

جامعة البحرين

قسم القانون العام



كلية الحقوق

جريمة الاحتيال باستخدام وسائل تقنية المعلومات في التشريع البحريني والمقارن

قدمت هذه الأطروحة كجزء من متطلبات الحصول على درجة الماجستير في القانون العام

إعداد

خالد علي سلمان عبد الله

الرقم الأكاديمي : ٢٠١٥٠٠٤٥

إشراف

د. عادل حامد بشير

أستاذ القانون الجنائي المشارك

جامعة البحرين

٢٠١٩

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿وَلَا تَأْكُلُوا أَمْوَالَكُم بَيْنَكُم بِالْبَاطِلِ وَتُدْءُوا بِهَا إِلَى
الْحُكَّامِ لِتَأْكُلُوا فَرِيقًا مِّنْ أَمْوَالِ النَّاسِ بِالْإِثْمِ وَأَنتُمْ
تَعْلَمُونَ﴾

[سورة البقرة الآية: ١٨٨]



صفحة الاعتماد من قبل لجنة التحكيم

جامعة البحرين

كلية الحقوق

قسم القانون العام

برنامج الماجستير - القسم العام

ناقش الطالب الرقم الجامعي
..... الأطروحة التي استكمل بها متطلبات الحصول على درجة الماجستير
في القانون - القسم العام،
والمعنونة.....
وذلك يوم

وتوصي اللجنة بمنحه درجة الماجستير في القانون العام بتقدير.....

لجنة المناقشة:

التوقيع

الاسم

_____	مشرفاً	_____
_____	ممتحناً خارجياً	_____
_____	ممتحناً داخلياً	_____

ختم القسم الأكاديمي المعني

ملخص الدراسة

تعد جريمة الاحتيال المعلوماتي صورة من صور الجرائم الواقعة باستخدام تقنية المعلومات، وتتمثل خطورة هذه الجريمة في الآثار التي تنتجها على الأنشطة الاقتصادية والاقتصاد القومي ككل، فهي تقع على أنظمة التحويل الإلكتروني للأموال والودائع المصرفية أو ما يسمى بالأموال الإلكترونية أو الافتراضية، نظراً لضخامة حجم ما يتم تداوله عبر هذه الأنظمة من أموال، واختزلها- أي تلك الأنظمة، كذلك المسافات بما يتيح تنفيذ الاحتيال عبر الحدود الإقليمية للعديد من الدول، واختزلها أيضاً الزمن اللازم لإتمام التعاملات والتحويلات المالية، وكذا الزمن لسلب الأموال بالاحتيال والغش إلى ثوان معدودة.

ويتم التلاعب - وفق الدلالة التقنية الواسعة - بمعطيات وسيلة من وسائل تقنية المعلومات المخزنة أو نظام المعالجة الآلية، وتتعدد الأساليب التقنية في التلاعب في معطيات وسيلة من وسائل تقنية المعلومات بقصد الاحتيال أهمها التلاعب في البيانات المدخلة، والتلاعب في البرامج والتلاعب في معطيات نظم تقنية المعلومات عن بعد، ويتم ذلك بعدة طرق كإدخال معلومات مصطنعة وإتلاف معلومات موجودة بالفعل في الحاسب الآلي ومحوها، أما فيما يخص التعدي على برامج النظام المعلوماتي فيتم عن طريق تعديل نظم هذه البرامج أو تعديل نظم التشغيل، أو عن طريق اصطناع برامج معينة لاستخدامها في عملية احتيال معلوماتي.

إن الهدف الرئيسي من جريمة الاحتيال يتمثل في الاستيلاء على مال منقول مملوك للغير بنية التملك عن طريق التلاعب بالبيانات والمعلومات للحصول على أموال وأصول مملوكة للغير، ومن بين البيانات الأكثر عرضةً للتلاعب تلك المتعلقة بالمستحقات المالية والإيداعات المصرفية وبطاقات الائتمان وحسابات ونتائج الميزانية. وتمتاز جريمة الاحتيال المعلوماتي بأن الأدلة التي قد يتركها الجاني تقع في بيئة الكترونية، إذ أنها تقوم على التلاعب في البيانات والبرامج، ويمتاز المجرم المعلوماتي بقدرته الهائلة على إخفاء جريمته والتلاعب بالأدلة، لذلك يجب على السلطات القضائية أن تتعامل مع هذه الجرائم بما يتناسب معها من أدلة الكترونية.

لذلك لجأت أغلب أنظمة دول المقارنة كالمرشع البحريني والإماراتي والسعودي وغيرها من الدول إلى سن قوانين تجرم هذه الجريمة وتوقع على مرتكبيها الجزاء بما يتناسب مع طبيعة هذه الجرائم.

ومن هنا أوصت الدراسة ضرورة أن تتضمن قوانين جرائم تقنية المعلومات على مواد يتم من خلالها إيضاح إجراءات التحقيق كالمعاينة والتفتيش والضبط، وذلك لإزالة اللبس في تفسير إجراءات التحقيق التي جاءت في قوانين الإجراءات الجنائية، وذلك للخصوصية التي تمتاز بها الجريمة المعلوماتية بشكل عام وجريمة الاحتيال المعلوماتي على وجه الخصوص. مع إشراك القضاة وأعضاء النيابة العامة وأعضاء الضبط القضائي بدورات متخصصة بالنظر في قضايا المعلوماتية وذلك لتأهيلهم فنياً وتقنياً وتعزيز التعاون المشترك في مجال القضاء بهذا الخصوص.

الإهداء

إلى من شاركوني ضحك الحياة
وهمومها، إلى من أرى نور
الحياة فيهم، إخواني وأولادي

شكر وتقدير

الشكر لله عز وجل الذي أنار لي الدرب، وفتح لي أبواب العلم والمعرفة، وأمدني بالصبر والإرادة، ووفقني لإكمال هذه الدراسة، فله الحمد حتى يبلغ الحمد منتهاه.

وأنتقدم بجزيل الشكر والعرفان إلى من شرفني بقبوله الإشراف على هذه الدراسة، ومن كان له الفضل بعد الله عز وجل في استكمال هذه الدراسة بصورتها الحالية، الأستاذ الدكتور عادل حامد بشير، وذلك على ما بذله من جهد، وتوجيه سليم، وإشراف مخلص، فله مني أصدق الشكر وأوفاه.

كما أتوجه بالشكر لأعضاء هيئة التدريس بكلية الحقوق بجامعة البحرين، على ما قدموه لي من جهد ومعرفة، ومساعدة علمية خلال فترة دراستي بكلية الحقوق، فلهم خالص الشكر والتقدير.

والشكر كذلك لكل من وقف معي، ومد لي يد العون والمساعدة لاستكمال هذه الدراسة، وخروجها بأفضل حال، فلهم مني جزيل الشكر والتقدير.

وفي الختام أسأل الله العظيم أن يجعل ما قدمت من جهد خالصاً لوجهه الكريم، وأن ينفع به الباحثين والمهتمين بهذا الشأن.

الفهرس

الرقم	الموضوع
أ	اعتماد لجنة المناقشة
ب	ملخص الدراسة
ج	الإهداء
د	الشكر والتقدير
١	الفهرس
٤	مقدمة
٥	مشكلة الدراسة
6	تساؤلات الدراسة
٦	أهداف الدراسة
٦	أهمية الدراسة
٨	منهج الدراسة
٨	الدراسات السابقة
14	مبحث تمهيدي: مفهوم وسائل تقنية المعلومات
15	المطلب الأول: تعريف وسائل تقنية المعلومات
21	المطلب الثاني: انواع وسائل تقنية المعلومات.
34	المطلب الثالث: الطبيعة القانونية لجرائم تقنية المعلومات.
الفصل الأول	
34	ماهية جريمة الاحتيال باستخدام وسائل تقنية المعلومات
44	المبحث الأول: مفهوم جريمة الاحتيال باستخدام وسائل تقنية المعلومات.
45	المطلب الأول: نشأة جريمة الاحتيال باستخدام وسائل تقنية المعلومات وتطورها.
49	المطلب الثاني: تعريف جريمة الاحتيال باستخدام وسائل تقنية المعلومات وخصائصها.

٥٩	المطلب الثالث: الآثار المترتبة على استخدام وسائل تقنية المعلومات في جريمة الاحتيال
٦٤	المبحث الثاني: ذاتية جريمة الاحتيال باستخدام وسائل تقنية المعلومات وصورها.
٦٥	المطلب الأول: ذاتية جريمة الاحتيال المعلوماتي.
٦٨	المطلب الثاني: الصور العامة للاحتيال المعلوماتي.
٧٧	المطلب الثالث: الصور الخاصة للاحتيال عن طريق بطاقات الائتمان.
٨٦	المبحث الثالث: مدى انسجام جريمة الاحتيال باستخدام وسائل تقنية المعلومات مع مفهومها التقليدي
٨٧	المطلب الأول: الركن الشرعي لجريمة الاحتيال المعلوماتي.
٩١	المطلب الثاني: الركن المادي لجريمة الاحتيال المعلوماتي.
١٠٠	المطلب الثالث: الركن المعنوي لجريمة الاحتيال المعلوماتي.
١٠٦	الفصل الثاني موضوع جرائم الاحتيال باستخدام وسائل تقنية المعلومات.
١٠٧	المبحث الأول: وسائل الاحتيال باستخدام تقنية المعلومات.
١٠٨	المطلب الأول: التلاعب في مدخلات النظام المعلوماتي.
١١٥	المطلب الثاني: التلاعب في البرامج.
١٢٠	المطلب الثالث: إتلاف البيانات.
١٢٧	المبحث الثاني: الاحتيال على أنظمة التحويل الإلكتروني للأموال.
١٢٨	المطلب الأول: الإطار النظري لنظم التحويل الإلكتروني للأموال.
١٣٥	المطلب الثاني: مزايا وعيوب نظم التحويل الإلكتروني للأموال.
١٣٩	المطلب الثالث: طرق التلاعب في نظم التحويل الإلكتروني للأموال.
١٤٢	المبحث الثالث: محل جريمة الاحتيال باستخدام وسائل تقنية المعلومات.
١٤٣	المطلب الأول: شروط موضوع جريمة الاحتيال المعلوماتي.
١٤٩	المطلب الثاني: موضوع تسليم المال في جريمة الاحتيال المعلوماتي.
١٥٦	المطلب الثالث: الضرر في جريمة الاحتيال المعلوماتي.
١٦١	الفصل الثالث الطبيعة الإجرائية لإثبات جريمة الاحتيال باستخدام وسائل تقنية المعلومات

١٦٢	المبحث الأول: الإجراءات القانونية لإثبات جريمة الاحتيال باستخدام وسائل تقنية المعلومات
١٦٣	المطلب الأول: البلاغ والشكوى في جريمة الاحتيال المعلوماتي.
١٦٨	المطلب الثاني: معاناة جريمة الاحتيال المعلوماتي.
١٧٤	المطلب الثالث: إجراءات التفتيش والضبط في جريمة الاحتيال المعلوماتي.
١٩٢	المبحث الثاني: الأدلة الجنائية في إثبات جريمة الاحتيال باستخدام وسائل تقنية المعلومات.
١٩٣	المطلب الأول: دور الأدلة التقليدية في إثبات جريمة الاحتيال المعلوماتي.
١٩٧	المطلب الثاني: الدليل الرقمي ودوره في اثبات جريمة الاحتيال المعلوماتي.
٢٠١	المطلب الثالث: مدى قبول الأدلة الرقمية كأدلة إثبات جريمة الاحتيال المعلوماتي.
٢٠٩	المبحث الثالث: الجهود الدولية والوطنية لمواجهة جريمة الاحتيال باستخدام وسائل تقنية المعلومات.
٢١٠	المطلب الأول: مكافحة جريمة الاحتيال المعلوماتي على المستوى الدولي.
٢١٨	المطلب الثاني: مكافحة جريمة الاحتيال المعلوماتي على المستوى الوطني لدول المقارنة.
٢٢٤	المطلب الثالث: صعوبات مكافحة جريمة الاحتيال المعلوماتي على المستوى الدولي والوطني.
٢٢٩	خاتمة
٢٣٤	قائمة المراجع

المقدمة

تمثل التقنية الحديثة مظهراً من المظاهر المتقدمة في عالمنا المعاصر حتى غدت من مستلزمات الحياة الأساسية، فهي تؤدي دوراً كبيراً في التواصل بين الأفراد والمؤسسات والدول، وشأنها شأن غيرها من المصطلحات القانونية فقد تناول الفقه المقارن تعريفات مختلفة لوسائل تقنية المعلومات.

وقد ساعد هذا التطور الملحوظ في وسائل تقنية المعلومات على إفراز جرائم جديدة عكست مدى التطور الحاصل على أرض الواقع واستخدمت أدوات جديدة وسمات خاصة حتى أطلق عليها مصطلح "جرائم تقنية المعلومات" تماشياً مع المصطلح السائد الذي هو "عصر تقنية المعلومات".

وتعد جريمة الاحتيال المعلوماتي صورة من صور الجرائم الواقعة باستخدام تقنية المعلومات، فهي حديثة بأسلوب ارتكابها كما أن نتائجها وأهدافها أيضاً لا تخلو من الحداثة، فاستخدام التقنية الحديثة أفسح المجال أمام مستخدمي هذه التقنية بالطرق السلبية أن يقوموا بعمليات الاحتيال باستخدام وسائل تقنية المعلومات.

وتتسم جريمة الاحتيال باستخدام وسائل تقنية المعلومات بخصائص معينة تكتسبها من خلال ما تنسم به الوسيلة نفسها فهي ترتبط ارتباط وثيق بتلك الخصائص التي تمتاز بها الجرائم المعلوماتية بشكل عام وجريمة الاحتيال على وجه الخصوص، فتمتاز جريمة الاحتيال المعلوماتي بخصائص تؤكد استقلالها عن الجرائم الأخرى.

وتشير الإحصائيات إلى أن معدلات جرائم الاحتيال المعلوماتي في ارتفاع مستمر وخاصة في دول مجلس التعاون الخليجي، ويلاحظ أن أنماط الجرائم الالكترونية في دول مجلس التعاون الخليجي تنصب غالباً في الجرائم المالية التي تستهدف الشركات والمؤسسات الاقتصادية والمالية، ومن هنا تتأتى الخطورة الفعلية لجرائم الاحتيال المعلوماتي.

تتعدد صور جريمة الاحتيال المعلوماتي بتعدد وسائل تقنية المعلومات الحديثة، ففي الوقت التي تتطور فيه هذه الوسائل لمواكبة التكنولوجيا الحديثة يتطور معها مهارات رواد ومستخدمي هذه الوسائل أو ما يطلق عليهم محترفي البرمجيات أو الهاكرز وهذه السمة التي يمتاز بها مستخدمي التقنية المعلوماتية أتاحت لهم استغلال وسائل تقنية المعلومات عن طريق التلاعب بالبيانات للحصول على الأموال أو أي شيء آخر ذو قيمة مالية.

فبدأت أغلب البلدان في تنظيم تشريعاتها لمواجهة هذا النمط الجديد من الجرائم، والذي ظهر مصاحباً لاستخدام الحاسب الآلي، وقد ذهب في هذا الاتجاه كل من أنظمة دول المقارنة " المشرع البحريني والاماراتي والسعودي"، بعدما تنامي لديها الشعور بضرورة إقرار قوانين خاصة تنظم من خلالها هذا النوع من الجرائم.

والجدير بالذكر أن هناك اختلاف في استخدام المصطلحات في التشريعات المقارنة¹ بخصوص جريمة الاحتيال المعلوماتي، فبعض التشريعات تستخدم جريمة الاحتيال الالكتروني وتشريعات أخرى تستخدم الاحتيال المعلوماتي وهناك من التشريعات من تستخدم الاحتيال عبر الإنترنت أو باستخدام وسائل تقنية المعلومات، وبغض النظر عن هذا الاختلاف إلا أنها تدور كلها في فلك التقنية الحديثة كأداة من خلالها ترتكب هذه الجريمة، والتي يكون محلها البيانات والمعلومات أو النقود الالكترونية.

مشكلة الدراسة

بالرغم من أن جريمة الاحتيال باستخدام وسائل تقنية المعلومات جرمت في معظم الدول عبر التشريعات، إلا أن الإشكالية المطروحة هنا تكمن في محل جريمة الاحتيال المعلوماتي، حيث تعد تلك الجريمة من الجرائم التي يصعب كشفها نظراً للحيل الحديثة التي يستخدمها مرتكبوها، لا سيما وأن تلك الجريمة تعد من الجرائم التي انتشرت مؤخراً في دول العالم - وعلى وجه الخصوص الدول محل المقارنة -، وأن القانون الجنائي بشكل عام بنصوصه الحالية لا تكفي لإمكانية مواجهة تلك الصور المستحدثة من الجرائم، كما أن معظم الإجراءات الواردة في قانون الإجراءات الجنائية قد لا تتناسب مع الطبيعة الإجرائية وخصوصية جريمة الاحتيال المعلوماتي، ولا تفي بالغرض المطلوب وهو كشف ملبسات تلك الجريمة نظراً لأنها شرعت لكافة الجرائم العامة، الأمر الذي يؤكد على وجود إشكالية تعيق كشف تلك الجريمة.

¹ استعانت هذه الدراسة في تحليل موضوعها بكافة التشريعات التي هي محل المقارنة - التشريع البحريني، التشريع الإماراتي، التشريع السعودي، مع الأخذ بعين الاعتبار التشريعات الأجنبية الأخرى في محاولة لفهم الظاهرة موضوع البحث.

تساؤلات الدراسة

وتتمثل مشكلة الدراسة في الإجابة على التساؤلات التالية:

١. ما هي جريمة الاحتيال المعلوماتي في التشريعات المقارنة محل الدراسة؟ وما عناصرها؟
٢. هل هناك آثاراً قانونية توقعها جريمة الاحتيال المعلوماتي على الأفراد والدول؟
٣. كيف واجهت التشريعات المقارنة محل الدراسة الاحتيال المعلوماتي في تشريعاتها؟
٤. ما هي الأحكام الموضوعية والإجرائية لجريمة الاحتيال المعلوماتي؟
٥. ما الصعوبات والمعوقات التي تواجهها الدول في تصديها لجريمة الاحتيال المعلوماتي؟

أهداف الدراسة

١. معرفة أهم الأسس القانونية المطبقة على جريمة الاحتيال المعلوماتي في التشريع البحريني والتشريعات المقارنة.
٢. إعطاء نظرية تحليلية متكاملة عن أهم الحلول التشريعية لمواجهة جريمة الاحتيال المعلوماتي ومدى قدرة الدول على الضبط القانوني لهذه الجريمة.
٣. تبين أهم المعوقات التي تعيق عمل الأجهزة المختصة في متابعة جريمة الاحتيال المعلوماتي.
٤. معرفة ماهية الآثار القانونية التي تحدثها جريمة الاحتيال المعلوماتي.

أهمية الدراسة

في ظل التطور الهائل لاستخدامات الكمبيوتر والشبكة العنكبوتية وما توفره من فضاء معلوماتي مهول وما يكتنفه من الأهمية في حياة الناس؛ أدى ذلك إلى كثرة الجرائم الخاصة بمجال الاحتيال المعلوماتي عبر الإنترنت، وما نجم عنه من آثار سلبية تمس حقوق الأفراد والدول مما استدعى ضرورة المعالجة القانونية والفقهية لهذه الجرائم.

كما تتمثل أهمية الدراسة في محاولة لتبيان الحجج والدلائل للوصول لمبدأ صلاحية القوانين النافذة بشكل عام لدول المقارنة، والقوانين البحرينية على وجه الخصوص، وقدرتها على مواكبة ومواجهة مستجدات التطورات الالكترونية، وما تخلفه من آثار سلبية على النظام القانوني للدول والأفراد.

ونظراً لحدائثة موضوع الاحتيال المعلوماتي، لا بد من الكشف عن الثغرات التي تعتري هذه الظاهرة من خلال التحليل والمقارنة لموضوع الدراسة، في ظل الصعوبات الموضوعية المرتبطة بقلّة البحوث والدراسات المتخصصة في موضوع الاحتيال المعلوماتي من الناحية القانونية بصفة عامة.

منهج الدراسة

لدراسة جريمة الاحتيال المعلوماتي وعناصرها والآثار التي تترتب عنها سيتم استخدام المنهج التحليلي والمقارن للتعرف على موقف التشريع البحريني ومقارنته بالتشريعات الأخرى، من خلال الاستئناس ببعض الأحكام القضائية والدراسات العلمية والآراء الفقهية، لفهم الكيفية التي تم تناول فيها بعض الفقه القانوني والنظام القانوني البحريني لجريمة الاحتيال المعلوماتي وما تنتجه من آثار قانونية تتأثر فيها عدة أطراف.

الدراسات السابقة

هنالك العديد من الدراسات لهذا الموضوع، ولكن في مجملها لم تتناول جريمة الاحتيال المعلوماتي بصورة موسعة بل من باب عرض جرائم المعلوماتية وعلى سبيل المثال منها:

١- دراسة للدكتور علي حسن الطوالة، "الجرائم الإلكترونية"، جامعة العلوم التطبيقية، جامعة البحرين، سلسلة الكتب القانونية ١٢، ٢٠٠٩.

تناولت الدراسة أهمية التطور التكنولوجي الكبير الذي أدى إلى ازدياد أهمية الحاسوب في شتى مجالات الحياة المعاصرة، هذا الأمر أدى إلى نشوء جرائم ناتجة عن استخدام الحاسب الآلي، هذه الجرائم أما ان تقع على الحاسوب ذاته وأما تقع بواسطة الحاسوب بحيث يعد الحاسوب أداة في يد الجاني يستخدمه لتحقيق أغراضه الإجرامية.

وتتبع أهمية هذه الدراسة من أهمية الموضوع نفسه كونه يركز على المشكلات القانونية التي تثيرها استخدام المعلوماتية في المجالات الحياتية المختلفة، فقد تثير الجرائم الإلكترونية مسألة تحديد الاختصاص القضائي والقانون الواجب التطبيق على الجرائم المرتكبة عبرها، فقد تثير مسألة التنازع الايجابي أو السلبي في الاختصاص في ما لو وقعت الجريمة ضمن اختصاص محكمتين قضائيتين أو أكثر داخل الدولة أو خارجها.

٢- دراسة للدكتور علي حسن الطوالة، "التفتيش الجنائي على نظم الحاسوب والإنترنت"، جامعة العلوم التطبيقية، جامعة البحرين، سلسلة الكتب القانونية ١٩، ٢٠١٠.

تناولت هذه الدراسة بالبحث والتحليل مسألة التفتيش الجنائي في نظم الحاسوب والإنترنت، التي تثيرها تقنية المعاومات على المستوى الإجرائي، تمهيدا لمواجهتها بأساليب تتفق

مع الطبيعة الخاصة بهذه التقنية، وتكفل في الوقت نفسه توازناً بين المتطلبات الفعلية لأنشطة الأجهزة القضائية في الخصوصية، مع استعانة الباحث بكافة الجهود المعرفية السابقة من خبرات الفقه المقارن الذي أعطى اهتماماً بهذه المشكلات، ومنها التفتيش على نظم الحاسوب والإنترنت.

يسعى الباحث في هذه الدراسة إلى تطبيق النصوص التقليدية في قانون الإجراءات الجنائية، على موضوع التفتيش والضبط على نظم الحاسوب والإنترنت، ومراقبة المشروعية، خصوصاً وأن هذا الموضوع يغمره الصعوبة في جانبه التقني والفني.

خلصت الدراسة على أن التشريعات العربية لم تعرف التفتيش واكتفت بالنص على أنه إجراء من إجراءات التحقيق، كما أنه تم تحديد الطبيعة القانونية للتفتيش الواقع على نظم الحاسوب والإنترنت، بأنه إجراء من إجراءات التحقيق الابتدائي وليس من إجراءات الاستدلال.

٣- دراسة لمحمد أمين الشوابكة بعنوان، "جرائم الحاسوب والإنترنت" الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الرابعة، ٢٠١١م.

تناول الباحث في هذه الدراسة إلى أهم جرائم الاعتداء على الأشخاص عبر الإنترنت، فتناول جريمة الذم والقدح والتحقير عبر الإنترنت فتطرق إلى مسألة التجريم والعقاب لهذه الجريمة باستخدام الإنترنت كما تطرق إلى ذاتية هذه الجريمة، واستعرض الباحث أيضاً جريمة الاعتداء على حرمة الحياة الخاصة وجرائم الاستغلال الجنسي للأطفال عبر الإنترنت، وفي الجزء الأخير من الدراسة تناول جريمة الاعتداء على الأموال عبر الإنترنت وناقش من خلاله صورة التحويل الإلكتروني كإحدى صور الاحتيال، وتطرق أيضاً لجريمة اتلاف نظم المعلوماتية عبر الإنترنت.

وما يؤخذ على هذه الدراسة أنها اختزلت جريمة الاحتيال بصورة واحدة وهي التحويل الإلكتروني غير المشروع للأموال، ولم يتطرق الباحث للصور الأخرى للاحتيال المعلوماتي.

٤- دراسة لمحمد طارق الخن بعنوان "جريمة الاحتيال عبر الإنترنت"، منشورات الحلبي الحقوقية، الطبعة الأولى، ٢٠١١م.

تناول الباحث في هذه الدراسة جريمة الاحتيال عبر الإنترنت، من خلال دراسة الأحكام الموضوعية لجريمة الاحتيال، فقام بتعريف الإنترنت وتطرق إلى مفهوم الإنترنت والجرائم الخاصة به بشكل عام وجريمة الاحتيال بشكل خاص، كما قام بعرض الأساليب التي يتم بها الاحتيال عبر الإنترنت وعالج من خلال مقارنته للاتجاهات التشريعية والأجنبية إشكاليات متعددة

منها موضوع الاحتيال ومحل الاحتيال ومدى انسجام الاحتيال عبر الإنترنت مع مفهومه التقليدي.

وفي محاولة منه أيضاً تطرق الباحث إلى دراسة القواعد الإجرائية لجريمة الاحتيال والتي حاول من خلالها قياس مدى فعالية أدلة الإثبات التقليدية في إثبات جريمة الاحتيال عبر الإنترنت كما وقام بدراسة تحليلية للدليل الرقمي وخصائصه وحجتيه في إثبات جريمة الاحتيال عبر الإنترنت.

وخلص الباحث في نهاية الدراسة إلى أن إجراءات إثبات جريمة الاحتيال التقليدية تنطبق في حالة جريمة الاحتيال عبر الإنترنت، وهذا ما يعتبر ثغرة في هذه الدراسة لكون جريمة الاحتيال عبر الإنترنت تمتاز بذاتية وخصوصية تختلف تماماً عن مفهومها التقليدي، مما يتطلب إجراءات خاصة بهذه الجريمة، ففاعلية الإجراءات التقليدية لا كأدلة إثبات قد لا تأتي بثمارها في جريمة الاحتيال عبر الإنترنت.

٥- دراسة لفهد العازمي بعنوان "الإجراءات الجنائية المعلوماتية"، رسالة لنيل درجة الدكتوراه في الحقوق، عين شمس، القاهرة، ٢٠١٢م.

تناول الباحث في هذه الدراسة الجريمة المعلوماتية وأنواعها ودور الحاسب الآلي فيها، واستعرض من خلال الدراسة محل الجريمة المعلوماتية والتقدير القانوني للأموال المعنوية، كما تطرق الباحث إلى الدور التي تلعبه التقنية الحديثة في الإجراءات الجنائية لمواجهة الجرائم المعلوماتية وما هي أهم صعوبات مواجهة هذه الجرائم، بالإضافة إلى ذلك فقد تناول الباحث المراحل المتعددة للتحقيق في هذه الجرائم منها مرحلة الاستدلال ومرحلة التحقيق الابتدائي ودور الضبط القضائي في هذه الإجراءات، كما استعرض أهم إجراءات التحقيق منها المعاينة والتفتيش والضبط وناقش الباحث من خلال دراسته دور الأدلة الرقمية في إثبات الجريمة المعلوماتية ومدى حجيتها.

وفي الجزء الثاني من الدراسة تناول الباحث دور الملاحقة الجنائية في مجال التعاون الدولي لمواجهة جرائم المعلوماتية الرقمية، ومن النتائج التي توصل إليها الباحث أن الجرائم المعلوماتية من الجرائم العابرة للحدود والتي لا يمكن مواجهتها بجهود محلية، بل يجب أن تتكاتف الجهود على الصعيد الوطني والإقليمي والدولي لمواجهة هذه الجرائم وذلك بتكثيف الاتفاقيات الدولية التي تقدم المساعدة في هذا المجال، بالإضافة إلى تدريب جهاز مختص يكون

قادر على التعامل مع هذه الجرائم، وتناولت الدراسة الجريمة المعلوماتية بشكل عام ولم تدرس جريمة الاحتيال المعلوماتي على وجه الخصوص.

٦- دراسة للباحث عبد الله الكيتوب بعنوان "الأحكام الإجرائية لجريمة الاحتيال المعلوماتي"، دار النهضة العربية، القاهرة، ٢٠١٣م.

جاء في هذه الدراسة التعريف بجرائم الاحتيال المعلوماتي، وتم التعريف بالاحتيال المعلوماتي والطبيعة القانونية له، كما تطرقت الدراسة إلى مراحل جمع الاستدلالات فقام الباحث بدراسة الضبط الإداري والقضائي كمرحلة استدلال لجريمة الاحتيال المعلوماتي، كما استعرض أيضاً دور مأمور الضبط القضائي في مرحلة جمع الاستدلال.

كما تناولت الدراسة مرحلة التحقيق الابتدائي لجريمة الاحتيال المعلوماتي والجهات المختصة بالتحقيق بهذه الجريمة، وإجراءات التحقيق الخاصة بجريمة الاحتيال المعلوماتي، كالمعينة والتفتيش والضبط، وفي الجزء الأخير من الدراسة تناول الباحث قواعد التعاون الدولي لمكافحة جريمة الاحتيال المعلوماتي، واستعرض الباحث كيفية تطوير المواجهة الأمنية للجرائم المعلوماتية.

٧- دراسة لسالم الجبوري بعنوان "جريمة الاحتيال الإلكتروني" دراسة مقارنة"، منشورات زين الحقوقية، بيروت، لبنان، الطبعة الأولى، ٢٠١٨م.

تناولت الدراسة ماهية الجريمة الإلكترونية بدراسة الاتجاهات المختلفة التي تناولت تعريفها والتي حدد من خلالها مفهوم جريمة الاحتيال الإلكتروني وقارن بينها وبين مفهومها التقليدي واستعرض الباحث ذاتية جريمة الاحتيال والآثار المترتبة عليها، والمراحل التاريخية التي مرت بها الجريمة الإلكترونية، كما تناول وسائل الاحتيال الإلكتروني والجريمة المعلوماتية من خلال استعمال الطرق الاحتيالية، وتسلم مال الغير دون وجه حق بالإضافة لدراسة الاحتيال المعلوماتي في مجال أنظمة التمويل الإلكتروني، وتطرق الباحث من خلال هذه الدراسة إلى أنواع الجرائم الإلكترونية والمعالجة الجنائية لها وأهم المشكلات القانونية والعلمية المترتبة عن استخدام الحاسوب في الاتصال مع الإنترنت.

وتوصل الباحث من خلال هذه الدراسة إلى أن هناك صعوبة علمية في تطبيق الأفكار التقليدية للقانون الجنائي كمبدأ تطبيق القانون الوطني من حيث المكان واختصاص القضاء

الوطني، وأن استخدام الحاسب الآلي يثير مشاكل تخص جرائم الاعتداء على الأشخاص والأموال وجرائم الاعتداء على الملكية الأدبية والفكرية، وما يؤخذ على هذه الدراسة أنها خصصت جزء كبير من الدراسة على جرائم الإنترنت بكافة أنواعها ولم تعط الأولوية لجريمة الاحتيال الإلكتروني كما جاء في عنوان الدراسة.

هيكلية البحث:

قد تناول الباحث هذا الموضوع من خلال ثلاثة فصول مسبقة بمبحث تمهيدي، حيث تضمن في هذا المبحث مفهوم وسائل تقنية المعلومات، ومن ثم تطرق الباحث في الفصل الأول إلى ماهية جريمة الاحتيال باستخدام وسائل تقنية المعلومات، أما الفصل الثاني فقد تطرق الباحث موضوع جرائم الاحتيال باستخدام وسائل تقنية المعلومات، وأخيراً فقد بين الباحث الفصل الثالث الطبيعة الإجرائية لإثبات جريمة الاحتيال باستخدام وسائل تقنية المعلومات.

مبحث تمهيدي
مفهوم وسائل تقنية المعلومات

مبحث تمهيدي

مفهوم وسائل تقنية المعلومات

يشهد عالمنا الحاضر تطوراً متسارعاً في تقنية المعلومات، وأصبحت هذه التقنية ضرورة حتمية وعنصراً أساسياً من مستلزمات الحياة سواء أكان ذلك على المستوى الخاص أو العام، وذلك لما لها من دور كبير ومهم في التواصل على المستوى الداخلي والخارجي، فغدت مظهراً من مظاهر التطور الذي لامس كافة نواحي الحياة، فأخذت الأجهزة التقنية تشمل كل من الحاسب الآلي والهاتف النقال وما يقترن بها من وسائل كالشبكات المعلوماتية وغيرها من الأجهزة الحديثة التي تشهد تطوراً سريعاً.

ولقد ساهمت وسائل تقنية المعلومات بدور إيجابي وفعال نظراً لما أحدثته من سرعة في التواصل والاتصال، إلا أنها لا تخلو من السلبيات والتي تجسدت في ظهور نوع جديد من الجرائم ترتكب بوسائل تقنية المعلومات.

ونظراً لما تمثله التقنية المتمثلة في الوسائل الحديثة وتقنية المعلوماتية من أهمية؛ سوف يتطرق الباحث لمفهوم وسائل تقنية المعلومات والطبيعة كمدخل تمهيدي للتعريف بجريمة الاحتيال باستخدام وسائل تقنية المعلومات وهي محور هذه الدراسة، وسيتم تقسيم المبحث على النحو التالي:

المطلب الأول: تعريف وسائل تقنية المعلومات.

المطلب الثاني: أنواع وسائل تقنية المعلومات.

المطلب الثالث: الطبيعة القانونية لجرائم تقنية المعلومات.

المطلب الأول

تعريف وسائل تقنية المعلومات

مع تزايد المعلومات بطريقة متواترة وبقفزات سريعة جداً وواسعة بدت الطرق التقليدية عاجزة على جمعها وتنظيمها، لذا ظهرت مساعٍ للتغلب على هذه المشكلة بمسارين رئيسيين: تمثل أولهما في تحسين وتطوير عملية الفهم لطبيعة المعلومات ومكوناتها وتجميعها وتحليلها بهدف الاستفادة منها بفاعلية، أما الثاني فقد تمثل في الحاجة لتقنية متقدمة للتحكم في المعلومات وتجميعها ومعالجتها واختزالها واسترجاعها كالحاسبات والوسائط المتنوعة ووسائل الاتصال، والتي تشكل اندماجها معاً بما يعرف بتقنية المعلومات Information Technology (It) أو المعلوماتية (Informatics).

وتمثل التقنية الحديثة مظهراً من المظاهر المتقدمة في عالمنا المعاصر حتى غدت من مستلزمات الحياة الأساسية فهي تؤدي دوراً كبيراً في التواصل بين الأفراد والمؤسسات والدول، شأنها شأن غيرها من المصطلحات القانونية، فقد تناول الفقه المقارن تعريفات مختلفة لوسائل تقنية المعلومات.

وسنقوم بتقسيم المطلب إلى فرعين على النحو الآتي:

الفرع الأول: التعريف الفقهي لوسائل تقنية المعلومات.

الفرع الثاني: التعريف القانوني لوسائل تقنية المعلومات.

الفرع الأول: المفهوم الفقهي لوسائل تقنية المعلومات.

إن وسائل تقنية المعلومات من أبرز سمات التكنولوجيا الحديثة في عالمنا المتمدن، إذ تشمل فرعين متقاربين ومندمجين هما الحاسوب والاتصال، فهناك من لا يفرق بينهما ولكن ضرورة الموضوعية للمعالجة تفرض التفريق بينهما في كون الحاسوب يقوم على استخدام وسائل تقنية لإدارة وتنظيم البيانات ومعالجتها في إطار علم الحساب والمنطق، أما الاتصال فوظيفته القيام بتقنية نقل المعلومات بجميع دلالاتها التي تشمل الرسائل والأخبار والبيانات والمعرفة ومع اندماج هذين الفرعين أصبح الحديث عن تقنية المعلومات والتي تمثل النظم الآلية والالكترونية للتعامل مع المعلومات وتشمل وسائل الحوسبة والاتصال^١.

يشتق مصطلح "المعلوماتية" من المعلومة أو المعلومات، وفنياً هناك علاقة بين البيانات والمعلومات، فالبيانات هي مجموعة من الحقائق أو المشاهدات أو القياسات التي تكون عادة في شكل حروف أو أرقام أو أشكال خاصة توصف أو تمثل فكرة أو موضوعاً أو هدفاً أو شرطاً أو أية عوامل أخرى، وتمثل البيانات المادة الأساسية التي يتم تجهيزها للحصول على المعلومات، فالبيانات تعد مصطلحاً عاماً لكل الحقائق والأرقام والرموز والحروف، فهي معطيات أولية يمكن معالجتها وإنتاجها عن طريق نظم المعلومات، فبعد المعالجة الفنية والعلمية للبيانات فإنها تتحول إلى معلومات^٢.

أولاً وبناءً على ما سبق، يمكن تعريف تقنية المعلومات بأنها: "مجموعة من الأدوات التي تساعد المستفيد للعمل مع المعلومات وإنجاز الواجب المتعلق بمعالجتها"، وتقنية المعلومات يقصد بها التعامل الفوري مع المعلومة، وهي علم التعامل المنطقي مع المعلومات باعتبارها ناقلة المعارف الإنسانية، والعلاقة وثيقة بين القانون وتقنية المعلومات، فالقانون يحدد القواعد التي تحكم أنماط السلوك المختلفة والكثير من أنماط السلوك تتعامل الآن مع تقنية المعلومات كظاهرة تفرض نفسها على الواقع الاقتصادي والسياسي والاجتماعي والعسكري^٣.

^١ نوفل علومحمد عزت، "جريمة إنشاء موقع أو نشر معلومات مخلة بالآداب العامة بوسائل تقنية المعلومات"، مجلة الرافدين للحقوق، العراق، المجلد ١٢، العدد ٤٤، ٢٠١٠، ص ٢٨١.

^٢ هدى حامد قشقوش، "الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني"، بحوث مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، من ١-٣ مايو ٢٠٠٠م، ط٢، ص ٨٨٧.

^٣ هدى حامد قشقوش، "مرجع سابق"، ص ٨٨٧.

وتعتبر الوسائل الالكترونية من أبرز مظاهر التكنولوجيا الحديثة والمتمثلة في الحوسبة والاتصال، ففي الحوسبة تقوم وسائل التقنية على إدارة وتنظيم البيانات في إطار مهام محددة تتصل بالحساب والمنطق، أما الاتصال فتستخدم وسائل التقنية فيه لنقل المعلومات بكافة دلالاتها^١.

مما سبق يبرز اصطلاح تقنية المعلومات أو التقنية العالية والتي تمثل النظم الآلية أو الالكترونية للتعامل مع المعلومات وتشمل الحوسبة والاتصال وما نتج من اندماجها مع وسائط تقنية عالية يعبر عنها بنظام الكمبيوتر.

فقد عرفت منظمة اليونسكو وسائل تقنية المعلومات بأنها: "الفروع العلمية والتقنية الهندسية وأساليب الإدارة في تداول ومعالجة المعلومات وفي تطبيقها والمتعلقة بالحواسيب وتفاعلها مع الانسان والآلات وما يرتبط بذلك من أمور اجتماعية واقتصادية وثقافية"^٢.

ولكن ما يؤخذ على هذا التعريف بالرغم من شموليته لكافة أساليب التقنية الحديثة إلا أنه اقتصر فقط على وسيلة الحاسوب وتجاهل الوسائل الأخرى كالهاتف النقال.

كما عرفها بعض الفقه بأنها: "خليط من أجهزة الكمبيوتر ووسائل الاتصال ابتداء من الألياف الضوئية إلى الأقمار الصناعية والتقنيات والمصغرات الفلمية والاستنساخ، تمثل مجموعة كبيرة من الاختراعات التي تستخدم المعلومات خارج العقل البشري"^٣. وعُرفت أيضا بكونها "القاعدة الأساسية التي تبنى في ضوئها المنظمات الإدارية والمنشآت ميزتها التنافسية"، ويقصد بالتقنية هنا كل أنواع المعرفة الفنية والعلمية والتطبيقية التي يمكن أن تسهم في توفير الوسائل، المعدات، الآلات، الأجهزة الميكانيكية والإلكترونية ذات الكفاءة العالية والأداء الأفضل التي تسهل للإنسان الجهد وتوفير الوقت وتحقيق للمنظمة أهدافها النوعية والكمية بكفاءة وفاعلية"^٤.

^١ يونس العرب، ورقة عمل بعنوان، "التشريعات والقوانين المتعلقة بالإنترنت في الدول العربية"، مقدمة إلى مؤتمر ومعرض التكنولوجيات المصرفية العربية والدولية، اتحاد المصارف العربية، الأردن، ٢٨-٢٩ تشرين أول ٢٠٠٢، ص ٢.

^٢ مقال بعنوان، "جرائم الكمبيوتر والإنترنت"، منشور على الشبكة القانونية، فروع القانون، ٢٧/٣/٢٠١٣: www.Alablav.Org.

^٣ محمد الهادي، "تكنولوجيا المعلومات وتطبيقاتها"، دار الشروق، القاهرة، ١٩٨٩، ص ٣٢.

^٤ راجع في ذلك، شاهر فلاح العرود وطلال حمدون شكر، "جودة تكنولوجيا المعلومات وأثرها في كفاءة التدقيق الداخلي في الشركات الصناعية والخدمية المساهمة العامة الأردنية"، المجلة الأردنية في إدارة الأعمال، الأردن، المجلد ٥، العدد ٤، ٢٠٠٩، ص ٤٧٨.

أما وزارة التجارة والصناعة البريطانية فوضعت تعريفاً شاملاً لوسائل تقنية المعلومات هو "الحصول على البيانات ومعالجتها وتخزينها وتوصيلها وإرسالها في صورة معلومات مصورة أو صوتية أو مكتوبة أو في صورة رقمية، ذلك بواسطة توليفة من الآلات الإلكترونية وطرق المواصلات السلكية واللاسلكية"^١.

ومن خلال هذه التعريفات يتضح لنا أن تقنية المعلومات تتمثل في مختلف الوظائف من تجميع للبيانات وتحليلها وتخزينها واسترجاع المعلومات وذلك عن طريق التكامل بين الآلات الإلكترونية ونظم الاتصالات الحديثة.

الفرع الثاني: التعريف القانوني لوسائل تقنية المعلومات.

نظراً لما أحدثته وسائل التقنية المعلوماتية من تطوراً هائلاً على الصعيد الجنائي، وذلك بظهور نوع جديد من الجرائم جراء استخدام هذه الوسائل، فقد شرعت معظم الدول إلى مواجهة هذه الظاهرة المستحدثة، وذهبت في تشريعاتها إلى تعريف وسائل تقنية المعلومات^٢، فقد عرف المشرع البحريني في المادة الأولى من القانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات بأنها "تشمل كل أشكال التقنية المستخدمة لإنشاء ومعالجة وتخزين وتبادل واستخدام وعرض المعلومات بمختلف صيغها".

وفي ذات المادة عرفت وسيلة تقنية المعلومات بأنها: "أية أداة أو وسيلة إلكترونية أو مغناطيسية أو بصرية أو كهروكيميائية أو أية أداة تدمج بين تقنيات الاتصال والحوسبة أو أية أداة أخرى لديها القدرة على استقبال أو إرسال البيانات ومعالجتها وتخزينها واسترجاعها بسرعة فائقة"، وعرف المشرع البحريني أيضاً نظام تقنية المعلومات بكونها: "أداة أو مجموعة أدوات متصلة أو ذات صلة ببعضها، ويقوم واحد منها أو أكثر بمعالجة آلية البيانات وسيلة تقنية المعلومات وفقاً لبرنامج"، وعرف كذلك بيانات وسيلة تقنية المعلومات بأنها "تمثيل لحقائق أو لوقائع أو لمعلومات أو لمفاهيم في صورة مناسبة تسمح لنظام تقنية المعلومات بمعالجتها".

^١ راجع في ذلك بوحنية قوي، "الاتصالات الإدارية داخل المنظمات المعاصرة"، ديوان المطبوعات الجامعية، الجزائر، ٢٠١٠، ص ٨٦.

^٢ أنظر: "تعريف المعلومات"، من ذات الرسالة، ص ١١٣.

ونجد بأن المشرع البحريني قد وضع تعريفاً أكثر دقة ووضوحاً بحيث أنه لم يغفل أن تكون كافة وسائل تقنية المعلومات خاضعة لهذا التعريف فلم يحدد تقنية المعلومات بوسيلة واحدة بل أنها كانت بعدة وسائل تشمل الحاسب الآلي والشبكة المعلوماتية وأجهزة الموبايل وأية وسيلة تنشأ في المستقبل تحمل المعطيات التي جاء بها التعريف.

