أو أن يتجاوز الدخول حدود التصريح الممنوح للجاني، وهو ما يعني استبعاد جميع الحالات التي يكون فيها الاحتيال المعلوماتي قد تم بناء على دخول تم التصريح به إلى نظام الحاسب الآلي وهي على وجه الخصوص الحالات المتعلقة باستخدام بطاقات الائتمان . ويقتصر تطبيق النص السابق على الحاسبات الآلية المحمية وهي الحاسبات المستخدمة في الأجهزة الفدرالية الحكومية للولايات المتحدة. كما جرم قانون ولاية كاليفورنيا الأمريكية (State of California) الدخول إلى أنظمة الحاسبات الآلية (Computer Systems) وإلى شبكة المعلومات لأغراض احتيالية وبنية الحصول على ممتلكات أو خدمات باستخدام الطرق الاحتيالية . وقد توسع القانون في تحديد الممتلكات التي يمكن أن تكون محلاً للاحتيال المعلوماتي، بحيث أصبح النص ينطبق في جميع الحالات التي يستخدم فيها الحاسب الآلي للحصول على أي نوع من الممتلكات سواء كانت مادية أو غير مادية [٢].

ثانياً: الجمهورية الفرنسية

لم يورد المشرع الفرنسي نصاً خاصاً يجرم الاحتيال في مجال المعلوماتية ولكن يمكن تطبيق النصوص الواردة في قانون العقوبات في المادة (٤٠٥) منه على تجريم الاستيلاء على مال الغير. وقد حدد المشرع الفرنسي على سبيل الحصر الأساليب التي يقع بها الاحتيال كأحد عناصر النصب وهي استعمال الطرق الاحتيالية والتصرف في مال الغير واتخاذ اسم

(١) القانون الفديرالي الأمريكي رقم ١٠٣٠ (أ) (٤).

(٢) قانون العقوبات لولاية كالفورنيا رقم (٥٠٢) (ب).

كاذب أو صفة غير صحيحة (الشوابكة، ٢٠٠٤)، (قشقوش، ١٩٩٢)، (Nimmer ,2008). ويمكن انطباق النص السابق المتعلق بالطرق الاحتيالية على التلاعب المعلوماتي ليشكل أحد أساليب الاحتيال.

والحاسب الآلي يستخدم كوسيط للاحتيال، ويرى الفقه الفرنسي أنه من المتصور وقوع فعل الاحتيال على نظام الحاسب وبالتالي إيقاعه في غلط بقصد سلب المال لأن هنا الفعل تتوافر فيه الطرق الاحتيالية بمفهومها المستقر ككذب تدعمه أعمال مادية أو وقائع خارجية حيث تتوافر فيه إضافة إلى الكذب واقعة خارجية هي تقديم المستندات أو المعلومات المدخلة إلى الحاسب الآلي. كما تتحقق هذه الطرق كذلك باستخدام المستندات غير الصحيحة التي يخرجها الحاسب بناء على ما حصل في برامجه أو في البيانات المخزنة داخله من التلاعب كي يستولى على أموال لا حق له فيها. ويستند أنصار هذا الرأي إلى حكم محكمة النقض الفرنسية بتطبيق عقوبة النصب على شخص وضع قطعاً معدنية بدلاً من قطعة النقود في عداد أماكن وقوف السيارات وترتب على ذلك تشغيل الماكينة، واعتبرت المحكمة هذا الفعل من قبيل الطرق الاحتيالية (الشوا، ١٩٩٨). كما نص قانون العقوبات الفرنسي الجديد في المادة (٣١٣) منه على أنه يعد احتيالاً جميع أفعال التلاعب في عملية البرمجة أو في البيانات المدخلة إلى الحاسب الآلي والمنقولة عبر شبكة الإنترنت والتي قد تؤدي إلى إلغاء رصيد الدائن أو خلق رصيد دائن بمبالغ غير مستحقة، وتتعدد الأساليب المستخدمة في هذا الشأن، فقد يحدث ذلك عن طريق التقاط أمر التحويل بواسطة الجاني، وتزييفه بالأمر بتحويل نفس المبلغ لحسابه الخاص أو عن طريق التلاعب في عملية البرمجة بغرض تحويل فوائد حساب شخص ما إلى حساب الفاعل، وأخيراً عن طريق انتحال الفاعل لشخصية الغير ومباشرته لعملية تحويل الأموال.

ثالثاً: إنجلترا

في بريطانيا تم إضافة مادة جديدة على القانون الخاص بالسرقة لعام ١٩٦٨م وذلك بعد الحكم الصادر من مجلس اللوردات البريطاني (House of Lords) والذي يعتبر أعلى جهة قضائية في بريطانيا في قضية (RV . Preddy) في عام ١٩٩٦م والذي رفض تطبيق المادة ١٥ (١) من القانون الخاص بالسرقة لعام ١٩٦٨م، والتي تتعلق بالحصول على ممتلكات الغير عن طريق الاحتيال، على التحويل الإلكتروني غير المشروع للأموال من رصيد لآخر، فتمت إضافة المادة ١٥ (أ) إلى القانون السالف الذكر بمقتضى التعديل الذي شمله عام ١٩٩٦م. وتعاقب المادة المذكورة كل شخص يحصل عن طريق الاحتيال على تحويل إلكتروني للأموال له أو للغير. ويتم التحويل عندما يتم سحب مبلغ ما من حساب بنكي ليتم إيداعه في حساب آخر. وقد ذكر تقرير صادر من مؤسسة جارليك (Garlik) البريطانية المتخصصة في مجال كشف حالات الغش عبر الإنترنت عن تسجيل أكثر من ٢٥٠,٠٠٠