أما المشرع الإماراتي فعرف وسيلة تقنية المعلومات في المادة (١) من القانون الاتحادي لدولة الإمارات العربية المتحدة رقم (٢) لسنة ٢٠٠٦م بشأن مكافحة تقنية المعلومات. بأنها: "أية أداة الكترونية مغناطيسية، بصرية، كهروكيميائية أو أداة أخرى تستخدم لمعالجة البيانات وأداة المنطق والحساب أو الوظائف التخزينية وتشمل أيضاً أية قدرة تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الأداة".

وجاء في المادة (١) من وثيقة الرياض للنظام (القانون) الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون لدول الخليج العربية لسنة ٢٠١٣م تعريف لوسيلة تقنية المعلومات وهي: "أية أداة الكترونية مغناطيسية، بصرية، كهروكيميائية أو أداة أخرى تستخدم لمعالجة البيانات وأداة المنطق والحساب أو الوظائف التخزينية وتشمل أيضاً أية قدرة تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الأداة".

كما وجاءت المادة (٢) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المصادق عليها من قبل مملكة البحرين بالقانون رقم (٢) لسنة ٢٠١٧م بتعريف لوسيلة تقنية المعلومات بأنها "أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقاً للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكياً أو لاسلكياً في نظام أو شبكة".

وبعد البحث في تشريعات كل من مملكة البحرين ودولة الإمارات المتحدة نجد بأن كلا المشرعين البحريني والإماراتي قد تناولوا وبشكل مباشر تعريف شامل وجامع لوسائل تقنية المعلومات وكل ما له صلة بالوسائل الحديثة المستخدمة في هذه التقنية، وذلك ضمن تشريعات مواجهة الجرائم التي تستخدم فيها هذه التقنية الحديثة، حيث لم يقتصر التعريف فقط على الآلة أو الأداة كوسيلة من وسائل التقنية، بل أنها اشتملت على كل ما له صلة في هذه الوسائل من برامج وأدوات أخرى يستطيع من خلالها الجاني الدخول أو الولوج إلى النظام المعلوماتي، وبذلك فالتعريف شمل الوسائل المادية وغير المادية.

يتبين من خلال ما سبق، أن المشرع البحريني والإماراتي قد وفقا من خلال تركهما للمصطلحات المتعلقة بوسائل تقنية المعلومات على عموميتها دون تخصيص نظراً لعدم حصر هذه الوسائل المرتبطة بالجرائم المعلوماتية ووسائلها، والتي ترتبط بهذه الجريمة وسماتها المتطورة، حيث إن عمومية التعريف المطروح لوسائل تقنية المعلومات يشمل على كافة الوسائل المادية وغير المادية والتي من شأنها أن تستخدم في جرائم الاحتيال المعلوماتي.

أما المشرع السعودي فلم يتطرق إلى تعريف صريح لوسائل تقنية المعلومات في نظام مكافحة الجرائم المعلوماتية، وعليه فيرى الباحث ضرورة أن يقوم المشرع السعودي بتعريف صريح لوسائل تقنية المعلومات ليغلق الباب أمام التذرع بالجهل وعدم الدراية بوسائل تقنية المعلومات أمام الجناة، وبذلك يكون قد قطع الشك باليقين بتحديد نطاقها وإساءة استخدامها.

المطلب الثاني

أنواع وسائل تقنية المعلومات

تتنوع الوسائل التي تستخدم في تقنية المعلومات في عالمنا المعاصر فهي تتنوع بتنوع نوع الجريمة المرتكبة، وهذا ما يميز الجرائم باستخدام وسائل تقنية المعلومات عن الجرائم التقليدية، حيث تتدخل التكنولوجيا بصورها المتعددة في هذه الوسائل والتي ينتج عنها الجريمة لهذه الأفعال، وتتخذ وسائل تقنية المعلومات أنواع متعددة وعليه سيتم تقسيم هذا المطلب إلى خمسة فروع على النحو الآتي :

الفرع الأول: الحاسب الآلي.

الفرع الثاني: الشبكة المعلوماتية.

الفرع الثالث: شبكة الإنترنت.

الفرع الرابع: الهاتف النقال.

الفرع الخامس: البلوتوث.

الفرع الأول: الحاسب الآلي.

إن مصطلح الحاسب الآلي مصطلح جديد، أفرزه التقدم العلمي في مجال التكنولوجيا، فظهور الحاسب الآلي جاء نتيجة التطور العلمي والتقدم التقني، الذي أدى إلى تدخل أنظمة المعالجة الآلية للمعلومات في كافة مجالات الحياة اليومية، نظراً لما يتمتع به الحاسب الآلي من قدرة فائقة على تخزين أكبر قدر من البيانات والمعلومات، وللحاسب الآلي عدة مسميات، وقد اختلف الفقه والعلم على هذه المسميات، وسيتناول الباحث بعض من التعريفات التي لها علاقة في موضوع البحث.

أولاً: تعريف الحاسب الآلي علمياً.

عرف الحاسب الآلي علمياً بأنه "آلة حاسبة إلكترونية، ذات سرعة فائقة ودقة متناهية، يمكنها قبول البيانات وتخزينها ومعالجتها، للوصول إلى النتائج المطلوبة"^١.

وذهب فقه آخر إلى أنه يعد الحاسب الآلي من أهم الوسائل المستخدمة في تقنية المعلومات لما له من أهمية في بناء النظام المعلوماتي وذلك للاندماج الحاصل بين نظام الحوسبة والاتصال، وهي آلة تستقبل البيانات وتشغيلها بواسطة برامج معينة للوصول إلى النتائج المطلوبة^٢.

ثانياً: تعريف الحاسب الآلي فقهياً.

ويعرف الحاسب الآلي فقهياً على أنه "كل وحدة أو مجموعة وحدات قادرة على معالجة أو تخزين البرامج والمعلومات أو أجزاء الدخول أو الخروج أو الارتباط والتي تهدف إلى نتيجة محددة تشكل موضوعاً للحماية بنظام الأمن"^٣، وعرفه مجلس الشيوخ الفرنسي على أنه "مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، إذ يربط فيما بينها مجموعة العلاقات التي عن طريقها يمكن تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون المركب خاضع للحماية التقنية"^٤.

فوفقاً للتعريفات المطروحة يتكون الحاسب الآلي من مجموعة أجزاء مادية وغير مادية، فمن الأجزاء المادية الأسطوانات وآلات الطباعة والشبكات والشاشة ولوحة المفاتيح والفأرة وغير ذلك من الأجهزة التي تظهر بفضل التقدم التكنولوجي، أم الأجزاء غير المادية، فتشمل البرامج والأساليب المتعلقة بوحدة معالجة البيانات أي الكيان المنطقي للحاسب الآلي.

^١ عوض منصور محمد أبو النور، "مقدمة في علم الحاسب الإلكتروني وبرمجة بيسك"، دار الأمل، إربد، الأردن، ١٩٩٦م، ط٥، ص ٢٨.

^٢ للمزيد أنظر، عفيفي كامل عفيفي، "جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون"، منشورات الحلبي الحقوقية، بيروت ٢٠٠٣م، ص ٩.

^٣ نقلًا عن: الدكتور محمد الهيبي، "جريمة الدخول إلى النظام الآلي لمعالجة المعطيات عن طريق الغش - دراسة في ضوء التشريع الفرنسي"، مجلة النهرين، العراق، المجلد ٩، العدد ١٥، شباط، ٢٠٠٦م، ص ٥٦-٥٨.

^٤ محمد الهيبي، "مرجع سابق"، ص ٥٦-٥٨.

ثالثاً تعريف الحاسب الآلي في التشريعات المقارنة.

لم يقوم كل من المشرع البحريني والإماراتي بتعريف الحاسب الآلي في القوانين النازمة للجرائم تقنية المعلومات، فقد عرفه المشرع السعودي الحاسب الآلي بأنه "أي جهاز إلكتروني ثابت أو منقول سلكي أو لا سلكي يحتوي على نظام معالجة البيانات، وتخزينها، أو إرسالها، أو استقبالها، أو تصفحها، يؤدي وظائف محددة بحسب البرامج، والأوامر المعطاة له"^١.

ويعرف الحاسب الآلي في المادة الأولى من الاتفاقية الأوروبية حول الجريمة على الانترنت، بأنه "أية آلة أو مجموعة مرتبطة فيما بينها أو ذات علاقة من الآلات، يمكن بإضافة برمجية إلى واحد أو أكثر منها، أن تقوم بمعالجة آلية للبيانات"^٢.

يتضح من خلال التعريفات السابقة بأن الحاسب الآلي ليس مجرد جهاز أو آلة، لكنه نظام كامل متكامل يتكون من مجموعة من الأجهزة والتعليمات المخزنة، وتكون مدخلات هذا النظام البيانات التي يقوم بمعالجتها وتخزينها أو كليهما، في حين تتمثل مخرجاته بالمعلومات والنتائج، فالحاسب الآلي يمتاز بقدرة تخزينية كبيرة، وسرعة عالية في كتابة البيانات المطلوبة، وتحويلها إلى معلومات، مع إمكانية حذفها، وتعديلها أكثر من مرة، وكل ذلك بفضل التقنية العالية في الطريقة التي تسجل فيها البيانات، والبرامج المرتبطة بالحاسب الآلي^٣.

ويرى الباحث أن التعريفات السابقة الخاصة بالحاسب الآلي قد أدخلت الكثير من وسائل تقنية المعلومات في مفهوم الحاسب الآلي كالهاتف النقال الذي من شأنه أن يقوم بمهام الحاسب الآلي، وبالإضافة إلى ذلك فإن التعريفات لم تقتصر فقط على الأشياء المادية المكونة للحاسب الآلي بل أنها أدخلت في نطاقها البيانات والمعطيات والبرامج فيما بينها، وعليه فإن التعريفات السابقة فضفاضة وواسعة.

^١ المادة (١) من نظام مكافحة جرائم المعلوماتية الصادر بتعميم وزير العدل بالنيابة الموافق ١٤٢٨ / ٣ / ٧، الموافق ٢٠٠٧ / ٣ / ٢٦. جريدة أم القرى، الجريدة الرسمية للملكة العربية السعودية، العدد ٤١٤٤، بتاريخ ١٤٢٨ / ٣ / ٢٥ هـ، ص ٦٠٥.

^٢ انظر: عبدالعال الديري، محمد صادق إسماعيل، "الجرائم الإلكترونية" - دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت، المركز القومي للإصدارات القانونية، القاهرة، ط ١، ٢٠١٢، ص ٢٧.

^٣ محمد علي العريان، "الجرائم المعلوماتية"، دار الجامعة الجديدة، المكتبة القانونية، الاسكندرية، ٢٠٠٤م، ص ٥٩.

وعند الحديث عن علاقة الحاسب الآلي في الجريمة المستحدثة والتي تقع إحدى صورها في الجرائم التي تستخدم تقنية المعلومات كأداة لارتكابها، فقد يكون الحاسب الآلي موضوع الجريمة أو يكون وسيلة لارتكاب جرائم أخرى تقليدية أو إلكترونية^١.

ويمكن تصنيف جرائم الحاسب الآلي إلى مجموعات، منها الجرائم المتعلقة بالأفعال التي تستهدف عناصر (السرية والسلامة)، وكذلك الجرائم المرتبطة بالمحتوى كجريمة الاحتيال الإلكتروني والدخول غير المشروع للمواقع الإلكترونية وسرقة البيانات الشخصية، والجرائم المتعلقة بالأفعال اللاأخلاقية وغير ذلك^٢.

الفرع الثاني: الشبكة المعلوماتية.

في هذا الجزء من الدراسة سيتم التطرق الي ماهية الشبكة المعلوماتية من خلال التعريف الفقهي والتشريعات المقارنة للشبكة المعلوماتية، وذلك وفقاً للآتي:

أولاً: التعريف الفقهي للشبكة المعلوماتية.

تعرف الشبكة المعلوماتية بأنها: "وصل جهازين أو أكثر معاً من أجل تبادل المعلومات"^٣، فيتضح أن شبكة الإنترنت ما هي إلا صورة من صور الشبكة المعلوماتية، بحيث تعد الشبكة المعلوماتية أوسع وأشمل من شبكة الإنترنت وربما هذا اللبس الذي يقع فيه الكثير من الباحثين.

ومما سبق يتبين أن الشبكة المعلوماتية هي عبارة عن آلية من خلالها يتم ربط مجموعة من الأجهزة فيما بينها للقيام بمهام معينة يتم من خلالها تبادل البيانات والمعلومات للقيام بمهمة ما، فهي أوسع وأشمل في استخداماتها من أية وسيلة أخرى يتم من خلالها التواصل والاتصال لتبادل المعلومات.

^١ هلال البياتي وآخرون، "تدوة القانون والحاسوب"، سلسلة المائدة الحرة، رقم (٣٧)، بيت الحكمة، بغداد، مطبعة اليرموك، العراق، ١٩٩٩م، ص ٢٤.

^٢ عفيفي كامل، "مرجع سابق"، ص ٣٧.

^٣ هلال البياتي وآخرون، "مرجع سابق"، ص ٢٤.

ثانياً: تعريف الشبكة المعلوماتية في التشريعات المقارنة.

لم يتناول المشرع البحريني تعريف خاص بالشبكة المعلوماتية ولا حتى شبكة الإنترنت إنما اكتفى بتعريف وبيان نظام تقنية المعلومات والوسائل التقنية الحديثة التي تم الإشارة إليها في المطلب الأول.

وعرفها المشرع الإماراتي في المادة (١) من القانون الاتحادي الإماراتي لمكافحة جرائم تقنية المعلومات لسنة ٢٠٠٦م بأنها "ارتباط بين أكثر من وسيلة لتقنية المعلومات للحصول على المعلومات وتبادلها".

أما المشرع السعودي فقد عرف الشبكة المعلوماتية في المادة (١) من النظام السعودي لمكافحة جرائم المعلوماتية أنها "ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة وشبكة الإنترنت".

من خلال التعريفات السابقة يتضح أن الشبكة المعلوماتية لم تقتصر فقط على الحواسيب وضرورة ارتباطها ببعضها البعض عبر تقنيات معينة، إنما اشترط بأن تكون ارتباط أكثر من وسيلة من وسائل تقنية المعلومات التي عرفها المشرع كما أشرنا سابقاً وهذا ما يفسر تعدد وتنوع وسائل تقنية المعلومات وعدم قصورها على الحاسب الآلي وذلك بدا واضحاً في ظل التطور التكنولوجي الذي كان نتاجه وسائل أخرى كالهواتف النقالة الحديثة.

الفرع الثالث: شبكة الإنترنت.

تعتبر شبكة الإنترنت من أهم تقنيات العصر الحديث وذلك لانتساع نطاق استخدام الشبكة في الحياة العملية والعلمية وقد اكتسبت هذه الشبكة أهمية كبيرة في ظل البيئة الرقمية التي كافة المجالات.

أولاً: نشأة شبكة الإنترنت.

تعود فكرة إنشاء شبكة إنترنت إلى العام (١٩٦٩م) حيث عمدت وكالة المشاريع والبحوث في وزارة الدفاع الأمريكية إلى بناء شبكة لتبادل معلومات البحوث المتقدمة بين مراكز البحوث المتعاونة مع وزارة الدفاع، الموزعة على مناطق متباعدة في الولايات المتحدة الأمريكية، وقد

أثمرت جهود هذه الوكالة عن ولادة شبكة متواضعة تتألف من أربعة حواسيب، كانت هي المنطلق نحو التطورات اللاحقة، إذ حققت هذه الشبكات نمواً سريعاً، حتى أصبحت في عام (١٩٧٢م) شبكة واسعة تحتوي (٣٧) عقدة معلوماتية، وأطلق عليها حينئذ اسم (ARPANET)، كان الهدف منها إنشاء شبكة لا يمكن أن تعطلها الحروب^١.

وتفرض الواقعية نفسها في تبني اصطلاح شبكة الإنترنت وذلك لأن معظم الجرائم الواقعة باستخدام وسائل تقنية المعلومات تأخذ من شبكة الإنترنت وسيلة رئيسية لارتكاب هذه الجرائم، وهذا ما يفرض علينا التعريف بشبكة الإنترنت كوسيلة من وسائل تقنية المعلومات.

ثانياً: تعريف شبكة الإنترنت.

تعددت التعاريف الفقهية التي تناولت مفهوم الإنترنت ومن هذه التعاريف: تعرف شبكة الإنترنت بأنها "عبارة عن آلية اتصال مكونة من مفاتيح وأسلاك وأماكن تخزين للبيانات، ودوام توصيل، وروابط اتصال، تعمل بوتقة واحدة بفضل بروتوكول الإنترنت"^٢.

وعُرفت بأنها "شبكة الشبكات، حيث تتكون من عدد كبير من شبكات الحاسوب المترابطة والمتناثرة في أنحاء العالم، ويحكم ترابط تلك الأجهزة وتحادثها بروتوكول موحد يسمى بروتوكول ترانسل الإنترنت"^٣، ومن الناحية التقنية تعرف الشبكة العنكبوتية بأنها "الوسيلة أو الأداة التواصلية بين شبكات المعلومات، دون اعتبار للحدود الدولية"^٤.

يحتوي الإنترنت على عدة تطبيقات ووسائل للتواصل، مثل البريد الإلكتروني والماسنجر والتي تستعمل في أفق الإنترنت، ولكنها ليست هي والإنترنت شيئاً واحداً، فالإنترنت يشبه الطريق للمدن، في حين أن تلك التطبيقات المذكورة هي وسائل المواصلات التي تستخدم لهذا الطريق^٥.

^١ نوفل الصفو ومحمد عزت فاضل، "جرائم تقنية المعلومات المخلة بالأخلاق العامة -دراسة مقارنة"، مكتبة السنهوري، بيروت، ٢٠١٧م، ص ٢٣.

^٢ راجع في ذلك، محمد طارق الخن، "جريمة الاحتيال عبر الإنترنت" الاحكام الموضوعية والأحكام الإجرائية"، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠١١م، ط ١، ص ٢٢.

^٣ عبد الفتاح مراد، "شرح جرائم الكمبيوتر والإنترنت"، دار الكتب والوثائق المصرية، دون سنة نشر ص ٣٨.

^٤ محمد طارق الخن، "مرجع سابق"، ص ٢٢.

^٥ إيهاب السنباطي، "موسوعة الإطار القانوني للتجارة الإلكترونية"، دار النهضة العربية، القاهرة، ٢٠٠٧م، ص ٨٠.

وتعرف شبكة الإنترنت أيضاً بأنها: "مجموعة كبيرة من شبكات الحاسوب المرتبطة ببعضها البعض باستخدام وسائل ربط متنوعة كالأسلاك والكوابل النحاسية أو أبراج الاتصال اللاسلكي التي تعمل من خلال تبادل الموجات الكهرومغناطيسية أو الأقمار الصناعية أو بالجمع بينهما عبر مختلف أنحاء العالم". وفي ظل الحداثة والتطور التي يشهدها عالمنا المعاصر أصبح للإنترنت استخدامات متعددة ومتنوعة بحيث تقدم خدمات للقطاعات العامة والخاصة، وأصبحت هذه الشبكة في متناول الجميع، ومن الخدمات التي تقدمها هذه الشبكة، خدمة الويب، وخدمة نقل الملفات، وخدمة البريد الإلكتروني، وغرف الدردشة وخدمة التلنيت^٢.

ثالثاً: مزايا وعيوب شبكة الإنترنت.

وتتسم شبكة الإنترنت بسرعة فائقة في نقل المعلومات كما سهلت طريقة التواصل على كافة المستويات وذلك عبر التقنية التي تمتاز بها مما أثر بشكل إيجابي وفعال في تقديم الخدمات عبر العالم كونها شبكة عالمية لا تتقيد بحدود جغرافية، وهي خدمة في متناول الجميع حيث لا تقتصر على فئة دون أخرى، وبالرغم من هذه الإيجابيات التي تمتاز بها هذه الشبكة العالمية إلا أن استخدامها بالطرق السلبية أدى إلى ظهور نوع جديد من الجرائم حيث يتم من خلالها ارتكاب جرائم توظف بعد ذلك للابتزاز أي أنها مهدت الطريق أمام نوع جديد من الجرائم يتم من خلالها الاعتداء على الحياة الخاصة للأفراد، وقد تتجاوز الاعتداء على حرية الأفراد إلى تهديد أمن الدول وذلك بالتلاعب في البيانات والمعلومات الخاصة بأمن الدول^٣.

يتبين أن ما وفرته شبكة الإنترنت من مزايا على الصعيد المعلوماتي وتوفير قاعدة معلومات لا حصر لها، وما قدمته من اختصار الوقت وسرعة في الأداء ساهم في انجاز المهام العامة والخاصة في وقت قياسي حيث أصبحت هذه المعلومات وما يتعلق فيها في متناول

^١ بشار دودين، "الإطار القانوني للعقد المبرم عبر شبكة الإنترنت"، دار الثقافة للنشر والتوزيع، عمان، ط١، ٢٠٠٦م، ص ٢١.

^٢ خدمة الويب أو ما يعبر عنها بالشبكة العنكبوتية تحتوي على ملايين الوثائق والأبحاث والتقارير المترجمة من مختلف المصادر المعلوماتية، وخدمة نقل الملفات هي عبارة عن نسخ الملفات من حاسب إلى آخر عبر الإنترنت، وخدمة البريد الإلكتروني هي خدمة تتيح للمستخدم تبادل الرسائل بسرعة فائقة بأقل التكاليف وفي أي وقت، وخدمة التلنيت تمكن المستخدم من الدخول في أجهزة حاسوب موجودة في أماكن بعيدة عبر بروتوكول خاص للاتصال يوصله عن بعد إلى الحاسوب المطلوب، وخدمة الغرف الخاصة بالدردشة تتيح لمستخدميها بالمحادثة مع بعضهم البعض. أنظر، نوفل الصفو ومحمد عزت فاضل، "مرجع سابق"، ص ٢٥-٢٦. أنظر أيضاً: محمد طارق الخن، "مرجع سابق"، ص ١٩-٢١.

^٣ محمد طارق الخن، "مرجع سابق"، ص ٢٢-٢٤.

الجميع، عوضاً عن ذلك فإن الشبكة أيضاً قدمت تقنيات وبرامج سهلت من خلالها من عملية التواصل والاتصال حتى أصبح العالم معها كقرية صغيرة لا عوائق فيها، إلا أن ذلك لا يخلو من السلبيات فالاستخدام السيء لشبكة الإنترنت وتقنياتها قد أفرز أنواعاً جديدة من الجرائم، حيث يستطيع خبراء رواد هذه الشبكة أن يحصلوا على البيانات والمعلومات الشخصية للأفراد كما يمكنهم الاطلاع على معلومات خطيرة وخاصة بأمن الدول وأنظمتها العسكرية والأمنية والاقتصادية بما فيها البنوك، وبالرغم من الجهود المبذولة لتحسين برامج الإنترنت ومعلوماتها للحيلولة دون الوصول إليها بطرق غير مشروعة، إلا أن ذلك لا يمنع من محاولة اختراقها من قبل المختصين.

كما وتجدر الإشارة هنا أيضاً، بأنه لا تقتصر الجرائم في الحصول على المعلومات أو الولوج غير المشروع لأنظمة الحاسوب فقط، فقد تستخدم هذه الشبكة في جرائم التشهير والسب والقذف، حتى ممارسة التجارة غير الشرعية والمحركة دولياً، حتى أصبحت اليوم هذه الشبكة بمثابة السوق العالمية التي يتم ترويج ونشر السلع أو المعلومات بها، وباتت تصل إلى أعداد مهولة ويشاهدها ملايين البشر.

ومن هنا يمكن القول، أنه لا بد من الدول أن تراقب استخدام تلك الشبكة عبر سن التشريعات وتقنياتها، مع ضمان الحريات التي لا تتعارض مع النظام العام في الدولة.

الفرع الرابع: الهاتف النقال.

تتعدد الخدمات التي يقوم بها الهاتف النقال فلم تعد تقتصر فقط على إجراء المحادثات الصوتية والتواصل من خلاله عبر الرسائل، بل امتدت هذه الخدمات وخاصة في ظل ربط الهواتف النقالة في خدمة الإنترنت.

أولاً: تعريف الهاتف النقال لغةً.

للهاتف بصورة عامة معنيان أحدهما لغوياً وهي مشتقة من الفعل (هتف): الهتف أو الهتاف: الصوت الجافي العالي، وقيل الصوت العالي، وقيل سمعت هاتفاً يهتف إذ كنت تسمع الصوت ولا تبصر أحداً^١.

ويقتصر التعريف اللغوي للهاتف النقال على الكلام أو المناداة بصوت مرتفع في حالة لا يمكن معها مشاهدة المتكلم أو صاحب الكلام.

ثانياً: تعريف الهاتف النقال اصطلاحاً.

إن المعنى الاصطلاحي لكلمة الهاتف هو: "الآلة التي تحول الصوت والإشارات الصحيحة الأخرى إلى الشكل الذي يمكن أن يرسل إلى المواقع البعيدة حيث يستلزمان ويعيدان الموجات إلى الإشارات الصحيحة"^٢.

وتتنوع المسميات الخاصة بالهاتف النقال بحيث يسمى أيضاً بالهاتف الخلوي أو الهاتف الجوال أو الهاتف المحمول، كما ويعتبر أحد أشكال أدوات الاتصال والذي يعتمد على الاتصال اللاسلكي عن طريق شبكة من أبراج البث الموزعة ضمن مساحة معينة، أو عبر الأقمار الصناعية، ويعتبر الهاتف النقال من الوسائل الرقمية الحديثة وهي وسيلة للاتصال سواء كان بالمحادثة أم عن طريق الرسائل.

ويعرف الهاتف النقال على أنه "جهاز يستخدم لنقل المكالمات الشخصية بين نقطتين يوجد في أحدهما المرسل ويوجد في الآخر المستقبل ويعمل على تحويل الذبذبات التي يحدثها

^١ ابن منظور، "لسان العرب"، دار المعارف للنشر، القاهرة، ط١، ص ٤٦١٢.

^٢ مي عبد الله، "نظريات الاتصال"، دار النهضة العربية، بيروت، ٢٠٠٦م، ص ٢٣.

الصوت إلى موجات مغناطيسية تنتقل عبر أبراج اتصال تتحول بالنهاية إلى ذبذبات صوتية، كما بإمكانه بنفس الطريقة نقل الرسائل المحررة إلكترونياً^١.

ثالثاً: مزايا وعيوب استخدام الهاتف النقال.

لقد أصبح للهواتف النقالة استخدامات متعددة حتى عدت حواسيب متنقلة، فمن خلالها يمكن تصفح الإنترنت وتحميل برامج الربط مع الشبكة العنكبوتية، فبواسطتها يقوم المستخدم بتقديم معلومات أو خدمات إعلامية للمستخدمين، وتزداد الخدمات أيضاً لهذه الوسيلة مع تطور الهواتف النقالة في ظل الحداثة والتقدم التكنولوجي^٢.

إن ما قدمته هذه التقنية كوسيلة من وسائل تقنية المعلومات من خدمات، يمكن من خلالها للأفراد التواصل والاتصال والمحادثة وتناقل الرسائل كان له الأثر الإيجابي كونها قربت المسافات واختصرت الوقت والجهد، ولكن الاستخدام السلبي والسيء لهذه الوسيلة كونها كما أسلفنا تعتبر حاسوب متنقل وذلك في ظل التقنية العالية التي تمتاز بها وربطها بوسائل معلوماتية أخرى كشبكة الإنترنت والبلوتوث، أتاح لدى مستخدميها بالطرق السلبية - خاصةً بجريمة الاحتيال المعلوماتي - إمكانية ارتكاب جرائم متعددة بتعدد طبيعة الاستخدام كذلك المتعلقة بالآداب العامة والنظام العام والتي تقع على شكل تناقل الصور بحيث تكون ماسة بالشرف وتمتاز بالتعدي على الحياة الخاصة للأفراد^٣.

كما يمكن استخدام الهاتف النقال كحاسوب عند ربطه بشبكة الإنترنت بحيث يؤدي نفس المهام التي يمكن أن يؤديها الحاسوب في ظل تمتعه بالتقنية العالية، فمن خلاله يمكن الدخول إلى البريد الإلكتروني وسرقة البيانات الخاصة والاستيلاء على الأموال وارتكاب العديد من الجرائم كما أشرنا سابقاً.

كما ساهمت القفزة النوعية التي تحققت بالفعل في استخدام الهاتف النقال في يومنا هذا كونه أصبح كمبيوتر متنقل متصل بشبكة الإنترنت، باتساع إساءة استخدامه في ارتكاب جرائم

^١ نوفل الصفو ومحمد عزت، "مرجع سابق"، ص ٢٧.

^٢ نوفل الصفو ومحمد عزت، "مرجع سابق"، ص ٢٨.

^٣ ندى محمود دنون، "عقد الاشتراك بخدمات الاتصالات (دراسة مقارنة)"، رسالة ماجستير، جامعة الموصل، ٢٠٠٩م، ص ١٠-١١.

أكثر خطورة ومنها الجرائم المستحدثة، وهذه الجرائم منها ما ترتكب عليه وأخرى ترتكب بواسطته، فبحسب الأسلوب المتبع في الجريمة أو الباعث والدافع لارتكاب الجريمة^١.

الفرع الخامس: البلوتوث.

يعد البلوتوث إحدى وسائل التقنية الحديثة التي لها مميزات معينة وهي تقنية يتم من خلالها وصل جهازين أو أكثر لتتبادل الملفات والصور وعليه سنقوم بالتعرف على ماهية البلوتوث، وسنستعرض الآلية التي تعمل بها هذه التقنية.

أولاً: ماهية البلوتوث.

هذه التقنية قد توجد في الحاسوب وفي الهواتف النقالة وهي عبارة عن معيار تم تطويره من مجموعة شركات إلكترونية من خلاله يسمح لأي جهازين سواء كان هواتف نقالة أو حواسيب أن يقوموا بعملية اتصال دون أسلاك أو كابلات، ولا يشترط ربطها بشبكة الإنترنت، ولا يتعدى المجال الجغرافي لهذه التقنية الـ ١٠ أمتار^٢.

^١ ترجع بداية ظهور الهواتف النقالة إلى ما كان يعرف باسم التلغراف الضوئي في سنة ١٧٩٣م ثم التلغراف الكهربائي (مرس) سنة ١٨٣٧م والتي من خلاله تم إدخال معايير قياسية اعتمدت أبجدية مورس كنظام ترميز مشترك يسر ظهور شبكات اتصال دولية، وبعد براءة اختراع الهاتف عام ١٨٧٦م بواسطة (غراهام بل) انتشرت هذه الأجهزة بسرعة، أما الهواتف اللاسلكية فترجع إلى ظهور المذياع الهاتفي الذي نتج عنه تطور التلغرافيا اللاسلكية في أوائل القرن العشرين. أنظر، فضيل دليو، "تاريخ وسائل الاتصال"، مطبعة crita copy، قسنطينة، الجزائر، ٢٠٠٦م، ص ١٥٢.

^٢ قبل ظهور هذه التقنية كان يستخدم الاتصال اللاسلكي في العديد من التطبيقات كالتوصيل من خلال استخدام الأشعة تحت الحمراء - وهي أشعة ضوئية لا ترى بالعين المجردة، وسميت بهذا الاسم لأن ترددها أصغر من تردد الضوء الأحمر، وتستخدم الأشعة في أجهزة التحكم بالتلفزيون (الريموت كونترول) ونظراً لأن خاصية الأشعة الحمراء تعمل في مدى الرؤية فقط أي أنه يجب توجيه الريموت كونترول إلى التلفزيون مباشرة للتحكم به، وأن إمكانية تبادل المعلومات تحدث فقط بين جهازين أي لا يمكن ربط أكثر من جهاز في آن واحد بهذه الخاصية، لذلك كانت الحاجة إلى تقنية بديلة عن تقنية الأشعة تحت الحمراء للتغلب على القصور التي واجهتها الأخيرة، مما أثمر في ظهور تقنية البلوتوث. عائشة الريملي، "تقنية البلوتوث (الإيجابيات - المخاطر - الحلول) دراسة ميدانية"، شرطة الشارقة، مركز بحوث الشرطة، الإمارات، ٢٠٠٦م، ص ٨.

وعليه يمكن لنا تعريف البلوتوث على أنه: "تقنية من خلالها يتم ربط مجموعة من الأجهزة المحمولة أو الثابتة مع بعضها البعض، كالحاسب الآلي والحاسب المحمول والهاتف النقال والكاميرات الرقمية والأجهزة السمعية... الخ، وتساهم في نقل المعلومات بسهولة وسرعة عبر تقنية اللاسلكي.

وتستخدم هذه التقنية دون الحاجة إلى ربط الأجهزة عبر أسلاك كهربائية وكابلات الإنترنت، ولا يتطلب ربطها بشبكة الإنترنت أيضاً، فقد يتم تناقل البيانات والمعلومات المخزنة من جهاز إلى آخر شريطة أن يتم ربطها بنفس التقنية، وهي عبارة عن موجات تلتقي فيما بينها ويتم تعريفها بالأجهزة المتصلة بها بمجرد تشغيل تقنية البلوتوث ولا تحتاج إلى أرقام هواتف ولا أسلاك كهربائية كما ذكرنا سابقاً.

ثانياً: مزايا وسلبيات تقنية البلوتوث.

من مزايا هذه التقنية أنها لا تحتاج إلى توصيل الأجهزة والحواسيب بأسلاك مما يسهل عملها عند الانتقال من مكان لآخر، فهي توفر أيضاً السرعة والجهد في تناقل المعلومات، وعادة ما تستخدم هذه التقنية في تناقل الصور وملفات الفيديو دون أي مقابل يذكر فهي تقنية مجانية مقترنة بالأجهزة الحديثة، بالإضافة إلى أنها تقنية لا تحتاج لتدخل المستخدم إلا في تشغيل أيقونة البلوتوث الموجودة بالجهاز.

وعن مخاطر هذه التقنية فإن الاستخدام السيئ والسلبي لهذه الوسيلة كتناقل الصور المخلة بالآداب العامة وتناقل مقاطع الفيديو الإباحية، والتعدي على الخصوصية، ففي حالة ترك البلوتوث في وضع التشغيل فإنه سيستقبل أي صورة أو مقطع فيديو أو فيروسات بحيث لم تقتصر تقنية البلوتوث على تناقل الصور مقاطع الفيديو، ومن المخاطر الناجمة عنها أيضاً أن بعض الشركات والجهات صنعت جهازاً يمكن من خلاله وبعد توصيله بعدة ملحقات كالحاسوب سحب المعلومات المخزنة في الهاتف المتحرك الذي توجد فيه خاصية البلوتوث، كما ويسهل تحديد مكان تواجد الشخص الذي يحمل جهازاً فيه هذه التقنية مما يعني إمكانية استخدامه في أعمال التجسس^١.

وتكمن خطورة هذه التقنية في استخدامها في الأمور اللاأخلاقية من قبل بعض الأفراد كتبادل الرسائل المصورة لابتزاز الأفراد، وأيضاً تسمح هذه الخاصية بتبادل الأرقام والملفات

^١ عائشة البريملي، "مرجع سابق"، ص ٩.

والصور المخلة بالآداب، بالإضافة إلى أن ما يتم تخزينه واسطة هذه التقنية يصعب مسحه من ملفات الهاتف.

ويتبين أن شمولية شبكة الإنترنت وتطور تقنياتها اللاسلكية قد أفقدت تقنية البلوتوث على حد ما قيمتها وأهميتها، حيث أصبح في ظل الحداثة استخدام شبكة الإنترنت كبديل عن البلوتوث، فاستخدام البلوتوث أصبح في أضيق الحدود، ولكن لا يقلل ذلك من أهميته في غياب الإنترنت، وبالنسبة للمخاطر الخاصة بتقنية البلوتوث فهي متوقفة على تشغيل التقنية نفسها حيث يمكن تفادي هذه المخاطر في حال إيقاف تشغيلها، وعليه فإن مخاطرها تكاد تكون محصورة في طبيعة استخدامها.

وقد تم تطوير هذه التقنية بما يسمى (بندقية البلوتوث) وهي مصممة لاختراق الأجهزة العاملة بواسطة البلوتوث ووصلت لمسافة ميل ونصف، بحيث تقوم هذه التقنية بسرقة بيانات الضحية المتوفرة على هاتفه النقال، بل يمكن التلاعب بهاتف الضحية عبر التحكم بالهاتف وكتابة الرسائل وإرسالها وإجراء الاتصال دون علم الضحية، كما ويمكن التنصت على هاتف الضحية عبر هذه التقنية ومراقبة كافة الأعمال التي يقوم بها على هاتفه من إجراء المكالمات وإرسال الرسائل، بل ويمكن من التنصت على الحديث الخاص للضحية والأطراف الأخرى أينما وجد الهاتف^١.

خلاصة القول إن تعدد وسائل تقنية المعلومات وتنوعها أدى إلى تعدد صور ارتكاب الجريمة المعلوماتية بتعدد وسائل التقنية، ويبدو أن المشرع البحريني والمشرع الإماراتي قد وقفا باستخدام مصطلح تقنية المعلومات والوسائل الخاصة بهذه التقنية والتي أصبحت لاحقاً تستخدم كأدوات ترتكب بواسطتها جريمة الاحتيال المعلوماتي أو قد تكون هدفاً لمثل هذه الجريمة.

^١ نوفل الصفو ومحمد عزت فاضل، "مرجع سابق"، ص ٣٠.

المطلب الثالث

الطبيعة القانونية لجرائم تقنية المعلومات

تعتبر جرائم تقنية المعلومات المستخدمة بواسطة الإنترنت والحاسوب من الجرائم المستحدثة في عالمنا المعاصر^١، وهي مختلفة عن الجرائم التقليدية، لكونها جرائم عابرة للحدود تتم داخل عدد من الدول وتكون آثار تمتد لعدد غير محدود من الدول، ويكون محل هذه الجريمة دائما المعطيات إما بذاتها أو بما تمثله بدلالاتها الواسعة - البيانات المدخلة والمخرجة والمخزنة والبرامج على أنواعها بعد المزوجة بين الحاسوب وتقنية الإنترنت؛ مما دفع بعض الفقهاء إلى التفريق بين الجرائم المستخدمة عن طريق الحاسوب والجرائم الأخرى المستخدمة عبر الإنترنت، فليست كل جريمة ناشئة عن طريق الحاسوب تعد من جرائم الإنترنت بل هناك جرائم كانت وسيلتها الإنترنت لذلك يذهب البعض لتجريم الوسائل المستخدمة في العمل الإجرامي^٢. وسنقوم بتقسيم المطلب إلى ثلاثة فروع كالآتي:

الفرع الأول: تطور جرائم تقنية المعلومات.

الفرع الثاني: موقف الفقه من طبيعة جرائم تقنية المعلومات.

الفرع الثالث: موقف التشريعات المقارنة من طبيعة جرائم تقنية المعلومات.

^١ نوفل الصفر ومحمد عزت، "مرجع سابق"، ص ٢٧٧.

^٢ عبد العال الديري، محمد صادق إسماعيل، "الجرائم الإلكترونية -دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت، المركز القومي للإصدارات القانونية، القاهرة، ط١، ٢٠١٢م، ص ٢٣

الفرع الأول: تطور جرائم تقنية المعلومات.

إن سرعة انتشار تقنيات المعلومات في المجتمعات والدول المتقدمة والنامية وفي جميع المجالات الحياتية كوسائل النقل والاتصال وحركة الاقتصاد والتجارة، وأدوات التعليم والصحة وفي الحرب والسلم وغيرها من المجالات الأخرى، أدى إلى تطور الجريمة المستعملة لوسائل تقنية المعلومات وظهر نوع من المجرمين انتقلوا بالجريمة من مفهومها التقليدي إلى مفهومها المعاصر المتعدد والمتشابك في أركانها وتعتمد بالأساس على التقنيات الحديثة لنظم المعلومات^١.

وقد ساعد هذا التطور الملحوظ في وسائل تقنية المعلومات على إفراز جرائم جديدة عكست مدى التطور الحاصل على أرض الواقع واستخدمت أدوات جديدة وسمات خاصة حتى أطلق عليها مصطلح "جرائم تقنية المعلومات" تماشياً مع المصطلح السائد عصر تقنية المعلومات^٢.

ومع هذا التطور أصبح العائق أمام القانونيين في صعوبة إثبات هذه الجريمة، فالبحث في الطبيعة القانونية لجرائم تقنية المعلومات يعني البحث عن الإطار القانوني المنظم لهذه الجرائم على كافة أشكالها ووسائلها المتشابكة والمتداخلة في ظل عصرة المجتمعات بوسائل تقنية المعلومات؛ وهنا يبقى السؤال المطروح: هل يمكن وصف الخدمات والتطبيقات في شبكة المعلومات بأنها تدخل في إطار أحكام البريد أو مفهوم الصحافة والمطبوعات أو المؤسسات التلفزيونية والإذاعية؟ هناك من يرى في هذا الاتجاه أن الطبيعة القانونية لهذه الجرائم يمكن تحديدها من خلال المجال الذي ترتكب فيه والمكان الذي يقع فيه الجرم محل الاعتداء، هذا ما يدفعنا للقول أنه لا خلاف حول تطبيق القواعد التقليدية على الجرائم المنظمة مسبقاً، ولكن هل الجرائم المستحدثة تحتاج لقواعد ناظمة تختلف عن القواعد التقليدية وتحدد المسؤولية الجنائية لمرتكبي هذه الأفعال^٣؟

^١ طالب محمد جواد عباس، عبد الجبار ضاحي عواد، "جرائم تقنية المعلومات وإثباتها"، مجلة كلية الرافدين الجامعية للعلوم، العدد ٢٨، السنة الثالثة عشر، ٢٠١١، ص ٥٣.

^٢ خالد حامد مصطفى، "المسؤولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الاجتماعي"، مجلة رؤى استراتيجية، مركز الإمارات للدراسات والبحوث الاستراتيجية، المجلد الأول، العدد ٢، مارس ٢٠١٣، ص ٨.

^٣ محمد عزت فاضل، نوفل علي الصفو، "مرجع سابق"، ص ٣٣.

إن تزايد الجرائم المتعلقة بتقنية المعلومات دفع بالدول المتمدنة إلى وضع تشريعات جنائية خاصة لمكافحة هذه الجرائم التي تعتبرها ظاهرة مستحدثة على علم الإجرام، فقد نشر معهد "ستانفورد" في الولايات المتحدة الأمريكية أول جريمة ترتكب بإساءة استخدام الكمبيوتر عام ١٩٥٨، مما سمح لظهور مجموعة من القوانين الوطنية والدولية^١.

وقد أرجع الفقه الجنائي هذه الجرائم المستخدمة بوسائل تقنية المعلومات لعام ١٩٦٠ التي استخدم فيها الحاسوب، وجرائم الإنترنت لعام ١٩٨٨، فكانت البدايات الأولى لهذه الجرائم باستخدام جرائم العدوان الفيروسي والمعروفة قانونياً "جريمة دودة موريس"^٢، تعود واقعة جريمة "دودة موريس" إلى ١٩٨٨/١١/٢، وهي أول جريمة ترتكب عبر الإنترنت إذ استطاع موريس أن ينشر فيروس إلكتروني تمكن من خلاله تدمير آلاف الحواسيب المرتبطة بالإنترنت وقدرت الخسائر مائة مليون دولار^٣.

وانطلاقاً من ذلك وللحفاظ على خصوصية الأفراد من الانتهاك وحمايتهم بدأت عملية التوجهات العالمية لوضع الضوابط القانونية لهذه الجرائم فكان أول الفقهاء المتقدمين لذلك Alan Westin، من خلال مؤلفه Privacy And Freedom، وكتاب Miller حول The Assault On Privacy، وكتاب Private Lives And Public Surveillance لمؤلفه Rule؛ ولتضييق منع استخدام البيانات الشخصية للأفراد عبر تقنية المعلومات عمدت أمريكا وأوروبا في البداية إلى وضع حزمة من المبادئ التي سميت "مبادئ السلوك" أهمها التأكيد على الاستخدام العادل للبيانات الشخصية والتدخل بالحدود الدنيا والتضييق على استخدام البيانات، هذا المفهوم -الخصوصية - كان البداية والدافع لتقنين الوسائل المعلوماتية مع تطور إنشاء البنوك المعلوماتية وإجراء عمليات المعالجة والتحليل بواسطة الكمبيوتر، ويجب التنكير أن أول معالجة

^١ للمزيد أنظر، عبد العال الديري، محمد صادق إسماعيل، "مرجع السابق"، ص ٨-٩.

^٢ عبد العال الديري، محمد صادق إسماعيل، "مرجع سابق"، ص ٢٣.

^٣ محمد طارق عبد الرؤوف الخن، "مرجع سابق"، ص ٢٩-٣٠.

^٤ تباينت التعريفات المعطاة لمفهوم الخصوصية فمنهم من أعطاه طابع إيجابي من حيث أنها الحق في الحفاظ على حرمة الحياة الخاصة، أما التعريف السلبي فقد اعتبرها نقيض للحياة الخاصة، فترتبط الخصوصية بحرية الفرد في الإفصاح عن أسراره ومكنوناته للغير في الوقت الذي يراه مناسب ولمن يريد الإفصاح أمامهم ويمكن أن تكون الخصوصية مادية معلوماتية أو خصوصية الفرد في اتخاذ قراراته، بمعنى آخر تعني الخصوصية حرية الفرد في جسده وسلوكه وأفكاره. - مروة زين العابدين صالح، "الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني"، مركز الدراسات العربية للنشر والتوزيع، مصر-الجيزة، ٢٠١٦، ط ١، ص ٣٥-٣٦.

قانونية شرعت حماية البيانات في "ولاية هيس الألمانية" عام ١٩٧٠، وتلتها السويد عام ١٩٧٣ ثم الولايات المتحدة عام ١٩٧٤ ثم ألمانيا على المستوى الفدرالي عام ١٩٧٧ وفرنسا عام ١٩٧٨.^١

وتلا ذلك أن أصدر مجلس أوروبا اتفاقية حماية الفرد من مخاطر المعالجة الآلية للبيانات الشخصية، كما وضعت منظمة التعاون الاقتصادي والتنمية دليل إرشادي وقواعد تضمن حماية نقل البيانات في كل مرحلة من مرحلة الجمع إلى التخزين والمعالجة ومن ثم النشر.^٢

انطلاقاً مما سبق، يتبين أن المعضلة الأساسية في البحث عن الطبيعة القانونية لجرائم تقنية المعلومات تكمن في عدم انطباق النصوص التقليدية القانونية عليها كون هذه الجرائم غير المادية تتطلب معالجة تشريعية تتسجم مع طبيعة هذه الجرائم، وهذا ما أكدته الفقه الجنائي في أسانيده في عدم كفاية القواعد التقليدية خصوصاً في مسألة الإثبات، فيمكن لمرتكب الجريمة أن يدمر كافة الأدلة في وقت قصير قبل كشف العملية الإجرامية أو يمكن أن تكون المعلومات أو البيانات التي يجري البحث عنها مشفرة ويصعب الوصول إليها إلا عن طريق صاحبها، ومما يزيد المسألة تعقيداً هو البحث في البداية عن مدى مشروعية إجبار الشخص على فك الشيفرة أولاً، وهناك صعوبة أخرى في كيفية ملاحقة الجناة ممن يرتكبوا جرائمهم في دول أخرى لا تربط الدولة محل العمل الإجرامي باتفاقيات تسليم المجرمين أو قد يكون هذا السلوك في بعض الدول غير مجرم، ونظراً لاتساع الحدود الجغرافية لهذه الجريمة وصعوبة إثباتها يجب توسيع الحماية الجنائية للسلوك الإجرامي النامي عن وسائل التقنية المعلوماتية نظراً لطبيعة الخاصة المحيطة بها، لذلك يفترض أن تواكب القواعد الإجرائية الجنائية في مجال الضبط والتفتيش والتحقيق والاختصاص القضائي طبيعة الجريمة محل البحث عل نحو يضمن الحق في حماية الحق في الوصول للمعلومات وبين متطلبات العدالة الجنائية.^٣

^١ للمزيد أنظر، مروة زين العابدين صالح، "مرجع سابق"، ص ٤١-٤٧.

^٢ مروة زين العابدين صالح، "مرجع سابق"، ص ٤٧.

^٣ نوفل الصفر ومحمد عزت فاضل، "مرجع سابق"، ص ٣٤-٣٥.

الفرع الثاني: موقف الفقه من طبيعة جرائم تقنية المعلومات.

اختلف الفقه الجنائي حول وضع تعريف شامل لمفهوم جريمة تقنية المعلومات فمنهم مع استند على العديد من المعايير أولها المعيار الموضوعي الذي قدمته منظمة التعاون الاقتصادي والتنمية عام ١٩٨٣ في اجتماعها المعقد في باريس بكونها "كل سلوك للمناقشات غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها"، وعرفها البعض الآخر بكونها كل سلوك سواء إيجابي أو سلبي يتم بموجبه الاعتداء على المعلومات والبيانات والبرامج للاستفادة منها بأي صورة من الصور؛ إلى جانب هذا المعيار هناك من اعتمد على معيار وسيلة ارتكاب الجريمة منهم جون فوستر وبال الذي عرفها بأنها: "فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية"، أما David Thompson فقد اعتمد على معيار السمات الشخصية للجاني وعرفها بأنها جريمة أحد متطلباتها أن يعرف الجاني تقنية الحاسوب^١.

وعلى الرغم من المعايير السابقة إلا أنه يمكن استخلاص الطبيعة القانونية لجرائم تقنية المعلومات من خلال تحديد المجال الذي ترتكب فيه إلى جانب محل ارتكاب الجريمة الذي وقع عليه الاعتداء^٢.

وذهب جانب من الفقه لتحديد الطبيعة القانونية لجرائم تقنية المعلومات إلى ضرورة إخضاع هذه الجرائم للقواعد العامة وهذا ما عرضه فريق من الفقهاء بكون إخضاعها للقواعد العامة التقليدية يؤدي إلى تشويه المبادئ المستقرة في النظام الجنائي، لذلك وجب الإسراع في وضع أطرها القانونية لتفادي التأثيرات السلبية ليس فقط على الجانب الجنائي بل الجوانب الأخرى كتأثيرها على العلاقات العقدية والإثبات والعمل المصرفي والحقوق العينية والاستثمار والتجارة وغيرها من الجوانب الأخرى المرتبطة بوسائل تقنية المعلومات^٣.

وما يدفع أيضا بضرورة توفير إطار قانوني لهذه الجرائم هو عدم كفاية الوسائل التقنية في حماية برامج الحاسوب، إلى جانب ضخامة الاستثمارات المالية والجهود البشرية في سبيل

^١ انظر: نوفل الصفو ومحمد عزت، "مرجع سابق"، ص ٢٨٧-٢٨٨.

^٢ صغير يوسف، "الجريمة المرتكبة عبر الإنترنت"، جامعة مولود معمري، الجزائر، رسالة لنيل شهادة الماجستير، ٢٠١٣، ص ٤٤.

^٣ انظر: نوفل الصفو ومحمد عزت، "مرجع سابق"، ص ٢.

إنتاج برامج حاسوب، لذلك باتت الضرورة ملحة لحماية هذه البرامج لتفادي أثار الجرائم الإلكترونية الواقعة على الأموال والأشخاص بشكل خاص^١.

الفرع الثالث: موقف التشريعات المقارنة من طبيعة جرائم تقنية المعلومات.

لم يعرف المشرع البحريني الجريمة المعلوماتية في قانون جرائم تقنية المعلومات رقم (٦٠) لسنة ٢٠١٤^٢، بل اكتفى بتعريف بعض المصطلحات كالمشرع الإماراتي، هذا التوسع والاختلاف في التوصيف المفاهيمي لتقنية المعلومات سيؤدي إلى التوسع في مفهوم الجريمة المعلوماتية، على اعتبار أن تحديد المصطلحات والمفاهيم هي الركيزة الأساسية للتشريع وعن طريقها يمكن ضبط ما المقصود بالجريمة المعلوماتية ويسهل معرفة خصائصها ووسائلها والضوابط القانونية التي يمكن التحكم بها^٣.

ذهب المشرع الإماراتي في تحديده للطبيعة القانونية للجرائم المعلوماتية من خلال إصداره لقانون رقم (٢) لسنة ٢٠٠٦ وتعديلاته بالقانون الاتحادي رقم (٥) لسنة ٢٠١٢ الذي تضمن تعريفات جديدة لمكافحة جرائم تقنية المعلومات مع تغليظ العقوبة، كما تم تعديله بقانون رقم (١٢) لسنة ٢٠١٦، وقد تضمن هذا القانون وتعديلاته في مواده تحديد الأفعال التي تشكل خطراً للنظم التقنية المستخدمة وأدواتها المختلفة وحدد العقوبات المتعلقة بارتكاب هذه الأفعال من المادة ٢ إلى المادة ٢٣ من هذا القانون^٤، وهي على النحو الآتي:

١. التوصل بغير وجه حق إلى أي موقع أو نظام معلومات.
٢. الإلغاء أو الحذف أو التدمير أو الإنشاء أو الإتلاف أو التغيير أو إعادة النشر للبيانات والمعلومات الموجودة بالموقع أو النظام المعلوماتي.

^١ منوفل علي الصفو ومحمد عزت، "مرجع سابق"، ص ٣٥.

^٢ قانون جرائم تقنية المعلومات البحريني رقم (٦٠) لسنة ٢٠١٤، منشور على الرابط المختصر التالي:

<http://cutt.us/dQWsp>

^٣ لورنس سعيد الحوامدة، "الجرائم المعلوماتية أركانها وآلية مكافحتها -دراسة تحليلية مقارنة"، مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، ٢٠١٦-٢٠١٧، ص ٩.

^٤ راجع في ذلك القانون الاتحادي رقم (٢) لسنة ٢٠٠٦ وتعديلاته لسنة ٢٠١٢، منشور على البوابة الرسمية

لحكومة الإمارات العربية المتحدة على الموقع الرسمي التالي: www.government.ae

٣. التزوير الإلكتروني للمستندات الإلكترونية الحكومية الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية.
٤. الاستعمال للمستند الإلكتروني المزور مع العلم بتزويره.
٥. الإعاقة أو تعطيل الوصول إلى الخدمة أو الأجهزة والبرامج ومصادر البيانات والمعلومات بأية وسيلة كانت.
٦. الإيقاف أو التعطيل أو التدمير أو المسح أو الحذف أو الإتلاف لمحتويات الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.
٧. استخدام الشبكة المعلوماتية لأغراض التهديد والابتزاز للأشخاص أو للاستيلاء على إحدى وسائل تقنية المعلومات.
٨. استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات للوصول بدون وجه حق للبيانات والأرقام الخاصة بالبطاقة الائتمانية.
٩. استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات للإساءة للشعائر الإسلامية أو أحد المقدسات الدينية^١.

أما المشرع السعودي في تحديده للطبيعة القانونية لجرائم تقنية المعلومات فقد أرتكز في البداية على تعريف الجريمة المعلوماتية في المادة الأولى، إذ عرفها بأنها "أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"، وقد توسع المشرع السعودي في المواد (٣، ٤، ٥، ٦، ٧، ٨، ٩)، في توصيف الجرائم المعلوماتية المعاقب عليها وشدد العقوبات على مرتكبيها حرصاً منه على تفادي انتشار هذه الظاهرة^٢.

وشملت الجرائم المعاقب عليها أشكالاً عدة تمثلت في التنصت على ما هو مرسل أو التقاطه أو اعتراضه والدخول غير المشروع لتهديد شخص أو ابتزازه، والمساس بالحياة الخاصة والتشهير بالآخرين وإلحاق الضرر بهم، والاستيلاء على مال أو بيانات الغير، أو الدخول لبيانات خاصة والتصرف فيها وإيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو التصرف فيها، وإنتاج ما من شأنه المساس بالنظام العام أو القيم الدينية أو حرمة الحياة الخاصة، وإنشاء موقع للاتجار في الجنس البشري أو المواد الإباحية أو المخدرات أو لمنظمات إرهابية أو ترويج أفكارها أو نشر

^١ عبيد صالح حسن، "سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية"، مجلة الفكر الشرطي، المجلد

الرابع والعشرون، العدد ٩٥، أكتوبر ٢٠١٥، ص ٤٣-٤٤.

^٢ نظام مكافحة جرائم المعلوماتية الصادر بتعميم وزير العدل بالنيابة الموافق ١٤٢٨/٣/٧، الموافق ٢٠٠٧/٣/٢٦. جريدة أم القرى، الجريدة الرسمية للملكة العربية السعودية، العدد ٤١٤٤، بتاريخ ٢٥/٣/١٤٢٨هـ، ص ٦٠٥.

كيفية صنع المتفجرات أو محاولة الحصول على بيانات تمس الأمن الداخلي أو الخارجي أو اقتصادها الوطني^١.

من خلال مراجعتنا للدول محل البحث والمقارنة وقوانينها المتعلقة بجرائم تقنية المعلومات على مختلف مفاهيمها المستخدمة نلاحظ أن القانون البحريني ونظام مكافحة الجرائم السعودي لم يركزا على النتيجة الإجرامية، مثال على ذلك لم ينص الطرفين بشكل صريح على سرقة المعلومات لأهميتها في مكافحة الجرائم المعلوماتية، أما المشرع الإماراتي من القانون الاتحادي رقم (٢) لسنة ٢٠٠٦ وتعديلاته لسنة ٢٠١٢ فقد استخدم كلمة نسخ في المادة (٢) الفقرة الثانية بقوله: "تكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسون ألف درهم أو بإحدى هاتين العقوبتين إذا ترتب على أي فعل من الأفعال المنصوص عليها بالفقرة (١) من هذه المادة إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات".

ويرى الباحث أن الجرائم المستخدمة بوسائل تقنية المعلومات من الجرائم المستجدة والمستحدثة تهدد المجتمعات المعاصرة نتيجة سرعة انتشارها وسهولة القيام بها وحجم الخسائر الناجمة عن ارتكابها وصعوبة إثباتها، في ظل اعتبار وسيلة تقنية المعلومات محدد من محددات تطور المجتمعات والدول وهو المحدد الاستراتيجي للبناء الثقافي والتطور الاقتصادي.

^١ راجع في ذلك، "نظام مكافحة جرائم المعلوماتية السعودي".

الفصل الأول

ماهية جريمة الاحتيال

باستخدام وسائل تقنية المعلومات

الفصل الأول

ماهية جريمة الاحتيال باستخدام وسائل تقنية المعلومات

تمهيد وتقسيم: -

إن تطور التقنية الحديثة فرضت على المجتمعات مواكبة هذه الطفرة من خلال إدخال هذه التقنية في تعاملاتها اليومية لما لها من مميزات، فهي توفر الوقت والجهد وتعطي نتائج أكثر دقة، وكما أن لهذه التقنية إيجابيات فهي بالمقابل لها سلبيات إذ ساهمت بظهور نوع جديد من الجرائم باستخدام وسائل تقنية المعلومات وهي الجرائم المستحدثة.

وتعد جريمة الاحتيال المعلوماتي صورة من صور الجرائم الواقعة باستخدام تقنية المعلومات، فهي حديثة بأسلوب ارتكابها كما أن نتائجها وأهدافها أيضاً لا تخلو من الحداثة، فاستخدام التقنية الحديثة أفسح المجال أمام مستخدمي هذه التقنية بالطرق السلبية أن يقوموا بعمليات الاحتيال باستخدام وسائل تقنية المعلومات كما سنبين ذلك في الدراسة لاحقاً.

إن لكل تقنية مستحدثة ينشأ عنها في أي لحظة وفي أي مرحلة من مراحل تطورها ظاهرة إجرامية خاصة بها، فجريمة الاحتيال تعد صورة من صور الجريمة المعلوماتية، ولإحاطة أكثر بجريمة الاحتيال المعلوماتي سيتم تقسيم هذا الفصل إلى ثلاثة مباحث وعلى النحو الآتي:

المبحث الأول: مفهوم جريمة الاحتيال باستخدام وسائل تقنية المعلومات.

المبحث الثاني: ذاتية جريمة الاحتيال باستخدام وسائل تقنية المعلومات وصورها.

المبحث الثالث: مدى انسجام جريمة الاحتيال باستخدام وسائل تقنية المعلومات مع مفهومها التقليدي.

المبحث الأول

مفهوم جريمة الاحتيال باستخدام وسائل تقنية المعلومات

مع انتشار وسائل تقنية المعلومات في المجتمعات وتواتر استخدامات هذه التقنية، بنفس الوقت اتسعت رقعة وقوع جريمة الاحتيال، فلذلك يعد الاحتيال من الظواهر الإجرامية المتفشية في معظم المجتمعات، ذلك بسبب الخصائص التي تمتاز بها هذه الجريمة.

ولا يمكن تناول جريمة الاحتيال باستخدام وسائل تقنية المعلومات قبل التعريف بهذه الجريمة إلا من خلال دراسة خصائصها والتطرق إلى نشأة وتطور هذه الجريمة، بالإضافة إلى دراسة مدى خطورة هذه الجريمة، والآثار المترتبة عليها، لذلك قُسم هذا المبحث إلى ثلاثة مطالب كالآتي:

المطلب الأول: نشأة جريمة الاحتيال باستخدام وسائل تقنية المعلومات وتطورها.

المطلب الثاني: تعريف جريمة الاحتيال باستخدام وسائل تقنية المعلومات وخصائصها.

المطلب الثالث: الآثار المترتبة على استخدام وسائل تقنية المعلومات في جريمة الاحتيال.

المطلب الأول

نشأة جريمة الاحتيال باستخدام وسائل تقنية المعلومات وتطورها

تعتبر جريمة الاحتيال المعلوماتي من الجرائم المستحدثة، ومع ظهور التقنية الحديثة في وسائل تقنية المعلومات وتطورها أفرزت أنواعاً مختلفة من الجرائم التي ترتكب بوسائل تختلف عن تلك الوسائل التقليدية، وتمتاز هذه الوسائل بحدائتها في ظل التطور السريع في وسائل التكنولوجيا الحديثة، ولطالما ارتبطت نشأة وتطور جريمة الاحتيال المعلوماتي بنشأة وسائل التقنية الحديثة وأبرزها المتعلقة بشبكة الإنترنت وتكنولوجيا المعلومات والهاتف النقال وما ينبثق عن هذه التقنية من وسائل اتصال تساهم بشكل أو بآخر بظهور جريمة الاحتيال المعلوماتي، وقد تعددت مراحل تطور هذه الجريمة، وليبيان ذلك سنقسم المطلب إلى فرعين كالآتي:

الفرع الأول: المرحلة الأولى.

الفرع الثاني: المرحلة الثانية.

الفرع الأول: المرحلة الأولى

لقد مرت جريمة الاحتيال المعلوماتي بعدة مراحل تبعاً لتطور وسائل تقنية المعلومات فبدأت المرحلة الأولى بظهور استخدام الحاسب الآلي وربط مجموعة من الحواسيب فيما بينها في شبكة واحدة، فظهر مع هذا الربط جرائم تتعلق بالتلاعب بالبيانات المخزنة وتدمير أنظمة الحاسب الآلي والتجسس المعلوماتي، فكانت تلك المرحلة في بداية الستينيات من القرن الماضي، في الوقت ذاته شكلت هذه الظاهرة موضوع تساؤل رئيسي حول ما إذا كانت هذه الوقائع مجرد حالة عابرة أم ظاهرة جرمية مستجدة؟ وهل هي جرائم بالمعنى القانوني أم مجرد سلوكيات أخلاقية في مجال المعلوماتية؟ إلا أنها بقيت محصورة في إطار السلوك اللاأخلاقي دون النطاق القانوني، ولكن مع تنامي هذه الظاهرة خلال سبعينيات القرن الماضي بدأ الحديث يدور عنها كظاهرة إجرامية جديدة.

فمنذ أن حققت شبكة الإنترنت انتشاراً عالمياً دخلت إليها عمليات الاحتيال والنصب من أبواب مختلفة وكانت أشكال الاحتيال الأولى في مواقع الإنترنت، بعدها انتقلت إلى وسائل الدفع الإلكتروني معتمداً على بساطة الناس وعفوية تعاملهم مع سواهم، والمبالغ التي يتم الاستيلاء عليها قد تصل إلى مئات الملايين من الدولارات وخصوصاً عندما يمنح أحدهم رقم حسابه المصرفي لشخص عبر البريد الإلكتروني، وتنتشر مراكز عمل المحتالين في البلدان التي تنخفض فيها الرقابة على النشاط المعلوماتي وخصوصاً في أفريقيا^١.

فتطور جريمة الاحتيال المعلوماتي مرتبط بتطور شبكة الإنترنت من خلال التعامل الواسع لمستخدمي هذه الشبكة، كما ارتبط تطور هذه الشبكة بتطور السلوك الاجرامي والتي نتج عنه نشأة جريمة الاحتيال المعلوماتي والتي تعد نوعاً من أنواع الجريمة المعلوماتية بشكل عام، وبمعنى آخر إن الحديث عن نشأة جريمة الاحتيال المعلوماتي متصل اتصال كلي بنشأة وتطور الجريمة المعلوماتية^٢.

ففي العام ١٩٦٤م أوكلت وزارة الدفاع الأمريكية مهمة إنشاء شبكة من الحواسيب تكون قادرة على الاستمرار في العمل في حال حدوث ضربات قد تؤدي إلى فقدان النظام المعلوماتي الخاص بالترسانة النووية^٣.

وفي العام ١٩٦٩ تم إنشاء الشركة المتخصصة بغرض عدم فقدان النظام المعلوماتي، وهي شبكة خاصة تحمل اسم (Arpanet)، حيث تم ربط أربعة حواسيب آلية ضخمة في أول عملية تجريبية. وفي العام ١٩٧٤ تم أوصول الأربانت بمعظم جامعات الولايات المتحدة الأمريكية وفي العام ١٩٧٣م بدأ الاتصال بهذه الشبكة من إنجلترا والنرويج، وهذا ما أفرز الحاجة إلى إيجاد وسيلة تتم من خلالها عمل الحواسيب واتصالها ببعضها بما يضمن التخاطب باللغات المختلفة وقرائنها، وهذا ما تم فعلياً في اكتشاف بروتوكول الإنترنت (TCP/IP)^٤.

^١ محمد محرم علي، "جريمة النصب والاحتيال والتجارة الالكترونية"، دار النهضة العربية، القاهرة، ١٩٩٨م، ص ٨.

^٢ سالم الجبوري، "جريمة الاحتيال الإلكتروني دراسة مقارنة"، مكتبة زين الحقوقية، ط ١، ٢٠١٨م، ص ٤٥.

^٣ محمد طارق الخن، "مرجع سابق"، ص ٢٠.

^٤ (TCP/IP) هو بروتوكول تقني حول الاتصالات يتضمن بروتوكولين هما: بروتوكول التحكم في النقل Transfer Control Protocol وبروتوكول الإنترنت Internet Protocol عبد الحسن الحسيني، "القاموس الموسوعي في المعلومات والاتصالات المعلوماتية القانونية"، مكتبة صادر، بيروت، ط ١، ٢٠٠٤م، ص ٧٩٢.

وفي العام ١٩٨٦ تم إدخال أربانت إلى مؤسسة العلوم الوطنية وقطاع الطيران المدني ووكالة الفضاء الأمريكية وإدارة الطاقة، فقد أصبحت هذه التقنية الحديثة تدخل في كافة أشكال البحث العلمي ومعظم قطاعات الولايات المتحدة الأمريكية.

ومع نهاية الحرب الباردة والتي كان إحدى نتائجها سقوط وتفكك الاتحاد السوفيتي لم يعد جدوى من انحصار عمل هذه التقنية في المجال العسكري فقط، مما فتح المجال من الاستفادة من هذه التقنية فأطلقت وزارة الدفاع الأمريكية هذه الشبكة لتكون في متناول الجميع مما يخدم كافة قطاعات الدولة، فأصبح لها إدارة خاصة ربحية وتحولت أربانت إلى مسماها الحالي وهو Internet.

وشبكة الإنترنت كما أشرنا سابقاً هي شبكة تسمح بالربط بين عدة شبكات معلوماتية متعددة ومتنوعة وتم بواسطتها تبادل المعلومات بفضل استخدام بروتوكول موحد للبريد والملفات وللمعلومات والآراء وكذلك بنوك المعلومات^١.

ولم تكن المعاملات التجارية عبر شبكة الإنترنت مصرح بها بل كانت محظورة، لكن مع تطور شبكة المعلومات الدولية (www)^٢، اكتسبت هذه الشبكة طابعاً شعبياً فتنامى لدى جميع الشركات وأصحاب الأعمال الحرة والتجارية ضرورة امتلاك موقعاً عبر هذه الشبكة للتسويق لمنتجاتهم.

فانتشار هذه التقنية الحديثة ساهم بشكل كبير في ظهور جريمة الاحتيال المعلوماتي نتيجة سوء استخدام شبكة الإنترنت ووسائل التقنية الحديثة، مما تسبب بمشاكل اقتصادية وأمنية فظهر المتطفلون والمحتالون مما عرض أمن المستخدمين لهذه التقنية للخطر بالاستيلاء على معلوماتهم وأموالهم وتدمير ملفاتهم الخاصة وتحريف البرامج الخاصة بهذه التقنية للاستخدام في الاحتيال والنصب والغش^٣.

^١ سالم الجبوري، "مرجع سابق"، ص ٤٧.

^٢ اختصار لشبكة المعلومات الدولية (Web World wide)

^٣ عبد الحميد بسيوني، "طرق وبرامج الهاكرز وقرصنة المعلومات"، دار الكتب العلمية، للنشر والتوزيع، القاهرة، ٢٠١٣، ص ٥٥.

الفرع الثاني: المرحلة الثانية

انتشار شبكة الإنترنت بشكل سريع بعد ما كانت مجرد شبكة صغيرة وتحولت إلى بيئة متكاملة للاستثمار والعمل والإنتاج والإعلام والاتصال والحصول على المعلومات حتى أصبحت من مستلزمات الحياة، فكانت في بداية ظهورها لم تكن الأهمية تنصب على مسائل الأمن بقدر ما كان الاهتمام يتمحور حول بناء وتطوير الشبكة وتوسيع مجال نشاطها واستخدامها، دون مراعاة تحديات أمن المعلومات، فالاهتمام تركز على الربط والدخول ولم يكن الأمن من بين الموضوعات الهامة في بناء الشبكة وهذه الثغرة التي شجعت تنامي جريمة الاختيال المعلوماتي مما تسبب بأضرار بالغة، مما زاد من ضرورة الحاجة إلى توفير معايير الأمن للشبكة^١.

فقد تعددت الوقائع والأحداث التي تعتبر أمثلة حية على جرائم الاختيال المعلوماتي عبر العالم، والتي تزايدت وتيرتها بتطور المنظومة المعلوماتية ووسائل تقنية المعلومات، فزادت الحاجة إلى ضرورة مواجهة هذه المخاطر التي أفرزتها هذه الظواهر الإجرامية، فبدأ التركيز على الصعيد الدولي في مجال التعاون المشترك والمتمثل في المعاهدات والمؤتمرات الدولية وفي إصدار القوانين والتشريعات الخاصة بهذه الجرائم على الصعيد الوطني في محاولة للحد من هذه الظاهرة^٢.

^١ محمد طارق الخن، "مرجع سابق"، ص ٣٦-٣٧.

^٢ سليمان أحمد فضل، "المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية"، القاهرة، ٢٠٠٧م، ص ١٩٧.

المطلب الثاني

تعريف جريمة الاحتيال باستخدام وسائل تقنية المعلومات وخصائصها

الاحتيال سلوك إجرامي بموجبه يقوم الجاني بخداع المجني عليه بطريقة تؤدي الى الاقتناع المباشر بالمظهر الخارجي - أي انخدع بحيلة الجاني-، كما أن للاحتيال أدوات متعددة وأساليب تقليدية بالإضافة إلى الأساليب التي ظهرت في ظل تطور التقنية الحديثة، وهنا نحن بصدد تعريف جريمة الاحتيال باستخدام وسائل تقنية المعلومات، كما سنقوم بتقسيم المطلب إلى فرعين كالآتي:

الفرع الأول: تعريف جريمة الاحتيال باستخدام وسائل تقنية المعلومات.

الفرع الثاني: خصائص جريمة الاحتيال باستخدام وسائل تقنية المعلومات.

الفرع الأول: تعريف جريمة الاحتيال باستخدام وسائل تقنية المعلومات.

سنستعرض تعريف جريمة الاحتيال وفقاً لمفهومها اللغوي والفقهية، بالإضافة للتعريف القانوني للاحتيال باستخدام وسائل تقنية المعلومات.

أولاً: التعريف اللغوي لجريمة الاحتيال.

الاحتيال هو الحُذْق، وجودة النظر، والقدرة على دقة التصرف، ويقال رجل حُول: ذو حيل، ويقال هو أحول من أي أكثر حيله، وما أحوله، ورجل حول، بتشديد الواو أي بصير بتحويل الامور، ويقال تحول الرجل وأحتال إذا طلب الحيلة، والاحتيال والمحاولة: مطالبتك الشيء بالحيل^١. والحيلة لغة وعرفاً المكر والخديعة والكيد لكل فعل يقصد فاعلة به خلاف ما يقتضيه ظاهرة^٢.

^١ ابن منظور، لسان العرب المحيط ، الجزء الاول دار اللسان العربي، بيروت، بدون سنة طبع، ص ٧٥٩

^٢ اياد حسين عباس العزاوي، جريمة الاحتيال في القانون العراقي، دراسة مقارنة، رسالة ماجستير مقدمة إلى

كلية القانون والسياسة جامعة بغداد، ١٩٨٨، ص ٣١

مما سبق يتضح أن للاحتيال معنيان في اللغة وهي: الحذق أي جودة النظر والقدرة على التصور، والمعنى الآخر هو ما يتوصل به إلى حالة خفية بقلب الحقائق وتزوير المظاهر.

ثانياً: التعريف الفقهي للاحتيال.

تتنوع تعريفات الاحتيال اصطلاحاً بتنوع واختلاف الزاوية التي ينظر منها كل فقيه فيعرف الاحتيال على أنه "سقوط الواجب أو حل الحرام بفعل ما لم يقصد به ما جعل ذلك الفعل له"^١.

كما وعرف الاحتيال على أنه "نوع مخصوص من التصرف والعمل الذي يتحول به فاعله من حال إلى حال، ثم غلب عليها بالعرف استعمالها في سلوك الطرق الخفية التي يتوصل بها الرجل إلى حصول غرضه بحيث لا يتفطن له إلا بنوع من الذكاء والفتنة فهذا أخص من موضوعها في أصل اللغة، وسواء كان المقصود أمراً جائزاً أو محرماً، أخص من هذا استعمالها في التوصل إلى الغرض الممنوع منه شرعاً أو عقلاً أو عادة، فهذا هو الغالب عليها في عرف الناس"^٢.

ويعرف الاحتيال على أنه "كل تظاهر أو إحياء يكون صالحاً لإيقاع المجني عليه في الغلط بطريقة تؤدي إلى الاقتناع المباشر بالمظهر المادي الخارجي، أي أن المجني عليه في جريمة الاحتيال هو من حازت عليه حيلة الجاني، فانخدع بها وسلمه ماله"^٣.

وفي الفقه القانون الجنائي، تعاريف متعددة للاحتيال فمنهم من عرفه بأنه "الاستيلاء على شيء مملوك بطريقة احتيالية بقصد تملك ذلك الشيء"^٤. وعرف أيضاً بأنه: "سلوك احتيالي ينتهج منهج الحوسبة بنية الحصول على امتياز مالي"^٥.

^١ أحمد بن تيمية، "الفتاوي الكبرى"، تحقيق محمد عبد القادر عطا، دار الكتب العلمية، بيروت، ط٣، ١٤٢٥هـ، ج ٣، ص ٩٩.

^٢ شمس الدين ابن القيم، "إعلام الموقعين عن رب العالمين"، تحقيق وضبط عبد الرحمن وكيل، دار إحياء التراث العربي، بيروت، د.ط، ١٤١٣هـ، ج ٣، ص ٣٠٤.

^٣ أنظر: على حسن الطوالة، "الجرائم الالكترونية"، جامعة العلوم التطبيقية - مملكة البحرين، مؤسسة فخراوي للدراسات والنشر - البحرين، الطبعة الثانية، ٢٠٠٩م، ص ١٨٠.

^٤ مصطفى هرجة، "النصب وخيانة الأمانة وأحكام الشيك"، دارالثقافة للطباعة والنشر، القاهرة، ١٩٨٩م، ص ٧.

^٥ راجع في ذلك، عمر بن يونس، "الجرائم الناشئة عن استخدام الإنترنت"، دار النهضة العربية، القاهرة، ٢٠٠٤م، ط١، ص ٤١١.

ويعرف الاحتيال على أنه "كل تظاهر أو إيهاء يكون صالحاً لإيقاع المجني عليه في الغلط يؤدي إلى الاقتناع المباشر بالمظهر المادي الخارجي، أي أن المجني عليه في جريمة الاحتيال هو من حازت عليه حيلة الجاني فانخدع بها وسلمه مالا"^١.

كما ويعرف الاحتيال على أنه "الاستيلاء على مال منقول مملوك للغير عن طريق مناورات احتيالية بخداعه وحمله على تسليم ذلك المال"^٢.

ويرى الباحث بأن التعريف اللغوي للاحتيال لا يختلف عن التعريف الاصطلاحي أو الفقهي فالتقارب بينهما واضح من خلال المعنى العام للاحتيال باعتباره كل فعل كيد، إلا أن الفقهاء قاموا بتعريف الاحتيال اصطلاحاً من منظور شرعي، وعليه يشترط في الاحتيال أن يقوم بطريقة الإيهاء بمشروعية الفعل والذي يتولد عنه اقتناع المجني عليه فيقوم طواعية بتسليم المال للجاني، وهنا تجدر الإشارة بأن هذا المفهوم لا يعدو أن يكون تقليدي حيث لم يواكب التطور الحادث في طبيعة المال وهذا ما يتولد مفهوم تكييف الأشياء المادية منها والمعنوية بالمال.

ثالثاً: التعريف القانوني للاحتيال باستخدام وسائل تقنية المعلومات.

لم تخل التشريعات المقارنة من تحديد مفهوم الاحتيال بصورته التقليدية، فقد أشار المشرع البحريني إلى الاحتيال بطريقة غير مباشرة وذلك بنص المادة (٢٦) من المرسوم بقانون رقم (٥٤) لسنة ٢٠١٨ بإصدار قانون الخطابات والمعاملات الإلكترونية، البند (٣) والتي جاء فيها "... كل من أنشأ أو نشر أو حرّف أو استعمل شهادة أو توقيعاً إلكترونياً أو ختماً إلكترونياً، أو قام بأية خدمة ثقة أخرى لغرض احتيالي أو لأي غرض غير مشروع"....

كما أشار المشرع البحريني إلى الصور التي يعاقب عليها القانون لجريمة الاحتيال المعلوماتي وجاء في المادة (٨) من جرائم تقنية المعلومات بأنه "يعاقب بالحبس من توصل دون مسوغ قانوني إلى الاستيلاء على مال مملوك للغير أو حصل على أية مزية لنفسه أو لغيره أو

^١ محمد الشوابكة، "جرائم الحاسوب والإنترنت- الجريمة المعلوماتية"، دار النهضة العربية، القاهرة، ط١، ٢٠٠٧م، ص ١٨٥.

^٢ محمود نجيب حسني، "جرائم الاعتداء على الأموال في قانون العقوبات اللبناني"، منشورات الحلبي الحقوقية، ١٩٩٨م، ط٣، ص ٣٧٩.

إلى توقيع سند أو إلغائه أو إتلافه أو تعديله باتخاذ اسم كاذب أو صفة غير صحيحة أو بالاستعانة بطريقة احتيالية^١.

وهنا يتعين على المشرع البحريني أن يورد مادة خاصة بالاحتيال المعلوماتي في ذات القانون ويفصلها عن جريمة الدخول غير المشروع، فينبغي إعادة النظر في المادة (٨) حيث أنها اشتملت على نوعين من الجرائم: أما الأولى فهي الدخول دون مسوغ قانوني أي الدخول غير المشروع في نطاق جرائم المعلومات تعتبر جريمة منفصلة يقتضي إيراد نص خاص فيها، أما الثانية فهي جريمة الاحتيال المعلوماتي التي لا تقتصر فقط بالدخول غير المشروع أو دون مسوغ قانوني، فقد يكون الدخول مشروعاً وبعلم المجني عليه إلا أن ذلك لا يمنع بأن يقوم الجاني بخداع المجني عليه والإيحاء له بأن ما يقوم به مشروعاً، وعليه يقوم هذا الأخير بتسليمه المال طواعيةً.

ومما سبق نستنتج بأن المشرع البحريني أعطى مفهوماً واسعاً للاحتيال ولم يقصره فقط على المال المادي، حيث أدخل في نطاقه النسخ والحيابة والتحريف وإفشاء الشهادة والتوقيع الإلكتروني وحتى صفة غير صحيحة، فجميعها أيضاً صور للاحتيال والتي من خلالها يمكن خداع المجني عليه.

وقد عرف المشرع الإماراتي الاحتيال بنص المادة (١٠) من قانون اتحادي رقم (٢) لسنة ٢٠١٦ في شأن مكافحة جرائم تقنية المعلومات على أنه "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 المجني عليه".

وهنا يمكن القول أن المشرع الإماراتي قد جانب الصواب في عدم اشتراطه لوقوع جريمة الاحتيال المعلوماتي الدخول غير المشروع، وقد اشترط فيها خداع المجني عليه سواء كان بالدخول المشروع أو الدخول غير المشروع.

^١ لقد حدد المشرع البحريني الطرق التي يقع عليها الاحتيال على النظام المعلوماتي وأشار إليها وفق ما ورد من قانون رقم (٦٠) لعام ٢٠١٤م بشأن جرائم تقنية المعلومات وهي كالتالي:

أ- إدخال أو تعيب أو تعطيل أو إلغاء أو حذف أو تدمير أو تغيير أو تعديل أو تحريف أو حجب بيانات وسيلة تقنية المعلومات.

ب- القيام بأي تدخل في عمل نظام تقنية المعلومات.

وقد أشار المشرع السعودي للاحتيال بطريقة غير مباشرة وأقر لها عقوبة خاصة^١، وقد عرف الاحتيال المعلوماتي ضمن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة (١١) على أنه: "التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير"^٢.

وعُرف الاحتيال المعلوماتي ضمن وثيقة الرياض للنظام (القانون) الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون الخليجي لعام ٢٠١٣م بنص المادة (١) على أنه "التأثير في نظام المعلومات الإلكتروني أو وسيلة تقنية المعلومات عن طريق البرمجة أو التدخل أثناء تطبيق البرنامج أو إدخال بيانات غير صحيحة أو غير مكتملة أو بأية طريقة أخرى".

نجد أن اغلب التشريعات العربية لم تورد تعريفاً لهذه الجريمة في متون قوانينها، وفي تقديرنا هذا مسلك جيد في مثل هذه الجريمة التي تتطوي على أنماط عديدة، وإنها تخضع لتطورات الزمان وتسايره، والمعلوم أن صياغة التعريف ليست من مهام المشرع وإنما من اختصاص الفقهاء. وإن وضع تعريف لها لا يخلو من ضرر لأن هذا التعريف مهما بذل في صياغته من جهد ودقة فلن يأتي جامعاً لكل المعاني المطلوبة، وإن جاء كذلك في زمن فقد لا يستمر في زمن آخر.

وخلاصة القول يتضح أن جريمة الاحتيال المعلوماتي ذات طبيعة خاصة وتختلف عن مفهومها التقليدي في الأداة المستخدمة في الاحتيال فقد ارتبطت بوسائل التقنية الحديثة التي من شأنها أن توقع المجني عليه في الغلط ويترتب عليه الاستيلاء على ماله، ويرى الباحث أن

^١ تنص المادة (٤) من نظام مكافحة الجرائم المعلوماتية السعودي لعام (١٤٢٨هـ) على: "يعاقب بالسجن مدة لا تزيد عن ثلاث سنوات أو بغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيّاً من الجرائم المعلوماتية الآتية:

أ- 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

ب- 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 تنتجها من خدمات.

^٢ وقد حددت ضمن نص المادة (١٢) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الطرق التي من خلالها يقع الاحتيال المعلوماتي وهي:

أ- إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات.

ب- التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها.

ت- تعطيل الأجهزة والبرامج والمواقع الالكترونية.

الجريمة تتعدّد بقصد الجنائي من خلال تحقق فيها الركن المادي والمعنوي كما سنبين لاحقاً، ومن جانبنا نميل إلى التعريف الذي أورده المشرع الإماراتي في تعريفه لجريمة الاحتيال المعلوماتي لشموليته وإدخاله لكافة وسائل التقنية الحديثة في إطار جريمة الاحتيال المعلوماتي.

الفرع الثاني: خصائص جريمة الاحتيال باستخدام وسائل تقنية المعلومات.

تتسم جريمة الاحتيال باستخدام وسائل تقنية المعلومات بخصائص معينة تكتسبها من خلال ما تتسم به الوسيلة نفسها فهي ترتبط ارتباطاً وثيقاً بتلك الخصائص التي تمتاز بها الجرائم المعلوماتية بشكل عام وجريمة الاحتيال على وجه الخصوص، فتمتاز جريمة الاحتيال المعلوماتي بخصائص تؤكد استقلالها عن الجرائم الأخرى.

وتمتاز الجرائم الإلكترونية عن الجرائم التقليدية بعدة خصائص تعطيها صفة استثنائية عن تلك الجرائم التقليدية، ويترتب على هذه الخصائص إجراءات متابعة ومواجهة من قبل جهة الاختصاص لهذه الخصائص ومن بين هذه الخصائص.

أولاً: جريمة الاحتيال المعلوماتي هي جرائم عابرة للحدود.

إن جرائم الاحتيال المعلوماتي هي شكل من أشكال الجرائم العابرة للحدود، فمسرحة الجريمة لم يعد محلياً بل أصبح عالمياً، إذ أن الفاعل لا يتواجد مادياً على مسرح الجريمة وهذا التباعد في المسافات بين الفعل المرتكب من خلال الحاسوب والفاعل وبين المعلومات التي كانت محل الاعتداء، فالجاني يستطيع القيام بجريمته بالدخول إلى ذاكرة الحاسوب الآلي الموجود في بلد آخر وهذا الفعل قد يضر شخصاً ثالثاً في بلد آخر^١.

فجريمة الاحتيال المعلوماتي جريمة داخلية عندما تقع داخل حدود الدولة أي ترتكب في النطاق الجغرافي للدولة، وهي جريمة دولية عندما تتجاوز حدود الدولة أي تتعلق بالقانون الدولي^٢.

^١ سعيد نعيم، "آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري"، رسالة ماجستير، جامعة الحاج لخضر، باتنة، ٢٠١٣، ص ٣٢.

^٢ محمد طارق الخن، "مرجع سابق"، ص ٣٤.

والجدير بالذكر إن انتشار الشبكة المعلوماتية وما يتصل بها من برامج اتصالات عالمية عبر الإنترنت أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر دول العالم فيما بينها، حيث ومن خلال هذا الربط بين أجهزة الحاسوب عن طريق الشبكات والبرامج أصبح بإمكان الجاني أن يقوم بجريمته في بلد ما وتكون الضحية أو المجني عليه في بلد آخر وهذا ما يميز هذه الجريمة عن الجرائم التقليدية الأخرى، أي إنها جريمة تتسم بالعالمية^١.

ثانياً: صعوبة اكتشاف وإثبات جرائم الاحتيال المعلوماتي.

تمتاز جريمة الاحتيال المعلوماتي بصعوبة الاكتشاف والإثبات لعدم ترك الجاني آثار تدل على إجرامه، فالجرائم التي تتم بواسطة إدخال الرموز والأرقام هي جرائم دقيقة ويصعب اكتشافها وإثباتها لهذا عادة ما يتم اكتشافها بالصدفة وغالباً لا يتم معاقبة المجرمين وذلك لعدم وجود أدلة قائمة في حقهم^٢.

كما ويصعب في جريمة الاحتيال المعلوماتي العثور على دليل مادي للجريمة وذلك راجع إلى استخدام الجاني وسائل فنية وتقنية معقدة في كثير من الأحيان، وهذا السلوك المادي في ارتكابها لا يستغرق إلا ثواني معدودة ويتم فيها محو الدليل أو التلاعب به^٣.

ومن الأمور التي تميز جريمة الاحتيال المعلوماتي أن الجناة يستخدمون أساليب لا يمكن الكشف عن هوية مرتكبيها كما ويمكنهم تدمير ما يتخلف عنها من آثار بحيث لا تعد دليلاً يمكن الاستفادة منه، وقد لا يرتكب المجرم فعله الإجرامي عن طريق جهازه الخاص وذلك وفقاً لطبيعة جريمة الاحتيال المعلوماتي نفسها، وبالإضافة لذلك قد يستخدم الجناة أسلوب الترميز أو التشفير يصعب من خلالها قراءة المعلومات^٤.

^١ عبد الفتاح مراد، "مرجع السابق"، ص ٤٢.

^٢ معتوق عبد اللطيف، "الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن"، رسالة ماجستير، ٢٠١١-٢٠١٢، ص ص ٢٤-٨٨.

^٣ هشام محمد فريد رستم، "الجوانب الإجرائية للجرائم المعلوماتية"، مكتبة الآلات الحديثة، أسبوط، ط١، ١٩٩٤م، ص ٨٢.

^٤ محمد حماد مرهج الهيتي، "الجريمة المعلوماتية نماذج من تطبيقاتها دراسة مقارنة"، دار الكتب القانونية، مصر، ٢٠١٤م، ص ١٠٣-١٠٤.

فجريمة الاحتيال المعلوماتي جريمة صعبة الاكتشاف، لأن الجاني من الممكن أن يستخدم اسماً مستعاراً، أو أن يرتكب جريمته من خلال إحدى مقاهي الإنترنت، إضافة إلى إنها صعبة الإثبات لأنها لا تترك أثراً مادياً، بسبب سهولة حذف وإخفاء آثار الجريمة خلال ثوان^١.