حادثة غش مالي عبر شبكة الإنترنت في بريطانيا في عام ٢٠٠٧م وحده، بزيادة قدرها ٢٠٪ عن تلك التي تم تسجيلها في العام الذي سبقه . وقدر التقرير السابق أن أكثر من ثلاثة ملايين ونصف جريمة إلكترونية قد تمت، بزيادة قدرها ٩٪ مقارنة بعام ٢٠٠٦م . وأضاف التقرير أن حالات الغش المتعلقة بجرائم الهوية بلغت ٨٤,٠٠٠ حالة . وسجلت أعلى حالات سرقة للوثائق عبر شبكة الإنترنت، معلومات تتعلق بجوازات السفر، وبطاقات الائتمان وفواتير الخدمات والتحويل الغير مشروع للأموال، وجرائم الاحتيال المعلوماتي . وبين التقرير الذي تم نشره على موقع وزارة الاتصالات وتقنية المعلومات البريطانية أن الركود الاقتصادي العالمي وزيادة معرفة الأشخاص بالاحتيال والسرقات عبر شبكة الإنترنت ربما تؤدي إلى زيادة عدد الأفراد الذين يلجؤون إلى جرائم الحاسب والإنترنت . وذكر التقرير أن الجرائم الإلكترونية تسببت في خسائر تقدر بحوالي ٥٣٥ مليون جنيه إسترليني . كما أظهر التقرير أن هناك انخفاضاً كبيراً في حالات الغش المصرفية عبر شبكة الإنترنت بفضل الضوابط المطبقة من قبل البنوك البريطانية . وأوضح التقرير أن على الأفراد وخصوصاً في هذا الوقت من الأزمة المالية أن يكونوا على يقظة وانتباه فيما يتعلق بمعلوماتهم الشخصية (Personal Information)، لأنه طالما استمرت الضغوط الائتمانية (Credit Crunch) ، فيمكن أن نتوقع زيادة كبيرة في جرائم الاحتيال عبر الإنترنت (جريدة الرياض، ١٤٢٩)، ((Friedman, 1997)، (Heymann,1997)، (Katyal,2001)) .

رابعاً: الجمهورية الألمانية

نص قانون العقوبات الألماني في المادة (٢٦٣) (أ) منه على تجريم الاحتيال المعلوماتي، حيث تنص هذه المادة على أنه يعد مرتكباً لجريمة الاحتيال المعلوماتي كل من يقوم بنية تحقيق ربح غير مشروع له أو للغير وإلحاق ضرر بالغير بالتأثير في نتيجة المعالجة الآلية للمعلومات عن طريق برمجة غير سليمة أو استعمال بيانات غير صحيحة أو غير مكتملة أو عن طريق الاستعمال غير المصرح به للبيانات أو عن طريق التدخل غير المصرح به في عملية المعالجة ذاتها (Simon ,2004) .

المطلب الثاني: موقف بعض التشريعات العربية

أولاً: الإمارات العربية المتحدة

حدد المشرع الإماراتي في المادة (٣٣٩) من قانون العقوبات الإتحادي محل الاستيلاء في جريمة الاحتيال بأنه مال منقول أو سند أو توقيع هذا السند أو إلغائه أو إتلافه أو تعديله وذلك بالاستعانة بإحدى الطرق المذكورة على سبيل الحصر . كما نص المشرع الإماراتي في المادة (٤٠٤) من قانون العقوبات الإماراتي على جريمة خيانة الأمانة بقوله " يعاقب بالحبس أو بالغرامة كل من اختلس أو استعمل أو بدد مبالغ أو سندات أو أي مال آخر منقول إضراراً بأصحاب الحق عليه متى

كان قد سلم إليه على وجه الوديعة أو الإجارة أو الرهن أو عارية الاستعمال أو الوكالة . وفي تطبيق هذا النص يعتبر في حكم الوكيل الشريك على المال المشترك والفضولي على مال صاحب الشأن ومن تسلم شيئاً لاستعماله في أمر معين لمنفعة صاحبه أو غيره".

كما نصت المادة (٤٠٤) من قانون العقوبات الإماراتي على أن فعل خيانة الأمانة يقع على مبالغ أو سندات أو أي مال آخر منقول، فالشرط الأساسي للمال أن يكون مالاً منقولاً مملوكاً لغير الجاني وقد أورد المشرع الإماراتي في المادة السابقة أنواعاً من هذه الأموال على سبيل المثال وهي المبالغ والسندات ثم أضاف إلى ذلك أو أي مال آخر منقول(عبدالله، ٢٠٠٧)، (الكعبي، بدون تاريخ).

وقد قضت المحكمة الاتحادية الإماراتية بأن " القصد الجنائي في خيانة الأمانة يتحقق باتجاه إرادة الجاني إلى ارتكاب فعل الاختلاس أو التبديد أو الاستعمال أو إنزال الضرر ولو في صورة احتمالية بالمجنى عليه أو غيره، ويعتبر خيانة أمانة استيلاء الوكيل على الشيء الذي أؤتمن عليه لحساب موكله فاستعمله في غير مصلحته " [٣].

كما أصدر المشرع الإماراتي القانون الاتحادي رقم (٢) لعام ٢٠٠٦م في شأن مكافحة جرائم تقنية المعلومات وهو يعد الإطار القانوني لمكافحة هذا النوع من الجرائم، وقد نص المشرع الإماراتي في المادة (١٠) من هذا القانون على أن " كل من توصل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات إلى الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجنى عليه يعاقب بالحبس مدة لا تقل عن سنة وبالغرامة التي لا تقل عن ثلاثين ألف درهم أو بإحدى هاتين العقوبتين . وقد حذر خبراء في أمن المعلومات من انتشار الجرائم الإلكترونية وبخاصة القرصنة، والتي تهدف إلى سرقة أرقام الحسابات المصرفية، إضافة إلى استخدامها في الابتزاز، وغياب إدارات مكافحة الجرائم الإلكترونية في خمس إمارات من الإمارات العربية المتحدة، ووجودها في دبي وأبوظبي فقط . وأوضح مدير إدارة المباحث الإلكترونية في دبي، الرائد سعيد الهاجري، أن الإدارة حققت في نحو (٢٢٢) قضية قرصنة خلال عام ٢٠٠٨م . فيما أكد قانونيون خطورة عدم وجود إدارات للجرائم الإلكترونية في الإمارات الخمس، على الرغم من وقوع جرائم إلكترونية غير ظاهرة، مشيرين إلى أنها في ازدياد وتهدف بشكل رئيس إلى سرقة أرقام الحسابات المصرفية، والاستغلال الجنسي. وكانت بنوك داخل دولة الإمارات قد تعرضت في سبتمبر ٢٠٠٨م لسطو منظم، نجم عنه سحب أرصدة متعاملين

(٣) طعن رقم ٧٥ لسنة ١٨ قضائية جلسة ١٩٩٨/٢/٢٥ المحكمة الاتحادية العليا الإماراتية، وردت في محمد عبيد الكعبي، المرجع السابق، ص ٢٠٦ .

عديدين ووفقاً لإحصاءات نشرتها مؤسسة (أي . دي . سي) (IDC) للأبحاث، فقد حققت الإمارات أدنى معدلات القرصنة في الشرق الأوسط بنسبة ٣٥٪ وهي الدولة الوحيدة في المنطقة المصنفة ضمن القائمة العالمية لأفضل ٢٠ دولة في مجال مكافحة القرصنة ، وأكد مسؤولون في هيئة تنظيم الاتصالات الإماراتية وشركة الاتصالات المتكاملة (دو)، عدم تعرض أي من المواقع الإلكترونية في الدولة إلى الاختراقات، لافتين إلى أنها قد تنتج بسبب المستخدمين الزوار وأصحاب المواقع وليس المشغلين . ولفت خبراء في أمن المعلومات إلى أن نحو ٩٥٪ من المواقع التي توفر خدمات للقرصنة مزيفة وهدفها ربحي، منوهين إلى ضرورة التأكد من العناوين الإلكترونية التي يزورونها، خصوصاً التي تتطلب معلومات سرية خاصة بهم وببطاقات ائتمانهم وحساباتهم البنكية . وذكر مدير إدارة المباحث الإلكترونية في دبي أن هناك صوراً مختلفة من الاختراقات تعاملت معها الإدارة، منها اختراق الحاسبات الآلية أو أجهزة الحاسبات الشخصية بواسطة برامج محددة يستخدمها القراصنة عبر الإنترنت . ومن القضايا التي حققت فيها هذه الإدارة قضية بنك (اتش اس بي سي) (HSBC) الذي قام مجهولون بنسخ موقع مزيف له وحاولوا مخاطبة العملاء من خلاله . ولفت الهاجري إلى أن وزارات خدمية في دولة الإمارات مثل التربية والتعليم تعرضت للمشكلة ذاتها وتعاملت معها على الفور من خلال تحذير أفراد المجتمع عبر وسائل الإعلام وتم تحديد هوية أصحاب المواقع المزيف وإغلاقه . ووفقاً للهاجري، فقد بلغ عدد القضايا التي تابعتها إدارة المباحث الإلكترونية في شرطة دبي خلال العام الجاري (٢٢٢) قضية بواقع ٨٧ قضية نصب وجرائم مالية، و٣٨ جريمة اختراق شبكات و ٩٢ قضية تشهير وابتزاز وخمس قضايا لمواقع وهمية قصد بها الاحتيال على المتعاملين . وبين الهاجري وجود ثغرات قانونية في التشريعات المتعلقة بالجرائم الإلكترونية موضحاً أن المشكلة تكمن في أن أقسام وإدارات الشرطة في خمس إمارات تخلو من المؤهلات الموجودة في دبي وأبوظبي، للتعامل مع مثل هذه الجرائم . مشيراً إلى ضرورة إيجاد إدارات وبخبرات من هذا النوع من الجرائم التي أصبحت تتزايد بشكل كبير مع تطور التقنية وأصبح معه القراصنة يتربصون بأرقام الحسابات البنكية وغيره (جريدة الجزيرة، ١٤٣٠) .

كما نصت المادة (١١) من القانون ذاته على أن " كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، في الوصول من دون وجه حق إلى أرقام أو بيانات بطاقة ائتمانية أو غيرها من البطاقات الإلكترونية يعاقب بالحبس وبالغرامة، فإن قصد من ذلك استخدامها في الحصول على أموال الغير، أو ما تتيحه من خدمات، يعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة أو بإحدى هاتين العقوبتين، وتكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن ثلاثين ألف درهم أو بإحدى هاتين

العقوبتين إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال الغير".

ثانياً: الجمهورية التونسية

يعد القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية رقم (٨٣) لعام ٢٠٠٠م هو الإطار القانوني لمكافحة هذا النوع من الجرائم. وطبقاً لأحكام الفصل (٥٠) من هذا القانون يعاقب كل من استغل ضعف أو جهل شخص في إطار عمليات البيع الإلكتروني بدفعه للالتزام حاضراً أو آجلاً بأي شكل من الأشكال، بعقوبة تتراوح بين ١,٠٠٠ و ٢٠,٠٠٠ دينار، وذلك إذا ثبت من ظروف الواقعة أن هذا الشخص غير قادر على تمييز أبعاد تعهداته أو كشف الحيل والخدع المعتمدة بالالتزام أو إذا ثبت أنه كان تحت الضغط مع مراعاة أحكام المجلة الجنائية.

كما ينص الفصل (٥١) من القانون نفسه على أن يعاقب كل مخالف لأحكام الفصلين (٣٨) و (٣٩) بعقوبة تتراوح بين ١٠٠٠ و ١٠,٠٠٠ دينار (حجازي، ٢٠٠٢).

ثالثاً: المملكة العربية السعودية

أقرت المملكة نظامي التعاملات الإلكترونية ومكافحة الجرائم المعلوماتية ويهدف نظام التعاملات الإلكترونية إلى ضبط التعاملات والتوقيعات الإلكترونية، وتنظيمها، وتوفير إطار نظامي لها وبما يؤدي إلى تحقيق ما يلي:

١- إرساء قواعد نظامية موحدة لاستخدام التعاملات والتوقيعات الإلكترونية، وتسهيل تطبيقها في القطاعين العام والخاص، بواسطة سجلات إلكترونية يُعوَّل عليها.