وتكمن صعوبة متابعة جريمة الاحتيال المعلوماتي في أنها لا تترك أثراً، فهي مجرد أرقام تتغير في سجلات، فكما تم الإشارة سابقاً أن اكتشافها يأتي بالصدفة وبعد وقت طويل من ارتكابها، فالجرائم التي لم تكتشف أكثر بكثير من الجرائم التي تم اكتشافها لأنها تفنقر إلى الدليل المادي التقليدي كال بصمات، كما ويصعب الاحتفاظ الفني بآثارها إن وجدت، فهي تحتاج إلى الخبرة الفنية الخاصة بهذه الجرائم والتي يتعذر على المحقق التقليدي منالها أو التعامل معها^٢.

ثالثاً: تتميز جريمة الاحتيال المعلوماتي في الأداة المستخدمة لارتكاب الجريمة.

إن الجرائم المعلوماتية يستلزم للقيام بها توفر وسيلة من وسائل تقنية المعلومات كالهاتف النقال، فلا يمكن الحديث عن الجريمة المعلوماتية دون أن تكون الأداة المستخدمة في الجريمة ذات طابع تقني إلكتروني، سواء أكان باستخدام الحاسب الآلي الموصول بشبكة الإنترنت، أو بوسائل تقنية المعلومات كبطاقات الائتمان والتي من خلالها يتم تشفير بياناتها والتلاعب بها بإحدى الطرق التكنولوجية الحديثة.

فوسائل ارتكاب جريمة الاحتيال المعلوماتي ذات طبيعة خاصة تختلف عن تلك الوسائل التقليدية، فهي ترتكب بوسائل غير تقليدية لا تتماثل في طبيعتها ولا آثارها مع الوسائل التي ترتكب بها الجرائم الأخرى، فجريمة الاحتيال المعلوماتي محلها كيان غير مادي وهو النظام الآلي وما يحتويه من برامج ومعطيات وبيانات ومعلومات، والتي يسعى الجاني إلى استخدامها والتعامل معها للوصول إلى القصد الجنائي المراد، فهي عبارة عن موجات مغناطيسية ونبضات إلكترونية تتربط فيما بينها عبر منظومة شبكات أو شبكة اتصالات^٣.

^١ محمد طارق الخن، "مرجع سابق"، ص ٣٤.

^٢ هشام محمد رستم، "الجرائم المعلوماتية-أصول التحقيق الجنائي الفني"، مجلة الأمن والقانون، دبي، العدد ٢، ١٩٩٩م، ص ٢٤.

^٣ محمد الهيئي، "مرجع سابق"، ص ١٠٨.

رابعاً: تعتبر جريمة الاحتيال المعلوماتي أقل عنفاً في التنفيذ.

لا تتطلب الجرائم الإلكترونية عنفاً لتنفيذها أو مجهوداً كبيراً، فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعاً من المجهود العضلي الذي يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف^١.

فإذا كانت الجرائم التقليدية تحتاج إلى مجهود عضلي في ارتكابها كجريمة السرقة والقتل فجريمة الاحتيال المعلوماتي لا تتطلب أدنى مجهود عضلي ممكن، بل تعتمد على المجهود الذهني المحكم، والتفكير العلمي المدروس القائم على معرفة تقنية ممتازة بوسائل تقنية المعلومات والتعامل السليم بهذه الوسائل، فالغرض الأساسي لمجرمي هذه الطائفة من الجرائم يسعون إلى تحقيق مصلحة خاصة كحصولهم على الأموال أو المعلومات والبيانات التي تمثل قيمة مادية.

خامساً: يمتاز مرتكب جريمة الاحتيال بالذكاء الإلكتروني بالخبرة الفائقة والمعرفة العالية بمجال تقنية المعلومات:

إن الجرائم التقليدية لا تتأثر بالمستوى العلمي للمجرم كقاعدة عامة، ولكن الأمر يختلف في جريمة الاحتيال المعلوماتي أو الجرائم الإلكترونية بشكل عام، إذ لابد من مرتكب جريمة الاحتيال المعلوماتي أن يكون ذو خبرة واسعة ومعرفة عالية بمجال تقنية المعلومات لارتكاب جريمته عبر شبكة الإنترنت بحيث تمكنه من تنفيذ جريمته والعمل على عدم اكتشافها، ولذلك نجد أن معظم مرتكبي جرائم الاحتيال المعلوماتي من خبراء تقنية المعلومات وإن الشرطة أول ما تبحث عنه هم خبراء الكمبيوتر عند ارتكاب جرائم الاحتيال المعلوماتي^٢.

ويتم تصنيف مجرمي جرائم الاحتيال المعلوماتي وفقاً لأنواع التالية:

(١) **المخترقون:** وهم أشخاص بارعون في استخدام تقنية المعلومات، ويمتلكون من الفضول قدراً كافياً لاختراق الحسابات الشخصية بطرق غير مشروعة، وهذا النوع من الجناة تطغى عليهم الصفة التطفلية لإبراز ما لديهم من قدرات ذهنية وتقنية في مجال التقنية الحديثة،

^١ ذياب موسى البداينة، "دور الأجهزة الأمنية في مكافحة جرائم الإرهاب المعلوماتي"، الدورة التدريبية حول مكافحة الجرائم الإرهابية المعلوماتية، المنعقدة بكلية التدريب قسم البرامج التدريبية، القنيطرة، المملكة المغربية، أيام ٩-١٣، إبريل ٢٠٠٦م، ص ٢٠.

^٢ سامر سلمان الجبوري، "جريمة الاحتيال الإلكتروني دراسة مقارنة"، مكتبة زين الحقوقية، ط ١، ٢٠١٨م، ص ٣٣.

وغالباً ما يكونوا في سن الشباب وتتجه اختراقاتهم نحو المواقع الرسمية، وفي بعض الأحيان يقوموا باختراق حسابات خاصة لإثبات الذات^١.

(٢) **المحترفون:** هذه الفئة من الجناة الأكثر خطورة بين المجرمين، فهم يهدفون إلى تحقيق الكسب الغير مشروع عبر الاعتداء واختراق الحسابات البنكية، كما قد يكون للبعض منهم أهداف سياسية فيقوم باختراق المواقع الرسمية.

(٣) **الحاقدون:** وهذا النوع من المجرمين لا توجد لديه أهداف سياسية ولا يرغبون في تحقيق الكسب بقدر ما يكون الدافع لارتكابهم للجرائم نابع من رغبة في الانتقام والثأر، فالدافع وراء ارتكابهم لهذه الجرائم قد يكون طائفي أو عقائدي^٢.

^١ نائلة قورة، "جرائم الحاسب الآلي الاقتصادية"، منشورات الحلبي الحقوقية، بيروت، ط١، ٢٠١٢م، ص ١٧٨.

^٢ خالد إبراهيم، "فن التحقيق الجنائي في الجرائم المعلوماتية"، دار الفكر الجامعي، الإسكندرية، ط١، ٢٠٠٩م،

المطلب الثالث

الآثار المترتبة على استخدام وسائل تقنية المعلومات في جريمة الاحتيال

شأنها شأن غيرها من الجرائم الأخرى سواء كانت تقليدية أم مستحدثة، فإن جريمة الاحتيال المعلوماتي باستخدام وسائل التقنية المعلوماتية يترتب عنها آثار ومخاطر جمة، حيث تطل هذه المخاطر قطاعات متعددة في المجتمع، وسنقوم بتقسيم هذا المطلب إلى ثلاث فروع كالآتي:

الفرع الأول: المخاطر الاقتصادية.

الفرع الثاني: المخاطر الأمنية.

الفرع الثالث: المخاطر الاجتماعية والنظامية.

الفرع الأول: المخاطر الاقتصادية.

إن الهدف الرئيسي للتلاعب الذي يتحقق به الاحتيال المعلوماتي في قطاع المعلومات هو البيانات التي تمثل في نظم معلومات الحاسبات الإلكترونية أموالاً وموجودات، وأكثر البيانات استهدافاً لهذا التلاعب هو المتعلق منها بالمستحقات المالية والإيداعات المصرفية وتقديرات الائتمان وحسابات ونتائج الميزانيات، وأكثر ما يرد عليه التلاعب - وفقاً لما تم الكشف عنه من حالات الاحتيال والغش المعلوماتي - هو حسابات المرتبات والمعاشات وأوامر الدفع وحسابات التكلفة والنفقات، بالإضافة إلى قوائم المبيعات وكشوف الإعانات الاجتماعية، والحسابات المعدة بواسطة الحاسبات الآلية لميزانيات البنوك والشركات وقطاعات الأعمال^١.

أما الخطورة الأكبر التي تنتجها جريمة الاحتيال المعلوماتي فهي تلك التي تقع على الأنشطة الاقتصادية والاقتصاد القومي ككل، فهي تتمثل فيما يقع على أنظمة التحويل الإلكتروني للأموال والودائع المصرفية أو ما يسمى بالأموال الإلكترونية أو الافتراضية، نظراً

^١ محمد عبد الله سلامة، "موسوعة جرائم المعلوماتية"، منشأة المعارف، الإسكندرية، ٢٠٠٦م، ص ١٦٧.

لضخامة حجم ما يتم تداوله عبر هذه الأنظمة من أموال، واختزالها- أي تلك الأنظمة، كذلك المسافات بما يتيح تنفيذ الاحتيال عبر الحدود الإقليمية للعديد من الدول، واختزالها أيضاً الزمن اللازم لإتمام التعاملات والتحويلات المالية، وكذا الزمن لسلب الأموال بالاحتيال والغش إلى ثوان معدودة، وهو ما عكس صيرورة الأموال المتداولة عبر هذه الأنظمة هدفاً من أهداف الجريمة المنظمة والقوى الخارجية المعادية من جهة، وفي فداحة الخسائر الناجمة عن عمليات الاحتيال الواقعة في محيط هذه الأنظمة من جهة أخرى^١.

وتتعدد صور جريمة الاحتيال بتعدد وسائل التقنية المعلوماتية الحديثة، ففي الوقت الذي تتطور فيه هذه الوسائل لمواكبة التكنولوجيا الحديثة يتطور معها مهارات رواد ومستخدمي هذه الوسائل أو ما يطلق عليهم محترفي الكمبيوتر أو الهاكرز وهذه السمة التي يمتاز بها مستخدمي التقنية المعلوماتية أتاحت لهم استغلال وسائل تقنية المعلومات عن طريق التلاعب بالبيانات للحصول على الأموال أو أي شيء آخر ذات قيمة^٢.

فالهدف الرئيسي من جريمة الاحتيال يتمثل في الاستيلاء على مال منقول مملوك للغير بنية التملك عن طريق التلاعب بالبيانات والمعلومات للحصول على أموال وأصول مملوكة للغير، ومن بين البيانات الأكثر عرضةً للتلاعب تلك المتعلقة بالمستحقات المالية والإيداعات المصرفية وبطاقات الائتمان وحسابات ونتائج الميزانية^٣.

فكما أشرنا سابقاً فإن استغلال شبكة الإنترنت من قبل محترفي الكمبيوتر لجني الأموال عن طريق التلاعب بالبيانات عبر الترويج لمشاريع وهمية أو خدمات أو منتجات للوصول إلى أرقام بطائق ائتمانية ومن ثم استغلال هذه البيانات والمعلومات في عمليات شراء غير مشروعة أو الوفاء بمبالغ مقابل خدمات للجاني، بالإضافة إلى التلاعب بالأسهم المالية وإدارة المحافظ الالكترونية ومزادات البضائع على الإنترنت.

حيث إن هذه الجرائم لا تنحصر خطورتها على المجني عليه وحده، بل إنها تطل النظام الاقتصادي للدولة بأكمله، فانتشار هذه الجرائم أصبح بمثابة الرعب الذي يورق شركات الإنترنت والقائمين عليها.

^١ محمد عبد الله سلامة، "مرجع سابق"، ص ١٦٨.

^٢ محمد أحمد طه، "المواجهة التشريعية لجرائم الكمبيوتر والإنترنت"، دار الفكر والقانون للنشر والتوزيع، المنصورة، ٢٠١٦-٢٠١٧م، ص ١٤٤.

^٣ محمد أبو بكر محمد سلامة، "موسوعة جرائم المعلوماتية"، منشأة المعارف، الإسكندرية، ٢٠٠٦م، ص ١٦٨.

والاحتيال لا يقع على الشخص الطبيعي فقط، بل أنه من المسلم به صلاحية الشخص المعنوي لاعتباره مجنياً عليه، فالشركات والمؤسسات العامة أو الخاصة هي من الأشخاص الاعتبارية في نظر القانون، وحيث إن الحاسوب والشبكات الداخلية للمنشأة تعد من فروع الشركة أو المؤسسة، فإنها تكون صالحة للتحايل عليها^١.

ونظراً لخطورة جريمة الاحتيال المعلوماتي بدأت الكثير من الوسائل الإعلامية تصدر تقاريرها الخاصة بهذه الجريمة وما يترتب عنه من خسائر فادحة، خاصة في ظل تنامي هذه الظاهرة بالتوازي مع انتشار الإنترنت، فالاختراقات الحاصلة عبر شبكة الإنترنت وما تسفر عنه من سرقة بيانات من قبل الهاكرز أدت الاهتمام المتزايد من قبل مراكز الدراسات ووسائل الاعلام والجهات المختصة إلى دراسة ونشر حجم الخسائر الناجمة عن جريمة الاحتيال المعلوماتي.

ويلاحظ أن معدلات جريمة الاحتيال المعلوماتي في ارتفاع مستمر، وفي وتيرة أسرع في المجتمع الخليجي^٢.

وفقاً لدراسة لكاسبر سكاي، أشار إلى أن دولة الإمارات العربية المتحدة احتلت طليعة دول الشرق الأوسط الأكثر استهدافاً وعرضه لجرائم الاحتيال الالكتروني بنسبة تقدر ٣٨,٨%، تليها المملكة العربية السعودية بنسبة ٢٩,٣%، تليهم دولة قطر بنسبة ٩,٦٤%، والكويت بنسبة ٦,٩٢%، وجاءت المملكة العربية السعودية ضمن تصنيف (عالي المخاطر) في مجال التهديدات والمخاطر المتعلقة بالاتصالات وتقنية المعلومات والشبكات المعلوماتية^٣.

خلاصة القول: يتضح أن معدلات جرائم الاحتيال المعلوماتي في ارتفاع مستمر وخاصة في دول مجلس التعاون الخليجي، ويلاحظ أن أنماط الجرائم المعلوماتية في دول مجلس التعاون الخليجي تنصب غالباً في الجرائم المالية التي تستهدف الشركات والمؤسسات الاقتصادية والمالية، ومن هنا تتأتى الخطورة الفعلية لجرائم الاحتيال المعلوماتي.

^١ انظر: د. علي حسن الطويلة، "مرجع سابق"، ص ١٨١.

^٢ أنظر مجمع البحوث والدراسات، "الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها"، مجمع البحوث والدراسات، أكاديمية السلطان قابوس لعلوم الشرطة، سلطنة عمان، ٢٠١٦، ص ٣٧-٣٨.

^٣ مجمع البحوث والدراسات، "الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها"، مرجع سابق، ص ٣٧-٣٨.

الفرع الثاني: المخاطر الأمنية.

يعتبر الدافع المادي من أهم دوافع ارتكاب جريمة الاحتيال المعلوماتي، وذلك لأن الاحتيال لا يقتصر فقط على الأشخاص الطبيعيين بل أنه يقع أيضاً على البنوك وما بداخل هذه البنوك من حسابات وأرصدة لشركات ومصارف، فالاحتيال المعلوماتي يطل أيضاً هذه المؤسسات التي تعتبر الركيزة الأساسية لاقتصاد الدولة، بل قد يتم التلاعب والاستيلاء على أرصدة خاصة بأموال الدولة، فالمقدرة والقدرة التي يتمتع بها مرتكب جريمة الاحتيال المعلوماتي مع علمه بالتقنية الحديثة والذكاء المعلوماتي، تجعل كافة شرائح وقطاعات المجتمع عرضة لأهدافه، فليس هناك محرمات في مجال جريمة الاحتيال المعلوماتي، فالاستيلاء على هذه الأموال يلقي بضلاله على النظام الاقتصادي للدولة والتي بدوره ينعكس على القطاع الأمني حيث يؤثر على المقدرة المالية للدولة لتلبية احتياجات أفرادها فيؤثر ذلك على النظام العام للدولة وقد يحدث خللاً اقتصادياً يؤثر على بنية النظام السياسي بمجمله.

عوضاً عن ذلك فإن من خصائص جريمة الاحتيال المعلوماتي أنها جرائم تتجاوز الحدود الإقليمية للدولة، إذا أن الضرر المترتب عن هذه الجرائم يقع على أشخاص أو مؤسسات خارج حدود الدولة التي ارتكبت فيها الجريمة، فهذا مفاده التعدي على سيادة الدول الأخرى وعدم احترام سلطتها، فانتهاك سيادة الدول يترتب عليه مخاطر وانعكاسات قد تطل العلاقات بين الدول بكافة صورها ، فمفهوم السيادة يعني السيطرة والتحكم من قبل الدولة على إقليمها، أما مثل هذه الجرائم فإنها تؤدي إلى إلغاء مفهوم السيادة وما يتصل به¹.

الفرع الثالث: المخاطر الاجتماعية والنظامية.

فانتشار جريمة الاحتيال المعلوماتي عبر هذه التقنية الحديثة أصبح يمثل هاجساً لدى الأفراد مما يدفعهم لعدم الثقة بهذه التقنية ووسائلها، وهذا بدوره يؤثر بالسلب على مستقبل هذه التقنية الحديثة التي هي في تطور مطرد لا يمكن الحد منه في عالم متسارع قائم على المعلومات وتخزينها وإخراجها.

فالمجتمعات تعاني من آثار الجرائم التقليدية وهي معاناة أزلية، فلم يخلُ عصر من العصور أو دولة من الدول أو حتى مجتمع من المجتمعات من وجود جرائم تقليدية استدعت وجود نظام قانوني لتحقيق الأمن والحد من وقوع هذه الجرائم.

¹ ربيع أنور فتح الباب، "النظم السياسية (السلطة، الدولة، الحكومة صورها وأساليبها)"، دار نصر للطباعة الحديثة، القاهرة، ٢٠٠٣م، ص ٤٥.

ومع ظهور جريمة الاحتيال المعلوماتي أضيف عبء جديد على أجهزة الدولة ومؤسساتها، مع التسليم بأن هذه الجريمة ليست كغيرها فلها من الخصوصية مكانة، فهي جريمة مستحدثة لا ينطبق عليها النظام القانوني التقليدي لما لها من خصوصية.

إن تزايد نسب جرائم الاحتيال المعلوماتي في ظل تزايد مستخدمي شبكة الإنترنت ومستخدمي التقنية الحديثة يفتح المجال أمام هؤلاء الجناة إلى استخدام الشبكة المعلوماتية وما يروج عن طريقها من طرق احتيالية سلعة تباع وتشتري عبر هذه الشبكة كتسديد فواتير الكهرباء والماء لأفراد آخرين بتكلفة أقل من التكلفة الأصلية، فالترويج أصبح هو وسيلة احتيالية^١.

كما أدت جريمة الاحتيال المعلوماتي إلى انتهاك الخصوصية للأشخاص والتعدي على مستودع أسرارهم، حيث تزايد الاعتماد في ظل الطفرة التكنولوجية على الأدوات والوسائل الإلكترونية المتعددة والمتنوعة التي أفرزتها تلك الطفرة لغرض حفظ بياناتهم ومعلوماتهم والتي تتعقب أمورهم الخاصة الاجتماعية والمالية والتي يرغبون في الاحتفاظ بها وعدم إطلاع الغير عليها، حتى أصبحت أجهزة الحاسوب بمثابة مستودع السر الذي يحتفظ بكافة الأسرار والخبايا، فطبيعة هذه الجرائم قائمة على الاستيلاء إما على أموال هؤلاء الأشخاص أو بياناتهم الشخصية وممتلكاتهم العلمية والمعلوماتية، والقيام باستغلال هذه المعلومات.

^١ في حال نجاح محاولات الاحتيال فإن ذلك يترتب عنه مخاطر اقتصادية وأمنية كبيرة، ومن الأمثلة على ذلك: استطاعت مجموعة من المستخدمين الإداريين خلال سنوات عديدة ان يضاعفوا من رواتبهم عن طريق استخدام الحاسبات الآلية، حتى لحظة الكشف عن تلك الأفعال بمحض الصدفة. قام بعض المستخدمين الإداريين أيضاً بتقاضي ساعات إضافية لم يتم تنفيذها على الإطلاق عن طريق استبدال قوائم الحاسبات بساعات عمل. قام مستخدم بمكتب القوى العاملة في ألمانيا كان مكلفاً بتوزيع الإعانات العائلية -بتحويل مبلغ وقدره ٥٠٠ ألف مارك ألماني لحاسبه الخاص في شكل مرتبات، وقد نفذ ذلك عن طريق إزالة الرقم الأول لتلك المبالغ من المنفذ الخاص بمراقبة الحاسب الآلي. أنظر: محمد أبو بكر محمد سلامة، "مرجع سابق"، ص ١٧١-١٧٢.

المبحث الثاني

ذاتية جريمة الاحتيال باستخدام وسائل تقنية المعلومات وصورها

لقد تنوعت الأشكال التي تتم من خلالها الجرائم المعلوماتية أو الجرائم بواسطة تقنية المعلومات، وأخذت منحى آخر في ظل تطور وانتشار وسائل تقنية المعلومات، ومن هذه الأشكال اختراق الحواسيب الآلية بهدف تدمير البرامج الموجود فيها أو التعديل عليها، أو الدخول لشبكة الحاسوب للإطلاع على أسرار الغير من أشخاص وشركات، أو دخول الحواسيب البنكية للحصول على مبالغ مالية أو سرقة بيانات العملاء من حسابات وبطاقات الائتمان بغرض سرقتها واستخدامها في الجريمة المعلوماتية، أو استخدام فيروسات مضرّة بالبيانات والبرامج غرض إتلافها، كل ذلك أدى إلى تعدد صور الاحتيال المعلوماتي وصعوبة ضبطها قانونيا في ظل انتشارها الواسع^١.

وقد استغل المحتالون هذا التطور في توسيع أساليبهم الاحتيالية بما يتناسب مع التقدم التكنولوجي وأبدعوا في اكتشاف طرق وصور جديدة استطاعوا من خلالها الوصول لأنماط مستحدثة من جرائم الاحتيال التي تتسم بالخطورة العالية، إذا ما قسنا ضخامة الأموال المحصل عليها من قبل المحتالون^٢، وعليه سيتم تقسيم المبحث إلى ثلاثة مطالب على النحو الآتي:

المطلب الأول: ذاتية جريمة الاحتيال المعلوماتي.

المطلب الثاني: الصور العامة للاحتيال المعلوماتي.

المطلب الثالث: الصور الخاصة للاحتيال عن طريق بطاقات الائتمان.

^١ كامل فريد السالك، "الجريمة المعلوماتية"، الجمعية السورية للمعلوماتية، حلب، محاضرة أُلقيت في مؤتمر الجمعية السورية للمعلوماتية، ٢٠٠٠، ص ٣-٤.

^٢ بدر بن أحمد بن محمد الزهراني، "جريمة الاحتيال الإلكتروني في النظام السعودي -دراسة مقارنة"، جامعة نايف العربية للعلوم الأمنية، الرياض، رسالة ماجستير، ١٤٣٦ - ٢٠١٥، ص ٣٧.

المطلب الاول

ذاتية جريمة الاحتيال المعلوماتي

تعتبر جريمة الاحتيال والسرقة وخيانة الأمانة من الجرائم الواقعة على الأموال، فهي جرائم ذات أثر وبالتالي تنطوي على الاعتداء على حق الملكية، وسنبين من خلال هذا الجزء من الدراسة الذاتية الخاصة لجريمة الاحتيال المعلوماتي وما يميزها عن غيرها من الجرائم ذات الصلة، وسيتم تقسيم المطلب إلى فرعين كالآتي:

الفرع الأول: الأحكام المشتركة بين جريمة الاحتيال والسرقة وخيانة الأمانة.

الفرع الثاني: الاختلافات بين الاحتيال والسرقة وخيانة الأمانة.

الفرع الأول: الأحكام المشتركة بين جريمة الاحتيال والسرقة وخيانة الأمانة

قبلولوج في دراسة النقاط المشتركة بين هذه الجرائم لابد من التعريف بها، وقد سبق تعريف جريمة الاحتيال، أما السرقة وكما عرفها الفقه هي "أخذ مال منقول مملوك للغير بنية التملك"^١.

وتعرف جريمة خيانة الأمانة على أنها "استيلاء شخص على منقول يحوزه بناء على عقد حدده القانون عن طريق خيانة الثقة التي أودعت فيه بموجب هذا العقد وذلك بتحويله نيته في حيازة الشيء من حيازة وقتية أو ناقصة إلى حيازة كاملة بقصد التملك، فيحول بذلك صفته من حائز لحساب مالكة إلى مدع لملكيته"^٢.

^١ فوزية عبد الستار، "شرح قانون العقوبات" القسم الخاص"، دار النهضة العربية، القاهرة، ١٩٨٢م، ص ٦٦٦.

^٢ محمود نجيب حسني، "جرائم الاعتداء على الأموال في قانون العقوبات اللبناني"، دار النهضة العربية، القاهرة، ١٩٨٤م، ص ٣٦٤.

مما سبق يتضح بأن هذه الجرائم تشترك في عدة عناصر رئيسية، فمن الناحية المادية فهي عبارة عن اعتداء على حق الملكية، ومن الناحية المعنوية فهي تتطوي على نية مرتكبيها في تملك المال الواقع عليه الفعل الجرمي، ولذلك يجب أن يتوافر في موضوع الاعتداء شرطين:

الشرط الأول: أن يكون المعتدى عليه مالاً حتى يكون محلاً للحق، وأن يكون مملوكاً للغير حتى يثبت اعتداء المجرم على ملكية غيره^١.

أما الشرط الثاني: فهو القصد الجنائي، ما يعني توافر إرادة لاعتداء على الملكية وبناءً عليه تعتبر هذه الجرائم من الجرائم العمدية، أي لا يكفي لقيامها توفر القصد العام، بل لابد من توفر القصد الخاص وهو نية التملك لدى المجرم وهذا ما سنبينه لاحقاً في الدراسة.

الفرع الثاني: الاختلافات بين جريمة الاحتيال والسرقة وخيانة الأمانة

بالرغم من الأحكام المشتركة بين هذه الجرائم إلا أن هناك اختلافاً بينها تجعل من الاحتيال جريمة ذاتية بالنسبة للجرائم الأخرى، بحيث تبرز الفروق بينهما في عدة نقاط:

أولاً: من حيث الركن المادي في كل منها.

الاحتيال يقوم على فعل الخداع باستخدام أساليب تدليس تعيب إرادة المجني عليه، ونتيجة جرمية هي تسليم المجني عليه المال إلى الجاني ورابطة سببية وهي الغلط الناتج عن الخداع والتصرف المبني عليه، والتسليم لا يتنافر مع هذا الفعل بل هو نتيجة جرمية وهو تسليم صادر عن إرادة فاسدة.

لكن في جريمة السرقة يختلف الأمر فالركن المادي يقوم على فعل الأخذ الذي يتحقق عن طريق إهدار الحيازة وإخراج المال موضوع السرقة من حيازة المجني عليه وإدخاله في حيازة ثانية^٢.

أما الركن المادي في جريمة إساءة الأمانة فيقوم على فعل يخون فيه المجرم الثقة التي وضعها فيه المجني عليه عندما سلمه المال فيكتم الجاني أو يختلس أو يبدد أو يتلف المال الذي

^١ عبد العظيم مرسي وزير، "شرح قانون العقوبات"، دار النهضة العربية، القاهرة، ١٩٩٣م، ص ١٢.

^٢ محمد علي جعفر، "قانون العقوبات" القسم الخاص"، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، ٢٠٠٦، ص ٣٣٨.

سلمه المجني عليه، وبدلاً من الإقرار في حق الملكية للمجني عليه يجحد ذلك الحق، والتسليم في جريمة إساءة الائتمان ليس نتيجة جرمية بل هو عمل سابق على الفعل الجرمي لا يتنافر معه بل يفترضه وهو تسليم صادر عن إرادة صحيحة بموجب عقد قانوني^١.

ثانياً: من حيث دور المجني عليه

في جريمة الاحتيال إرادة المجني عليه تلعب دور أساسي، فعن طريق الخداع يواجه المحتال إرادة المجني عليه إلى تسليمه المال، ومن هنا فإن لإرادة المجني عليه دوراً في تحقيق عناصر الركن المادي ولكنها إرادة معيبة غير سليمة لما شابها من غلط بسبب خداع المحتال^٢. وفي جريمة إساءة الأمانة فإن لإرادة المجني عليه دوراً في تهيئة الظروف التي أتاحت لمسيء الائتمان ارتكاب الفعل الجرمي، فبتسليمه المال يصبح للجاني فرصة الاستيلاء على المال والتحول من أمين إلى خائن، وهذه تعتبر إرادة صحيحة وفرت بعض الشروط المادية لقيام الجريمة. أما جريمة السرقة فلا يوجد أي دور للمجني عليه لأن السارق يأخذ الشيء عنوة^٣. مما سبق يتضح أن اختلاف دور المجني عليه يترتب عليه اختلاف التكيف القانوني للجريمة من حيث تسليم المال، فتسليم المجني عليه المال للجاني تسليماً ناقلاً للحيازة بناء على إرادة معيبة في هذه الحالة تعتبر جريمة الاحتيال، بخلاف تسليم المجني عليه للمال للجاني تسليماً ناقلاً للحيازة الذي يعتبر خيانة الأمانة.

ثالثاً: من حيث الوسيلة

في الاحتيال يحصل الجاني على المال من صاحبه وبرضاه من خلال الطرق الاحتيالية، وفي السرقة ينتزع الجاني الأموال بغير رضا صاحبها، أما في إساءة الائتمان يغير الجاني نيته في الحيازة من حيازة وقتية أو ناقصة إلى حيازة كاملة بنية التملك^٤.

وسيتم التطرق فيما بعد من هذا البحث للذاتية الخاصة بجريمة الاحتيال المعلوماتي والمتمثلة في أركان جريمة الاحتيال المعلوماتي، وطبيعة هذه الجريمة.

^١ على القهوجي، "شرح قانون العقوبات" القسم الخاص"، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٣م، ص ٣٦٥.

^٢ مأمون سلامة، "شرح قانون الإجراءات الجنائية"، دار الفكر العربي، القاهرة، ١٩٨١م، ص ١٧.

^٣ محمود نجيب حسني، "مرجع سابق"، ص ٢١٣.

^٤ عبد العظيم مرسي وزير، "مرجع سابق"، ص ١١.

المطلب الثاني

الصور العامة للاحتيال المعلوماتي

إن صور ووسائل الجريمة الاحتيالية المرتكبة عبر تقنية المعلومات متنوعة ومتجددة ومسايرة للتطور الإلكتروني الحاصل، وهنا تكمن صعوبة رصد كافة صور الاحتيال، لذلك ارتأينا الحديث عن الصور العامة والتي يمكن رصد بعضها لفهم طبيعة الجريمة المرتكبة بوسائل تقنية المعلومات، من خلال تقسيم المطلب إلى أربعة فروع كالتالي:

الفرع الأول: الاستيلاء على أموال المصارف.

الفرع الثاني: الاحتيال التجاري.

الفرع الثالث: الاحتيال بواسطة الأوراق المالية

الفرع الرابع: الاحتيال عبر انتحال الشخصية والبريد الإلكتروني.

الفرع الأول: الاستيلاء على أموال المصارف.

إن استخدام وسائل تقنية المعلومات في العمليات المصرفية سهل للعملاء الاطلاع على كشوفاتهم وحساباتهم وإجراء التحويلات المصرفية على شبكة الإنترنت بكل سهولة ويسر، وفي خضم هذا التداول المالي انتهز بعض المجرمين -الهاكرز^١ ذلك مما سمح لعمليات الاحتيال على هذه الأموال وسرقتها من خلال اقتحام أنظمة المعلومات للمصارف عبر الشبكة العنكبوتية للتلاعب في حسابات وكشوفات العملاء مع القيام بنقل الأرصدة والحسابات من حساب لآخر^٢.

^١ يتم تعريف الهاكرز Hackers Theat على أنه أي شخص يستطيع النفاذ خفية إلى الأنظمة الحاسوبية والعبث بالبرامج والمعلومات فيها دون أن يكون مخولاً بذلك. ساري محمد الخالد، "اتجاهات في أمن المعلومات وأمانها-أهمية تقنيات التعمية (الشفرة)"، مكتبة العبيكان للنشر، ٢٠١٨، ط ١، ص ٩٥.

^٢ محمد طارق الخن، "مرجع سابق"، ص ٤٨.

وقد عرفت السرقة بأنها اختلاس الشيء المنقول والمملوك للغير بدون رضاه بنية امتلاكه عن طريق استخدام السارق للمعلومات الشخصية -الاسم، العنوان، الأرقام الخاصة بالمجني عليهم، واستخدام هذه البيانات بطرق غير شرعية، ليبدأ بذلك عملية الاحتيال المعلوماتي على الأموال^١ عن طريق التحويل البنكي للحسابات المصرفية^٢.

ومن أمثلة الجرائم الواقعة على الأموال الإلكترونية ؛ ففي البحرين ما بين عامي ٢٠٠٩ و ٢٠١١ قام المتهم باستعمال توقيع الكتروني خاص بالمجني عليه مثبت في سجل إلكتروني مدون على وسيط عبارة عن بطاقة ائتمان مملوكة له صادرة عن بنك الإسكان للتجارة والتمويل وذلك بغرض احتيالي بأن أظهر نفسه بأنه صاحب الحق في استعمالها بما تحتويه البطاقة من توقيع إلكتروني مدونة باسم المجني عليه وذلك لسداد قيمة مشترياته في المحال والمؤسسات التجارية وغيرها، كما أنه توصل إلى الاستيلاء على مبالغ نقدية تم احتسابها في حساب تلك البطاقة وذلك بالاستعانة بطرق احتيالية بأن اتخذ صفة غير صحيحة بأنه صاحب الحق في استعمال تلك البطاقة في سداد مشترياته وذلك على خلاف الحقيقة، وقام بتزوير توقيع المجني عليه على نماذج استلام البطائق الائتمانية الصادرة من البنك المذكور^٣.

ومن أشهر الجرائم ما حصل في الإمارات العربية المتحدة خصوصاً بإمارة دبي في نهاية عام ٢٠٠١، ومن مقتضياتها أن قام مهندس حسابات بالعديد من السرقات المالية لعملاء في (١٣) ثلاثة عشر بنكاً عالمياً ومحلياً وتحويلها إلى حسابات وهمية قام هو بإنشائها، إلى جانب قيامه بشراء وبيع سلع وخدمات عبر الإنترنت مستخدماً بطاقات الائتمان وحسابات شخصية لعدد كبير من الضحايا بلغ إجمالي الأموال (٣٠٠) ثلاثمائة ألف درهم إماراتي من البنوك المحلية فقط^٤.

وفي فرنسا قضت محكمة الجench الفرنسية على موظف قام بنسخ برامج معلوماتية تابعة لشركة بيجو" على قرص إلكتروني وقام باستخدامها بعد أن عمل في شركة أخرى منافسة، وأدانت

^١ محمد نصر محمد، "الوسيط في الجرائم المعلوماتية"، مركز الدراسات العربية للنشر والتوزيع، ٢٠١٥، ط١، ص ١٦٣.

^٢ محمد أمين أحمد الشوابكة، "جرائم الحاسوب والإنترنت"، مكتبة دار الثقافة والتوزيع، عمان، ٢٠٠٤، ط١، ص ١٣٨.

^٣ الطعن رقم ٢٣٦ لسنة ٢٠١٣، جلسة ٣١ أغسطس سنة ٢٠١٤.

^٤ محمد علي قطب، "الجرائم المعلوماتية وطرق مواجهتها"، الجزء الثاني، وزارة الداخلية، الأكاديمية الملكية للشرطة، مارس ٢٠١٠، ص ١٢.

المحكمة هذا الفعل واعتبرته سرقة على أساس سرقة برامج إلكترونية^١، وهو ما أكدته المشرع الإماراتي على أن: "كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول 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 تنتجه 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 إحدى هاتين العقوبتين إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال الغير"^٢.

وتعتبر قضية بنك الباسيفيك الوطني من القضايا المشهورة في الولايات المتحدة الأمريكية والمتعلقة بالاستيلاء على أموال المصارف، إذ عمد أحد المواطنين الأمريكيين وهو "ستانلي مارك" وهو أحد موظفي البنك ومتخصص بالحسابات، حيث اكتشف بالمصادفة الشيفرة التي يمكن من خلالها تحويل حسابات العملاء من بنك لآخر، فقام بتحويل مبالغ مالية قدرت بأربعة ملايين دولار لحسابه الخاص الموجود بالبنوك السويسرية وقام بالسفر إلى جنيف وسحب المبلغ بالكامل دون ملاحظة أحد أو معرفة حقيقة ما حدث لولا اعترافه بالجريمة وهو في حالة سكر^٣.

الفرع الثاني: الاحتيال التجاري.

تعد جريمة الاحتيال التجاري إحدى صور الجريمة المستخدمة بوسائل تقنية المعلومات، وتتم عند عدم تسليم البضائع للمشتري الذي دفع ثمنها إلكترونياً، وقد انتشرت هذه الجرائم مع انتشار البيع والشراء على الإنترنت^٤، كمن يستخدم المواقع الوهمية كأحد أشكال الهجمات التي يتم توظيفها في ارتكاب الأفعال غير القانونية مثل انتحال الهوية والاحتيال الإلكتروني من خلال

^١ يوسف خليل يوسف العفيفي، "الجرائم الإلكترونية في التشريع الفلسطيني-دراسة تحليلية مقارنة"، الجامعة الإسلامية، غزة، رسالة ماجستير، ١٤٣٥ / ٢٠١٣، ص ٢٣-٢٤.

^٢ أنظر المادة (١١) من قانون اتحادي رقم (٢) لسنة ٢٠١٦ في شأن مكافحة جرائم تقنية المعلومات.

^٣ محمد طارق الخن، "مرجع سابق"، ص ٤٨-٤٩.

^٤ خالد ممدوح العزي، "الجرائم المالية الإلكترونية الجرائم المصرفية انموذجاً"، مركز جيل البحث العلمي، المؤتمر الدولي الرابع عشر، طرابلس ٢٤-٢٥ مارس ٢٠١٧، ص ١٤٧.

محاكاة هذه المواقع للواجهة الخاصة للمواقع الرسمية المعروفة مثل e-bay لخداع المستخدمين للإفصاح عن بياناتهم الشخصية والبنكية^١.

ومن أمثلة الاحتيال التجاري ما قضت به محكمة جورجيا التي قامت باستدعاء أربعة متهمين بتهمة الاحتيال عبر الإنترنت عبر موقع e-bay حيث قام المتهمين باستخدام الموقع لبيع إطارات سيارات ولكن المشتريين لم تصلهم البضائع بعد أن قاموا بتحويل الأموال عبر الإنترنت، فقد قدر ما تم دفعه للمتهمين ٥٣٩,٠٠٠ دولار ثمن لبضائع لم يتم توصيلها^٢.

ولتفادي عمليات الاحتيال التجاري عبر الإنترنت ينصح بالآتي:^٣

١. رفض العروض الدعائية التي تأتي عن طريق البريد الإلكتروني.
٢. الابتعاد عن العروض التي تعرض العمل في المنزل.
٣. عدم الشراء من المواقع الإلكترونية التي لا تذكر عنوانها البريدي أو أرقام هواتفها.
٤. عدم الطلب من أي شخص القيام بتعديل السجلات الانتمانية.

الفرع الثالث: الاحتيال بواسطة الأوراق المالية.

لقد ارتبط تطور الأوراق المالية بالتطور التاريخي بالاقتصاد والصناعة في معظم دول العالم خصوصاً الدول الرأسمالية، مما سمح بتزايد انتشارها عند المستثمرين، لكونها تسمح لهم بعمليات البيع والشراء من منازلهم باستخدام حواسيبهم الشخصية، هذا الأمر سمح لعمليات الاحتيال الإلكتروني على المستثمرين عن طريق^٤:

^١ بدر بن أحمد بن محمد الزهراني، "مرجع سابق"، ص ٨٩.

^٢ محمد طارق الخن، "مرجع سابق"، ص ٥١.

^٣ مروة شبل عجيزة، خالد بطي الشمري، "مرجع سابق"، ص ٦١-٦٢.

^٤ عبد القادر أحمد محمد الصباغ، "قيد الأوراق المالية في البورصة دراسة مقارنة بين النظامين المصري والسعودي"، المركز العربي للنشر والتوزيع، مصر، ٢٠١٨، ط١، ص ٢٥.

١. توفر هذه العملية للمحتالين القدرة على الاتصال الإلكتروني بآلاف الضحايا من خلال استخدام مواقع احتيالية إشهارية عن توفير معلومات استثمارية صحيحة للمستثمرين.

٢. يصعب العثور على المحتالين باستخدام هذه العملية لكون المحتال مجهول الهوية على الإنترنت ويمكن أي يرتكب جريمته من أي مكان بالعالم وفي أي زمان مما يجعل الأمر غاية في الصعوبة في كشف جريمته والقبض عليه.

ويتم استخدام هذه الصورة أيضاً من خلال نشر معلومات غير صحيحة عن أسهم بعض الشركات من أجل زيادة الاستثمار في الشركة، هذا الأمر يزيد من قيمة الأسهم، في هذه الحالة ومع ارتفاع قيمة الأسهم يسهل على المحتالين بيع الأسهم التي يملكونها في هذه الشركة بمبالغ وأرباح طائلة، وفي الجانب الآخر من اشترى هذه الأسهم بناء على معلومات مغلوطة سيخسرون مبالغ مالية كبيرة عن قيامهم بإعادة بيع الأسهم^١.

ومن الصور الأخرى أن يتم الترويج لشراء أسهم من قبل محتالين تابعين لشركات غير معروفة وعمل دعاية مضللة للشركة وإرسال رسائل الكترونية ونشر معلومات غير صحيحة عن الشركة في غرف الحوار بغية تضليل المشتركين عن طبيعة هذه الشركة وأرباحها الطائلة في حال تم شراء أسهمها في السوق المالية، وبعد ارتفاع أسعار الشركة يتم بيعها والحصول على أرباح طائلة انطلاقاً من المعلومات المغلوطة التي تم نشرها سابقاً حول الشركة وأسهمها^٢.

ذهب المشرع البحريني في المادة الثانية من القانون رقم ٤ لسنة ١٩٨٧ الخاص بإنشاء وتنظيم سوق البحرين للأوراق المالية بقوله يقصد بالأوراق المالية في تطبيق أحكام هذا القانون أسهم وسندات الشركات المساهمة البحرينية والسندات والأذونات التي تصدرها الحكومة أو إحدى الهيئات والمؤسسات العامة البحرينية أو أية أوراق مالية أخرى بحرينية أو غير بحرينية مرخص بتداولها من مجلس إدارة السوق. ونظمها أيضاً المشرع البحريني في المادة الأولى من قانون رقم ٦٤ لسنة ٢٠٠٦ بشأن قانون مصرف البحرين المركزي والمؤسسات المالية، بقوله يعتبر سوق الأوراق المالية سوق مرخص له من قبل المصرف المركزي ليتم من خلاله تداول الأوراق المالية وفقاً لأحكام هذا القانون، وحدد في نفس الوقت في نفس المادة المقصود بالأوراق المالية وهي الأسهم والسندات التي تصدرها الشركات المساهمة وأدوات الدين العام وأية أدوات مالية أخرى يعتمد عليها المصرف المركزي كأوراق مالية.

^١ محمد طارق الخن، "مرجع سابق"، ص ٥٢.

^٢ بدر بن أحمد بن محمد الزهراني، "مرجع سابق"، ص ٣٨.

إلى جانب تنظيمه لعملية تداول الأوراق المالية ومن له الحق في طلب التراخيص لتقديم الخدمات المصرفية، ووفقاً للقرار رقم ٢٣ لسنة ٢٠١٩ الصادر عن المصرف المركزي بوضع لائحة للتعامل في الأوراق المالية عن طريق الإقتراض والبيع على المكشوف قضى فيه في المادة الثالثة أن التعامل في الأوراق المالية تخضع للضوابط والإجراءات المنصوص عليها في القانون وفي هذه اللائحة نفسها والتعليمات الصادرة تنفيذا لهما.

أما المشرع الإماراتي فقد ورد بقانون هيئة وسوق الإمارات للأوراق المالية والسلع رقم ٤ لسنة ٢٠٠٠ على أنه يقصد بالأوراق المالية الاسهم والسندات والاذونات المالية التي تصدرها الشركات المساهمة والسندات والاذونات التي تصدرها الحكومة الاتحادية أو الحكومات المحلية والهيئات العامة والمؤسسات العامة في الدولة واية ادوات مالية اخرى محلية او غير محلية تقبلها الهيئة .