٢- إضفاء الثقة في صحة التعاملات والتوقيعات والسجلات الإلكترونية وسلامتها.

٣- تيسير استخدام التعاملات والتوقيعات الإلكترونية على الصعيدين المحلي والدولي، للاستفادة منها في جميع المجالات، كالإجراءات الحكومية، والتجارة، والطب، والتعليم، والدفع المالي الإلكتروني.

٤- إزالة العوائق أمام استخدام التعاملات والتوقيعات الإلكترونية.

٥- منع إساءة الاستخدام والاحتيال في التعاملات والتوقيعات الإلكترونية.

كما نص نظام التعاملات الإلكترونية في المادة (٢٠) منه على تحمل مقدم خدمات التصديق مسؤولية ضمان صحة المعلومات المصدقة التي تضمنتها الشهادة وقت تسليمها، وصحة العلاقة بين صاحب الشهادة وبياناتها الإلكترونية. وتقع عليه مسؤولية الضرر الذي يحدث لأي شخص وثق -بحسن نية- بصحة ذلك (نظام التعاملات الإلكترونية، ١٤٢٨).

كما نصت المادة (٢٢) (٢) من نفس النظام على أن على صاحب الشهادة الإلكترونية تقديم المعلومات الصحيحة لمقدم خدمات التصديق، أو

لجميع الأطراف المطلوب منها أن تثق في توقيعه الإلكتروني .

كما عد نظام التعاملات الإلكترونية مخالفة لأحكامه ما يلي :

١- قيام مقدم خدمات التصديق بتقديم بيانات كاذبة أو معلومات مضللة للهيئة، أو أي سوء استخدام لخدمات التصديق.

٢- إنشاء شهادة رقمية أو توقيع إلكتروني، أو نشرها، أو استعمالها لغرض احتيالي، أو لأي غرض غير مشروع .

٣- تزوير مسجل إلكتروني، أو توقيع إلكتروني، أو شهادة تصديق رقمي، أو استعمال أي من ذلك مع العلم بتزويره .

٤- تقديم معلومات خاطئة عمداً إلى مقدم خدمات التصديق، أو تقديم معلومات خاطئة عمداً عن التوقيع الإلكتروني إلى أي من الأطراف الذين وثقوا بذلك التوقيع بموجب هذا النظام .

٥- الدخول على منظومة توقيع إلكتروني لشخص آخر دون تفويض صحيح، أو نسخها، أو إعادة تكوينها، أو الاستيلاء عليها .

٦- انتحال شخص هوية آخر، أو ادعاؤه زوراً بأنه مفوض عنه بطلب الحصول على شهادة التصديق الرقمي أو قبولها، أو طلب تعليق العمل بها، أو إلغائها .

٧- نشر شهادة مصادقة رقمية مزورة أو غير صحيحة أو ملغاة أو موقوف العمل بها، أو وضعها في متناول شخص آخر، مع العلم بحالها، ويستثنى من ذلك حق مقدم خدمات التصديق الوارد في الفقرة (٤) من المادة (١٨) .

كما نصت المادة (٤) من نظام التعاملات الإلكتروني على أنه " مع عدم الإخلال بأي عقوبة أشد ينص عليها في نظام آخر، يعاقب كل من يرتكب أياً من الأعمال المنصوص عليها في المادة (الثالثة والعشرين) من هذا النظام بغرامة لا تزيد على خمسة ملايين ريال، أو بالسجن مدة لا تزيد على خمس سنوات، أو بهما معاً، ويجوز الحكم بمصادرة الأجهزة والمنظومات والبرامج المستخدمة في ارتكاب المخالفة .

أما نظام مكافحة جرائم المعلوماتية فيهدف إلى الحد من وقوع جرائم المعلوماتية وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، وبما يؤدي إلى ما يأتي :

١- المساعدة على تحقيق الأمن المعلوماتي .

٢- حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية .

٣- حماية المصلحة العامة، والأخلاق والآداب العامة .

٤- حماية الاقتصاد الوطني(نظام مكافحة الجرائم المعلوماتية، ١٤٢٨).

كما نص نظام مكافحة جرائم المعلوماتية على فرض عقوبة السجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، على كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية :

١- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي – دون مسوغ نظامي صحيح – أو التقاطه أو اعتراضه.

٢- الدخول غير المشروع لتهديد شخص أو ابتزازه، لحمله على القيام بفعل أو الامتناع عنه ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً .

٣- الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه .

كما نص نظام مكافحة جرائم المعلوماتية في المادة (٤) على أنه : " يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية :

١- الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة .

٢- الوصول – دون مسوغ نظامي صحيح – إلى بيانات بنكية أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات أو معلومات، أو أموال، أو ما تتيحه من خدمات ".

كما أصدرت المملكة ضوابط تطبيق التعاملات الإلكترونية الحكومية، والتي نصت في المادة (٢١) منها على أنه " تقوم كل جهة حكومية بحماية معلوماتها وبياناتها وأنظمتها المعلوماتية وفق المعايير ذات العلاقة، وحسب معايير استرشادية يقدمها البرنامج لهذا الغرض " .

وقد أحسن المنظم في المملكة بإصدار هاذين النظامين حيث أنهما يشكلان خطوة هامة نحو حماية التعاملات الإلكترونية ومكافحة جرائم المعلوماتية ومكافحة الاحتيال المعلوماتي .

كما أصدرت مؤسسة النقد العربي السعودي (ساما) لائحة مكافحة الاحتيال في شركات التأمين وشركات المهن الحرة، والتي تتضمن الحد الأدنى من المعايير التي يجب أن تلتزم بها شركات التأمين وإعادة

التأمين لمنع – أو على الأقل – الحد من ممارسات الاحتيال، وترسيخ معايير عالية للكشف عن الاحتيال ومنعه. وتنطبق أحكام هذه اللائحة على شهادة التأمين وإعادة التأمين وشركات المهن الحرة بما فيها وسطاء التأمين، ووكلاء التأمين، وسطاء إعادة التأمين، ووكلاء إعادة التأمين. وطالبت "ساما" في اللائحة الشركات بان تحتفظ بسجلات ملائمة لإثبات التزامها بالمتطلبات المنصوص عليها في هذه اللائحة. وحثت اللائحة الشركات على اعتماد إستراتيجية واضحة لمكافحة الاحتيال بما ينسجم مع إجمال المخاطر. مشيرة إلى أن إستراتيجيات مكافحة الاحتيال يجب أن تشتمل على تحديد واضح لمستوى وقوع الشركات ضحية للاحتيال، ووضع قائمة مفصلة تشمل السياسات وإجراءات المراقبة الداخلية الهادفة إلى الكشف عن الاحتيال وقياسه والحد منه ومراقبته، وتخطيط شامل لإجراءات التجديد والمصادقة والتنفيذ لإستراتيجية مكافحة الاحتيال. وحثت اللائحة الشركات على توفير بيئة مناسب لتنفيذ إستراتيجية مكافحة الاحتيال فيها والإشراف عليها، على أن يكون مجلس إدارة الشركة مسؤولاً عن إدارة مخاطر الاحتيال. وحددت اللائحة مهام مجلس الإدارة في هذا الصدد بالموافقة على إستراتيجية مكافحة الاحتيال، وحشد الموارد الداخلية الضرورية للكشف عن مخاطر الاحتيال وقياسها والحد منها ومراقبتها بأنسب الطرق وتعزيز قيم وإستراتيجية مكافحة الاحتيال في الشركة على امتداد هيكلها التنظيمي وفي السوق. وحثت اللائحة المذكورة الشركات على إنشاء إدارات لمكافحة الاحتيال على أن تقدم هذه الإدارة تقاريرها إلى الإدارة العليا للشركة فيما يخص جميع أنواع الاحتيال، وأكدت اللائحة ضرورة قيام الشركات بصياغة السياسات والإجراءات الواضحة والهادفة إلى تطبيق إستراتيجية مكافحة الاحتيال، كإجراءات الكشف عن مخاطر الاحتيال وقياسها والحد منها ومراقبتها، إضافة إلى إجراءات رفع التقارير بشأن حالات الاحتيال وقديها في السجلات. كما أكدت اللائحة على ضرورة الحفاظ على الأدلة الناتجة عن عمليات الاحتيال واشترطت اللائحة على أن تقوم الشركات بإجراءات داخلية للإبلاغ عن نشاطات الاحتيال والنشاطات المشكوك بأمرها للجهات المختصة داخل وخارج الشركة، مع ضمان سرية المعلومة وعدم ذكر هوية المبلغ. وأكدت اللائحة على ضرورة تبادل المعلومات التي تملكها عن عمليات الاحتيال والمحتالين مع السلطات المختصة ومع المؤسسة.

كما أفردت اللائحة الباب الثالث للحديث عن معايير مكافحة الاحتيال، وذكرت اللائحة أنه يمكن أن يرتكب الاحتيال الداخلي أعضاء مجلس إدارة الشركة والإدارة والموظفين في أي عمل من أعمال الشركة وأنه يمكن الكشف عن الاحتيال في ممارسات العمل الإجمالية أو في السلوك والتصرف الشخصي. كما ذكرت اللائحة أنه يجب أن تضع الشركات

سياسات وإجراءات واضحة وجيدة التوثيق لقياس الاحتيال الداخلي، وأنه يجب التحقق من تطبيق هذه الإجراءات ومن فاعليتها بواسطة المراجعين الداخليين في الشركة سنوياً، وضرورة إعداد تقرير لمجلس إدارة الشركة حول حالات الاحتيال والتوجهات ذات الصلة، إضافة إلى فعالية الحد من الاحتيال، مؤكدة ضرورة تحديد الشركات السياسات والشفافية الشاملة عند التعامل مع حالات الاحتيال الداخلي.

وأكدت اللائحة على أهمية منع الشركات المحتالين من الوصول إلى النقود والتحويلات الإلكترونية بواسطة وضع تدابير أمنية مادية وإجرائية للحد من إمكانية الوصول إلى النقود والأصول ونظم المعلومات واستخدامها والحرص على التعامل مع النقود والتحويلات الإلكترونية بواسطة أكثر من شخص، كما أكدت اللائحة أيضاً على أهمية تطبيق الشركات قواعد صارمة خاصة تقنية المعلومات. وتشمل تلك القواعد فرض قيود على إمكان الوصول المادي إلى غرف خادم الحاسبات الآلية، ومراقبة حقوق الدخول إلى الشبكات، والحد من إمكان الوصول عن بُعد إلى الشبكات ومراقبتها، وضبط وتحديد كلمات سر دخول الشبكات (Passwords) بشكل منتظم، وتنفيذ تطبيقات أمن الشبكة وتدقيق الحسابات المنتظم. وأكدت اللائحة أنه يجب على الشركات تعزيز ثقافة النزاهة والمساءلة ضمن منظمتها، عبر تطوير دليل داخلي خاص بالسلوك الأخلاقي الذي من شأنه الترويج للتصرف المناسب والقيم السامية. وطالبت بأن تحتفظ الشركات لسجلات شاملة وكاملة حول الموظفين لمنصبهم لدى الشركة يمكن مراجعة هذه السجلات عند طلب مراقبي أو مفتشي المؤسسة. وفيما يتعلق بالرقابة، أكدت اللائحة على وجوب تطبيق الشركات سياسات رقابة صارمة على الإدارة والموظفين، خصوصاً على مستوى المناصب الرئيسية ضمن المنظمة وإخضاع النشاطات ذات الطبيعة الحساسة لمبدأ التطبيق المشدد. انظر لائحة مكافحة الاحتيال في شركات التامين وشركات المهن الحرة لعام ٢٠٠٨م (جريدة الحياة، ٢٠٠٨). أما بالنسبة للاحتيال الممارس من شركات المهن الحرة، ذكرت اللائحة أن شركات التأمين مطالبة بتدعيم أوامر التعاون مع شركات المهن الحرة لكشف الاحتيال الممارس في داخل شركات التامين أو من المؤمن لهم، ومحاربة هذا الاحتيال مع مراقبة شركات المهنة الحرة نفسها للتحقق مما إذا كانت تمارس الاحتيال أم لا.