وقد نظمت عملية تداول الأوراق المالية عند المشرع الإماراتي، حيث اقتصر التعامل في الأوراق المالية المدرجة في السوق على الوسطاء المرخص لهم وفقاً لنص المادة رقم ٢٤-٣ من ذات القانون.

وأكد المشرع السعودي التعاملات في الأوراق المالية المقيدة فيها من خلال سمسرة يتم تنظيم عملهم قانونياً - من أجل حماية المتعاملين الذين ليس لهم خبرة - وتوهمهم للقيام بعملية البيع والشراء في سوق الأوراق المالية من تلقاء أنفسهم فلا يستطيعون دخول ما تسمى مقصورة تنفيذ العمليات الخاصة بهم إلا من خلال سمسار لحمايتهم وعدم تعرضهم لقرصنة المضاربين، كما تعتبر هذه الطريقة قصر التعامل بالأوراق المالية على المختصين وضمان لحسن سير السوق وتوحيد القواعد المتعلقة به^١.

كما ونظم عمليات الاحتيال الواقعة بواسطة الأوراق المالية في المادة ٤٩ - ٥٠ من نظام السوق المالية السعودي رقم ٣٠ والصادر بتاريخ ٢٠١٤/٦/٢ بقولها:

أ- يعد مخالفاً لأحكام هذا النظام أي شخص يقوم عمداً بعمل أو يشارك في أي إجراء يوجد انطباعاً غير صحيح أو مضللاً بشأن السوق، أو الأسعار، أو قيمة أي ورقة مالية،

^١ عبد القادر أحمد محمد الصباغ، "مرجع سابق"، ص ٥٠.

^٢ راجع نظام السوق المالية السعودي رقم ٣٠ والصادر بتاريخ ٢٠١٤/٦/٢، على الموقع الإلكتروني التالي:

<http://cutt.us/aEodA>

بقصد إيجاد ذلك الانطباع، أو لحث الآخرين على الشراء أو البيع أو الاكتتاب في تلك الورقة، أو الإحجام عن ذلك أو لحثهم على ممارسة أي حقوق تمنحها هذه الورقة، أو الإحجام عن ممارستها.

ب- تضع الهيئة القواعد التي تحدد الأعمال والتصرفات التي تشكل مخالفات للفقرة (أ) من هذه المادة. وتحدد تلك القواعد الأعمال والممارسات المستثناة من تطبيق أحكام الفقرة (أ) من هذه المادة. وتشمل صلاحيتها المنصوص عليها في هذه الفقرة وضع القواعد، وتحديد الظروف والإجراءات الهادفة للمحافظة على استقرار أسعار الأوراق المالية المعروضة للجمهور، والأسلوب والوقت الذي يتعين فيه اتخاذ هذه الإجراءات .

ت- يدخل في الأعمال والتصرفات التي تعد من أنواع الاحتيال التي تحظرها الفقرة (أ) من هذه المادة التصرفات الآتية:

١. القيام بأي عمل أو تصرف بهدف إيجاد انطباع كاذب أو مضلل يوحي بوجود عمليات تداول نشط في ورقة مالية خلافاً للحقيقة. ويدخل في تلك الأعمال والتصرفات على سبيل المثال لا الحصر ما يأتي:

أ- القيام بعقد صفقات في أوراق مالية لا تتطوي على انتقال حقيقي لملكية تلك الأوراق المالية .

ب- القيام بإدخال أمر أو أوامر لشراء ورقة مالية معينة مع العلم المسبق بأن هناك أمراً أو أوامر بيع مشابهة من حيث الحجم والسعر والتوقيت قد أدخلت أو ستدخل من قبل طرف أو أطراف أخرى مختلفة لنفس الورقة المالية .

ت- القيام بإدخال أمر أو أوامر لبيع ورقة مالية معينة مع العلم المسبق بأن هناك أمراً أو أوامر شراء مشابهة من حيث الحجم والسعر والتوقيت قد أدخلت أو ستدخل من قبل طرف أو أطراف أخرى مختلفة لنفس الورقة المالية.

٢. التأثير بشكل منفرد أو مع آخرين على سعر ورقة أو أوراق مالية معينة متداولة بالسوق، عن طريق إجراء سلسلة من العمليات في تلك الورقة أو الأوراق المالية من شأنه أن يحدث طلبات فعلية أو ظاهرية نشطة في التداول، أو يحدث ارتفاعاً أو انخفاضاً في أسعار تلك الأوراق بهدف جذب الآخرين، وحثهم على شراء أو بيع هذه الأوراق حسب واقع الحال.

٣. التأثير بشكل منفرد أو مع آخرين بإجراء سلسلة من الصفقات كشراء أو بيع، أو كليهما معاً، ورقة مالية متداولة في السوق بهدف تثبيت أو المحافظة على استقرار سعر تلك الورقة، بالمخالفة للقواعد التي تضعها الهيئة لسلامة السوق وحماية المستثمرين.

الفرع الرابع: الاحتيال عبر انتحال الشخصية والبريد الإلكتروني.

يعتبر انتحال الشخصية أو الصفة شكل من أشكال السرقة عبر الإنترنت عن طريق استخدام البريد الإلكتروني للاحتيال على الشخص المتلقي للبريد، والذي يكون مرتبط برابط ومواقع احتيالية بغية خداعهم وجعلهم يفشون بياناتهم الشخصية والمالية كإدخال أرقام بطائهم الإلكترونية وأرقامهم السرية، ويعرف هذا الاحتيال بأنه: "الحصول بوسائل احتيالية على معلومات من الإنترنت تخص شخصاً معيناً مثل الاسم وتاريخ الميلاد والمهنة والجنسية دون علمه، ويقع ذلك في الأغلب بهدف ارتكاب جرائم احتيال بوسائل تقنية المعلومات، ومن خلال هذه البيانات يمكن للمنتحل الحصول على قروض وبطاقات ائتمان أو يقوم بفتح حسابات مصرفية بأسماء أشخاص حقيقيين"^١.

ومن أمثلة هذا الأسلوب القيام بإرسال رسالة إلكترونية عبر البريد للعميل تفيد بضرورة تحديث بياناته بمعلومات مالية محددة وإلا أضطر الموقع محل التعامل بإغلاق حسابه، دون ملاحظة أن الرسالة تحتوي على رابط احتيالي يتم الضغط عليه لإدخال البيانات الشخصية والمالية، في هذه الحالة سيلاحظ العميل أنه خسر مئات الآلاف عن طريق هذه الوسيلة الاحتيالية^٢.

وهناك وسائل أخرى تتم بواسطة البريد الإلكتروني أبرزها (البريد الإلكتروني النيجيري) الذي يتلقى الضحية رسالة تفيد بأنه الوريث الشرعي لابن الرئيس، أو أن مستلم الرسالة سيحصل على مبالغ نقدية وكل ما هو مطلوب إرسال مبلغ نقدي زهيد كجزء من أجرة المحامي وعليه يتم الطلب من الضحية الاسم الثلاثي وعنوان السكن ورقم الهاتف وصورة الهوية وبياناته البنكية والمالية^٣.

وفي هذا الإطار قد أوضحت إحدى المؤسسات البحثية الأمريكية (مؤسسة غارتنر) أنه في الأشهر ١٢ المنتهية في مايو ٢٠٠٥ بلغ ثلاثة وسبعين مليون رسالة في الولايات المتحدة تلقى خلال العام كل شخص على الأقل ٥ رسائل أو أكثر من رسائل البريد الإلكتروني الاحتيالية، وبلغ نسبة الخسائر المالية ١,٢ مليون دولار في مايو ٢٠٠٤ و ٢٠٠٥ نتيجة

^١ خالد حامد مصطفى، "مرجع سابق"، ص ١١.

^٢ محمد طارق الخن، "مرجع سابق"، ص ٦٤.

^٣ خالد حامد مصطفى، "مرجع سابق"، ص ١٢. محمد طارق الخن، "مرجع سابق"، ص ٦٦.

الاحتيال الإلكتروني، وفي تقرير التهديدات الأمنية على الإنترنت الصادر في سبتمبر ٢٠٠٦ من قبل شركة Symantec أن الشركة اكتشفت ما يقارب ١٥٧,٤٧٧ رسالة احتيالية تهدف إلى سرقة البيانات الشخصية ومن الغريب في الأمر أن كل رسالة احتيالية تختلف عن الأخرى وطريقة مختلفة لمحاولة خداع الأشخاص للحصول على بياناتهم الشخصية^١.

إلى جانب الصور السابقة يتبين أن صور الاحتيال تتطور مع التطور التكنولوجي الحاصل فلا يمكن حصر هذه الصور نظراً لتنوع الأساليب المستخدمة في عمليات الاحتيال المعلوماتي^٢، إلى جانب ما ذكر من صور إلا أن هناك صور متعددة كالاختيال عبر البريد الإلكتروني الذي بدوره تنتج الطرق التي تتم من خلاله، وهناك الاحتيال المهني الذي يرتكبه الموظف أو العامل داخل المؤسسة، والاحتيال في مجال الاتصالات وغيرها من الصور لذلك آثرنا أن نتحدث عن الصور الشائعة مع الاقتصار على التطرق إلى صورة الاحتيال بواسطة بطاقة الائتمان لأهميتها في المطلب الثاني على أساس اعتبارها نموذج وصورة خاصة من صور الاحتيال المستخدمة بواسطة تقنية المعلومات.

¹ Rika Butler (2007). "A framework of anti-phishing measures aimed at protecting the online consumer's identity", The Electronic Library, Vol. 25 Issue: 5, pp.517-533. <https://www.researchgate.net/publication/220677176/download>

² للمزيد حول الصور الأخرى للاختيال أنظر، رضا أحمد المزغني، "أساليب وصور الاحتيال المنظم"، جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث قسم الندوات واللقاءات العلمية، ندوة نظمت بالمنصورة بتاريخ ٢٠٠٧-٢٠-١٨ حول العلاقة بين جرائم الاحتيال والإجرام المنظم، ص ١١-٢١.

المطلب الثالث

الصور الخاصة للاحتيال عن طريق بطاقات الائتمان

انتشر مفهوم التجارة الإلكترونية في سبعينات القرن الماضي لسهولة الاتصال بين الأطراف واختزال المعاملات الورقية والبشرية، إضافة لسرعة إرسال البيانات وتخفيض القدرة التشغيلية لبعض الشركات والبنوك، وتحولت كافة الأعمال عبر الإنترنت، وتلا ذلك خطر يهدد هذه التجارة وهذا ما أثبتته شبكة Msnbc بسهولة الحصول على بطاقات الائتمان^١.

وتعتبر بطاقات الائتمان من أشهر الوسائل التي تتعرض للاحتيال باستخدام وسائل تقنية المعلومات، وهي ليست بعيدة عن صور احتيال البيانات الشخصية والبريد الإلكتروني فهذه الصور مترابطة في الهدف وهو الاحتيال على الأشخاص لسرقة الأموال أو استخدام هذه البيانات في سرقتها، ففي الولايات المتحدة تم اكتشاف ثمانية عشر شخصاً سرقوا مما يقارب ٢٠٠ مليون دولار باستخدام بطاقات الائتمان^٢.

ونسنتعرض في هذا المطلب تعريف بطاقات الائتمان وتوضيح أنواعها كما سنبيين كيفية وقوع الاحتيال بواسطة بطاقات الائتمان وإساءة استعمالها، وعليه سنقوم بتقسيم المطلب إلى أربعة فروع كالآتي:

الفرع الأول: تعريف بطاقات الائتمان.

الفرع الثاني: أنواع بطاقات الائتمان.

الفرع الثالث: الحماية القانونية لبطاقات الائتمان.

الفرع الرابع: الاحتيال بواسطة بطاقات الائتمان وإساءة استعمالها.

^١ محمد سالم الزعبي، "الجرائم الواقعة على السمعة عبر تقنية المعلومات الإلكترونية"، المجلس الوطني للإعلام، الإمارات، ٢٠١٤، ط١، ص ٢٥.

^٢ بدر بن أحمد بن محمد الزهراني، "مرجع سابق"، ص ٨١.

الفرع الأول: تعريف بطاقات الائتمان.

عرفت بطاقة الائتمان على أنها الكارت الممغنط الذي يطلق عليه الفيزا كارت، ويعبر عنه بعلاقة تعاقدية بين العميل والبنك يتم على أثره إعطاء العميل الحق في سحب النقود من أجهزة الصراف الآلي التابعة للبنك وكذلك عمليات الشراء من خلال ما هو مسموح به على الشبكة المعلوماتية والمرتبطة بالبنك، مع تحديد الحد الأدنى والأقصى لعمليات سحب النقود وتختلف من كل دولة إلى أخرى ومن بطاقة لأخرى ومن بنك لبنك، هذه الفيزا مرتبطة برقم سري يحتفظ به العميل وباستعماله عن طريق إدخاله إلى نظام المعالجة الآلية للبيانات الخاص بالبنك، وبمجرد إدخال الفيزا وإدخال الرقم السري يتم سحب النقود^١.

وتعتبر هذه البطاقة أداة للتعامل المالي والدفع بها على مستوى العالم، ناتجة عن عقد ثلاثي، تصدر من بنك تجاري، تمكّن حاملها من إجراء عقود خاصة والحصول على خدمات خاصة^٢، وهي بطاقة مصنوعة من مادة بلاستيكية تحتوي على شريط ممغنط يتضمن بيانات عن حساب العميل لدى البنك، كما يتضمن شريطاً لاصقاً مدوناً عليه توقيع صاحب الحساب، بالإضافة إلى صورة شخصية للعميل، تستخدم في سحب المبالغ النقدية وفي دفع ثمن المشتريات^٣.

وهناك من عرفها بأنها بطاقة يصدرها البنك أو المصرف لعميله، تمكنه من الحصول على السلع، والخدمات من محلات وأماكن معينة، ويقوم بائع السلع أو الخدمات بتقديم الفاتورة الموقعة من العميل إلى البنك أو المصرف مصدر البطاقة فيسدد قيمتها، ويقدم البنك أو المصرف للعميل كشفاً شهرياً بإجمالي القيمة لتسديدها أو خصمها من حسابه الجاري^٤.

^١ بلال أمين زين الدين، "جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية"، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨، ط١، ص ١٤٦.

^٢ أبو الوفا محمد أبو الوفا إبراهيم، "المسؤولية الجنائية عن الاستخدام غير المشروع لبطاقة الائتمان في القانون المقارن والفقه الإسلامي"، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون لكلية الشريعة والقانون وغرفة تجارة وصناعة دبي والذي عقد في دولة الإمارات العربية المتحدة للفترة من ١٠-١٢/٥/٢٠٠٣، ٢٠٠٣، ص ٢٠٤٤.

^٣ محمد حماد مرهج الهيبي، "الحماية الجنائية لبطاقات الائتمان الممغنطة"، دار الكتب القانونية، مصر، ٢٠٠٩، ص ٣٩.

^٤ سمير دنون، "العقود الإلكترونية في إطار تنظيم التجارة الإلكترونية"، المؤسسة الحديثة للكتاب، لبنان، ٢٠١٢، ط١، ص ١٦٥.

كما وعرفها مجمع الفقه الإسلامي بأنها: "مستند يعطيه مصدره، لشخص طبيعي أو اعتباري - بناء على عقد بينهما - يمكنه من شراء السلع، أو الخدمات ممن يعتمد المستند، دون دفع الثمن حالاً، لتضمنه التزام المصرف بالدفع ومن أنواع هذا المستند ما يمكن من سحب نقود من المصارف"^١.

الفرع الثاني: أنواع بطاقات الائتمان.

إن البطاقات الائتمانية ذات طبيعة خاصة تختلف عن الأوراق المالية الأخرى لذا انعكست الجرائم الواقعة عليها بطبيعة خاصة تميزها عن الجرائم الأخرى، لذلك لا بد من توضيح أنواع هذه البطائق لمعرفة طرق الاحتيال المستخدمة عن طريقها وهي:

١. **بطاقات الحساب:** تتيح هذه البطاقات لمستخدمها الدفع من خلالها وخصم من رصيده في نهاية الشهر.

٢. **بطاقات الصراف الآلي:** تمكن هذه البطاقات حاملها من الدخول أو السحب من رصيده البنكي أو الإيداع من خلال جهاز خارج البنك أو المصرف، وتتميز هذه البطاقة عن غيرها من البطائق بكونها مرتبطة بحساب حاملها الصراف الآلي مباشرة، حيث يعتمد السحب الآلي للنقود على أجهزة الاتصال الإلكتروني، فلا يمكن إن تعمل بالطرق اليدوية وإنما بالخط المباشر حيث يرتبط حامل البطاقة بالجهاز الآلي بقسم المحاسبة للعملاء، عند إجراء أي معاملة^٢.

٣. **بطاقات ضمان الشيكات:** يكون على ظهر البطاقة مجموعة من البيانات ويستوجب الدفع لحاملها حتى دون وجود رصيد، حيث يقوم صاحب البطاقة بتقديم البطاقة لدائنه الذي يقوم بتعبئة بياناتها على ظهر الشيك، فكتابة البيانات والتوقيع عليه يضمن للمستفيد قيمته من طرف البنك المصدر للبطاقة سواء كان بها رصيد أو غير متوفرة على رصيد^٣.

^١ محمد جلال عبد الرحمن، "الجرائم الإلكترونية في الفقه الإسلامي والقوانين المقارنة" دراسة مقارنة، مكتبة القانون والاقتصاد، الرياض، ط١، ٢٠١٥م، ص ٢٥٧.

^٢ محمد حماد مرهج الهيتي، "مرجع سابق"، ص ٤٧.

^٣ كوثر فرام، "الجريمة المعلوماتية على ضوء العمل القضائي المغربي"، المعهد العالي للقضاء، وزارة العدل، ٢٠٠٩، ص ٣٥.

٤. البطاقات الذكية: عبارة عن بطاقات بلاستيكية تتشابه مع بطاقات الائتمان وهي مزودة بحاسوب به ذاكرة تسمح بتخزين بيانات يمكن استخراجها بصورة منظمة، وتشحن هذه البطاقة بمبلغ من المال بحيث يمكن الاقتطاع منه آلياً عن الوفاء بجهاز خاص^١.

الفرع الثالث: الحماية القانونية لبطاقات الائتمان.

نظراً لتطور تقنية المعلومات الذي شهده هذا العصر، والذي قد لا تواكبه النصوص العقابية التقليدية وجعل بعض الوقائع تفلت من التجريم على الرغم من خطورتها، مما جعل بعض التشريعات تضع الحماية القانونية لبطاقة الائتمان لكونها إحدى مظاهر التطور في هذه التقنية.

فقد جرم المشرع البحريني بالاعتداء على بطاقات الائتمان من قانون جرائم تقنية المعلومات حيث نص في المادة السادسة على أنه:

"يعاقب بالحبس مدة لا تزيد على سنة وبالغرامة التي لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين، من قام بقصد ارتكاب أي من الجرائم المنصوص عليها في المواد (١، ٢، ٣، ٤، ٥) من هذا القانون بإنتاج أو استيراد أو شراء أو بيع، أو عرض للبيع أو للاستخدام، أو توزيع أو تداول أو حيازة أو نشر أو إتاحة:

أ- أداة - بما في ذلك أي برامج - تم تصميمها أو تحويلها بصفة أساسية لغرض ارتكاب أي من الجرائم المشار إليها.

ب- كلمة مرور أو شفرة دخول أو أي رمز دخول أو أية بيانات وسيلة تقنية المعلومات أخرى مماثلة، يمكن بواسطتها الدخول إلى نظام تقنية المعلومات أو أي جزء منه".

كما جرم المشرع الفرنسي مجموعة من الأفعال التي محلها بطاقات إلكترونية من خلال النص في المادة (١١) من القانون رقم ١٣٨٢-٩١ الصادر عام ١٩٩١ على تجريم ثلاث أفعال يكون محلها بطاقة إلكترونية الأول يتمثل بجريمة تزوير أو تقليد بطاقات الوفاء، والثاني جريمة استعمال أو محاولة استعمال بطاقة مقلدة أو مزورة، أما الثالث فهو جريمة قبول الوفاء بواسطة بطاقة مقلدة أو مزورة، ويتبين أن المشرع الفرنسي اقتصر في التجريم على أفعال التزوير والتقليد

^١ علي حسن الطوالبة، "مرجع سابق"، ص ١٦٢.

دون التطرق لأفعال إساءة استخدام البطاقات الإلكترونية^١. وعرفها في المادة الثانية من ذات القانون على إنها: "أداة تصدر من إحدى مؤسسات الائتمان، أو إحدى الجهات المنصوص عليها في المادة (٨) من القانون رقم ٨٤/٤٦ والخاص بنشاط ورقابة مؤسسات الائتمان، وتسمح لحاملها بسحب أو تحويل النقود من حسابه"^٢.

أما المشرع الإماراتي فقد نص على تجريم الاستيلاء المعلوماتي في المادة (١٢) من خلال عقوبة الحبس والغرامة أو بإحدى هاتين العقوبتين لكل من توصل بغير حق، عن طريق استخدام الشبكة العنكبوتية أو نظام معلوماتي إلكتروني أو إحدى وسائل تقنية المعلومات، إلى أرقام أو بيانات إلكترونية بطاقة ائتمانية أو أرقام أو بيانات حسابات مصرفية^٣.

كما نص المشرع السعودي من نظام مكافحة جرائم المعلوماتية على عقاب الوصول - دون مسوغ نظامي صحيح - إلى بيانات بنكية أو ائتمانية أو أموال، وقد قرر لها عقوبة السجن لمدة لا تزيد عن ثلاث سنوات وغرامة لا تزيد على مليوني ريال أو إحدى هاتين العقوبتين^٤.

ويرى الباحث أن التعدد في استخدامات البطاقات الائتمانية والتنوع هو من أضفى عليها عنصر التداخل والغموض، وذلك بما تحمله من معلومات وبيانات مشفرة، وإن الاعتداء عليها سواء بالسرقة أو بالتزوير أو بالحصول على معلوماتها وبياناتها بطرق غير مشروعة يعد بحد ذاته اعتداء على ما تحمله هذه البطاقات من أموال بغض النظر عن طبيعة تكييف هذه الأموال وفي ذات الوقت هو اعتداء على الملكية الخاصة لصاحب هذه البطاقة.

^١ محمد جلال عبد الرحمن، "مرجع سابق"، ص ٢٧٦.

^٢ Gaston Stefanie, (1995). G.Levasseur, B Baulac, dreuit penal general D 15, Dolla, 2, p.236.

^٣ أيمن عبدالله فكري، "الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية"، مكتبة القانون والاقتصاد، الرياض، ط١، ٢٠١٥م، ص٦٠٢.

^٤ قرار رقم (١٧) الصادر بتاريخ ١٤٢٨/٣/٧هـ، بشأن نظام مكافحة جرائم المعلوماتية السعودي.

الفرع الرابع: الاحتيال بواسطة بطاقات الائتمان وإساءة استعمالها.

أن انتشار استخدام البطاقات الائتمانية من خلال شبكة الإنترنت أدى لظهور جرائم التسلل للسطو عليها على اعتبار أنها نقود إلكترونية وهو أمر بالنسبة للمتسلل غير ذات صعوبة فمثلا يستطيع المحتالون سرقة المئات من أرقام البطاقات وبيعها للآخرين، وتتم هذه العملية من خلال الحصول على كلمات السر المدرجة في أجهزة الكمبيوتر الخاصة بالمجني عليه.

وقد تنوعت الطرق الواقعة على بطاقات الائتمان نذكر منها:^١

١. تحميل العميل لفواتير مصطنعة.
٢. التحايل من أجل الحصول على البيانات الشخصية للعملاء للحصول على بطاقات ائتمانية صحيحة.
٣. استخدام بيانات شخصية مزورة للحصول على بطاقات ائتمانية صحيحة.
٤. يمكن أن يتم سرقة بطاقات إئتمانية صحيحة أو سرقة الأرقام السرية للأشخاص الحقيقيين في حال إرسالها من قبل البنوك والمصارف إلى عملائهم بواسطة موظفي البريد.
٥. الاحتيال باستخدام الهاتف عن طريق المودم لمعرفة كلمات المرور أو كلمة السر للحصول لاحقا للأرقام السرية لبطاقات الائتمان.
٦. إمكانية اختراق النظام وحسابات العملاء وأرقام هوياتهم الشخصية وبياناتهم واصطناع بطاقات مزيفة تحتوي على معلومات صحيحة يمكن قبولها من المصارف والبنوك.

وقد اختلف الفقه والقضاء بشأن الطرق الاحتيالية التي يستخدمها الجاني في إساءته لاستخدام بطاقات الائتمان، إذ يمكن أن يتحقق التلاعب في الأنظمة المعلوماتية باستخدام الطرق الاحتيالية عن طريق إدخال بطاقات الائتمان والبطاقات الإلكترونية البنكية سواء عن طريق صاحبها أو إذا كانت مسروقة أو معثور عليها، أو استعمال رمز صاحب البطاقة بعد التعرف عليه بطريقة ما لسحب أموال من رصيده البنكي.^٢

^١ بدر بن احمد بن محمد الزهراني، "مرجع سابق"، ص ٣٩ - ٤٠.

^٢ بلال أمين زين الدين، "مرجع سابق"، ص ١٤٧.

ويرى جانب آخر أن الصراف الآلي وسيط بحيث تكون جريمة الاحتيال قائمة لتوافر عناصر الاحتيال في مواجهة مالك الجهاز ذاته وليس الجهاز^١.

لذلك ارتأينا تقسيم حالات إساءة البطاقة الائتمانية وفقاً للآتي:

١. إساءة استخدام البطاقة أثناء صلاحيتها. تتم عملية إساءة استعمال هذه البطاقة أثناء

مدة صلاحيتها عند قيام صاحب البطاقة بشراء السلع وملء الاستمارة الإلكترونية مع علمه بعدم توافر الرصيد الكافي في البطاقة، أو أن يقوم بتحويل الرصيد لآخر متجاوزاً الحد المسموح له من طرف البنك، فقد تأرجحت الآراء الفقهية والقضائية حول اعتباره من جرائم الاحتيال أو خيانة الأمانة، فذهب القضاء الفرنسي على اعتبارها جريمة ووصفها بالسرقة، واعتبرها الفقه الإنجليزي من الطرق الاحتيالية التي تقوم على النصب؛ أما الفقه الأمريكي فعارض هذه الآراء واعتبر الفعل نصباً بتجاوز الرصيد المسموح به على أساس أن المصرف هو الذي سمح للعميل بالسحب من عدمه، واستخدم الطرق العادية للسحب ولم يحدث أن استعمل الطرق الاحتيالية، ويرفض اعتبارها من قبل خيانة الأمانة وفي حالة رفض العميل إعادة الأموال يوصف بخيانة الأمانة ويعاقب على أثرها^٢.

٢. إساءة استخدام البطاقة المنتهية صلاحيتها أو الملغاة. حيث إن استخدام البطاقة

في كلا الحالتين جريمة نصب تتوافر فيها أركان الجريمة، لأن صاحبها لم يتم بتجديدها أو أغلق حسابه في البنك، فهذا يعد وسيلة احتيالية تتجه لإقناع المجني عليه بوجود إئتمان وهمي، فإن سوء نية المتهم لا يمكن إنكاره فهو واضح في هذه الحالة حيث يتحقق ركن التسليم وهو قيام البنك بدفع ما هو مطلوب من مبالغ مالية من العميل، وهذا ما أخذت به محكمة باريس بحكمها الصادر عام ١٩٧٤ حيث قضت: "بأن هذا السلوك يعد من قبل الطرق الاحتيالية التي تهدف إلى الإقناع بوجود دين وهمي من أجل الحصول من البنك على المبالغ النقدية التي تم الاستيلاء عليها"^٣.

^١ بلال أمين زين الدين، "مرجع سابق"، ص ١٤٧.

^٢ محمد أمين أحمد الشوابكة، "مرجع سابق"، ص ١٩٥.

^٣ أحمد خليفة الملط، "الجرائم المعلوماتية-دراسة مقارنة"، كلية الحقوق جامعة القاهرة، أطروحة دكتوراه منشورة، ٢٠٠٥، ص ٤٠٩.

٣. إذا قام الغير باستخدام البطاقة المسروقة. جرت العادة بأن يتم تسليم البطاقات الائتمانية لحاملها مع التزامه بعدم إفشاء الرقم السري لأي شخص حتى لا يكون عرضة لعمليات السرقة والاحتيال والاستخدام غير المشروع لها من قبل الغير، وتظهر صورة الاحتيال عند قيام أحد الجناة بسرقة البطاقة الائتمانية من صاحبها الأصلي قبل تبليغ المجني عليه البنك، ودرجت المحاكم الفرنسية على اعتبار سرقة الأرقام والبيانات السرية الخاصة ببطاقة الائتمان واستخدامها بصورة غير مشروعة من قبل الغير يشكل جريمة نصب على أساس أن المتهم انتحل شخصية شخص آخر ومن ثم قد استخدم هذه الهوية لإقناع المجني عليه بوجود ائتمان^١.

٤. القيام بتزوير البطاقة الائتمانية. تعد هذه الطريقة من أخطر الصور الاحتيالية، ويعرفها الفقه على أنها: "تغيير الحقيقة في محرر بإحدى الطرق التي نص عليها القانون تغييراً من شأنه إحداث ضرر ومقترن بنية استعمال المزور فيما أعد له"، وتتم عملية تزوير بطاقات الائتمان في نطاق الشبكة المعلوماتية وتأخذ صورة تخليق أرقام بطاقات الائتمان خاصة ببنك معين، من خلال تزويد الحاسب بالرقم الخاص بالبنك مصدر البطاقة بواسطة برامج تشغيل خاصة، وعلى هذا الأمر اكتشفت بعض البنوك اعتراض بعض العملاء على عمليات لم يقوموا بها وتبين لاحقاً أنها من طرف الهاكرز والمخربين^٢.

ونجد أن بعض المحاكم البلجيكية قضت باعتبار من يستعمل بطاقة ائتمانية مسروقة أو مزورة سارقاً ويطبق عليه أحكام السرقة باستعمال مفتاح مصطنع، أما محكمة الفرنسية Rennes فاعتبرتها من الطرق الاحتيالية التي تقوم بها جريمة النصب كما قضت بالحكم على تاجر قبل التعامل بالبطاقة الائتمانية مع علمه بسرقتها وتقليدها واعتبرتها جريمة نصب، ويخضع للعقاب المنصوص عليه في المادة ٥٦٢/٥، التي تقابل المادة (٤٤١ / ٤١٠) من قانون العقوبات الفرنسي الصادر عام ١٩٨٨ والمعدل عام ١٩٩٤^٣، وكذلك وفقاً لنص المادة (٣١٧) من قانون العقوبات المصري^٤.

^١ محمد أمين أحمد الشوابكة، "مرجع سابق"، ص ٢٠٠. وراجع أيضاً، بلال أمين زين الدين، "مرجع سابق"، ص ١٤٩.

^٢ محمد أمين أحمد الشوابكة، "مرجع سابق"، ص ٢٠١.

^٣ بلال أمين زين الدين، "مرجع سابق"، ص ١٥٠ - ١٥١.

^٤ راجع في ذلك، أحمد خليفة الملط، "مرجع سابق"، ص ٤١١.

وفي هذا الإطار قضت محكمة الاستئناف بالمملكة المغربية الرباط في قرارها رقم ٢٩٩ بتاريخ ٢٣-٣-٢٠٠٦، بأن قيام مستخدمين أحدهما بمطعم بالرباط والآخر بمحطة الخطوط الجوية الهوية بمطار محمد الخامس الدولي بتمرير البطائق البنكية للزبناء بآلة مخصصة لقرصنة البطائق هو تزوير، لوجود النية الإجرامية، طبقا للفصل ٣٥٧ من القانون الجنائي المغربي^١.

كما وقضت المحكمة الفرنسية Rennes بأن استخدام البطاقة المزورة يعد من الطرق الاحتيالية التي تقوم بها جريمة النصب^٢.

وفي إحدى محاكم البحرين تم الطعن بالحكم بقضية نسخ التوقيعات الإلكترونية دون تفويض من أصحابها والاحتيايل والتزوير المؤيد لاسبابه والمكمل بالحكم المطعون فيه بين واقعة الدعوى في قوله أنها تتحصل في أنه في غضون شهر سبتمبر وحتى شهر ديسمبر من عام ٢٠٠٥ تردد المتهمان على المملكة بتأشيرات سياحية حيث كانا يقومان بالتنقل ليلا لدراسة أماكن أجهزة الصراف الآلي التابعة لبنوك الإسكان للتجارة والتمويل والبحريني السعودي والأهلي المتحد وستاندرد تشارترد بنك، وبنك البحرين الوطني وبنك البحرين الكويت، إذ يقوم المتهم الأول بتركيب أجهزة إلكترونية لنسخ البطاقات التي يقوم صاحبها بالسحب من البنوك من أجهزة الصراف الآلي عن طريق تثبيت كاميرا على الصراف بنفس لونه حتى لا تلفت الأنظار كي تلتقط الارقام السرية الخاصة بعملاء البنك، كما يقوم بتثبيت قطعة بلاستيكية على مكان إدخال البطاقة لقراءة المعلومات الموجودة على الشريط الممغنط الموجود بالبطاقة وحفظها وعن طريق أجهزة إرسال يتم استقبال كافة المعلومات التي تلتقطها تلك الأجهزة المثبتة بغرفة الصراف ثم يرسل المتهم الأول ما تضمنته الأجهزة من معلومات إلى جهة مجهولة، وأن المتهم الثاني كان يرافق الأول في تنقلاته بالسيارة المستأجرة من مطار البحرين والتغطية عليه حتى لا يتمكن أحد من رؤيته، وتمكنا من نسخ العديد من بطاقات الصراف الآلي لعملاء البنوك السالف بيانها وأرقامهم السرية والتي تم إرسالها إلى آخرين مجهولين تمكنوا من خلالها اصطناع بطاقات غير صحيحة بعد إفراغ تلك البيانات بها وسحبا بمقتضاها مبالغ من أرصدة أصحاب البطاقات الصحيحة دون علمهم^٣.

^١ كوثر فرام، "مرجع سابق"، ص ٤٥.

^٢ محمد أمين أحمد الشوابكة، "مرجع سابق"، ص ٢٠٢.

^٣ الطعن رقم ٩٦ جنائي لسنة ٢٠٠٧، منشور على الموقع التالي:

<http://elb-iis-web-303033976.eu-west-1.elb.amazonaws.com/Taan/>

المبحث الثالث

مدى انسجام جريمة الاحتيال باستخدام وسائل تقنية المعلومات مع

مفهومها التقليدي

جريمة الاحتيال بصفة عامة هي: "الاستيلاء على الحيازة الكاملة لمال بوسيلة يشوبها الخداع تسفر عن تسليم ذلك المال"^١، أي هو الاستيلاء بطريقة الاحتيال على شيء مملوك للغير بنية تملكه.

فجريمة الاحتيال تقوم على أركان وهي الركن الشرعي القائم على مبدأ شرعية التجريم لهذه الجريمة وفق ما يتم صياغته من قوانين خاصة متعلقة بتنظيم العقوبة الخاصة بهذه الجريمة وبيان نصوص هذه الأحكام المتعلقة بجريمة الاحتيال المعلوماتي بمفهومه الحالي، والركن المادي الذي يتألف من فعل وهو الكذب ووسيلة الاحتيال أو التدليس، ثم نتيجة تتمثل في الاستيلاء على مال الغير وعلاقة سببية بين الاحتيال والاستيلاء وهو ما يقتضي أن يكون التسليم مرحلة لاحقة لاستعمال التدليس، ويجب كذلك أن تكون الوسائل الاحتيالية من شأنها أن تؤدي إلى تسليم المال نتيجة انخداع الضحية بها^٢.

ومن أركان جريمة الاحتيال المعلوماتي الركن المعنوي، فهو يتخذ صور القصد العام بالإضافة إلى القصد الخاص وهو عبارة عن نية المتهم في الاستيلاء على مال الغير^٣. للإحاطة أكثر بماهية هذا الأركان ومدى انسجامها مع جريمة الاحتيال المعلوماتي قمنا بتقسيم هذا المبحث كالآتي:

المطلب الأول: الركن الشرعي لجريمة الاحتيال المعلوماتي.

المطلب الثاني: الركن المادي لجريمة الاحتيال المعلوماتي.

المطلب الثالث: الركن المعنوي لجريمة الاحتيال المعلوماتي.

^١ هشام محمد رستم، "قانون العقوبات ومخاطر تقنية المعلومات"، مكتبة الآلات الحديثة، القاهرة، ١٩٩٤م ص ٢٦٨.

^٢ احسن أبو سقيعة، "الجرائم ضد الأشخاص والجرائم ضد الأموال"، دار هومة، الجزائر، ٢٠٠٨م، ص ٣١٤.

^٣ أحسن أبو سقيعة، "مرجع سابق"، ص ٣١٥.

المطلب الأول

الركن الشرعي لجريمة الاحتيال المعلوماتي

إن تطور جريمة الاحتيال باستخدام وسائل تقنية المعلومات، وتعدد صورها، وضخامة ما تحدثه هذه الجرائم سواءً من المخاطر الاقتصادية والأمنية والاجتماعية أدى لتصدي بعض الدول لهذه الجريمة عبر نصوص قانونية خاصة للحد من سرعة انتشارها.

ولكن تجدر الإشارة هنا إلى حداثة هذه الجريمة فلا إشكالية تثار عند الحديث عن الأجهزة الإلكترونية المادية حيث تنطبق عليها نصوص التجريم التقليدية.

ويقصد هنا بالركن الشرعي عند فقهاء القانون هو البنيان القانوني للجريمة، وهو ما يطلق عليه أيضاً الركن القانوني للجريمة، ففي صياغة قديمة كان يعرف بنص التجريم الذي يخلق الجريمة، بمعنى أنه لا جريمة بدون نص، وهذا قول مردود عليه حيث لا يتصور أن يكون نص التجريم أحد أركان الجريمة، فإذا كان كذلك وجب العلم بنص التجريم لقيام القصد الجنائي، والجهل به ينفي وجود القصد الجنائي، وهذا يتنافى مع القاعدة العامة القائلة بأن الجهل بالقانون ليس عذراً^١.

ولذلك فقد تطور مفهوم الركن الشرعي حتى وصل إلى مفهومه الحالي والذي مفاده بأن المقصود من النص هي الصفة غير المشروعة للفعل المكون للجريمة، ويكتسب الفعل صفة التجريم إذا ما وجد نص يجرمه.

خلاصة القول يتبين مما سبق بأن الركن الشرعي للجريمة هو الصفة غير المشروعة للفعل وتتمثل قاعدة التجريم والعقاب للجريمة، وسيتم تقسيم المطلب إلى فرعين كالآتي:

الفرع الأول: مبدأ الشرعية الجزائية.

الفرع الثاني: قاعدة التجريم والعقاب لجريمة الاحتيال المعلوماتي في التشريعات المقارنة.

^١ احمد محمود مصطفى، "جرائم الحاسبات الآلية في التشريع المصري" دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠١٠م، ص ٩١.

الفرع الأول: مبدأ الشرعية الجزائية.

يقصد بمبدأ الشرعية الجزائية أن المشرع وحده هو الذي يملك تحديد الأفعال المعاقب عليها والمسماة بالجرائم وتحديد الجزاءات التي توقع على مرتكبيها والمسماة بالعقوبات.^١

وتجدر الإشارة هنا إلى أن هذا المبدأ يستوجب الأخذ بالفصل بين السلطات، حيث إن السلطة التشريعية وحدها لها صلاحية بيان الأفعال التي تعد جرائم وتقرر الجزاء الواجب على مثل هذه الأفعال لأنها صاحبة الاختصاص الأصيل في تشريع القوانين، فتتصرف سلطة القاضي في تطبيق التشريعات والقوانين الصادرة عن السلطة التشريعية، فلا يمكن لقاضي أن يعتبر فعلاً ما جريمة إلا إذا وجد نص قانوني يقضي بذلك، فإذا وجد الفعل مجزماً فلا يمكن أن يوقع سوى العقوبة الواردة في القانون.^٢

كما لا يمكن للسلطة التنفيذية توقيع جزاءات جنائية غير التي قضت بها الأحكام القضائية ولا تنفذ هذه الأحكام بأسلوب يغير ما نصت عليه القوانين.

إلا أن مبدأ الشرعية تعرض لانتقادات منها أنه يقيض سلطة القاضي الجزائي ويحول دون تحقيق العدالة المجتمعية إذا ارتبط الأمر بالتطور التقني وتأخر المشرع في إصدار قوانين تواكب هذا التطور مما يعطي المجال أمام مرتكبي الأفعال التي تضر بمصالح الأفراد والمجتمع وتنتال من أمنه، حيث أن التدخل التشريعي العقابي غالباً ما يأتي متأخراً.^٣

وقد طرأ تطوراً ملحوظاً على مبدأ الشرعية، تمثل في منح القاضي مرونة وسلطة تقديرية فيما يتعلق بتقدير العقوبة التي تتفق وظروف الجريمة، فقد تطور التشريع وجعل للعقوبة حداً أقصى وأدنى يتخير القاضي من بينهما ما يراه أكثر ملائمة مع وضع الجاني بل يذهب إلى أبعد من ذلك حين منح القاضي سلطة الأمر بوقف تنفيذ العقوبة متى ما تبين له من ماضي المتهم وأخلاقه وظروفه.^٤

^١ على حسين الخلف وسلطان عبد القادر الشاوي، "المبادئ العامة في قانون العقوبات"، مطابع الرسالة، الكويت، ١٩٨٢م، ص ٣٠.

^٢ على حسين الخلف وسلطان عبد القادر الشاوي، "مرجع سابق"، ص ٣٠.

^٣ فخري عبد الرزاق الحديشي، "شرح قانون العقوبات"، القسم العام، بغداد، ١٩٩٢م، ص ٣٦.

^٤ على الخلف وسلطان الشاوي، "مرجع سابق"، ص ٣٥.

كما وأعطيت السلطة التنفيذية حق التدخل في تنفيذ العقوبة بما تراه محققاً للغاية منها، مثل قرار العفو وتخفيف العقوبة والإفراج الشرطي عن المسجون قبل انتهاء مدة عقوبته إذا ثبت صلاحه^١.

خلاصة القول بالرغم من المرونة التي طرأت على مبدأ الشرعية إلا أنها اقتصررت على شقه الثاني وهو تقدير العقوبة دون أن تدخل ضمن الشق الأول وهو التجريم، فمنع القاضي من أي سلطة تقديرية في شأن تقدير الجرائم.

الفرع الثاني: قاعدة التجريم والعقاب لجريمة الاحتيال المعلوماتي في التشريعات المقارنة.

إن أغلب النصوص في التشريعات المقارنة لم تنص بشكل صريح على جريمة الاحتيال المعلوماتي، ولكن نجد بأن تجريم فعل الاحتيال يأتي في مضمون ودلالات النصوص التشريعية المختلفة.

وقد أورد المشرع البحريني الصور الخاصة التي يقع عليها الاحتيال المعلوماتي باستخدام وسائل تقنية المعلومات وأقر لها عقوبة^٢، وقد أشار المشرع السعودي على تجريم الاحتيال المعلوماتي وعقوبتها^٣. وأكد المشرع الإماراتي على تجريم الاحتيال المعلوماتي والعقوبة المقررة لها^٤، وقد خصص المشرع الإماراتي الطرق الاحتيالية الواقعة على البطائق الائتمانية والمصارف والبنوك ووسائل الدفع الالكتروني، وقد نص المشرع العماني على تجريم الاحتيال باستخدام وسائل تقنية وأقر لها عقوبة^٥.

ونصت المادة (٤) من المشروع النموذجي العربي الموحد على تجريم الاحتيال المعلوماتي والتي جاء فيها: "كل من استحوذ بالالتقاط بطريق التحايل على البرامج والبيانات المخزنة بالحاسب والمسجلة على شريط أو أسطوانات ممغنطة أو التي تظهر على الشاشة يعاقب..."^٦.

^١ فخري الحديثي، "مرجع سابق"، ص ٤٢.

^٢ أنظر نص المادة (٨) من قانون رقم ٦٠ لعام ٢٠١٤.

^٣ انظر رقم المادة (٤) من نظام مكافحة الجرائم المعلوماتية السعودي.

^٤ انظر نص المادة (١١) من مرسوم بقانون رقم (٥) لعام ٢٠١٢م.

^٥ أنظر المادة رقم (١٢) والمادة (١٣) من القانون الصادر بموجب القرار السلطاني رقم (١٢) لعام ٢٠١١م.

^٦ راجع في ذلك، محمد أحمد طه، "مرجع سابق"، ص ١٤٦.

وقد أقرت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠ تجريم الاحتيال المعلوماتي في المادة (١١) على أنه: "التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير، عن طريق:

١- إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات.

٢- التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها.

٣- تعطيل الأجهزة والبرامج والمواقع الالكترونية".

أما القوانين الأمريكية فهي ذهبت إلى تجريم الاحتيال عبر عدة قوانين تناولت من خلالها أشكالاً مختلفة من الاحتيال، ومعظمها يغطي التلاعب بالحواسيب كجزء من المخطط الاحتيالي ومنها قانون التآمر للاحتيال على الولايات المتحدة، وفي بريطانيا صدر قانون الاحتيال لعام ٢٠٠٦م والذي أورد في نصوص المواد (٢-٣-٤) ثلاث وسائل يمكن أن يرتكب بها الاحتيال^١.

أما المشرع الفرنسي فقد أقر قانون رقم ١٩ لعام ١٩٨٨م الخاص بحماية نظم المعالجة الآلية للبيانات، والذي أدرج فيما بعد ضمن قانون العقوبات وطبق في ١/٣/١٩٩٤م، والذي نصت مواده من (١-٣٢٣) من قانون العقوبات على تجريم الاحتيال المعلوماتي والبقاء غير المشروع داخل النظام أو في جزء منه^٢.

وبالرغم من أن المشرع في دول المقارنة وفي الدول الأجنبية قد قام بتحديد صور الاحتيال المعلوماتي وإقرار عقوبة لها، إلا أن الباحث يرى أن العقوبة يجب أن تتناسب مع تأثير الجريمة، فإذا ما وقعت بقصد التسلية والفضول فإن العقوبة يجب أن تكون أخف قياساً بالجرائم التي ترتب آثاراً جسيمة كتلك الماسة بالحقوق والمعلومات، وعليه يمكن إقتران العقوبة بالقصد وبما ترتبه من آثار.

^١ محمد طارق الخن، "مرجع سابق"، ص ١٠٥-١٠٦.

^٢ نص المادة (٣١٣/١) يعاقب كل شخص قام باستخدام اسم أو صفة زائفة أو باستخدام أساليب احتيالية بالإيهام بوجود شركات وهمية أو بالقدرة على إيجاد اعتقاد وهمي أو بالعمل على خلس الآمال أو التخويف من نجاح أو الإيهام بأي حدث وهمي ليجعل الغير، يسلم له مالا أو منقولات أو سندات أو تعهدات أو مخالصة أو إبراء، واستطاع بواسطة الاستعانة بهذه الوسائل من أن يحتال أو يحاول الاحتيال على كل أو جزء من أموال الغير... الخ". محمد طارق الخن، "مرجع سابق"، ص ١٠٩.

المطلب الثاني

الركن المادي لجريمة الاحتيال المعلوماتي

كغيرها من الجرائم، فإن جريمة الاحتيال المعلوماتي تتكون من الركن المادي، والذي يفترض وجوده لقيام الجريمة، ولا يختلف الركن المادي في جرائم الاحتيال المعلوماتي عنه في الجرائم التقليدية، فلا جريمة دون أن يتوفر فيها الركن المادي والمتمثل في السلوك الذي يقوم به الجاني من أجل تحقيق غايته وهي دفع المجني عليه تسليم ماله إلى الجاني بفعل الخداع^١، إلا أن تحديد الركن المادي في جريمة الاحتيال المعلوماتي تكتنفه بعض الصعوبات فيما يتعلق بتحديد النتيجة الإجرامية والرابطة السببية، وبناءً عليه فإن للركن المادي في الجرائم قواعد عامة سنبين مدى تطابقها مع جريمة الاحتيال المعلوماتي، وسيتم تقسيم المطلب إلى فرعين كالآتي:

الفرع الأول: ماهية الركن المادي.

الفرع الثاني: تحقق الركن المادي لجريمة الاحتيال المعلوماتي.

الفرع الأول: ماهية الركن المادي.

يتمثل الركن المادي في السلوك الاجرامي الذي يتخذه الجاني بموجب وسائل وأساليب كاذبة يترتب عليها أن يسلم المجني عليه ماله بطوعية للجاني، والركن المادي هو المظهر الخارجي للجريمة المتمثل في الإرادة الجرمية، فالجريمة هي فعل أو سلوك جرمي حدده القانون ورتب له عقوبة مناسبة، وتكتمل الجريمة بتوافر عناصر معينة وهي الفعل الإجرامي والإرادة الآثمة ونتيجة محددة، وعلاقة سببية بين الفعل والنتيجة، فلولاً هذا الفعل ما وقعت النتيجة، فثمة ارتباط عضوي بين هذه العناصر^٢.

^١ هدى قشقوش، "جرائم الحاسب في التشريع المقارن"، مرجع سابق، ص ٧٦٢.

^٢ عبد القادر عبد الحافظ الشخلي، "جرائم الاحتيال المعاصرة"، جامعة نايف العربية للعلوم الأمنية، الرياض، ط١، ٢٠٠٥م، ص ٤٧.

أولاً: الفعل أو السلوك غير المشروع (النشاط الإجرامي).

المقصود بالسلوك الإجرامي هو فعل الجاني الذي يحدثه في العالم الخارجي، فلا يمكن محاسبة الشخص على نواياه وهواجسه الداخلية، وما يترتب عن هذا السلوك من تغيير للحقيقة في واقعة ما، حيث ينقسم السلوك الاجرامي إلى نوعين:

١- **السلوك الإيجابي:** وهو كل قول أو فعل يجرمه القانون يصدر عن الجاني ويؤدي إلى نتيجة في الجرائم، وكذلك يعتبر سلوكاً إجرامياً في ذاته في الجرائم الشكلية، وجريمة الاحتيال المعلوماتي تدخل ضمن السلوك الإيجابي لما يحدثه من نتيجة. أي أن النشاط الإجرامي في السلوك الايجابي يقصد بفعل الخداع تغيير الحقيقة في واقعة ما تغييراً من شأنه وقوع المجني عليه في غلط يدفعه إلى تسليم ماله إلى الجاني. فجوهر الخداع هو الكذب الذي يتخذه الجاني حيال المجني عليه ولكن لا يكفي الكذب لتحقيق النشاط الجرمي بل يلزم أن يقترن بإحدى الوسائل الاحتمالية^١.

٢- **السلوك السلبي:** يتمثل هذا الفعل بسلوك أو موقف يتخذه المكلف بقاعدة قانونية تفرض عليه أن يعمل فلا يعمل، فيقوم السلوك السلبي نتيجة امتناع أو إحجام الشخص عن القيام بعمل يوجبه عليه القانون إذا كان باستطاعته القيام به، ومن المتعارف عليه فقهيّاً أن السلوك المادي لجرائم الاحتيال المعلوماتي يشترط وجود بيئة رقمية واتصال بالإنترنت بالإضافة إلى معرفة بداية النشاط الإجرامي ونتيجته، فمرتكب جريمة الاحتيال المعلوماتي يجب عليه تجهيز وسيلة تقنية المعلومات المراد استخدامها في الجريمة وأن يقوم بإعداد البرامج، وكذلك قد يحتاج إلى تهيئة صفحات ومعلومات أخرى كالفيروسات تمهيداً لاستخدامها في الجريمة^٢.

من خلال ما سبق يتطلب للقيام بمثل هذه الجريمة أعمالاً تحضيرية، كشراء البرامج المعدة لاختراق أنظمة الحاسوب أو لفك الشفرات وسرقة كلمات السر الخاصة بالمقتنيات الالكترونية كبطاقات الائتمان والبريد الالكتروني، وهذا النشاط الإجرامي يتطلب الدخول غير المشروع أو غير المصرح به للتلاعب في البيانات لانتهاك الخصوصية الشخصية للأفراد إلحاق

^١ علي القهوجي، "مرجع سابق"، ص ٧٦٢.

^٢ برنامج الفيروس له تأثير كبير على برامج الحاسب الآلي لما له من قدرة على إحداث تغيير في البرامج والبيانات المتداولة على الحاسب تصل إلى الائتلاف الكلي للبرامج، وأول ظهور برامج الفيروس عام ١٩٥٩م. أيمن عبد الحفيظ، "الاتجاهات الفقهية والأمنية لمواجهة الجرائم المعلوماتية"، دون سنة، ٢٠٠٥م، ص ٦٧.

الضرر بصاحبها أو لتحويل الأموال والاستيلاء عليها وهذا النشاط الإجرامي من أهم صور الركن المادي لجريمة الاحتيال المعلوماتي^١.

ويرى الباحث بأنه وإن كانت بعض الجرائم قد تتحقق بوجود سلوك سلبي، إلا أنه يصعب قيام السلوك السلبي في جريمة الاحتيال المعلوماتي، نظراً لأن مرتكب تلك الجريمة لابد أن يتدخل بسلوك إيجابي لإرتكاب تلك الجريمة.

ثانياً: النتيجة الإجرامية.

يقصد بالنتيجة الإجرامية، الأثر الذي يحدثه السلوك الإجرامي في الواقع الخارجي، فقد يحدث تغييراً حسياً ملموساً في الواقع الخارجي، ولكن تجدر الإشارة هنا بأن النتيجة كعنصر من عناصر الركن المادي تقوم على أساس ما يعتد به المشرع ويرتب عليه نتائج، بغض النظر عما يمكن أن يحدثه هذا السلوك الإجرامي^٢.

فعلى سبيل المثال قد لا يحدث السلوك الإجرامي أثراً مادياً ملموساً كأن يقوم الجاني بمحاولة اختراق نظام معلومات حاسب آلي للاستيلاء على معلومات وبيانات أرصدة أو مستندات مالية لكي يقوم بتحويلها لحسابه الخاص ولكن نظام الحماية لهذا الحاسب لم تسمح للجاني بالدخول إلى هذه البيانات والمعلومات، ففي هذه الحالة لم يحقق السلوك الإجرامي نتيجته وهي الاستيلاء على المال.

إن الهدف الذي يسعى إلى تحقيقه الجاني في جريمة الاحتيال المعلوماتي هو الاستيلاء على مال منقول مملوك للغير وذلك باستعمال وسائل تقنية المعلومات، وفي حال لم تتحقق النتيجة من السلوك الإجرامي نكون أمام الشروع في ارتكاب هذه الجرائم^٣.

إذ يعتبر الشروع جريمة بدأت فيها الأفعال التنفيذية إلا أن النتيجة الجرمية لم تتحقق لظروف خارجية عن إرادة الفاعل، فالشروع بنوعيه التام والناقص يمكن تصوره في جريمة الاحتيال المعلوماتي، فمن يقوم باختراق نظام معلوماتي لأحد المصارف عن طريق الإنترنت، ويقوم بإدخال البيانات اللازمة لإجراء عملية الاحتيال عن طريق تحويل الأموال غير المشروعة،

^١ محمد علي العريان، "مرجع سابق"، ص ١٤٧.

^٢ محمد نجيب حسني، "مرجع سابق"، ص ٣٦٣.

^٣ احمد محمود مصطفى، "مرجع سابق"، ص ١٠٧.

ولا تتم النتيجة الإجرامية ولا تتحقق أي لم يتم التحويل بسبب خلل في إدخال البيانات، فإن هذا النشاط للفاعل يشكل فعل احتيالي^١.

ثالثاً: العلاقة السببية.

موضع علاقة السببية في النظرية العامة للجريمة يأتي في الركن المادي للجريمة، فهي حلقة الاتصال بين السلوك الإجرامي والنتيجة الجرمية، ودورها يكون بيان ما كان للفعل من نصيب في إحداث النتيجة، أو في تغيير آخر إثبات أن الفعل كان سبب حدوث النتيجة^٢.

ويلزم أن يكون تسليم المال من المجني عليه إلى الجاني في جريمة الاحتيال بناءً على الكذب والخداع والمناورات الاحتيالية التي استخدمها الجاني، فإذا سلم المجني عليه ماله للجاني دون أن تكون الطرق الاحتيالية سبباً بذلك، فإن ذلك ينفي صفة السببية بين الاحتيال والتسليم وبالتالي لا قيام لجريمة الاحتيال^٣.

وعنصر السببية ضروري في كل الجرائم حيث يكون العنصر رابط ما بين السلوك الإجرامي والنتيجة المترتبة عنه، غير أن في جريمة الاحتيال المعلوماتي قد لا تترتب النتيجة الإجرامية حتماً عن السلوك الإجرامي ولا بحكم طبيعة الأشياء ففي هذه الحالة تكون عنصر السببية ذو أهمية بالغة وعنصراً قائماً بذاته^٤.

فقد يقوم المجني عليه بتسليم ماله للجاني ليس لما انطلى عليه من الأساليب الاحتيالية من قبل الجاني، ولكن شفقة منه على الجاني، أو للقبض عليه متلبساً.

الفرع الثاني: تحقق الركن المادي لجريمة الاحتيال المعلوماتي.

يستلزم لتوافر الركن المادي لجريمة الاحتيال المعلوماتي تحديد وسيلة الاحتيال باستخدام تقنية المعلومات، ومن هذا المنطلق يتضح بأن هناك إشكالية تثار كما أوردنا ذلك سابقاً ألا وهي أن الاحتيال المعلوماتي يدور حول التلاعب في البيانات أو البرامج بهدف الحصول على مال أو

^١ محمد طارق الخن، "مرجع سابق"، ص ١٧٧-١٧٨.

^٢ عبد القادر الشبخلي، "مرجع سابق"، ص ٧٣.

^٣ بلال أمين زين الدين، "مرجع سابق"، ص ١٥٧.

^٤ بلال زين الدين، "مرجع سابق"، ص ١٥٨.

أي شيء آخر ذا قيمة، وكما هو متعارف عليه أن الفقه حدد الأسس والطرق الاحتمالية القائمة بالدرجة الأولى على الكذب والذي مؤداه الإقناع بالمظهر المادي الخارجي حيث ينخدع به المجني عليه ويسلمه ماله، وفي مجال الاحتمال المعلوماتي تختلف الطرق الاحتمالية عنها في الاحتمال التقليدي.

حيث إن التلاعب في البيانات أو البرامج باستخدام الطرق الاحتمالية على النظام المعلوماتي يعتبر أساس ممارسة فعل الاحتمال على النظام وإيقاعه في الغلط، حيث اختلف الفقه في شأن مدى توافر هذا الفعل حتى يمكن تطبيق القواعد العامة لجريمة الاحتمال التقليدي عليه.

أولاً: مدى وقوع الحاسب الآلي ضحية لفعل الاحتمال.

إن الصعوبات بشأن تطبيق جريمة الاحتمال تتمثل في مدى اعتبار التلاعب في البيانات والبرامج مكوناً أساسياً في الجريمة. فكما بينا بأن الاحتمال هو كل تظاهر أو إحياء يكون صالحاً لإيقاع المجني عليه في الغلط على نحو يجعله يعتد بالمظهر المادي الخارجي، ويترتب عليه تسليم ماله إلى الجاني وعليه تثار الإشكالية التي مفادها مدى إمكانية وقوع فعل الاحتمال على نظام الحاسب الآلي وإيقاعه في الغلط؟

وعليه يجب أن نشير أولاً إلى أن السلوك المادي المكون لجريمة الاحتمال يدور حول الكذب الواقع من جانب الجاني والذي بلغ معه درجة من الاحتمال أدت إلى قيام المجني عليه بتسليم أمواله إلى الجاني ثم قيام هذا الأخير بتسليمه من المجني عليه، وعليه تستوجب جريمة الاحتمال أن يكون الجاني قد خدع أنساناً طبيعياً مثله.

فذهب رأي بأن التلاعب المعلوماتي هو تلاعب في البرامج والبيانات للتغيير فيها بما يترتب عليه إيهام المجني عليه بصحتها، وبالتالي يمكن انطباق النص المتعلق بالجرائم الاحتمالية على التلاعب المعلوماتي باعتباره أحد أساليب الاحتمال وأن النظام المعلوماتي يستخدم كوسيط للتحايل، وهذا ما أقرته محكمة النقض الفرنسية، بالإضافة إلى ذلك فإن طبيعة جريمة الاحتمال المعلوماتي لا تضيف جديداً في مجال الاحتمال التقليدي إلا مجرد الوسيلة المستخدمة في الاحتمال^١.

^١ محمد أمين الشوابكة، "جرائم الحاسوب والإنترنت"، دار الثقافة للنشر والتوزيع، عمان، ط١، ٢٠٠٤م، ص

فالاختيال المعلوماتي باستخدام وسائل تقنية المعلومات يقع عندما يتلاعب الجاني في البيانات المخزنة في ذاكرة الحاسب الآلي أو في إحدى برامج الحاسب الآلي باستخدام أساليب متعددة كإدخال بيانات غير صحيحة بهدف تحويل كل أو بعض أرصدة الغير أو فوائدها إلى حسابه^١.

ويتم ذلك باستخدام الحاسبات الآلية لطبع فواتير مصطنعة أو فواتير ذات قيمة كبيرة مخالفة للحقيقة بغية استعمالها في تحقيق مكاسب مالية، فيقوم المستخدم بدفع هذه الفواتير وتسديدها بناءً على الثقة التامة بتلك الحاسبات ومصدرها^٢.

يرى الباحث أن السلوك الاجرامي لجريمة الاختيال المعلوماتي مرتبط بالمعلومة المخزنة داخل الحاسب الآلي سواء كان ذلك بانتهاك خصوصية معلومات شخصية أو بتحويل أموال أو سرقة بيانات ومعلومات خاصة، والسلوك الاجرامي قد يتحقق بضغطة زر في الحاسب الآلي أو أي وسيلة من وسائل تقنية المعلومات التي سبق الحديث عنها في الدراسة.

كما وتتعدد أساليب التلاعب في البيانات في مكونات الحاسب الآلي بحيث يتم تطويع هذه التقنية بمعطياتها بقصد الاختيال، فالتلاعب في البيانات المدخلة والبرامج والتلاعب في معطيات الحاسب الآلي عن بعد كلها تعد مقدمة للشروع في ارتكاب الجريمة وممارسة النشاط الإجرامي لجريمة الاختيال، والجدير بالذكر أيضاً أن كل من يحاول استخدام هذه الأساليب للقيام بالاختيال المعلوماتي ومنعه من ذلك نظام الحماية الخاص بالتقنية المراد الاستيلاء على الأموال منها، فإن ذلك يعد من قبيل الشروع في ارتكاب هذه الجريمة^٣.

ويتمثل النشاط الاجرامي في جريمة الاختيال المعلوماتي في الدخول غير المشروع في نظم وقواعد معالجة البيانات، سواء كان لهذا الدخول غير المشروع آثار متمثلة في التلاعب في البيانات أم لا، فمجرد الدخول غير المشروع لمواقع المعلومات أو البرامج فإن ذلك يعد جريمة بحد ذاته كما أسلفنا سابقاً.

ويتخذ النشاط الإجرامي عدة صور كانتهاك الخصوصية للبيانات الشخصية والإضرار بصاحبها والتحويل الإلكتروني لأرصدة دون علم أصحابها وذلك بالاستيلاء على بياناتهم

^١ على حسن الطولية، "مرجع سابق"، ص ١٧٤.

^٢ محمد أحمد طه، "مرجع سابق"، ص ١٤٩.

^٣ محمد أحمد طه، "مرجع سابق"، ص ١٥٠.

الشخصية والتلاعب بالبرامج، بالإضافة إلى تزوير البيانات في المعاملات والعمليات الالكترونية وهذا ما يمثل أهم صور الركن المادي للجريمة.

ولكن هناك إشكالية ما إذا كان بإمكان الجاني الاحتيال على النظام المعلوماتي وإيقاعه في غلط، أم أن الاحتيال رغم استعمال تقنية المعلومات لا يكون إلا ضد مال شخص آخر؟

هنا تجدر الإشارة بأن نطاق الاحتيال المعلوماتي لم يضيف شيئاً جديداً على جريمة الاحتيال التقليدية من الناحية النظرية، وبالتالي يمكن تطبيق النصوص العقابية في التشريعات المقارنة الخاصة بجريمة الاحتيال التقليدية، أما الشيء الجديد الذي جاء به نطاق الاحتيال المعلوماتي هو في الوسيلة المستخدمة لارتكاب هذه الجريمة.

فإمكانية الاحتيال على النظام المعلوماتي أي على الحاسب الآلي أو على وسيلة تقنية المعلومات لازالت محل خلاف كبير بين فقهاء القانون، فيرى الفقه الفرنسي أن الاحتيال على النظام المعلوماتي لسلب المال يتحقق بطرق الاحتيال بمفهومها المستقر وهي الكذب والخداع والتدليس والغش وغيرها من هذه الطرق المدعمة بجملة من الأعمال المادية أو الوقائع الخارجية المتمثلة في تقديم الجاني معطيات معلوماتية بواسطة إدخالها إلى نظام المعلوماتية، كما قد تتحقق محاولات الاحتيال باستخدام الجاني معطيات غير صحيحة أو خاطئة التي يخرجها من الجهاز المعلوماتي بعد أن تلاعب بالبرامج أو المعطيات المعلوماتية المخزنة فيه، وذلك بهدف الاستيلاء على أموال لا حق له فيها، وبالتالي يكفي أن يستولى الجاني بواسطة المعلوماتية كوسيلة احتيالية على أموال ليس له حق فيها حتى تعد جريمة احتيال معلوماتية¹.

وهناك من يرى في الفقه الفرنسي أن الاحتيال على الحواسيب لسلب المال، تتحقق به الطرق الاحتياطية باعتبارها أكاذيب تدعمها وقائع خارجية تتمثل في المعلومات والبيانات التي تم إدخالها إلى الحاسوب، وذلك على اعتبار أن هناك شخصاً طبعياً يقف وراء الحاسوب، هو الذي خدع بالطرق الاحتياطية².

إلا أن جانب آخر من الفقه يرى عدم إمكانية ارتكاب جريمة الاحتيال المعلوماتي إلا إذا كانت تنطوي على علاقة مباشرة بين شخصين (المحتال والمخدوع)، وهو ما ينتفي في حالة مباشرة الطريق الاحتياطية ضد جهاز معلوماتي، إلا أنه يمكن تفادي هذا العارض بالنظر إلى

¹ Pradel et Feuillard, (1985). Les infraction commises au money de l'ordinateur Rev, de La pen crim, P 29.

² للمزيد أنظر، طارق الخن، "مرجع سابق"، ص ١٥٥.

وسيلة الاحتيال في عملية الاحتيال باعتبارها مجرد وسيط شفاف، والقول بأن صاحب هذه الوسيلة هو الذي تم خداعه وسلب أمواله^١.

وفي الولايات المتحدة الأمريكية طبقت القوانين المتعلقة بالغش في مجال الاتصالات والبريد والمصارف على الاحتيال المعلوماتي، بالإضافة إلى اندراج هذا النوع من الاحتيال تحت سلطان قانون الاحتيال وإساءة استخدام الكمبيوتر الصادر عام ١٩٨٤م، وهو قانون يجرم شتى أنواع الاحتيال المعلوماتي^٢.

ويرى الباحث بالنسبة للتشريعات العربية محل المقارنة، فهي تؤيد الاتجاه القائل بأن فعل الخداع يمكن أن يقع على النظم الحاسوبية، لأن الحاسوب ليس إلا وسيط، يعبر عن إرادة المجني عليه، فهذا الأخير هو من يقوم ببرمجته وفقاً لمتطلباته، وبالتالي فخداع الحاسوب هو خداع للمجني عليه ولا يوجد هناك ما يمنع قانوناً من أن تمارس الوسائل الاحتيالية على الحاسوب.

وذهب القضاء الفرنسي في بعض أحكامه إلى تدعيم هذا الاتجاه وأقر بأن التلاعب بالبيانات الحاسوبية بقصد تحويل الأموال بطريقة غير مشروعة يعد من قبيل الاحتيال^٣.

ثانياً: تكيف الأموال الكتابية أو البنكية في جريمة الاحتيال المعلوماتي.

إن المحل المادي لجريمة الاحتيال يتمثل في الأشياء المادية، وبالتالي إذا قام شخص بالاحتيال على جهاز الحاسب الآلي وتوصل إلى الاستيلاء على منقول مادي أو مبالغ نقدية بأي طريقة، فلا غرو في وقوع هذه الحالة تحت طائلة العقاب بمقتضى جريمة الاحتيال، ولكن الصعوبة تكمن في كون هذا الاستيلاء قد تم عن طريق القيد الكتابي، كأن يتلاعب شخص في البيانات المخزنة في الحاسب الآلي كي يحول أرصدة الغير إلى حسابه، أي أنه يقوم بالاستيلاء على نقود كتابية أو نقود بنكية وهنا الإشكالية التي تثار بهذا الشأن فهل هنا ثمة استيلاء على المال أم لا ؟

^١ هشام رستم، "مرجع سابق"، ص ١٧٦.

^٢ محمد سامي الشوا، "ثورة المعلومات وانعكاساتها على قانون العقوبات"، دار النهضة العربية، القاهرة، ١٩٩٣م، ص ١٣٠.

^٣ Rennes 26 janvier 1981, D, 1982, IR500, obs M.Vasseur.

يرى الفقه الانجليزي بأن الاستيلاء الناشئ عن الاحتيال الآلي لا يثير أدنى مشكلة إذا كان محل الاستيلاء نقوداً أو أي منقول آخر له قيمة مادية، كأن يتم التلاعب في البيانات المدخلة أو المختزنة في الحاسب الآلي أو برامجه بواسطة شخص ما كي يستخرج الحاسب باسمه أو باسم شركاته شيكات أو فواتير مبالغ غير مستحقة يستولي عليها الجاني أو يتقاسمها مع شركائه. فذهبت تشريعات معظم الدول على عدم اعتبار النقود الكتابية بمثابة مال مادي، بل بوصفها من قبيل الديون والتي يستحيل أن تكون محلاً للاختلاس أو الاحتيال، وعلى النقيض من تلك التشريعات - فإن هناك تشريعات ذهبت إلى جواز اعتبار النقود الكتابية - على الرغم من طابعها غير المحسوس - من قبيل الأموال التي يصلح لأن تكون محلاً لجرائم الاحتيال^١.

بالنسبة للتشريع الفرنسي فقد ابتدع القضاء نظرية التسليم المعادل، والتي أقرتها محكمة النقض الفرنسية، إذ اعتبرت أن مجرد القيد الذي لا يقتضي تسليم شيء مادي أياً كان يعد من قبيل التسليم العادل^٢. وفي الولايات المتحدة الأمريكية قام المشرع الأمريكي بإصدار قوانين عرف من خلالها المال على أنه: كل شيء يمثل قيمة، ويشمل هذا التعريف جميع الأموال الكتابية أو البنكية، ولقد حذا المشرع الأمريكي في هذا الخصوص كل من المشرع الكندي والهولندي والسويسري^٣.

وعلى صعيد التشريعات العربية محل المقارنة فإن المشرع البحريني كذلك لم يقر بتحديد ما إذا كانت النقود الكتابية أو البنكية من قبيل الأموال المادية، وكذلك بالنسبة للمشرع السعودي والإماراتي، ولكن المشرع في هذه الدول قد جرم صراحة هذا الأفعال في قوانين مستحدثة.

^١ أمين الشوابكة، "مرجع سابق"، ص ١٩٢.

^٢ Crime du 10 de'c 1975, J.C.P. 1970-17977 nate Gassin.

^٣ محمد سامي الشوا، "مرجع سابق"، ص ١٣٤.

المطلب الثالث

الركن المعنوي لجريمة الاحتيال المعلوماتي

يدخل الركن المعنوي في جانب التحليل الشخصي والذاتي لبنيان الجريمة، إي إرادة الجاني ومسئوليته عن الفعل أو الامتناع المنسوب اليه، بالإضافة إلى علمه بأن فعله غير مشروع وأن القانون يعاقب على ارتكاب هكذا أفعال، بالإضافة إلى توفر القصد الجنائي بصوره المختلفة والذي يتحقق بتحقيق النتيجة الجريمة الجرمية وإصرار الجاني على هذا القصد، وسيتم تقسيم المطلب إلى فرعين كالآتي:

الفرع الأول: ماهية الركن المعنوي للجريمة.

الفرع الثاني: القصد الجنائي.

الفرع الثالث: تحقق الركن المعنوي في جريمة الاحتيال المعلوماتي.

الفرع الأول: ماهية الركن المعنوي للجريمة.

المقصود بالركن المعنوي هو العلاقة ما بين القصد الجنائي والإرادة المتوفرة لدى الجاني لارتكاب جريمته، أي اتجاه السلوك الإجرامي لتحقيق النتيجة الاجرامية. فوفقاً لذلك يلزم لقيام الجريمة في هذا التحليل أن يأتي الجاني الفعل أو الامتناع وهو متمتع بإرادة حرة، أي قادرة على الاختيار، وواعية وقادرة على الفهم والإدراك ومذنبه أو آثمة، أي جديرة باللوم^١.

بناءً على ما سبق يفترض الركن المعنوي التحقق من أن الفعل غير مشروع، لأنه إذا كان مشروعاً لم تكن العلاقة به محلاً للوم، ومن ثم كان التأكد من تجريم القانون سابقاً على التحقق من توافر الركن المعنوي، فكل جريمة لها طبيعة خاصة وعناصر ذاتية لتحقيق الركن المعنوي فيها^٢.

^١ أحمد عوض بلال، "الإثم الجنائي"، دار النهضة العربية، القاهرة، ٢٠٠٣م، ص ٢١.

^٢ أحمد محمود مصطفى، "مرجع سابق"، ص ١١٣.

فالركن المعنوي للجريمة ظاهرة نفسية، ولا يعني ذلك وجوب توفر مجموعة من العناصر النفسية بحيث يكون وجودها في ذاته محلاً للاعتداد بالقانون، بل يفترض أن تكتسب هذه العناصر تكييفاً قانونياً تصبح بموجبه محلاً للوم أمام القانون، وللركن المعنوي جانب وصفي يفترض مجرد وجود علاقة نفسية، وجانب معياري يتمثل في تقييم القانون لهذه العلاقة وحكمه عليها^١.

الركن المعنوي إذاً هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، فيكتسب الركن المعنوي أهمية في جريمة الاحتيال المعلوماتي، حيث بموجبه يمكن تحديد مناهل مسائل الجاني، وذلك بتحديد القصد الجنائي لديه، الذي بدونه لا يمكن أن يعاقب الشخص المرتكب للفعل.

الفرع الثاني: القصد الجنائي.

والقصد الجنائي هو الهدف المباشر للسلوك الإجرامي والذي ينحصر في حدود ارتكاب فعل الجريمة، وهو ما يتطلب توافر النتيجة وتأكيد وقوعها، والأصل في ذلك ارتكاب هذا الفعل غير المشروع، فلا يمكن انتفاء علمه كعنصر أساسي للقصد الجنائي.

وللقصد الجنائي عناصر يجب توافرها وهي:

أولاً: عناصر القصد الجنائي.

لا يمكن تحقق القصد الجنائي إلا إذا توافر فيه عنصري العلم والإرادة وهي كالتالي:-

١- العلم: لا يتحقق القصد الجنائي إلا إذا كان الجاني يعلم بالعناصر الأساسية لقيام الجريمة سواء تعلق ذلك بسلوكه الإجرامي أم بموضوع الاعتداء، ففي جريمة الاحتيال لا يتحقق القصد الجنائي إلا إذا كان الجاني يعلم أن المال الذي استولى عليه هو ملك لغيره.

٢- الإرادة: فالإرادة هي نشاط نفسي يهدف إلى تحقيق غرض معين، فإذا كان غرض الجاني تحقيق نتيجة إجرامية، كانت الإرادة المتجهة إلى الفعل المنطوي على إحداث النتيجة هي "القصد الجنائي"، والغرض هو الهدف القريب الذي تتجه إليه الإرادة، أما الباعث فهو عبارة عن الدافع إلى إشباع حاجة معينة وهذا الدافع له طبيعة نفسية

^١ أحمد محمود مصطفى، "مرجع سابق"، ص ١١٤.

بخلاف الغاية التي لها طبيعة موضوعية، فإذا أراد الجاني أن يحتال على المجني عليه لضائقة مالية مر بها، كانت الغاية التي يسعى لها هو الحصول على المال، أما الغرض فهو خداع المجني عليه للاستيلاء على أمواله، فهذا الغرض يتصور الجاني تحقيقه بخداع المجني والكذب عليه وإيهامه بصدق مناورات الاحتيال، أما الباعث على ما فعله فهو الاستيلاء على الأموال لسد الضائقة المالية التي يمر بها^١.

ثانياً: صور القصد الجنائي.

إن القصد الجنائي عنصر هام من عناصر الركن المعنوي للجريمة، وينقسم القصد الجنائي إلى قسمين، قصد عام وقصد خاص، بمعنى أن هناك جرائم لا بد من توفر القصد العام ليتحقق وجود الركن المعنوي وتنعقد المسؤولية الجنائية لهذه الجرائم، وهناك جرائم لا بد من توفر القصد الخاص إلى جانب القصد العام، وهذا ما سنبينه على النحو الآتي.

١- **القصد الجنائي العام:** يهدف الجاني عند ارتكابه الواقعة الإجرامية مع العلم بعناصرها إلى تحقيق غرض معين، كي تتم الجريمة ويتوافر لها القصد الجنائي العام، ففي جريمة الاحتيال المعلوماتي يكون الغرض من وراء هذه الجريمة الاستيلاء على مال مملوك للغير، وعليه فالقصد الجنائي العام أمر ضروري ومطلوب في جريمة الاحتيال المعلوماتي بشكل خاص والجرائم التقليدية والمستحدثة بشكل عام^٢.

نخلص مما سبق أن هناك ثلاثة شروط يجب توافرها لكي نكون بصدد وجود قصد عام في جريمة الاحتيال:

- علم الجاني بأن الأسلوب المستخدم هو أسلوب احتيالي من شأنه حمل الغير على تسليم ماله .
- علم الجاني بأن المال الذي يسعى إلى الحصول عليه مملوك للغير.
- انصراف إرادة الجاني إلى إثبات فعل ايجابي قائم على احد الأساليب الاحتيالية.

^١ أشرف توفيق شمس الدين، "شرح قانون العقوبات" النظرية العامة للجريمة والعقوبة"، دار النهضة العربية، القاهرة، ٢٠٠٩م، ص ١٥٥.

^٢ أحمد مصطفى محمود، "مرجع سابق"، ص ١١٥.

٢- **القصد الجنائي الخاص:** لا يختلف القصد الجنائي الخاص عن العام وذلك بالعناصر التي يجب توافرها ألا وهي الإرادة والعلم بالواقعة والعقوبة المقررة لها، إنما يزيد عنه في تحديد الإرادة الاجرامية لدى الجاني إما بباعث معين قد يدفعه إلى ارتكاب الجريمة، وأما بنتيجة محددة يريد بها الجاني.

وبناءً على ما سبق فإن القصد الجنائي العام متوفر في جريمة الاحتيال المعلوماتي وقد يكون القصد الجنائي الخاص متوفر في جريمة الاحتيال المعلوماتي على وجه الخصوص إذا ارتبط سلوك الجاني باستهداف شخص بعينه أو أي طرف آخر وأصر على إلحاق الضرر بهذا الشخص على وجه الخصوص، فالركن المعنوي للجريمة هو الوجه الخفي للسلوك الذي قام به الجاني المتمثل في توفر الإرادة والإصرار على هذا الفعل مع العلم بعدم شرعيته.

الفرع الثالث: تحقق الركن المعنوي في جريمة الاحتيال المعلوماتي.

الاحتيال المعلوماتي هي جريمة عمدية، ولقيام جريمة الاحتيال يجب توافر القصد الجنائي منها، أي أن على المتهم أن يعلم أن التلاعب في معطيات الحاسب الآلي وفي البيانات المدخلة على النظام المعلوماتي من شأنها أن تجعل الحاسب يستجيب وفقاً لهذه المعلومات، وعليه فإن الفاعل يجب أن يعلم أن ما يقوم به من إدخال للمعلومات هو من قبيل التلاعب بالمعلومات، ولا يلزم أن التلاعب يكون من خلال وسيلة معينة بل يكفي أن الوسيلة تنطوي على التلاعب بالمعلومات^١.

كما يجب أن يعلم الجاني أن المال الذي استولى عليه مملوك لغيره، كأن يكون مملوك للمجني عليه أو لغيره، فالغالب في جريمة الاحتيال المعلوماتي عدم علم الجاني بشخصية المجني عليه وخاصة في حالات التحويل الإلكتروني غير المشروع للأموال.

وهنا تجدر الإشارة إلى اختلاف الفقهاء حول وجوب توفر القصد الخاص لهذه الجريمة، فيرى البعض أن الاحتيال المعلوماتي جريمة يكفي لقيامها توافر القصد العام دون القصد الخاص، فالاستيلاء على المال هو نتيجة للاحتيال وإرادة النتيجة ما هي إلا نية تملك الشيء، فنية التملك لا تمثل غاية خاصة تخرج عن العناصر المكونة للجريمة.

^١ آمال عبد الرحيم عثمان، "شرح قانون العقوبات"، دار النهضة، القاهرة، ٢٠٠١م، ص ٥٤٠.

خلاصة القول جريمة الاحتيال المعلوماتي على اعتبار أنها جريمة عمدية لابد من توافر الركن المعنوي فيها وهو القصد الجنائي، حيث لا يكفي القصد الجنائي العام بعنصره العلم و الإرادة بل لابد من توافر القصد الجنائي الخاص، وهو اتجاه نية الجاني إلى تملك الشيء الذي تسلمه من المجني عليه، ولا عبء للبواحد الدافعة لارتكاب جريمة الاحتيال المعلوماتي، فالباحث ليس عنصراً من عناصر القصد الجنائي، فالجاني يقوم بالتلاعب في المعلومات التي يحتويها النظام المعلوماتي وذلك لإجراء تحويل إلكتروني للأموال لاستيفاء دين أو لإظهار قدرته ومهارته في مجال تكنولوجيا المعلومات فبالرغم من توفر الباعث إلا أن ذلك لا ينفي قصد الاحتيال.

ويرى الباحث أن سلطة الاتهام هي من يقع على عاتقها إثبات القصد الجنائي لدى الجاني في جريمة الاحتيال، من خلال التحقق بتوافر القصد العام والقصد الخاص لتتعدد المسؤولية الجنائية لهذه الجريمة .

الفصل الثاني

موضوع جرائم الاحتيال

باستخدام وسائل تقنية المعلومات

الفصل الثاني

موضوع جرائم الاحتيال باستخدام وسائل تقنية المعلومات

تمهيد وتقسيم:

في إطار المعلوماتية يجب أن يكون الجاني على قدر كبير من الإلمام بتقنية الحاسب الآلي وكيفية استخدامه والإحاطة بنظامه وبرامجه، وكيفية تسخير الوصول إلى تحقيق النتيجة المرجوة، فتتصب جريمة الاحتيال المعلوماتي على البيانات المخزنة في النظام الممثلة لأموال أو أصول أو خدمات، يهدف الجاني منها تحقيق مكاسب أو مزايا.

وتتم بالتلاعب - وفق الدلالة التقنية الواسعة - بمعطيات الكمبيوتر المخزنة أو نظام المعالجة الآلية، ومن أكثر صور الاحتيال المعلوماتي تحقيقاً للضرر الجرائم الواقعة على أنظمة التحويل الإلكتروني للأموال والودائع المصرفية أو ما يسمى بالأموال الإلكترونية أو الافتراضية.

وتتعدد الأساليب التقنية في التلاعب في معطيات الحاسب الآلي بقصد الاحتيال أهمها التلاعب في البيانات المدخلة، والتلاعب في البرامج والتلاعب في معطيات نظم الحاسب الآلي عن بعد، ويتم ذلك بعدة طرق كإدخال معلومات مصطنعة وإتلاف معلومات موجودة بالفعل في الحاسب الآلي ومحوها، أما فيما يخص التعدي على برامج النظام المعلوماتي فيتم عن طريق تعديل نظم هذه البرامج أو تعديل نظم التشغيل، أو عن طريق اصطناع برامج معينة لاستخدامها في عملية احتيال معلوماتي.

وبالرغم من أن جريمة الاحتيال المعلوماتي جرمت في معظم الدول عبر تشريعات ونصوص قانونية، فالمتعارف عليه أن جريمة الاحتيال تنصب في المقام الأول على الأموال، فالإشكالية المطروحة هنا هي فيما يخص محل وموضوع جريمة الاحتيال المعلوماتي، ورأي الفقه فيها، هذا ما سنتناوله في هذا الجزء من الدراسة، ولذلك قسمنا هذا الفصل من الدراسة على النحو الآتي:

المبحث الأول: وسائل الاحتيال باستخدام تقنية المعلومات.

المبحث الثاني: الاحتيال على أنظمة التحويل الإلكتروني للأموال.

المبحث الثالث: محل جريمة الاحتيال باستخدام وسائل تقنية المعلومات.

المبحث الأول

وسائل الاحتيال باستخدام تقنية المعلومات

نشأت جريمة الاحتيال المعلوماتي وتطورت بفعل تطور أنظمة الاتصالات والحاسوب في كافة المجالات الحياتية، وانعكس ذلك على أنظمة نقل وتحويل الأموال بالطريقة الإلكترونية Electronic Fund Transfer، إذ تزايدت هذه العمليات وقيمة الأموال المتداولة بهذه الطريقة مما جعلها موضوع لجرائم الاحتيال المعلوماتي غير المشروع للأموال^١، بسبب الجرائم المعلوماتية المتزايدة على الأموال المتداولة إلكترونياً، فالاحتيال بوسائل تقنيات المعلومات يتم نتيجة المعالجة الآلية للبيانات المؤدية لإلحاق خسائر مالية أو فقدان ملكية الشيء للغير، فأياً كان التلاعب بصيغة الغش أو الاحتيال تعتبر جريمة لانصرافها إلى الاعتداء على المعطيات المخزنة بنظام الحاسوب بما يحتويه من أصول وخدمات وأموال^٢.

لهذا سيتم تقسيم هذا المبحث إلى ما يأتي:

المطلب الأول: التلاعب في مدخلات النظام المعلوماتي.

المطلب الثاني: التلاعب في البرامج.

المطلب الثالث: إتلاف البيانات.

^١ في البداية يجب توضيح ما المقصود بالدخول غير المشروع قانونياً والذي يعرف على أنه: دخول شخص بطريقة مقصودة لجهاز الحاسب الآلي أو إلى موقع الكتروني، أو نظام معلوماتي أو شبكة حاسبات آلية غير مصرح له الدخول إليها، وعرفها الفقه بكونها: "عملية اقتحام الأنظمة أو الشبكات الخاصة بأفراد أو منظمة خاصة أو حكومية، بمساعدة بعض البرامج المتخصصة في فك وسرقة كلمات السر وتصريحات الدخول بهدف الاطلاع على المعلومات وتخريبها أو سرقتها". ضرغام جابر عطوش آل مواش، "جريمة التجسس المعلوماتي -دراسة مقارنة"، المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، ١٤٣٨ - ٢٠١٧، ط١، ص ١٧٢.

^٢ علي جبار صالح الحسيناوي، "مرجع سابق"، ص ٥٩.

المطلب الأول

التلاعب في مدخلات النظام المعلوماتي

تتصب أغلب وسائل الاحتيال المعلوماتي على التلاعب في المعلومات والبيانات التي يتم إدخالها للحاسب الآلي، وتظهر هذه الوسيلة عند إدخال بيانات مختلفة أو محرفة في النظام المعلوماتي، مما يدفع لتغيير البيانات الصحيحة من المدخلة أو الجمع بينهما وهي الطريقة الأسهل لمرتكبي الجرم الاحتيالي، إذ تتم في المراحل الأولى لتشغيل النظام، ففي هذه المرحلة يتم تجهيز البيانات لتحويلها إلى شكل أو لغة مقروءة يقبلها النظام وهنا يمكن له إدخال بيانات ووثائق معينة مغلوطة أو مزيفة^١.

وسيتم تقسم هذا المطلب إلى ما يأتي:

الفرع الأول: التلاعب في المدخلات.

الفرع الثاني: مراحل التلاعب في البيانات والمعلومات.

الفرع الأول: التلاعب في المدخلات.

بيننا سابقاً أن أغلب حالات الاحتيال المعلوماتي تتصب على التلاعب في المعلومات والبيانات التي يتم إدخالها إلى الحاسب الآلي، فقد أشارت بعض الإحصائيات أن ٦٢% من حالات الاحتيال التي تم اكتشافها في الولايات المتحدة الأمريكية وبريطانيا تنحصر في عملية التلاعب في البيانات قبل أو أثناء إدخالها على النظام المعلوماتي، أو في التلاعب بالمعلومات التي يتم إدخالها للحاسب الآلي أو في الوثائق التي يستمد منها البيانات، ومن أبرز حالات هذا التلاعب كان بوقف سداد مستحقات واجبة السداد^٢.

^١ محمد نصر محمد، "مرجع سابق"، ص ١٦١-١٦٢.

^٢ سامر سلمان الجبوري، "مرجع سابق"، ص ٨٦.

ويقصد هنا بالنظام المعلوماتي هو "إخضاع المعلومات في حصرها وتبويبها وتحليلها إلى مجموعة من نظم التشغيل، والمعالجة الحسابية والمنطقية لاستخلاص النتائج"، وهناك من أعطاهما تعريف آخر بكونها: "مجموعة من الإجراءات التي يتم من خلالها تجميع واسترجاع أو تشغيل وتخزين ونشر المعلومات بغرض دعم عمليات صنع القرار وتحقيق الرقابة داخل الجهة الإدارية أو أيًا كانت شكل تلك المنظمة"^١.

وعرفت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة (١) النظام المعلوماتي بأنه "مجموعة من التعليمات والأوامر، قابلة للتنفيذ باستخدام تقنية المعلومات ومعدة لإنجاز مهمة ما".