الخاتمة

أدى التطور الكبير في تقنية المعلومات والاتصالات وازدياد الاعتماد على استخدام الحاسبات الآلية وشبكة الإنترنت في إجراء مختلف العمليات إلى زيادة كبيرة في استخدام هذه التقنية في ارتكاب جرائم الاحتيال المعلوماتي والمالي. وهو ما أثار تحديات كبيرة في مجال مكافحة تلك الجرائم والوصول إلى مرتكبيها،

فهذه الجرائم لا تترك آثاراً مادية في مسرح الجريمة كغيرها من الجرائم ذات الطبيعة المادية .

وتستحوذ جرائم الاحتيال المعلوماتي على النصيب الأكبر من الجرائم التي يتعرض لها عملاء البنوك وتعتبر من أكثر الوسائل الإجرامية تعقيداً وأسرعها تطوراً، بالنظر إلى اعتمادها على تقنيات الحاسب الآلي والإنترنت والأجهزة الإلكترونية المصرفية كأجهزة الصراف الآلي (Automated Tellar Machines)، ونقاط البيع (Sale Points) . ونظراً لأهمية جرائم الاحتيال المعلوماتي والزيادة الكبيرة في ارتكابها فقد تعرضنا في هذا البحث لموضوع جرائم الاحتيال المعلوماتي لما لهذا الموضوع من أهمية كبرى . وقد توصلنا في ختام هذا البحث إلى النتائج والتوصيات الآتية :

أولاً: النتائج

١- أدى الانتشار الكبير في استخدام الحاسبات الآلية وشبكة الإنترنت إلى ازدياد جرائم الاحتيال المعلوماتي والمالي .

٢- أن جرائم الاحتيال المعلوماتي هي من الجرائم التي تمس الاقتصاد الوطني والعالمي وتؤثر في الأفراد والمؤسسات والشركات التي تقع ضحية لها.

٣- تتميز جرائم الاحتيال المعلوماتي بطبيعة خاصة تميزها عن جرائم الاحتيال التقليدي لأنها تتطلب لارتكابها معرفة تامة بتقنية الحاسب الآلي والإنترنت .

٤- أفردت بعض التشريعات نصوصاً لتجريم الاحتيال المعلوماتي، سواء أكان هذا التجريم بنص عام أم كان بتناول بعض صور الاحتيال المعلوماتي دون البعض الآخر . كما قامت تشريعات أخرى بمحاولة تطبيق النصوص التقليدية على الصور المختلفة للاحتيال المعلوماتي.

٥- أن تطبيق النصوص التقليدية كنصوص جرائم السرقة والنصب وخيانة الأمانة والتزوير على جرائم الاحتيال المعلوماتي سواء التحويل الإلكتروني غير المشروع للأموال أو الاستعمال غير المشروع للبطاقات الائتمانية يعترضه العديد من العقبات التي حالت في كثير من الأحيان دون تطبيقها، ولعل من أكبر هذه العقبات مسألة الاحتيال على الآلة والتي تتعارض مع أغلب التشريعات التي تتطلب أن يمارس الاحتيال في مواجهة شخص ما، وكذلك مسألة وجود المحرر الذي تتطلبه النصوص الخاصة بجريمة التزوير والذي لا يتحقق في جريمة الاحتيال المعلوماتي.

٦- لا بد من تدخل المشرعين في دول العالم المختلفة بتجريم الاحتيال المعلوماتي بشكل

صريح وواضح وبنصوص قانونية صريحة وواضحة.

٧- الطبيعة العالمية لجريمة الاحتيال المعلوماتي يترتب عليها إمكانية ارتكاب الجريمة عن طريق وحدة طرفية في دولة ما بينما تتحقق الجريمة في دولة أخرى، الشيء الذي يثير مسألة تحديد القانون الواجب التطبيق بين قوانين وتشريعات الدول المختلفة والمحكمة المختصة بنظر النزاع .

٨- تثير جرائم الاحتيال المعلوماتي بعض المشاكل في مسألة جمع الأدلة الجنائية، ففي نطاق شبكة الإنترنت يصعب على المحقق في هذه الجرائم تطبيق إجراءات جمع الأدلة والإثبات التقليدية على المعلومات وهي لها طبيعة معنوية .

٩- هناك ضعف وعدم فاعلية في التعاون الدولي في مجال مكافحة جرائم الاحتيال المعلوماتي .

ثانياً – التوصيات :

١- ينبغي مساواة المال المعلوماتي بالمال المتعارف عليه في النصوص التقليدية مع الاعتراف بإمكانية اقتراف جريمة الاحتيال على المال المعلوماتي.

٢- ضرورة توقيع اتفاقيات ثنائية بين الدول تتعلق بتنظيم المسائل الخاصة بالجرائم المعلوماتية وعلى وجه الخصوص جرائم الاحتيال المعلوماتي .

٣- ضرورة إصدار القوانين الخاصة بمكافحة الجرائم المعلوماتية وعلى وجه الخصوص جرائم الاحتيال المعلوماتي على أن يتم تجريم الاحتيال المعلوماتي بنص عام يتسع ليشمل الصور المختلفة للاحتيال المعلوماتي.

٤- وجوب إعطاء الدليل المستمد من الحاسب الآلي حجية كاملة في الإثبات فيما يتعلق بجرائم الاحتيال المعلوماتي وكذلك ضمان أن الأدلة التي يتم جمعها في دولة تقبل لدى تنظيمات ومحاكم الدول الأخرى .