أما المشرع البحريني فأسمهاها نظام تقنية المعلومات في المادة الأولى من قانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات في مملكة البحرين وعرفها بأنها "أداة أو مجموعة أدوات متصلة أو ذات صلة ببعضها، ويقود واحد منها أو أكثر بمعالجة آلية لبيانات وسيلة تقنية المعلومات وفقا للبرنامج"، وعرف ما المقصود بالبرنامج لتفادي اللبس في نفس المادة الأولى.

وفي وثيقة الرياض للنظام (القانون) الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون الخليجي عرف النظام المعلوماتي في المادة (١) بأنه "مجموعة البرامج والأدوات المعدة لمعالجة وإدارة البيانات أو المعلومات أو الرسائل الالكترونية أو غير ذلك".

كذلك عرف المشرع السعودي النظام المعلوماتي بكونه "مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحسابات الآلية"^٢، كذلك عرفها المشرع الإماراتي الذي أسماها بنظام المعلومات الالكتروني بأنها "مجموعة برامج معلوماتية ووسائل تقنية المعلومات المعدة لمعالجة وإدارة وتخزين المعلومات الإلكترونية أو ما شابه ذلك"^٣.

ويرى الباحث من خلال ما سبق أن النظام المعلوماتي هو ذلك النطاق أو الفضاء الإلكتروني الذي تخزن فيه المعلومات والبيانات، ويحتوي هذا الفضاء على برامج ومعطيات

^١ أيمن عبد الله فكري، "مرجع سابق"، ص ٢٣.

^٢ صدر نظام مكافحة جرائم المعلوماتية بقرار مجلس الوزراء رقم ٧٩ وتاريخ ١٤٢٨/٣/٧هـ، وتمت المصادقة عليه بموجب المرسوم الملكي الكريم رقم م/١٧ وتاريخ ١٤٢٨/٣/٨هـ.

^٣ المادة الأولى من قانون مكافحة جرائم تقنية المعلومات الإماراتي، وقد ذكرها، محمد حماد مرهج الهيبي، "الجريمة المعلوماتية نماذج من تطبيقاتها"، مرجع سابق، ص ٢٢١.

تستطيع من خلالها قراءة هذه المعلومات والبيانات وتخزينها واستخراجها وفق أوامر برمجية معينة.

وينتضح من خلال التعريفات الصادرة أن المهمة الرئيسية للبرنامج هي معالجة البيانات وإدارتها، أي إجراء عمليات حسابية ومنطقية على البيانات لاستخراج معلومات ونتائج محددة وفقاً للتعريف المعطاة من قبل معجم الحسابات الصادر عن مجمع اللغة العربية.

أما المعلومة بحد ذاتها فقد عرفها المشرع الفرنسي في قانون ٨٢-٦٥٢ الصادر في ٢٦ يوليو لسنة ١٩٨٢ بكونها صورة أو مستندات أو معطيات أو خطابات أياً كانت طبيعتها، وهنا توسع المشرع الأمريكي في تعريف المعلومات لتفادي أي تطور تكنولوجي جديد، في قانون المعاملات التجارية الإلكتروني الصادر عام ١٩٩٩ في فقرته ١٠ من المادة (٢) بأن المعلومات تشمل على البيانات والكلمات والصور والأصوات والوسائل وبرامج الكمبيوتر والبرامج المضغوطة والموضوعة على الأقراص المرنة وقواعد البيانات أو ما شابه ذلك^١.

وعرفها المشرع البحريني المعلومات في قانون جرائم تقنية المعلومات بالمادة الأولى بأنها: "كل ما يمكن تخزينه ومعالجته وتوليده ونقله باستخدام وسائل تقنية المعلومات وبوجه خاص الكتابة والصور الثابتة والمتحركة والصوت والأرقام والحروف والرموز والإشارات وغيرها.

أما المشرع الإماراتي من قانون الاتحادي رقم (١) لسنة ٢٠٠٦ في شأن المعاملات والتجارة الإلكترونية فقد عرف المعلومات الإلكترونية بأنها: "بيانات ومعلومات ذات خصائص إلكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج الحاسب الآلي أو غيرها"^٢. وعرفها في قانون مكافحة جرائم تقنية المعلومات بأنها: "أي معلومات يمكن تخزينها ومعالجتها وتوليدها ونقلها بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها".

وهنا أشار المشرع الإماراتي بأن المعلومة لا تقتصر فقط على الكتابة بل إنها شملت كافة الصور التي قد ترد فيها المعلومة، ومن جانبنا نؤيد ما ذهب إليه المشرع الإماراتي خاصة في ظل التقنية التي يعمل فيها النظام المعلوماتي كالرموز والاشارات والحروف المشفرة والتي تكيف

^١ للمزيد أنظر، عبد العال الديري، محمد صادق إسماعيل، "مرجع سابق"، ص ٤٣.

^٢ القانون الاتحادي رقم (١) بشأن المعاملات والتجارة الإلكترونية، الجريدة الرسمية، عدد ٤٤٢، صدر في يناير ٢٠٠٦.

على أنها معلومات نظراً لطبيعتها الخاصة وآلية تخزينها وقراءتها في وسط رقمي لا يقتصر فقط على قراءة الحروف والأرقام.

أما المشرع العماني في المادة الأولى من قانون مكافحة جرائم تقنية المعلومات العماني رقم ٢٠١١/١٢ فتوسع في تعريف البيانات والمعلومات الإلكترونية بقوله: "كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات أياً كانت شكله كالكتابة والصور والأصوات والرموز والإشارات.

أما المشرع السعودي في المادة الأولى فلم يفرق بين المعلومات والبيانات إذ قام بتعريف هذه الأخيرة بكونها: "المعلومات، أو الأوامر أو الرسائل أو الأصوات أو الصور التي تعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، كالأرقام والحروف والرموز وغيرها".^١

وعُرفت البيانات في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على أنها "كل ما يمكن تخزينه ومعالجته وتوليده ونقله باستخدام وسائل تقنية المعلومات وبوجه خاص الكتابة والصور الثابتة والمتحركة والصوت والأرقام والحروف والرموز والإشارات وغيرها".

وفي وثيقة الرياض الخاصة بمكافحة جرائم تقنية المعلومات من النظام (القانون) الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون الخليجي عُرِفَت المعلومات إلى جانب البيانات حيث لم تفرق الوثيقة بين المعلومات والبيانات فعُرِفَت على أنها "كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات.

ومن جانبنا نلاحظ من خلال التعريفات السابقة أنها لا تفرق بين المعلومات والبيانات، على الرغم من الاختلاف الجوهرى بينهما، وهو ما اختلف حوله الفقهاء ووضعوها معياراً للفرقة بين المعلومات والبيانات، بالقول أن المعلومات عنصرها الأساسي الدلالة لا الدعامة التي تجسدها فالمعلومات بحد ذاتها تنقسم إلى عنصرين عنصر مادي ويسمى بالعنصر الدال ويتمثل في الدعامة أو الوسيط أو الوعاء الذي يحتوي على المعلومة، والعنصر الآخر فكري أو ذهني يدل على المعنى وفحواه، ولكي تتكون المعلومة للآخرين يتوجب أن تتجسد في صورة مادية، أما البيانات التي يتم معالجتها إلكترونياً فهي في الأصل عنصر مادي تتجسد في نبضات إلكترونية أو إشارات ممغنطة يمكن تخزينها ونقلها واستغلالها كما يمكن تقديرها كمياً وقياسها فهي ليست شيء معنوي.

^١ راجع في ذلك المادة الأولى من نظام مكافحة جرائم المعلوماتية السعودي.

وهنا، كان لزاماً علينا التطرق إلى مفهوم النظام المعلوماتي لمعرفة الركن المادي محل الجريمة في عملية الاحتيال المعلوماتي، وللفهم حقاً كيف تتم عملية إدخال المعلومات والبيانات للحاسب الآلي محل جريمة الاحتيال المعلوماتي، وهذا ما سنتحدث عنه في الفقرة الثاني.

الفرع الثاني: مراحل التلاعب في البيانات والمعلومات.

تمر عملية التلاعب في البيانات والمعلومات بمجموعة من المراحل، قد تكون في البدايات الأولى لعملية الإدخال أو في مرحلة إعداد المعلومات لإدخالها ويمكن تصنيفها إلى ثلاث مراحل وهي كالآتي:-

- **المرحلة الأولى:** تتمثل هذه المرحلة في تغيير البيانات والمعلومات المراد إدخالها لنظام المعالجة دون حذف أي جزء منها سواء كان في مرحلة الإدخال أو الإعداد لمرحلة الإدخال للمعلومات داخل النظام، فقد يكون التغيير في البيانات والمعلومات كلياً أو جزئياً أو إضافة جزء على الأجزاء المحذوفة أو استبدال معلومات بأخرى، هذا الأمر يؤدي بالمجمل إلى تغيير ما يسمى المعلومة التي وضعناها سابقاً، بحيث تصبح المعلومات الموجودة داخل النظام غير معبرة عن الحقيقة التي كانت تمثلها سابقاً^١، أو قد يقوم الجاني أثناء عملية الإدخال بحذف جزء من المعلومات أو لعدة أجزاء أو حذف المعلومات بأكملها، مما يترتب آثاراً قانونية ونتائج سلبية نتيجة هذا الفعل^٢.

- **المرحلة الثانية:** تتمثل هذه المرحلة في محاولة إعاقة المعلومة من أداء وظيفتها الصحيحة عن طريق إخفائها في أماكن غير مخصص لها لا يستطيع النظام الوصول إليها، أي تغيير في مكونات وعمل النظام بصورة يصعب الوصول للمعلومة الصحيحة ومن أداء الدور المقرر لها في النظام الآلي^٣.

^١ سامر سلمان الجبوري، "مرجع سابق"، ص ٨٦ - ٨٧.

^٢ سامر سلمان الجبوري، "جريمة الاحتيال المعلوماتي"، جامعة النهرين، رسالة ماجستير، ١٤٣٥ - ٢٠١٤، ص ٦٥.

^٣ محمد حماد مرهج الهيتمي، "مرجع سابق"، ص ٢٢٤.

- **المرحلة الثالثة:** التدخل في المعطيات، وتتم هذه العملية عن طريق إدخال المعطيات أو البيانات في النظام الآلي للحاسب بهدف معالجتها، ويكون التدخل فيها بطريقتين إما بإدخال معلومات وهمية في النظام المعلوماتي أو بتزوير المعطيات الموجودة، ويقصد هنا بالمعلومات الوهمية أن يتم إدخال بيانات في نظام المعالجة الآلية لم تكن موجودة سابقاً ويتم إدخالها بغرض التشويش على البيانات الموجودة سابقاً في نظام المعالجة، أما المعلومات المزورة فتتم عن طريق إدخال بيانات ومعلومات غير صحيحة لبنية النظام بديلة للمعلومات الصحيحة المدرجة مسبقاً لتزييف مخرجات النظام لاحقاً، وتستهدف هذه العملية تزوير المستندات والبيانات المتعلقة بالمستحقات المالية والإيداعات المصرفية وحسابات ونتائج الميزانيات وأوامر الدفع وقوائم المبيعات وأنظمة التحويل الإلكتروني للأموال والتي سنتحدث عنها لاحقاً^١.

يتبين لنا من خلال ذكر المراحل كافة لعملية التلاعب بالبيانات والمعلومات، أن الجناة قد يكونوا بنسبة كبيرة ينتمون للمؤسسات المجني عليها باعتبارهم عاملين في هذه المؤسسات وعلى دراية بخلفية النظام الآلي وبكيفية عمل النظام وتخزين وتجميع المعلومات منذ بداية جمع هذه المعلومات حتى إلى عملية الإدخال داخل النظام، وما يساعدهم على ارتكاب جرائمهم عدم وجود رقابة كافية على أنظمة الحاسوب والإنترنت داخل هذه المؤسسات.

ومن الأمثلة الواقعية على عمليات التلاعب في المدخلات نذكر الأمثلة التالية على سبيل المثال لا الحصر لصعوبة ضبط وسائل التلاعب في المعلومات وهي:^٢

- قيام أحد الموظفين بأحد البنوك السويسرية والمختص بمعالجة البيانات بالتلاعب في التحويلات الخارجية للمصرف والتي تتم بشكل آلي، من خلال اعتراض أوامر التحويل التي يتم إرسالها من قبل العملاء وتغيير القيمة الحقيقية لهذه التحويلات، من خلال إدخال القيمة مضاعفة في ألف وبذلك قد أعطى أمر بسحب القيمة المضاعفة.

- قدم أحد الأشخاص طلب لشراء بعض المعدات الغالية الثمن من أحد المتاجر في كندا - متخصص في النظم الإلكترونية، فمن خلال خبرته في هذا المجال عمل اعتراض

^١ محمد أمين أحمد الشوابكة، "مرجع سابق"، ص ٢٣٢.

^٢ انظر: سامر سلمان الجبوري، "مرجع سابق"، ص ٩٠.

الملفات التي تحتوي على الأسعار الحقيقية وإدخالها في بيانات السلع المخفضة، وبذلك تغيرت الأسعار لاعتبار هذه السلعة مخزنة وفقاً لبيانات النظام تحت بند التخفيض وبذلك حصل المشتري على السعر غير الحقيقي لهذه المعدات.

من خلال ما سبق يتبين أن التلاعب في البيانات والمعلومات قد يحدث في أي مرحلة من مراحل العمليات المختلفة، فقد يحدث قبل إدخال المعلومات أو في مرحلة الإخراج أو بعد أن تم إدخالها بصورة صحيحة بحيث يتم التلاعب بها؛ وفي جميع الحالات سواء كانت بصورة التعديل أو مسح المعطيات والبيانات الموجودة داخل نظام المعالجة الآلية، فقد أوضحت التشريعات العربية النصوص الكافية لحماية هذه البرامج من الاختراق أو التلاعب بها.

المطلب الثاني

التلاعب في البرامج

هذا النوع من الجرائم يستوجب على الجناة أن يكونوا متخصصين ومحترفين في مجال الحاسب الآلي ويكون على قدر من المعرفة الفنية الدقيقة والعميقة في مجال برمجة الحاسبات الآلية، وهذا النوع من الأفعال تنسم بالصعوبة إلا أنه يمكن أن يتحقق في مراحل مختلفة من صنع برامج التشغيل أو التطبيق أو في لحظة صيانتها أو تحديثها. وسنقسم المطلب إلى فرعين على النحو التالي:-

الفرع الأول: الإطار القانوني لمصطلح برامج.

الفرع الثاني: طرق التلاعب في البرامج.

الفرع الأول: الإطار القانوني لمصطلح برامج.

يطلق لفظ برنامج على جميع المكونات غير المادية لنظام الحاسوب إلى جانب برامجه اللازمة للتشغيل وبرامج التطبيقات، وتعرف البرامج على أنها تعليمات مكتوبة بلغة ما، موجهة إلى جهاز تقني معقد ويسمى بالحاسب الإلكتروني بغرض الوصول إلى نتيجة معينة^١، أما المصطلح الدقيق للبرامج software هو الكيان المنطقي للحاسب الذي يضم البرامج والوثائق اللازمة والمصاحبة لهذا البرنامج وسائر البرامج المساعدة في تشغيل الحاسوب. وفي هذا الجانب عرف القانون الأمريكي الصادر عام ١٩٨٠ والخاص بحماية حق المؤلف البرنامج بأنه: "مجموعة توجيهات أو تعليمات يمكن للحاسب استخدامها بشكل مباشر أو غير مباشر للوصول إلى نتيجة معينة"^٢.

^١ أيمن عبد الله فكري، "مرجع سابق"، ص ٤٩.

^٢ عبد العال الديري، محمد صادق إسماعيل، "مرجع سابق"، ص ٢٠، ٢١.

وعرف المشرع البحريني البرنامج بأنه: "مجموعة تعليمات معبراً عنها بكلمات أو رموز أو طرق أو بصورة أخرى، إذا تضمنتها أي من الوسائط التي يمكن قراءتها آلياً، تكون قادرة على جعل وسيلة تقنية المعلومات تؤدي عملاً معيناً أو تحدث نتيجة محددة"^١.

أما المشرع الإماراتي في المادة الأولى من القانون الاتحادي رقم (٥) لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات فتوسع بتعريف البرنامج المعلوماتي بكونه: "مجموعة من البيانات والتعليمات والأوامر، القابلة للتنفيذ بوسائل تقنية المعلومات والمعدة لإنجاز مهمة معينة". والمشرع العماني عرفه بأنه: "مجموعة من البيانات والأوامر القابلة للتنفيذ باستخدام وسائل تقنية المعلومات ومعدة لإنجاز مهمة محددة"^٢.

وقد عرف المشرع السعودي برامج الحاسب الآلي على أنها مجموعة من الأوامر، والبيانات التي تتضمن توجيهات أو تطبيقات حين تشغيلها في الحاسب الآلي، أو شبكات الحاسب الآلي، وتقوم بأداء الوظيفة المطلوبة^٣.

كما عرف القرار الوزاري الفرنسي الصادر في ٢٢ نوفمبر ١٩٨١ بأنه "مجموعة الخطوات والإجراءات التي تهدف إلى تشغيل نظام متكامل لأنظمة المعالجة المعلوماتية وتوظيفها وفقاً لهذا الغرض الذي من أجله تم وضع هذا البرنامج"، وقد أخذ بهذا التعريف الموسع في أغلب التشريعات العربية^٤.

وعرفت البرامج في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على أنها "مجموعة تعليمات معبراً عنها بكلمات أو رموز أو طرق أو بصورة أخرى، إذ تضمنتها أي من الوسائط التي يمكن قراءتها آلياً، تكون قادرة على جعل وسيلة تقنية المعلومات تؤدي عملاً معيناً أو تحدث نتيجة محددة"^٥.

وفي وثيقة الرياض لمكافحة جرائم تقنية المعلومات عرفت المادة الأولى البرامج على أنها "مجموعة من الأوامر والتعليمات، القابلة للتنفيذ بوسائل تقنية المعلومات والمعدة لإيجاز مهمة ما".

^١ المادة الأولى من قانون رقم (٦٠) لسنة ٢٠١٤.

^٢ راجع المادة ٢ من قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ / ٢٠١١.

^٣ راجع في ذلك المادة الأولى من نظام مكافحة جرائم المعلوماتية السعودي.

^٤ أيمن عبد الله فكري، "مرجع سابق"، ص ٦٣.

^٥ الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربية الأمانة العامة، القاهرة، ٢٠١٠م.

ومما سبق نلاحظ أن التعريفات السابقة التي أوردها المشرع العربي في دول المقارنة انطلقت من نقطة واحدة وهي اعتبار أن البرامج ماهي إلا عبارة على بيانات وأوامر قابلة للتنفيذ لإنجاز مهمة ما، وهذا ما يفسر تعدد برامج الحاسب الآلي واختلاف وظائفها بحيث تكون معدة فقط لإنجاز عمل ما لا يمكن معه إنجاز أي عمل آخر خارج نطاق الوظيفة التي صممت من أجلها، وعليه فهي تعمل وفق عملية برمجية معدة مسبقاً.

الفرع الثاني: طرق التلاعب في البرامج.

يتبين من خلال معالجتنا للمطلب الأول أن عملية التلاعب في البيانات والمعلومات لا تتطلب الخبرة الكبيرة للقيام بالعمل الجرمي بخلاف عملية التلاعب في البرامج التي تتطلب من الفاعلين خبرة عميقة للتلاعب في البرامج لتعقيدات هذه العملية وما يعطينا فئة الجناة الذين يقومون بهذه العملية لذلك صنفنا هذه الوسيلة من أصعب وسائل الاحتيال المعلوماتي على الرغم من ندرة العمليات التي تمت بهذه الطريقة^١.

وتتم عملية التلاعب في البرامج عن طريق التدخل في الكيان المنطقي للحاسب والذي يضم مجموعة من البرامج المخصصة للقيام بالمعالجة عن طريق الحاسب الآلي، ويكون ذلك بطريقتين إما بتعديل البرنامج القائم أو خلق برنامج جديد، هما كالتالي:

١. **تعديل البرامج:** يعتبر البرنامج كياناً مادياً له أصوله ويمكن الاستحواذ عليه، وتعديله وفقاً للطرق الآتية:^٢

أ- **التلاعب في البرنامج:** ويتم عن طريق برمجة الجهاز الآلي والنظام المعلوماتي بصورة يمكن من خلالها إخفاء البيانات بشكل جزئي أو كلي.

ب- **اختلاس نتائج الحساب:** من خلال إعادة نسخ المعطيات الموجودة في النظام عن بعد أو عن طريق النقل الإلكتروني للبيانات بإتباع أسلوب التجسس بطريقة بث برامج خاصة بالنقاط البيانات المتبادلة على الشبكة المعلوماتية.

ت- **تغيير نظام التشغيل:** وتكون عن طريق تزويد نظام التشغيل نفسه ببيانات جديدة إضافية يسهل من خلالها لوصول إلى كلمة السر أو مفتاح الدخول الشيفرة، مما

^١ محمد عبد الله أبو بكر سلامة، "مرجع سابق"، ص ١٧٣.

^٢ غادة نصار، "الإرهاب والجريمة الإلكترونية"، العربي للنشر والتوزيع، القاهرة، ٢٠١٧، ط ١، ص ٢١.

يسمح للجاني الدخول لكافة المعطيات التي يتضمنها الحاسب الآلي ونظامه التشغيلي.

٢. **خلق برامج وهمية:** قد يكون البرنامج المصطنع ناقصاً من الناحية الفنية أو برنامج وهمي، ويقصد بهذا الأخير اصطلاحاً برنامج مخصص فقط لارتكاب الفعل الاحتيالي، ومثال ذلك ما قامت به إحدى الشركات الأمريكية من خلق عدداً وهمياً من المؤمنين عليهم عن طريق وثائق التأمين التي بلغ عددها ٦٤٠٠٠ وثيقة اقتصر فقط دورها على إدارة الحسابات، مع قيام الجناة بوضع شيفرة خاصة بحيث لا تظهر إلا الوثائق السليمة وحصل الجناة بهذه الوسيلة على ما يقارب ٢٠٠ مليون دولار. أما النوع الآخر القائم على استخدام برامج ناقصة من الناحية الفنية فتتم عن طريق إدخال فجوات ومساحات داخل البرنامج يسمح له بإدخال التعديلات الضرورية كإدخال شيفرات يمكن من خلالها التحكم بالنظام المعلوماتي^١.

ومن أمثلة التعدي على برامج التطبيق ونظم التشغيل، قيام مبرمج يعمل في أحد البنوك بتعديل برامج إدارة الحسابات داخل البنك يتيح له إضافة ١٠ سنتات كمصاريف إدارة الحسابات على كل ١٠ دولارات ودولار واحد على الحسابات التي تتعدى ١٠ دولارات وتحويل هذه المبالغ لحساب خاص تحت اسم مستعار، ولم يكتشف الأمر لولا قيام البنك بمكافئة أول وآخر عميل بمناسبة تأسيس الشركة ووفقاً للترتيب الأبجدي تم اكتشاف هذا الاسم المستعار^٢.

إلى جانب هذه الطرق هناك مجموعة من الوسائل التي يمكن من خلالها التلاعب في البرامج وهي على الشكل الآتي:

١. **الوسيلة الأولى:** قد تلجأ بعض المؤسسات إلى تعديل البرامج المعمول بها نتيجة الأخطاء الواقعة من قبل النظام، فيتم تعديل بيانات البرنامج ببيانات غير مرخص لها وغير محمية مما يسهل على الجناة الدخول لها، أما بتعديل البرنامج أو إدخال برامج خبيثة - فيروسات قد تؤدي نفس الطريقة^٣.

^١ محمد أمين أحمد الشوابكة، "مرجع سابق"، ص ٢٣٦ - ٢٣٧.

^٢ محمد عبد الله أبو بكر سلامة، "مرجع سابق"، ص ١٧٣.

^٣ محمد عبد الله أبو بكر سلامة، "مرجع سابق"، ص ١٧٥ - ١٧٦.

٢. تتمثل الوسيلة الثانية في إدخال برامج إضافية قد تكون معدة سلفاً من قبل الجناة لتعديل المعلومات في الحواسب الآلية عن طريق إجراء تعديلات في ذاكرة الحاسب أو قد يتم استخدام برامج معدة للاستخدام في وقت الأزمات لتخطي الإجراءات الأمنية الموضوعية، ولكن أغلب هذه الجرائم تتم من قبل أشخاص لهم ارتباطات بالمؤسسة لصعوبة التلاعب في البرامج^١.

ونسبق المثال التالي لهذا النمط، إذ قام بعض المتخصصين العاملين مع شركة التأمين بولاية لوس أنجلوس الأمريكية وبعلم الشركة قيد عدداً وهمياً من المؤمن عليهم والبالغ ٦٤ ألف بوليصة تأمين وتقاضت على أثرها الشركة من اتحاد شركات التأمين عمولة نتيجة عدد وثائق التأمين، واقتصر دورها فقط على إدارة الحسابات، ولتضليل أكثر قامت الشركة بتنشيط الملفات عن طريق تغيير بيانات الأشخاص للإيهام بحقيقة تلك الوثائق^٢.

^١ سامر سلمان الجبوري، "مرجع سابق"، ص ٩٢-٩٣.

^٢ محمد عبد الله أبو بكر سلامة، "مرجع سابق"، ص ١٧٦.

المطلب الثالث

إتلاف البيانات

تتم عملية إتلاف نظام المعلومات عن طريق الاعتداء على الوظائف الطبيعية الأساسية للحاسب الآلي، بالتعدي كما بينا سابقاً على البرامج والبيانات data المخزنة في النظام الآلي المحوسب داخل المؤسسة أو خارجها، ويكون ذلك بعدة طرق كالتلاعب في البيانات بإدخال معلومات مغلوطة غير صحيحة أو بإتلاف المعلومات الموجودة في النظام والمتبادلة على شبكة الإنترنت، ويكون الإتلاف بصورة متعمدة عن طريق محو البرامج والبيانات بصورة كلية أو جزئية إتلافها بالاعتداء على المكونات المادية للحاسب الآلي المكونة من أجهزة ودعامات وشرائط وأقراص ممغنطة وشاشات وكوابل وغيرها، أو إتلاف المعلومات والبيانات المخزنة في قواعد الحاسب الآلي والمتبادلة عبر شبكات الإنترنت^١. وسنقسم هذا المطلب على النحو الآتي:

الفرع الأول: ماهية الإتلاف الواقعة على النظام المعلوماتي.

الفرع الثاني: الوسائل الخاصة لإتلاف البيانات والمعلومات.

الفرع الأول: ماهية الإتلاف الواقعة على النظام المعلوماتي.

لقد تم تعريف الإتلاف بأنه: "قيام الجاني بتعيب الشيء على نحو يفقده قيمته الكلية أو الجزئية"، وعرف إتلاف البرامج بكونه: "تدمير البرامج إلكترونيا سواء أكان كلياً أو جزئياً أو إتلافها على نحو يجعلها غير صالحة للاستعمال"، وقد عاقب المشرع الفرنسي على عملية الإتلاف التي تتم على المعطيات في نظام المعالجة الآلية في قانون العقوبات^٢.

^١ محمد أمين أحمد الشوابكة، "مرجع سابق"، ص ٢١٦-٢١٧.

^٢ محمد جلال عبد الرحمن، "مرجع سابق"، ص ٢٤٩-٣٥٠.

وقد عرف المشرع البحريني في قانون جرائم تقنية المعلومات لعام ٢٠١٤م في المادة الأولى منه الاتلاف على أنه "تعيب أو تعطيل أو إلغاء أو حذف أو تدمير أو تغيير أو تعديل أو تحريف أو حجب بيانات وسيلة تقنية المعلومات، أو تعيب أو إعاقة نظام تقنية المعلومات".

وتتم عملية الاتلاف بصور وأشكال متعددة منها ما يؤثر في مكونات النظام المادية بالقيام بتعطيلها أو إيقافها عن العمل ومنها ما هو متعلق بالبرامج المعلوماتية، والنوع الآخر متعلق بإتلاف المعلومات نفسها، أو الإتلاف بالطرق المادية من خلال تخريبها وكسرها^١.

ويرى الفقه الجنائي أن هناك صور كثيرة للتعدي على البرامج والبيانات وإتلافها وتختلف دوافع الاعتداء متنوعة من شخص لآخر، وهي:^٢

١. محو البيانات ومسحها إلكترونياً وتدميرها أو أجزاء منها.
٢. إدخال بيانات في نظام المعالجة الآلية لم تكن موجود تشوش عمل النظام وعلى صحة البيانات المتواجدة فيه.
٣. تعديل البيانات أو تعديل طرق انتقالها، عبر وسائل مختلفة يتدخل فيها الجاني لابتكار وسائل جديدة^٣.

وهناك من ميز في عملية الاتلاف بين الأشياء المادية كأجهزة الحاسب الآلي وملحقاته كشاشة العرض والكابلات وغيرها...، والمعنوية غير المادية كالكيانات المنطقية والبرامج وغيرها من البيانات التي تعتبر أموال غير مادية. وهنا يجب التفرقة بين الحالتين:^٤

١. الحالة الأولى: إذا كان محل الإتلاف المال المعلوماتي ذو الطبيعة المادية والمتمثلة بأجهزة الحاسوب الآلي وشاشات العرض والاسطوانات والكابلات والأقراص الممغنطة وأي شيء مرتبط بالحاسب الآلي، فهذا الأمر لا يثير مشاكل قانونية عند تطبيق القواعد القانونية التقليدية لأنها تدخل في إطار الأموال المنقولة المادية، ويطبق عليها مواد قانون العقوبات المنصوص عليها في التشريعات محل المقارنة، وفي حال تم الاتلاف على معطيات موجودة على قرص تقوم عليها الجريمة كذلك لأنه أحدث تغيير وخلل في

^١ أيمن عبد الله فكري، "مرجع سابق"، ص ١٨٤.

^٢ راجع في ذلك: غادة نصار، "مرجع سابق"، ص ١٨.

^٣ محمد جلال عبد الرحمن، "مرجع سابق"، ص ٣٥٢.

^٤ أيمن عبد الله فكري، "مرجع سابق"، ص ١٨٤.

الجزئيات المعدنية الموجودة على سطح الدعامة بحيث أصبحت غير صالحة للغرض التي تم تصميمها لأجله.

٢. **الحالة الثانية:** والتي تتم على المكونات الغير المادية المنطقية للنظام نفسه، هناك من عارض تطبيق النصوص التقليدية على المكونات المعنوية للحاسب الآلي، ومنهم من برر تطبيقها لكونها - الأموال المعنوية - تخضع لفعل الإلتلاف على الرغم من أنها غير مادية، وبرروا موقفهم على أن الأشياء غير المادية ذات قيمة اقتصادية يمكن نقلها وتدميرها وإتلافها عن طريق التدخل فيها، فمن المنطق أن تخضع للتصرفات القانونية الواردة في حق الملكية، كما أن الأموال المعنوية صالحة لأن تكون محل لجريمة الإلتلاف لمسايرة التطور التكنولوجي والذي من الممكن أن تغير في طبيعتها المادية^١. وتتم هذه الوسيلة عن طريق تغيير البيانات والمعلومات الموجودة في النظام من خلال قيام الجاني بتعديل البيانات والتلاعب بها كي يتمكن لاحقاً من إجراء كافة التحويلات المالية غير المشروعة لصالحه أو لصالح الغير بكل يسر^٢.

الفرع الثاني: الوسائل الخاصة لإتلاف البيانات والمعلومات.

يمكن أن تتم عملية الإلتلاف بأكثر من وسيلة سواء بالطرق التقليدية أو الحديثة، كالحرق أو التفجير أو التكسير أو استخدام وسائل حديثة يقوم بها الجاني ويحقق إتلافاً معلوماتي واسع الأثر وهي كالاتي:

١. الفيروسات.

عرفت الفيروسات على أنها: "برامج مهاجمة تصيب أنظمة الحاسبات بأسلوب يماثل على حد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان"، لقدرتها على التخفي والخداع عن طريق ارتباطها ببرامج أخرى من أجل تمويه البرنامج الأصلي للدخول فيه لآلاف البيانات أو تعديلها وبعد فترة يبدأ بتدمير كافة بيانات وأنظمة النظام التشغيلي، وتتوعد هذه الفيروسات من

^١ محمد جلال عبد الرحمن، "مرجع سابق"، ص ٣٥٧ وما بعدها.

^٢ محمد نصر محمد، "مرجع سابق"، ص ١٦٢.

حيث درجة خطورتها، فمنها فيروس محاكاة الأخطاء، فيروس الإبطاء، الفيروسات النائمة، والفيروسات التطويرية، والفيروسات القاتلة، والفيروس الإسرائيلي، وفيروس السرطان، وفيروس القرد وفيروس حصان طروادة وغيرها من الفيروسات التي تظهر في مناسبات معينة كالأعياد^١.

وتستخدم هذه البرامج لهدفين: الأول لحماية النظام من خطر دخوله ونسخ بياناته غير المرخص لهم، إذ ينشط الفيروس تلقائياً ويدمر جهاز المتطفل الذي يعمل عليه، والثاني تخريبي أو للحصول على منافع شخصية، وتكون هذه البرامج مرافقة للبرامج التشغيلية لنظام الحاسب الآلي، وتنشط عند عمليات النسخ للبرامج من جهاز لآخر أو نقل المعلومات من خلال شبكة الإنترنت بحيث تكون هذه الفيروسات مخبأة داخل رسائل البريد الإلكتروني، مما يشكل تهديد للنظام ويؤدي إلى إتلافه وسحب بياناته. وينتشر هذا الفيروس وينتقل خلال عمليات النسخ للبرامج أو تحميل المعلومات والبيانات بحيث تنسخ نفسها بنفسها وتؤدي بالنهاية إلى السيطرة على النظام^٢.

٢. برامج الدودة.

تعمل هذه البرامج عن طريق اختراق نظام التشغيل والبحث عن الأخطاء الموجودة داخله من أجل الانتقال عبر الحواسيب من خلال الوصلات الرابطة بينهم وتتكاثر باستمرار كالبكتيريا مع استنساخ نفسها من أجل تحقيق الهدف المرجو منها وهي تعطيل أو إيقاف نظام الحاسب الآلي بشكل كامل^٣.

وقد أطلق هذا الفيروس من قبل طالب أمريكي يدعى "روبرت موريس"، تعتمد من خلاله بث برنامج الدودة لكي يثبت عدم ملائمة أساليب ووسائل الأمان عبر شبكات الإنترنت مما تسبب في تدمير الآلاف من شبكات الحاسب الآلي المنتشرة في الولايات المتحدة الأمريكية وخسائر مالية لمواجهة هذا النظام الفيروسي الذي ترتب عليه إصابة كافة نظم المعلومات في الأماكن الحيوية في أمريكا منها الجامعات والمواقع العسكرية ومراكز البحوث الطبية، وقدرت تكاليف إصلاح ما سببه الفيروس في كل منشأة ما بين ٢٠٠ دولار إلى ٥٣٠٠٠ ألف دولار، وأدين على أثرها Morris بانتهاك قانون الاحتيال وإساءة استخدام الكمبيوتر وحكم على أثرها

^١ محمد جلال عبد الرحمن، "مرجع سابق"، ص ٣٦٤ - ٣٦٥.

^٢ محمد أمين أحمد الشوابكة، "مرجع سابق"، ص ٢٣٨.

^٣ محمد جلال عبد الرحمن، "مرجع سابق"، ص ٣٦٥.

بالحبس لمدة ٣ سنوات وغرامة مالية قدرت ١٠,٥٠٠ دولار^١، ودافع موريس أن ليس له النية في تحقيق الضرر أي ليس له القصد الجنائي، فعللت المحكمة بالقول أنه لا يشترط أن تتجه النية إلى تحقيق الضرر بل يكفي أن تتجه النية إلى الدخول غير المشروع على نظام الحاسب الآلي^٢، وتبين هذه الواقعة مدى الترابط بين الدخول غير المشروع والجرائم المعلوماتية عامة وجريمة الاتلاف المعلوماتي بشكل خاص.

ومن الأمثلة الشهيرة بعملية إتلاف البرامج، ما قام به مبرمج الماني بزرع فيروس في النظام المعلوماتي للشركة التي يعمل بها وتم برمجة البرنامج الفيروسي على أن يعمل بإتلاف المعلومات وكافة بيانات الشركة من برامج وأنظمة بعد عامين من فصله من الشركة، وظل الفيروس يعمل وفقاً لتوقيت معين إلى أن جاء التوقيت الذي تم برمجته عليه فقام الفيروس بتوقيف العديد من طرفيات الاتصال والتي وصلت إلى ٣٠٠ طرفية، وهنا تكمن صعوبة اكتشاف الفاعل بسبب التباعد الزمني بين النشاط الإجرامي والنتيجة الجرمية^٣.

وفي هذا الإطار وانطلاقاً مما سبق، ذهبت أغلب التشريعات على تجريم وسائل الاحتيال المعلوماتي المرتكبة بتقنية المعلومات، وذهب المشرع البحريني بنفس الاتجاه من قانون جرائم تقنية المعلومات بمملكة البحرين في المادة (٧) بالمعاقبة بالسجن "يعاقب بالسجن مدة لا تزيد على عشر سنين من قام بإدخال أو تعيب أو تعطيل أو إلغاء أو حذف أو تدمير أو تغيير أو تعديل أو تحريف أو حجب بيانات وسيلة تقنية المعلومات تخص إحدى المصالح الحكومية أو الجهات التي ورد ذكرها في المادة (١٠٧) من قانون العقوبات، على نحو من شأنه إظهار بيانات غير صحيحة على أنها صحيحة، بنية استعمالها كبيانات صحيحة، سواء كانت هذه البيانات مفهومة بشكل مباشر أو غير مباشر. وتكون العقوبة الحبس إذا ارتكبت الجريمة بشأن بيانات وسيلة تقنية المعلومات لا تخص إحدى المصالح أو الجهات المشار إليها في الفقرة السابقة إذا كان من شأن ذلك إحداث ضرر".

وقد جرم المشرع الفرنسي في المادة (٤٦٢) في الفقرة الرابعة بموجب قانون العقوبات ١٩٨٨/١/٥ ذلك، حيث نصت على أن "كل من يتعرض بإرادته أو بمعرض عدم احترامه لحقوق أصحاب العلاقة بشكل مباشر أو غير مباشر فيدخل بعض المعلومات في النظام الآلي

^١ محمد أمين أحمد الشوابكة، "مرجع سابق"، ص ٢٤٠.

^٢ أيمن عبد الله فكري، "مرجع سابق"، ص ١٨٨.

^٣ راجع: أيمن عبد الله فكري، "مرجع سابق"، ص ١٨٩.

لمعالجة البيانات أو يمحو أو يعدل فيها أو في طريقة المعالجة أو النقل لهذه المعلومات يعاقب بالسجن من ثلاثة أشهر إلى ثلاث سنوات وبالغرامة من ألفين إلى خمسمائة ألف فرنك فرنسي أو إحدى هاتين العقوبتين^١.

أما المشروع النموذجي العربي في مادته الرابعة أكد على تجريم: "كل من استحوذ بالاتقاط بطريق التحايل على البرامج والبيانات المخزنة بالمحاسب والمسجلة على شريط أو اسطوانات ممغنطة و التي تظهر على الشاشة ..."^٢.

في حين المشرع الإماراتي جرم التلاعب في البيانات والمعلومات في المادة الثانية بقوله:

١. يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة.

٢. تكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسون ألف درهم أو بإحدى هاتين العقوبتين إذا ترتب على أي فعل من الأفعال المنصوص عليها بالفقرة (١) من هذه المادة إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات.

٣. تكون العقوبة الحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين إذا كانت البيانات أو المعلومات محل الأفعال الواردة في الفقرة (٢) من هذه المادة شخصية.^٣

وكذلك المشرع السعودي فقد جرم الجرائم الواقعة على البيانات من نظام مكافحة جرائم المعلوماتية وعرفها في المادة الأولى بكونها المعلومات أو الأوامر أو الرسائل، أو الأصوات، أو الصور التي تعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، كالأرقام والحروف

^١ علي جبار صالح الحسيناوي، "مرجع سابق"، ص ٥٦، ٥٨.

^٢ محمد أحمد طه، "مرجع سابق"، ص ١٤٦.

^٣ راجع في ذلك المادة الثانية والمواد اللاحقة من القانون الاتحادي الإماراتي رقم (٥) لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات، التي تجرم التلاعب في البيانات والمعلومات المدخلة للنظام الآلي.

والرموز وغيرها، وأفرد المشرع مجموعة من المواد التي تجرم هذه الأفعال خصوصا في المادة الثالثة وما بعدها.

أما المشرع العماني فقد أفرد فصل خاص وهو الفصل الثاني المسمى التعدي على سلامة وسرية وتوافر البيانات والمعلومات الإلكترونية والنظم المعلوماتية، وبين فيه عقوبة التعدي على المعلومات والبيانات، ولكن بين المشرع العماني بالتفصيل نوع المعلومات هل هي شخصية أو ارتكبت أثناء تأدية عمله أو تم إتلاف بيانات حكومية وبين عقوبة كل حالة على حده وشدد على الجرائم التي ترتكب ضد المعلومات والبيانات الحكومية^١.

^١ راجع المادة (٣)، (٤)، (٥)، (٦)، (٧)، (٨)، (٩)، (١٠)، من قانون مكافحة جرائم تقنية المعلومات العماني رقم ١٢ / ٢٠١١.

المبحث الثاني

الاحتيايل على أنظمة التحويل الإلكتروني للأموال

إن الاحتيايل المعلوماتي يتطور بتطور المجتمعات البشرية وتقدمها مما سمح لتنوع الأساليب الاحتيايلية والأنشطة الاجرامية المرتكبة لتتواءم مع التطور التكنولوجي ومنها التقنية المعلوماتية وما يسمح للمجرمين ارتكاب مخططاتهم الاحتيايلية بخداع المجني عليه باستخدام الوسائل والصور المتعددة التي يصعب حصرها^١، وقد تكون الصورة الظاهرة هي الواقعة على نظم التحويل الإلكتروني للأموال في قطاع البنوك والذي يساهم الحاسب الآلي في تحقيقها ونذكر من هذه الحالات - الاعتماد على الحاسب الآلي لخلق ضمانات وهمية للحصول على قروض ويتم ذلك بالتلاعب بالحاسب الآلي من قبل العاملين فيه، أو ما يعرف بالصكوك التالفة وهي الصكوك التي يتم قبولها من جانب البنك أو رفضها من قبل الحاسب الآلي المركزي لعب فيها ويتم إرجاعها إلى الفرع لاتخاذ اللازم بشأنها؛ هذا الاعتماد المتزايد على المعلومات المالية على هذا النوع من التحويل أصبح نقل الأموال وتحويلها يتم عبر الحسابات الآلية منشأة ما يسمى مجتمع اللانقود (cashless society). هذا الأمر سمح للتلاعب والاستيلاء على مبالغ مالية ضخمة يصعب ضبطها وتجريمها^٢.

لذلك سنحاول في هذا المبحث الحديث عن الإطار النظري لنظم التحويل الإلكتروني للأموال في المطلب الأول، موضحين مزايا وعيوب هذا النظام في المطلب الثاني، أما المطلب الثالث فسننتظر فيه إلى طرق التلاعب في نظم التحويل محاولين إعطاء أمثلة واقعية لمعرفة الوسائل المنتشرة لهذا النظام، وسيتم تقسيم هذا المبحث كالتالي:

المطلب الأول: الإطار النظري لنظم التحويل الإلكتروني للأموال.

المطلب الثاني: مزايا وعيوب نظم التحويل الإلكتروني للأموال.

المطلب الثالث: طرق التلاعب في نظم التحويل الإلكتروني للأموال.

^١ محمد نصر محمد، "مرجع سابق"، ص ١٦٠.

^٢ سامر سلمان الجبوري، "مرجع سابق"، ص ١١١-١١٢.

المطلب الأول

الإطار النظري لنظم التحويل الإلكتروني للأموال

تعتبر خدمة تحويل الأموال إلكترونياً من الخدمات التي تقدمها البنوك لعملائها عن طريق الشبكة الدولية، أو بإدخال برامج متطورة في أجهزة الحاسب الآلي مرتبطة بشبكة الاتصالات والمعلومات تسمح بإرسال واستقبال الأموال بكل سهولة ويسر، لذلك يتطلب في البداية تعريف نظم التحويل الإلكتروني للأموال في الفرع الأول إلى جانب توضيح أهم وأشهر نظم التحويل الإلكترونية، مع التطرق في الفرع الثاني إلى الأجزاء التي يتكون منها نظام التحويل لمعرفة كيف تتم عمليات الاحتيال باستخدام نظم التحويل الإلكتروني. وسيتم تقسيم المطلب إلى فرعين على النحو الآتي:

الفرع الأول: تعريف نظم التحويل الإلكتروني للأموال.

الفرع الثاني: الأجزاء التي يتكون منها نظام التحويل.

الفرع الأول: تعريف نظم التحويل الإلكتروني للأموال.