٥- وجوب تأهيل رجال الأمن والمحققين والقضاة في مجال الحاسب الآلي وكيفية التعامل مع هذه التقنية لتمكينهم من التحقيق والمحاكمة في الجرائم المرتكبة باستخدام الحاسب الآلي وبشكل خاص جرائم الاحتيال المعلوماتي .

٦- حث الدول على توحيد تشريعاتها المتعلقة بتسليم المجرمين وتبادل المساعدة القضائية في المسائل الجنائية فيما يتعلق بجرائم المعلوماتية وعلى وجه الخصوص جرائم الاحتيال المعلوماتي .

٧- ضرورة نشر الوعي بين مستخدمي شبكة الإنترنت بالقواعد الأمنية الواجب إتباعها

ومنها عدم استخدام البريد الإلكتروني في استقبال أو إرسال أي بيانات مالية قد تعرضها للسرقة أو الدخول إلى المواقع المشبوهة، وتوعيتهم بعدم نشر بياناتهم وصورهم وأرقام بطاقاتهم الائتمانية إلا في حالة الضرورة. وفي المواقع المعتمدة وغير المشبوهة، وعدم فتح الرسائل مجهولة المصدر أو المشبوهة.

٨- ضرورة توعية الجمهور بحالات الاحتيال المعلوماتي محلياً وإقليمياً ودولياً بنشر تلك الحالات في وسائل الإعلام المختلفة حتى لا يقع الناس ضحية لأعمال احتيالية معلوماتية مماثلة.

المراجع

أولاً: الكتب والأبحاث العربية

تمام، أحمد حسام طه. *الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية للحاسب الآلي): دراسة مقارنة*. القاهرة: دار النهضة العربية، ٢٠٠٠م.

حجازي، عبدالفتاح بيومي. *النظام القانوني لحماية التجارة الإلكترونية: نظام التجارة الإلكترونية وحمايتها مدنياً (الكتاب الأول)*. الإسكندرية: دار الفكر الجامعي، ٢٠٠٢م.

حسني، محمود نجيب. *شرح قانون العقوبات: القسم الخاص*. القاهرة: دار النهضة العربية، ١٩٩٣م.

رستم، هشام محمد فريد. *قانون العقوبات ومخاطر تقنية المعلومات*. أسيوط: مكتبة الآلات الحديثة، ٢٠٠٠م.

رضوان، رضا عبد الحكيم. "جرائم تزوير بطاقات الدفع الإلكتروني." *مجلة البحوث الأمنية*، م١٧، ع (٣٩)، ربيع الآخر، ١٤٢٩هـ/ إبريل (٢٠٠٨).

سرور، أحمد فتحي. *الوسيط في قانون العقوبات: القسم الخاص*. القاهرة: دار الطباعة الحديثة، ١٩٩١م.

الشوا، محمد سامي. *ثورة المعلومات وانعكاساتها على قانون العقوبات*. القاهرة: دار النهضة العربية، . ١٩٩٨م.

الشوابكة، محمد أمين. *جرائم الحاسوب والإنترنت: الجريمة المعلوماتية*. عمان: دار الثقافة للنشر والتوزيع، ٢٠٠٤م.

الصغير، جميل عبدالباقي. *الإنترنت والقانون الجنائي: الأحكام الموضوعية للجرائم المتعلقة بالإنترنت*. القاهرة: دار النهضة العربية، ٢٠٠١م.

الصغير، جميل عبدالباقي، *الحماية الجنائية والمدنية لبطاقات الإئتمان الممغنطة (دراسة تطبيقية في القضاء الفرنسي والمصري)*. القاهرة: دار النهضة العربية، ١٩٩٩م.

الصغير، جميل عبدالباقي. *القانون الجنائي والتكنولوجيا الحديثة: الجرائم الناشئة عن استخدام الحاسب الآلي (الكتاب الأول)*. القاهرة: دار النهضة العربية، ١٩٩٢م.

عبابنه، محمود أحمد. *جرائم الحاسوب وأبعادها الدولية*. عمان: دارالثقافة للنشروالتوزيع، ٢٠٠٥م.

عبدالله، عبدالكريم عبدالله. *جرائم المعلوماتية والإنترنت (الجرائم المعلوماتية)*. بيروت: منشورات الحلبي الحقوقية، ٢٠٠٧م.

العبيدي، أسامة بن غانم. "جرائم الحاسب الآلي والإنترنت: الصعوبات التي تعترض المكافحة." *دورية الإدارة العامة*، معهد الإدارة العامة، الرياض، م ٤٨، ع (١)، محرم (١٤٢٩هـ).

العريان، محمد علي. *الجرائم المعلوماتية*. الإسكندرية: دار الجامعة الجديد للنشر، ٢٠٠٤م.

عفيفي، عفيفي كامل. *جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة: دراسة مقارنة*. د.م: د.ن، د.ت.

فضل، سليمان أحمد. *المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)*. القاهرة: دار النهضة العربية، ٢٠٠٧م.

قايد، أسامة عبدالله. *الحماية الجنائية للحياة الخاصة وبنوك المعلومات: دراسة مقارنة*، القاهرة: دار النهضة العربية، ١٩٨٩م.

قشقوش، هدى حامد. *جرائم الحاسب الإلكتروني في التشريع المقارن*. القاهرة: دار النهضة العربية، ١٩٩٢م.

قورة، نائلة عادل. *جرائم الحاسب الآلي الاقتصادية: دراسة نظرية وتطبيقية*. بيروت: منشورات الحلبي الحقوقية، ٢٠٠٥م.

الكعبي، محمد عبيد. *الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت: دراسة مقارنة*. القاهرة: دار النهضة العربية، د.ت.

مصطفى، محمود محمود. *شرح قانون العقوبات: القسم الخاص*. القاهرة: مطبعة جامعة القاهرة، ١٩٨٤م.

المناعسة، أسامة أحمد، وآخرون. *جرائم الحاسب الآلي والإنترنت: دراسة تحليلية مقارنة*، عمان: دار وائل للنشر والتوزيع، ٢٠٠١م.

ثانياً: المراجع الأجنبية

Short, Greg, Combating software piracy : can felony Penalities for copyright in fringment custail the copying of computer software? Santa clara computer and high technology law journal, Vol. 10, 7-11(1994).

Mason, David R., Sentensing policy and Procedure as applied to cyber crimes: A call for reconsideration and Dialogue, Mississippi law journal Winter, 1-3 (2007).

Jordan, William, H, Cyber Attacks, information Theft, and the online shakedown: preparing for and responding to intrusions of computer systems, electronic banking law and commerce report, October, 1-4 (2001).

Simon, David, and Richard jones, intellectual property crimes, in the cyber world, Wisconsin lawyer, October 2-8 (2004).

Nimmer, Raymond T, chapter 12. Computer crime, part C. information and software theft crime, law of computer technology database, 1-6 April (2008).

Friedman, Mark S, and Kristin Bissinger, Infojacking: crimes on the information superhighway, S.J. proprietary Rts, 2,2 . (1997).

Heymann, Stephen, P, Legislating computer crime, 34 Harv. J. On Legis, 375, 379. (1997).

Katyal, Neal Kumar, Criminal Law in Cyberspace 14 .(2001).

Savage, Joseph F. Jr., and christina N. Smith, New wine in old Bottles; Searching for a Rational Approach to sentencing for new Economy Crimes, & BUS. Crime Bull. No.6, at 1 (2001).

ثالثاً: الصحف العربية

جريدة الاقتصادية، الثلاثاء، ١٦ محرم، ١٤٣٠هـ. العدد ٥٥٧٣، ص٦.

جريدة الرياض، الرياض الاقتصادي، السبت ٢٩ ذي الحجة، ١٤٢٩هـ، العدد ١٤٧٩٦، السنة الخامسة والأربعون، ص١١ .

جريدة الجزيرة، ملحق الاتصالات والعالم الرقمي، الأحد ٢٠ شوال، ١٤٢٩هـ، العدد ٢٦٥، ص ٣٠ .

جريدة الجزيرة، ملحق الاتصالات والعالم الرقمي، ٢٠٠٩/١/٢٥م، ص ٢١ .

جريدة الجزيرة، ملحق الاتصالات والعالم الرقمي، الأحد ١٤ محرم، ١٤٣٠هـ، العدد ٢٧٤، ص ٢٠ .

جريدة الشرق الأوسط، الثلاثاء، ٢٠٠٨/١١/٢٥م، العدد ١٠٩٥٥، ص ٨ .

جريدة الجزيرة، ملحق الاتصالات والعالم الرقمي، ٢٨ محرم، ١٤٣٠هـ، ص ٢٠ .

جريدة الجزيرة، ملحق الاتصالات والعالم الرقمي، الأحد ٢٧ شوال، ١٤٢٩هـ، ص ٢٠ .

جريدة الرياض، الرياض الاقتصادي، تقنية المعلومات، ٢٦ ذي الحجة ١٤٢٩هـ، العدد ١٤٧٩٤، السنة الخامسة والأربعون، ص١١ .

رابعاً: القوانين والأنظمة والضوابط

قانون العقوبات الفرنسي الجديد لعام ١٩٩٤م .

القانون الفدرالي الأمريكي رقم ١٠٣٠ .

قانون العقوبات لولاية كاليفورنيا .

نظام التعاملات الإلكترونية في المملكة، الصادر بقرار مجلس الوزراء رقم (٨٠) وتاريخ ١٤٢٨/٣/٧هـ .

نظام مكافحة جرائم المعلوماتية في المملكة، الصادر بقرار مجلس الوزراء رقم (٧٩) وتاريخ ١٤٢٨/٣/٧هـ .

ضوابط تطبيق التعاملات الإلكترونية الحكومية في المملكة، الصادر بقرار مجلس الوزراء رقم(٤٠)وتاريخ ١٤٢٧/٢/٢٧هـ .

خامساً: الأحكام القضائية

نقض، ٢٩ ديسمبر ١٩٥٩، س ١٠، رقم ٢٢٠، ص ٧٢ .

نقض، ٢ فبراير، عام ١٩٦٨ م . ص ١٩ ، رقم ٤٧ ، ص ٢٢٠ .

نقض، ٢٥ مايو، ١٩٧٥م، مجموعة أحكام محكمة النقض المصرية، ص ٧٦، رقم ١٠٦ . ص ٤٥٤ .

محكمة جنح باريس في حكم لها في ١٣ فبراير عام ١٩٩٠م.

طعن رقم ٧٥ لسنة ١٨ قضائية جلسة ١٩٨/٢/٢٥م، المحكمة الاتحادية الإماراتية.

نقض في ١٩٥٩/٥/١ س /٧ الموسوعة الذهبية، الجزء الثالث قاعدة ٥٧٢ ، ص ٢٨٢.

Cyber Fraud Crimes

Osama Ghanem Alobady
Associate Professor in Law,
Institute of Public Administration, Riyadh, Saudi Arabia

(Received 25/4/1430 H.; accepted for publication 12/1/1431 H.)

Abstract. Electronic or computer based crimes are on the rise. This is due to the substantial increase in the use of computers and the internet in performing wide range of transactions. This has led also to a substantial increase in cyber crimes and especially computer and internet fraud, where computers may be breached as the object of the crime or used as a tool to aid in the commission of the crime.
Cyber fraud crimes represent a substantial Part of crimes committed against bank customers. Cyber fraud is increasingly becoming one of the main challenges facing law enforcement around the world.
Such crimes are spreading
fast around the world due to the increased use of computers and the internet as well as automated teller machines and sale points.
This paper deals with cyber fraud and how it is dealt with by comparative laws and legislations.

- This paper defines cyber crimes in the first part.
- The second part deals with forms of cyber crimes and ways of commission of the crime.
- The third part discusses comparative laws regarding the combating of cyber crimes.
- The last part is the conclusion and findings and recommendations of the study.