عرف نظام التحويل الإلكتروني للأموال بأنه من الأنظمة الذكية ويتم عن طريقه تحويل الأموال من مصرف لآخر بطريقة إلكترونية آمنة^١. وقد عُرف أيضاً، بأنها العملية التي تتم في قيد مبلغ معين من المال في الجانب الدائن لحساب آخر، وقد يكون هذا المبلغ في حساب الشخص نفسه الأمر أو يقيد في حساب شخص آخر، وتتم هذه العملية بناءً على طلب الأمر في البنك نفسه أو في بنك آخر، وعرفها آخرون على أنها "علاقة في الغالب المرسل أو الأمر بالتحويل والمستفيد وبموجب هذه العلاقة ينشأ أمر التحويل من المرسل إلى بنكه الذي يسمى هنا

^١ عصمت عبد المجيد بكر، "دور التقنيات العلمية في تطوير العقد"، دار الكتب العلمية، لبنان، ٢٠١٥، ص

البنك الأصلي ومضمون هذا الأمر بأن يدفع هذا البنك للمستفيد مبلغاً نقدياً محدداً أو قابلاً للتحديد أو أن يأمر هذا البنك بنكاً آخر ويسمى البنك الثالث أو الوسيط بأن يقوم بهذه العملية^١.

وقد عُرِفَ نظام التحويل الإلكتروني من قبل القانون الفيدرالي الخاص بالولايات المتحدة الأمريكية على أنه يشمل كل تحويلات الأموال والذي يبدأ من نهاية طرفية إلكترونية أو أداة تلفونية أو حاسب آلي أو شريط مغناطيسي عن طريق إعطاء أمر وتعليمات التصريح لمؤسسة مالية بإجراء عمليات سحب وإيداع لإحدى الأرصدة. وعرفت النظم أيضاً بأنها عمليات تبادل القيم وألية تتم بوسائل إلكترونية، ويقصد أيضاً بها عمليات تبادل القيم المادية والتي تتم مرحلة بها أو أكثر بواسطة وسائل إلكترونية^٢.

وفي هذا الاتجاه نجد في القانون النموذجي للتحويلات الدولية الدائنة للنقود الصادر عام ١٩٩٢ عن لجنة الأمم المتحدة للقانون التجاري في المادة الثانية الفقرة الأولى قد عرف التحويل المصرفي الإلكتروني للأموال بأن: "التحويل الدائن يعني سلسلة من العمليات، تبدأ بأمر الدفع الصادر عن الأمر بهدف وضع قيمة التحويل تحت تصرف المستفيد ويشمل أمر الدفع أي أمر دفع صادر من مصرف الأمر أو مصرف وسيط بهدف تنفيذ أمر الدفع الصادر عن الأمر بالتحويل".

إن عمليات التحويل الإلكتروني للأموال أصبحت هاجس في ظل تزايد عمليات التسلل والسطو المالي على المصارف مما دفع المصارف للبحث عن طرق أكثر أماناً يتم من خلالها الدفع عن طريق الإنترنت دون إرسال معلوماتهم الائتمانية الشخصية إلى المصرف، من خلال أنظمة مصرفية خاصة بنظام التحويل الإلكتروني للأموال يتم من خلالها ربط البيانات الإلكترونية بالتحويل الإلكتروني للأموال الذي يسمح من خلاله لأي مؤسسة قبول مستندات الفواتير وإيراد المبالغ المسددة بعد التحقق من صحة المستندات، أو عن طريق الخصم المباشر من حساب العميل المصرفي أو من خلال آلات الإيداع والصرف التلقائي^٣.

^١ علي مؤيد سعيد، "التحويل الإلكتروني للأموال دراسة مقارنة"، البنك المركزي العراقي، قسم إدارة الموارد البشرية، ٢٠١٣، ص ٦-٧.

^٢ سامر سلمان الجبوري، "جريمة الاحتيال الإلكتروني دراسة مقارنة"، ص ١١٢-١١٣.

^٣ علي إبراهيم الخضر، "إدارة الأعمال الدولية"، دار رسلان للطباعة والنشر والتوزيع، ٢٠١٠، ص ٤٣٣.

وتعد النظم التالية أشهر نظم التحويل الإلكتروني للأموال وهي كالآتي:

١. نظام فيدا واير (FED) federal reserve wire network

يعتبر هذا النظام من الأنظمة الداخلية التي يتبعها المصرف الاحتياطي الفيدرالي بالولايات المتحدة الأمريكية، وبموجبه تقوم المؤسسات بالاتصال عبر الهاتف مع نظام FED لتبلغه بتعليماتها عن طريق شيفرة خاصة يتم الاتفاق عليها مسبقاً، ويقوم هذا النظام بالتأكد من الشيفرة ومدى مطابقتها، ويدخلها في الجهاز الإلكتروني ليتم معالجتها وترسل لاحقاً للجهة المستلمة، وفي حالة تلقيها اتصالات على هذا النظام لمؤسسة غير مدرجة على خط الاتصال يتم إبلاغ المؤسسة إما عبر الهاتف أو عن طريق إرسال صورة من إشارة هذا النظام إليها في اليوم التالي، ويتم التحويل الفعلي للأموال عبر هذا النظام على أوراق المصرف الاحتياطي الفيدرالي، أما إذا تعلق الأمر بالحالة المرسله لمؤسسة في منطقة نطاق المصرف الاحتياطي الفيدرالي فيقوم المصرف بمجرد تسلمه التعليمات من النظام التابع للمؤسسة المرسله بخصم المبلغ من حساب المرسل وتقييده في حساب المرسل إليه مباشرة^١.

٢. نظام شيبس Cleaning Inter Bank Payment System

يعتبر هذا النظام نظام وطني له أبعاد دولية، يتم من خلاله نقل الأموال آلياً إلى جانب عمله المقاصي بالنسبة للبنوك المنتمية لهذا النظام، ويتم التعامل بالدولار الأمريكي، ويحتكر هذا النظام كافة المعاملات والتحويلات المالية التي تتم بالدولار الأمريكي، ويعمل عن طريق نظام مركزي يتصل بحواسيب البنوك المرتبطة به بحيث يتم تحويل الأموال من البنوك الأمريكية والأجنبية خارج الولايات المتحدة الأمريكية^٢. وهو نظام المدفوعات بين المصارف التابعة لدار المقاصة، حيث ترسل الأموال بين البنوك كدائن ومدين عن طريق نظام المقاصة^٣.

^١ عبد الله بن جهيم الزمامي، "غسل الأموال في المملكة العربية السعودية دراسة مقارنة"، مكتبة القانون والاقتصاد للنشر والتوزيع، ٢٠١٠، ط١، ص ٤٧.

^٢ ليندة عبد الله، "تبييض الأموال عن طريق الاعتماد المستندي للأموال"، مجلة جيل للبحث العلمي، عدد خاص عن أعمال المؤتمر الدولي الرابع عشر، طرابلس ٢٤ - ٢٥ مارس ٢٠١٧، ص ١٧٩.

^٣ باسل عبد الله الضمور، "غسل الأموال في المصارف -دراسة مقارنة"، مكتبة القانون والاقتصاد، الرياض، ط١، ٢٠١٣م، ص ٤٥.

٣. نظام سويفت swift

هو اختصار لعبارة الاتصالات السلكية واللاسلكية المالية الدولية عبر العالم، وهي شبكة لنقل رسائل التحويلات عبر الحدود، وتعد أكبر شبكة عالمية لتحويل الأموال إلكترونياً. ويستخدم هذا النظام تسوية المدفوعات الدولية عن طريق إرسال البنوك تعليمات بالدفع بين كافة البنوك المشتركة في هذا النظام، وعليه يسمح هذا النظام بنقل الرسائل وتعليمات الدفع بين البنوك الدولية دون إجراء المقاصة بينها، ويستخدم هذا النوع بكثرة في التجارة الدولية في نقل التحويلات المالية المتعلقة بالصفقات^١.

وهنا يجب التوضيح أن هناك اختلافاً كبيراً بين مفهوم جريمة غسل الأموال و تحويل الأموال، لكون الأول جوهره تمويه وإخفاء طبيعة أموال ذات مصدر إجرامي وليس فقط إخفاءها كما في التحويل الإلكتروني للأموال^٢.

إلى جانب ما ذكرنا آنفاً، يبقى السؤال يدور حول طبيعة التحويلات المالية التي تتم وفق نظام التحويل الإلكتروني للأموال؟

ومن أجل فهم التحويلات المالية الإلكترونية للأموال، يتعين بيان الأنواع المختلفة للتحويلات المصرفية والتي تشمل على^٣:

- استبدال أوراق نقدية صغيرة بأخرى كبيرة ويسمى هذا النوع بالتحويلات المالية.
- شراء أشياء ذات قيمة كالمعدن والذهب والسيارات الغالية الثمن، ويتم سداد قيمة هذه الأشياء نقداً، وتباع في بلد آخر، وتم تسديد ثمنها بشيك يودع في البلد الأجنبي نفسه ويتم تسميته بالتحويل العيني.
- أما النوع الآخر من هذه التحويلات فيتحقق من خلال قيام البنك بنقل مبلغ مالي من حساب أحد العملاء وقيده في حساب آخر لنفس العميل أو لعميل آخر مستفيد.
- وهناك التحويلات الإلكترونية للأموال التي تتم داخل البلد أو خارجه والتي يصعب تتبعها لسرعة تحويلها.

ولفهم طبيعة التحويل المالي الإلكتروني للأموال يجب توضيح الأجزاء التي يتكون منها نظام التحويل في الفرع الثاني.

^١ ليندة عبد الله، "مرجع سابق"، ص ١٧٨ - ١٧٩.

^٢ عبد الله بن جهيم الزمامي، "مرجع سابق"، ص ٢٢.

^٣ عبد الله بن جهيم الزمامي، "مرجع سابق"، ص ١٢١.

الفرع الثاني: الأجزاء التي يتكون منها نظام التحويل.

تتم عملية التحويل الإلكتروني عن طريق مجموعة من الأجزاء التي يتكون منها النظام وهي كالآتي:

- **الحاسب الآلي المركزي:** يعتبر الحاسب الآلي جهاز متطور للتعامل مع المعلومات التي يزود بها بصورة سريعة وفي وقت قياسي، وذلك عن طريق تجميع المعلومات وتبويبها وترتيبها وتصنيفها إلى جانب تحليلها واسترجاعها في الوقت المطلوب، وقد عرف بأنه: "عبارة عن جهاز إلكتروني بإمكانه ترجمة أوامر مكتوبة لإدخال البيانات أو إخراج معلومات وإجراء عمليات حسابية ومنطقية، ويقوم بالكتابة على أجهزة الإخراج أو التخزين، والبيانات يتم إدخالها بواسطة مشغل الحاسب عن طريق وحدات الإدخال مثل لوحة المفاتيح أو استرجاعها من خلال المعالجة المركزية التي تقوم بإجراء العمليات الحسابية والعمليات المنطقية، وبعد معالجة البيانات تكتب على أجهزة الإخراج كالطابعات أو شرائط التخزين^١.

يعتمد نظام التحويل الإلكتروني للأموال على حاسب آلي مركزي، يتحكم في الأجزاء المختلفة للنظام والتنسيق بينها، إلى جانب القيام بخدمة النهايات الطرفية في المتاجر والبنوك وأجهزة الصراف الآلي والمؤسسات المختلفة الأخرى، ويحتفظ الحاسب المركزي بملفات خاصة لجميع العملاء وأرصدتهم الخاصة والموظفين، فأى عملية سحب أو إيداع لأي عميل مرتبط بالنظام تتم عن طريق هذا الحاسب^٢.

وقد جرم القانون الفدرالي الأمريكي الولوج إلى أنظمة الحاسب الآلي وإساءة استخدام الحاسب متى اعتبر الدخول غير شرعي إلى:

- كمبيوترات الحكومة.
- أي كمبيوتر يحتوي على بيانات ومعلومات حكومية.
- أي كمبيوتر يحتوي على تسجيلات مالية وتكوين الأموال.
- أي كمبيوتر يستخدم للحصول على بيانات ومعلومات حول البطاقات الائتمانية.

^١ محمد سالم الزعابي، "مرجع سابق" ص ٤.

^٢ سامر سلمان الجبوري، "مرجع سابق"، ص ١١٣.

وتتراوح العقوبة بناء على شكل الاعتداء بين الغرامة أو السجن سنة وتصل إلى ١٠ سنوات وفي حالة العود تصل إلى السجن من عام لعشرين عام معتمداً على طبيعة الاعتداء وآثاره^١.

- **نقاط البيع:** نجد ما يسمى النهايات الطرفية في كافة نقاط البيع في المتاجر والمحلات التي تستخدم البيع بواسطة النظم الالكترونية المختلفة، وتعمل النهايات الطرفية عن طريق اتصالها بالحاسب المركزي الآلي عن طريق خطوط الهاتف، فهي تقوم بتلقي بيانات المستخدم عن طريق إدخالها بلوحة مفاتيح خاصة ملحقة بها أو عن طريق البطاقة الإئتمانية الممغنطة على مختلف أنواعها يتم إدخالها في ملحق للنهايات الطرفية، وعن طريق هذا الشريط الممغنط يتم قراءة كافة بيانات المستخدم من اسم العميل ورقم الحساب وغيرها من البيانات المدونة في النظام الرئيسي، فعند عملية الشراء يقوم الموظف بإدخال قيمة السلعة المراد شرائها ورقمها وكميتها، ثم يتم إدخال البطاقة للتعرف على بيانات الشخص، في تلك اللحظة تكون كافة البيانات على الحاسب المركزي المرتبط عبر الهاتف، وتلقائياً يقوم الحاسب المركزي بإعطاء التصريح لإتمام العملية بعد دراسة حالة العميل المالية، فإذا سمح الحاسب ترسل النهاية الطرفية القيمة لحساب العميل وتودعها في رصيد البائع^٢.

وقد ترتبط الطرفيات مباشرة بحسابات البنوك دون المرور بالحاسب المركزي، أي أن بطاقة التحويل الإلكتروني للأموال عند نقاط البيع والشراء تحول بصورة فورية من حساب العميل إلى التاجر بشكل فوري^٣.

- **أجهزة الصراف الآلي:** تتصل مجموعة من أجهزة الصراف الآلي بنظام التحويل الإلكتروني للأموال، وتتيح هذه العملية لعملائها خدمات مالية لحاملها طول مدة عملها، إذ يقوم الشخص بإدخال البطاقة الممغنطة داخل الصراف، وبعد تسجيل الرقم السري الخاص بالبطاقة الممغنطة يقوم بإدخال العمل المراد تنفيذه سواء بالسحب أو الدفع أو التحويل من حساب لآخر وتقوم هذه الوحدة /الصراف بمراجعة الحسابات وتقوم بتنفيذ الطلب بعد الحصول على التصريح من الحاسب المركزي^٤.

^١ انظر: محمد أمين أحمد الشوابكة، "مرجع سابق"، ص ١٨٩ وما بعدها.

^٢ سامر سلمان الجبوري، "مرجع سابق"، ص ١١٤.

^٣ رياض فتح الله بصله، "جرائم بطاقات الائتمان دراسة معرفية تحليلية لمكوناتها وأساليب تزيفها وطرق التعرف عليها"، دار الشروق، ١٩٩٥، ط ١، ص ١٤.

^٤ سامر سلمان الجبوري، "مرجع سابق"، ص ١١٥.

ينظر إلى نظام تحويل الأموال كامتداد لماكينات الصراف الآلي وامتداداً أيضاً لنظام بطاقة الائتمان، حيث تسمح أجهزة الصراف الآلي بصرف مبالغ مالية نقدية والتي تعتبر إحدى الخدمات الناتجة عن التحويل الإلكتروني للأموال، على الرغم من اختلاف آليات استعمال بطاقة الصراف الآلي عن الآليات المستعملة لبطاقة الائتمان الممغنطة، ذلك أن طرق الدخول للنظام المركزي تعتمد بشكل رئيسي على مستندات تحقق ورقية وعلى التوقعات وذلك عند استعمال بطاقة الائتمان^١.

وتتم جريمة الاعتداء في هذا النظام في حالة استخدام الجهاز لصرف مبالغ مالية تتجاوز الرصيد الفعلي^٢.

- **دفع رواتب العاملين:** تتم عملية دفع الأجور ورواتب الموظفين عن طريق التحويل الإلكتروني للأموال، ويتم ذلك بأكثر من طريقة، إذ يقوم أصحاب العمل والمؤسسات بدفع رواتب موظفيهم بإرسال الشبكات الخاصة برواتب العاملين لديهم إلى البنوك عن طريق النظام المتصل بهم^٣.

^١ رياض فتح الله بصله، "مرجع سابق"، ص ١٦.

^٢ عبد الله دغذ العجمي، "المشكلات العملية والقانونية للجرائم الإلكترونية -دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط، ٢٠١٤، ص ٥٢.

^٣ سامر سلمان الجبوري، "مرجع سابق"، ص ١١٥.

المطلب الثاني

مزايا وعيوب نظم التحويل الإلكتروني للأموال

إن استخدام التكنولوجيا في مجال تحويل الأموال له إيجابيات جمة منها توفير الوقت والجهد إلى جانب توفر عامل السرعة، وعلى النقيض تماماً لنظم التحويل التقليدية، وبالرغم من هذه المزايا التي تتمتع بها نظم التحويل الإلكترونية للأموال إلا أنها لا تخلو من بعض السلبيات وذلك لما يتعرض له فضاء التقنية الحديثة من جرائم حتى أصبحت هذه التكنولوجيا تشكل خطراً على النظام الاقتصادي والمالي للدول والأفراد، وهذا ما سنحاول توضيحه في هذا الجزء من الدراسة. وسيتم تقسيم المطلب إلى فرعين على النحو الآتي::

الفرع الأول: مزايا نظم التحويل الإلكتروني.

الفرع الثاني: عيوب نظم التحويل الإلكتروني للأموال.

الفرع الأول: مزايا نظم التحويل الإلكتروني.

- على الرغم من المخاطر الجسيمة المرتبطة بنظام التحويل الإلكتروني للأموال، إلا أن هناك مزايا عديدة للبنوك وأصحاب الأعمال والعاملين والعملاء على حد سواء، ومن أهم مزاياه^١:
١. زيادة حجم المبيعات، فكثير من العملاء لديهم الاستعداد بالإنفاق بطريقة السداد من حسابهم بدل وسيلة الدفع نقداً ليرجع الأمر لعامل نفسي يسمى سيكولوجية تأجيل السداد في بيع السلع.
 ٢. ساعدت نظم التحويل الإلكتروني للأموال في تقليل النفقات التي كانت ناتجة عن تحويل الأموال بالأساليب التقليدية.

^١ سامر سلمان الجبوري، "مرجع سابق"، ص ١١٥-١١٦.

٣. قلل هذا النظام من وقوع الجريمة التقليدية التي كانت مواكبة لعملية تحويل الأموال بصيغتها التقليدية كالسرقة وضياع الأموال، على الرغم من فتح أنماط جديدة للجرائم المرتكبة نتيجة استخدام الوسائل الحديثة.

٤. عدم اقتصار نظام التحويل الإلكتروني على المؤسسات المالية بل امتد ليشمل المستهلك أيضاً، فبإمكان هذا الأخير الوصول إلى أمواله بكل يسر وسهولة وهو ما لا توفره الوسائل التقليدية للمؤسسات وحتى للمستهلك.

٥. إن عملية سرعة تحويل الأموال يخلق نوع من الأمان لدى الدائن والمدين كما ويخلق نوع من الاستقرار في المعاملات المالية لعلم كافة الأطراف بأوضاعهم المالية بشكل واضح.

٦. تيسر نظم التحويل الإلكتروني للأموال سرعة انتقال الأموال عبر النطاق الجغرافي، إذ تتيح لحاملي البطاقات الائتمانية تحويل أموالهم إلى أي مكان بالعالم بسهولة ويسر افتقدتها الوسائل التقليدية لتحويل الأموال.

ونذكر مجموعة من المزايا الأخرى العامة لنظام التحويل الإلكتروني للأموال وهي كالاتي:

١. توفير الوقت، فعادةً قد يستغرق التحويل الإلكتروني بصورته التقليدية عدة أيام، بينما يستغرق تحويل الأموال بين الحسابات الافتراضية بضع دقائق، ففي هذا الحالة لن يضيع الوقت في الانتظار في فروع البنك من أجل القيام بعمليات التحويل.

٢. السيطرة على النفقات، فإذا كان الشخص حريصاً على جعل نفقاته تحت السيطرة، فمن الضروري التحلي بالصبر بما يكفي لتدوين جميع المصروفات، والتي غالباً ما تأخذ جزءاً كبيراً من إجمالي المبالغ المدفوعة. أما في عملية التحويل الإلكتروني فيمكن له الحصول على تاريخ جميع المعاملات التي تشير إلى المتجر والمبلغ الذي أنفقه، ويمكنه التحقق من ذلك في أي وقت يريده. هذه الميزة يوفرها نظام التحويل الإلكتروني للأموال.

٣. تقليل مخاطر فقدان والسرقة، فلا يمكن أن ينسى الشخص المحفظة الافتراضية الخاصة به في مكان ما ولا يمكن أخذها من قبل اللصوص، على الرغم من وجود مجرمين محترفين لهذه العملية في الفضاء الإلكتروني.

٤. الراحة، يمكن إجراء جميع عمليات النقل في أي وقت وفي أي مكان، فيكفي أن يكون لديك وصول إلى الإنترنت^١.

¹ Advantages And Disadvantages Of Electronic Payment Systems, Unichange.Me.

الفرع الثاني: عيوب نظم التحويل الإلكتروني للأموال.

يحتوي نظام التحويل الإلكتروني للأموال على مجموعة من العيوب أهمها:

١. سمح نظام التحويل الإلكتروني لانتشار الأعمال الإجرامية المختلفة التي لم تكن معروفة في النظام التقليدي للتحويل، والتي اتسمت بالتعقيد لصعوبة الإمساك بمرتكبي هذه الأفعال الإجرامية.

٢. خلق النظام المعلوماتي بشكل عام مجموعة من المشكلات نتيجة الطبيعة المعلوماتية لنظم التحويل، الذي يعتبر بديل عن النظام النقدي والقائم على مجموعة من التحويلات للمعلومات والتي تعتبر ذات قيمة معنوية تشكل عامل نشط للأنشطة الإجرامية وللمجرمين المعلوماتيين.

٣. إن النظام المعلوماتي القائم عليه تحويل الأموال نظام مكلف مادياً، ففي حالة وجود خلل طبيعي في النظام يكلف المؤسسة مبالغ طائلة لإصلاحه، أما إذا كان الخلل نتيجة هجوم إجرامي فشكل الخسائر المادية منها والمعنوية هائلة جداً، فمثلاً إذا أصاب الحاسب الآلي المركزي خلل أو حدث خلل في النهايات الطرفية أو في وسيلة الاتصال فسوف ذلك ينعكس تدريجياً على كافة المنظومة ككل كتوقف بطاقات الائتمان أو إعطاء تصريح لحاملها في غير محله^١.

٤. القيود، فلكل نظام دفع حدوده فيما يتعلق بالحد الأقصى للمبلغ في الحساب، وعدد المعاملات في اليوم الواحد وكمية المخرجات.

٥. خطر التعرض للقرصنة، إذا اتبعت قواعد السلامة، فإن التهديد ضئيل، والوضع أخطر عندما يتم كسر نظم التحويل من قبل الهكر، لأنه يؤدي إلى تسرب البيانات الشخصية على البطاقات وأصحابها، حتى إذا لم يكن نظام الدفع الإلكتروني يطلق البطاقات البلاستيكية، يمكن أن يشارك في جرائم تتعلق بسرقة الهوية.

٦. مشكلة تحويل الأموال بين أنظمة الدفع المختلفة، في العادة لا تتعاون غالبية أنظمة الدفع الإلكترونية مع بعضها البعض، في هذه الحالة، يجب على العميل استخدام خدمات تبادل العملات الإلكترونية، مما يستغرق وقتاً طويلاً إذا لم تكن لديه خدمة موثوقة لهذا الغرض.

٧. عدم وجود خصوصية، يتم تخزين المعلومات حول جميع المعاملات بما في ذلك المبلغ والوقت والمتلقي في قاعدة بيانات نظام الدفع، وهذا يعني إمكانية الوصول إليها من قبل وكالات الاستخبارات التي لديها حق الوصول إلى هذه المعلومات.

٨. ضرورة الوصول إلى الإنترنت، إذا فشل اتصال الإنترنت فيصعب الوصول إلى حساب الشخص على الإنترنت.¹

على الرغم من العيوب الكثيرة في نظام التحويلات الإلكترونية للأموال إلا ان مزاياها تفوق عيوبها على الرغم من التهديدات والمخاطر المحيطة بها.

¹ Advantages And Disadvantages Of Electronic Payment Systems, Unichange.Me.
https://Unichange.Me/Articles/Advantages_Of_Electronic_Payment_Systems

المطلب الثالث

طرق التلاعب في نظم التحويل الإلكتروني للأموال

إن الهدف الأساسي الذي من أجله أنشأت نظم التحويل الإلكتروني للأموال بواسطة الحاسب الآلي هو تحقيق خصائص متعددة منها الدقة والسرعة والمرونة وسعة الطاقة التخزينية لديها، هذا الأمر جعلها محط أنظار الكثير من المجرمين بإساءة استخدامها لمصالحهم الخاصة التي تهدد بها الأمن الشخصي وأمن الدولة، فقد قدرت حجم خسائر جرائم الحاسب الآلي ما بين (٣٠,٠٠٠,٠٠٠) ثلاثين مليون دولار أمريكي في المملكة العربية السعودية، والإمارات العربية المتحدة، و (١,٤٠٠,٠٠٠) مليون وأربعمئة ألف دولار أمريكي في لبنان، وهذا كله نتيجة إساءة استخدام الحاسب الآلي بصورة غير مشروعة، ومن هذه الجرائم ما هو مرتبط بسرقة مكونات الحاسوب، وسيتم تقسيم المطلب إلى فرعين على النحو الآتي:-

الفرع الأول: الجرائم المرتبطة بسرقة مكونات الحاسوب.

الفرع الثاني: أنماط الأنشطة الإجرامية المرتكبة في نظم التحويل.

الفرع الأول: الجرائم المرتبطة بسرقة مكونات الحاسوب.

إن استغلال البيانات المخزنة على الحاسب الآلي من أخطر الجرائم المرتبطة بنظام التحويل الإلكتروني للأموال، ومن أمثلة ذلك الدخول إلى شبكة الحاسوب التي تحمل أرقام بطاقات بنكية إئتمانية من خلال استخدام الحاسب الشخصي، الذي من خلاله يستدعي المجرم رقماً معيناً لإحدى البطاقات ثم على أثرها يطلب من الحاسب المبالغ النقدية المرتبطة بهذا الرقم، ولا يمكن على أثرها كشف الجريمة إلا إذا كان هناك تشابه في الأسماء وأرقام البطاقات.

هناك جرائم تتم من خلال اختراق الحاسوب لتدمير البيانات والمعلومات المتواجدة داخل النظام، وهنا يقوم الموظف المختص بوضع الكلمات التي يفهمها الحاسوب، وعند ذلك يتم التنفيذ بناءً على الأمر المعطى من قبل الموظف، مع مسح كافة البيانات المرتبطة بالبرنامج، ويتم ذلك باستخدام فيروس لتلويث الحاسوب لتدمير البيانات أو تعطيلها بقصد ونية لدى الفاعل.

وبعض الجرائم تتمثل في الدخول القانوني للنظام من قبل أشخاص مصرح لهم بالدخول، كالقيام باستخدام الحاسب لأغراض شخصية بعيدة عن مصلحة المؤسسة^١.

ويمكن أن تتم عن طريق تصميم برامج معينة بهدف إجراء تحويلات مالية آلياً من حساب لآخر سواء كان من المصرف نفسه أو من حساب آخر في مصرف آخر، على أن يتم في موعد يحدده مبرمج النظام ومن أشهر هذه القضايا ما قام به أحد العاملين في مصرف الكويت التجاري، بتطوير برنامج للاستيلاء على مبالغ من المصرف، من خلال اختراقه لخمس حسابات مصرفية راكدة من خمسة فروع للمصرف نفسه، فمهمة البرنامج حددت بتحويل المبالغ المالية من هذه الحسابات إلى حساب آخر فتحت باسمه في الفروع نفسها على أن تتم عملية التحويل أثناء سفره للمملكة المتحدة بعد إنهاء عقد عمله^٢.

وتعد هذه الجرائم من أخطر الجرائم المستحدثة لارتباطها بمجموعة من العناصر أهمها:^٣

١. إنها تتسم بطابعها الخفي فيمكن أن ترتكب من مسافة بعيدة عن المؤسسة محل الجريمة وإزالة كافة دلالات الجريمة بكل سهولة مما يصعب إثبات الجرم المرتكب.
٢. سهولة الوصول إلى الحاسب الإلكتروني نتيجة الانتشار الواسع له .
٣. سهولة ارتباطات الحواسيب الشخصية بالحواسيب المؤسساتية بواسطة الهاتف للحصول على البيانات والمعلومات المخزنة والقيام بتحويل الأموال المصرفية.

الفرع الثاني: أنماط الأنشطة الإجرامية المرتكبة في نظم التحويل.

تحدث التقرير الصادر عن إدارة العدالة الأمريكية عام ١٩٨٢ عن جرائم الحاسب الآلي ونظم التحويل الإلكتروني للأموال، وحدد خمسة أنشطة إجرامية تقع على نظم التحويل الإلكتروني للأموال وهي على الشكل الآتي:^٤

^١ عبد الكريم خالد الردايدة، "الجرائم المستحدثة واستراتيجية مواجهتها"، دار ومكتبة الحامد للنشر والتوزيع، عمان، ٢٠١٣، ط١، ص ٥١-٥٢.

^٢ درار نسيم، "الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني -دراسة مقارنة، جامعة أبو بكر بلقايد، الجزائر، أطروحة دكتوراه، ٢٠١٥-٢٠١٦، ص ١٤٦.

^٣ عبد الكريم خالد الردايدة، "مرجع سابق"، ص ٥٢.

^٤ انظر: سامر سلمان الجبوري، "مرجع سابق"، ص ١١٨.

١. التلاعب في المكونات المادية للنظام: يمكن أن يتم التلاعب في نظم التحويل الإلكتروني للأموال من خلال استغلال خطوط الاتصال لتدمير أو تعديل أو إنشاء بيانات أو طلبات التحويل الخاصة بالأموال، أو استعمال البيانات الموجودة داخل النظام لأهداف خاصة كالاختيال على المؤسسات المالية.

٢. التلاعب في البرامج الخاصة بنظام التحويل للأموال لإجراء عمليات مالية غير مشروعة.

٣. يمكن أن يتم التلاعب بأشكال أخرى كالتدخل في الإجراءات الداخلية لنظام التحويل بغرض إصدار بطاقات ائتمانية مزدوجة.

٤. يمكن أن يتم الدخول لنظام التحويل واستخدام بطاقة شخص آخر لسحب مبالغ مالية نقدية من الرصيد الخاص بالعميل.

٥. هناك نمط آخر على الرغم من عدم تطبيق قواعد الجرائم المعلوماتية عليه، وهو قيام شخص بسرقة الأموال التي يقوم آخر بسحبها من ماكينات الصراف الآلي أثناء سحبها أو أن يقوم شخص بتكشير ماكينات الصراف وسرقة الأموال التي تحتويها.

وعلى الرغم من محاولة الكثير من المفكرين حصر وسائل الاختيال التي تتم على نظم التحويل الإلكتروني للأموال، إلا أننا نلاحظ صعوبة في وضع لائحة حصرية بكافة الوسائل والطرق التي تتم على نظم التحويل الإلكتروني للأموال، لكثرة الوسائل المستخدمة واختلاف الصور التي تتطور من مجرم إلى آخر مع تطور نظم التحويل، أو قد تستخدم بأي طريقة من طرق الاختيال المعلوماتية التي سبق الحديث عنها في المطلب السابق، فقد تتم في مراحل مختلفة كالتلاعب في البيانات والمعلومات أو في مرحلة إدخالها للنظام أو بعد ذلك أو التلاعب في البرامج المكونة للحاسب بشكل عام، ويعتبر نظام التحويل الإلكتروني مجال خصص لارتكاب الجريمة نظراً لضخامة الأموال المحصل عليها وسهولة ارتكابها وصعوبة كشف المجرمين في أغلب الحالات.

المبحث الثالث

محل جريمة الاحتيال باستخدام وسائل تقنية المعلومات

ينقسم المال المعلوماتي إلى نوعين منفصلين وفقاً لطبيعته، فهو إما أن يكون مالياً معلوماتياً ذو طبيعة معنوية ويتمثل في البرامج والمعلومات أياً كان نوعها، وإما أن يكون المال المعلوماتي ذو طبيعة مادية ويتمثل في أدوات وآلات الحاسب الآلي الملموسة، وهذا التنوع في المال المعلوماتي ينتج عنه تنوع في النتائج المترتبة عن فعل الاحتيال المعلوماتي، وتبعاً لذلك تكثر الاختلافات الفقهية بهذا الشأن، فقد يستعين المجرم في جريمة الاحتيال المعلوماتي للقيام بجريمة بالحاسب الآلي للاحتيال على شخص معين، وذلك باستخدامه أساليب متعددة كالتلاعب في البيانات والبرامج ومعطيات الحاسب الآلي، حيث يتمكن المجرم من الاستيلاء على أموال من الجمهور بهذه الأساليب الاحتيالية.

وقد يستعين المجرم بالحاسب الآلي للاحتيال على حاسب آلي آخر وهنا تثار إشكالية حول إذا ما كانت البرامج والمعطيات والبيانات محل الاحتيال من الأموال، بمعنى إمكانية وقوع وتحقيق فعل الاحتيال. ومن أجل قيام عملية الاحتيال يجب أن تؤدي إلى إيقاع المجني عليه وحمله على تسليم المال إلى الجاني بإرادته، فلا ينبغي أن يبذل الجاني جهداً لارتكاب جرمه بل يكفي أن يتم الإيقاع بالمجني ليسلم المال الخاص به للجاني تحت غطاء النصب أو الغلط الذي يقع فيه، أما إذا كان تسليم الأموال بناءً على أسباب أخرى انقطعت العلاقة السببية هنا، فكافة الأساليب الاحتيالية يجب أن تؤدي إلى نتيجة جرمية وهي الحصول على مال الغير بدون وجه حق لقيام عنصر التسليم في جريمة الاحتيال المعلوماتي، ولتفادي اللبس بمفهوم النتيجة الإجرامية والعلاقة السببية في جريمة الاحتيال.

وسنحاول في هذا المبحث توضيح المقصود بتسليم الأموال في جريمة الاحتيال المعلوماتي من خلال التعرف على شروط موضوع جريمة الاحتيال المعلوماتي في المطلب الأول، أما في المطلب الثاني سنعالج موضوع التسليم في جريمة الاحتيال المعلوماتي، ولتكمال جريمة الاحتيال المعلوماتي يجب تكامل ركن الضرر أي النتيجة الإجرامية وهو ما سيتم توضيحه في المطلب الثالث؛ لذلك سيتم تقسيم هذا المبحث إلى ثلاث مطالب على النحو الآتي:

المطلب الأول: شروط موضوع جريمة الاحتيال المعلوماتي.

المطلب الثاني: موضوع تسليم المال في جريمة الاحتيال المعلوماتي.

المطلب الثالث: الضرر في جريمة الاحتيال المعلوماتي.

المطلب الأول

شروط موضوع جريمة الاحتيال المعلوماتي

تطرقت أغلب التشريعات العربية إلى موضوع (محل) التسليم واعتبرته مال منقول، وحددت بعض الشروط التي ترد على المال موضوع التسليم، كأن يكون موضوع الاحتيال مالا، ومملوكاً للغير، وذو طبيعة مادية، فهل يمكن انطباق هذه الشروط على الجرائم المرتكبة بوسائل تقنية المعلومات.

إن الحديث عن المال في جريمة الاحتيال يرجعنا إلى القاعدة الأساسية في جريمة النصب في أن يكون محل النشاط مالا مادياً منقولاً ملموساً يسهل الاستيلاء عليه، ويمثل ذات قيمة في نظر القانون فيكون الشيء مقوماً ذات طبيعة مادية من أجل اعتباره مالا. لذلك سيتم تقسيم هذا المطلب إلى ثلاث فروع على النحو الآتي:-

الفرع الأول: أن يكون موضوع التسليم مالا مادياً.

الفرع الثاني: أن يكون موضوع (محل) الاحتيال مملوكاً للغير.

الفرع الثالث: أن يكون موضوع الاحتيال منقولاً.

الفرع الأول: أن يكون موضوع التسليم مالا مادياً.

يشترط في جريمة الاحتيال أن يتم الاعتداء على حق الملكية، ومحل الملكية في هذا الخصوص يجب أن يكون له صفة المال، والمقصود بالمال أن يكون محلاً لحق عيني، وبالتحديد حق الملكية، والأصل أن كل شيء نافع للإنسان يصلح لأن يكون هدفاً للاستثمار وإنشاء الحقوق عليه، فالإنسان لا يمكن أن يكون موضوعاً لجريمة الاحتيال، فإذا كان الشيء يصلح بطبيعته محلاً لحق عيني فهو مال^١.

^١ محمود نجيب حسني، "مرجع سابق"، ص ٣٤.

ويشترط في المال أن يكون ذو طبيعة مادية أي قابلاً للحيازة والتسليم والتملك، والشيء المادي في هذا الخصوص هو "كل ماله كيان ذاتي مستقل في العالم الخارجي، أو هو كل ما له طول وعرض وسمك، بصرف النظر عن حجمه أو وزنه أو هيئته"^١.

ووفقاً لما سبق فإن الأشياء المعنوية، أي غير المادية، لا تعتبر من قبيل الأموال، لأنها أشياء ليس لها كيان مادي كالأفكار والآراء والمخترعات الفنية، ولكن إذا ما تحقق إفراغ هذه الأشياء في وعاء مادي أصبحت من قبيل الأموال فلاستيلاء على هذه الأشياء بأساليب الخداع يتحقق فيه جرم الاحتيال^٢.

فالأشياء التي تصلح أن تكون موضوعاً للاحتيال يجب أن تكتسب صفة الأموال بغض النظر عن قيمة هذه الأشياء وعن طبيعتها سواء كانت مادية أم معنوية^٣.

وبناء عليه فإن جريمة الاحتيال المعلوماتي لا تخرج عن الأصل العام بشأن موضوع تسليم المال في أن يكون محل التسليم له صفة المال المادي، كالنقود والمنقولات والعقارات أو السندات التي تتضمن تعهداً أو إبراء، والأمثلة على ذلك كأن يقوم موقع لشركة وهمية على الإنترنت بعرض بضائع وبيع للبيع، ثم يستلم ثمنها عن طريق الدفع عبر الإنترنت من خلال بطاقات الائتمان، ولا يقوم بإرسال الشيء المبيع إلى المشتري. أو كمن يرسل رسالة إلكترونية تتضمن فوز المرسل إليه بجائزة، ويطلب من هذا الأخير إرسال بعض النقود من أجل تغطية كلفة شحن هذه الجائزة، وبعد أن يقوم المجني عليه بإرسال النقود المطلوبة يتبين بأن الجائزة وهمية^٤.

يعتبر التسليم أحد العناصر الأساسية المكونة لجريمة الاحتيال خصوصاً ركنها المادي، هذا السلوك يمثل النتيجة الإجرامية نتيجة استخدام وسائل احتيالية دفعت بالمجني عليه لتسليم المال، هذا الأمر لا يثير إشكالية لقيام عملية تسليم المال المنقول لآخر، ولكن في حال كان محل الاستيلاء بيانات ومعلومات مخزنة في الحاسب الآلي بهدف تحويل أجزاء من أرصدة الغير إلى حساب الجاني أو نقل معلومات ذات قيمة غير مادية، وهذا ما سنحاول توضيحه.

^١ على القهوجي، "مرجع سابق"، ص ٦٦٤.

^٢ محمد طارق الخن، "مرجع سابق"، ص ١٣٦.

^٣ محمود نجيب حسني، "مرجع سابق"، ص ٣٨٥.

^٤ محمد طارق الخن، "مرجع سابق"، ص ١٣٧.

أولاً: مدى انطباق صفة المال المادي على المعلومات والبرامج في جريمة الاحتيال.

إذا كان موضوع الاحتيال يقع على المعلومات والبرامج في مجال الجرائم المعلوماتية فهنا الإشكالية التي تثار هي: هل ينطبق وصف المال المادي على المعلومات والبرامج؟

ذهب جانب من الفقه إلى القول بأن التلاعب في البرامج والبيانات والتغيير فيها بما يترتب عليه إيهام المجني عليه بصحتها مما يجعله يسلم بها، يعد أحد أساليب التحايل، فمن وجه نظر هذا الاتجاه أن الحاسوب مجرد وسيط للتحايل^١، أما بعض الفقه الفرنسي، فذهب إلى أن جريمة الاحتيال تقوم في مثل هذه الحالات ومبرره في ذلك أن استعمال وسائل الغش وخداع الأنظمة تقع ضمن الطرق الاحتيالية، فخداع الآلة يمكن تصوره بأن وراء الآلة إنسان، وهو من قام ببرمجة الآلة وأن أي معلومات مدخلة على النظام المعلوماتي تمثل وقائع تدعم الكذب والخداع^٢.

إلا أن هناك آراءً فقهية ذهبت بعكس ما ذهب إليه هذا الفقه الفرنسي فرأت أن واقعة الاحتيال لا تتحقق، إذ لا بد أن يكون المخدوع شخصاً طبيعياً (إنسان)، فلا يتصور خداع الحاسب الآلي بوصفه آلة، ويمكن الرد على أصحاب هذا الاتجاه بأن المعلومات والبيانات هي مجموعة مستحدثة من القيم قابلة للاستحواذ مستقلة عن دعائها المادية، على سند من القول أن المعلومات لها قيمة اقتصادية قابلة لأن تحاز حيازة غير مشروعة، وهي ترتبط بمؤلفها عن طريق علاقة التبني التي تقوم بينهما كالعلاقة القانونية التي تتمثل في علاقة المالك بالشئ الذي يملكه، بمعنى أن المعلومات مال قابل للتملك أو الاستغلال على أساس قيمته الاقتصادية وليس على أساس كيانه المادي، ولذلك فهو يستحق الحماية القانونية ومعاملته معاملة المال^٣.

ومعظم التشريعات المقارنة أعطت المعلومات صفة المال، فالقوانين الفيدرالية الأمريكية، أضفت على المال مفهوماً واسعاً بحيث يشمل كل شيء ينطوي على قيمة، ويندرج تحت هذا التعريف الأموال المعنوية والبيانات المعالجة، وتعاقب هذه القوانين على الاستخدام غير المسموح به للحاسوب بغرض ارتكاب أفعال الغش أو الاستيلاء على الأموال^٤.

^١ راجع في ذلك، على الطولية، "مرجع سابق"، ص ١٨١.

^٢ Pradel et Feuillard, (1985). Les infraction commises au money de l'ordinateur Rev, de La pen crim, P 29.

^٣ راجع في ذلك، محمد جلال عبد الرحمن، "مرجع سابق"، ص ١٥٦.

^٤ محمد الشوابكة، "مرجع سابق"، ص ١٨٨.

ثانياً: مدى جواز اعتبار النقود الكتابية والبنكية أموالاً مادية.

كما ذكرنا سابقاً إذا كان الاستيلاء الناتج عن جريمة الاحتيال المعلوماتي نقوداً أو أي منقول آخر له قيمة مادية، فلا تثار أي إشكالية.

ولكن الإشكالية تثار في رأي الفقه في حال ما إذا كان الاستيلاء على نقود كتابية أو بنكية، كأن يقوم الجاني بالتلاعب في البيانات والمعلومات للاستيلاء على أرصدة الغير أو فوائدها فهل تعتبر هذه الأموال من قبيل الأموال المادية أم لا؟

هناك اختلافات في الأصل حول جواز اعتبار الأموال الكتابية محلاً لجريمة الاحتيال، فبعض التشريعات كالتشريع الألماني والتشريع الياباني لا تعتبره من الأموال الكتابية، إلا أن معظم التشريعات تعتبر النقود الكتابية من قبيل الأموال المادية، ويمكن وصفها من قبيل الديون التي يستحيل أن تكون محلاً للاختلاس أو السرقة. وبعض التشريعات اعتبرت النقود الكتابية من قبيل الأموال المادية التي تصلح لأن تكون محلاً لجرائم الاحتيال، ففي الولايات المتحدة صدرت عدة قوانين تدعم جواز اعتبار النقود الكتابية من قبيل الأموال المادية وعُرف المال في هذه التشريعات بأنه: "كل شيء يمثل قيمة، فهو تعريف يشمل جميع الأموال الكتابية أو البنكية"^١.

وفي التشريع الفرنسي أقرت محكمة النقض الفرنسية نظرية التسليم المعادل^٢، واعتبرت أن مجرد القيد الذي لا يقتضي تسليم شيء مادي أيّاً كان يعد من قبيل التسليم المعادل^٣.

الفرع الثاني: أن يكون موضوع (محل) الاحتيال مملوكاً للغير.

في جريمة الاحتيال يجب أن يكون الاعتداء على حق الملكية مملوكاً للغير، بمعنى لا يمكن وقوع جريمة الاحتيال إذا كان المال مباحاً أو مملوكاً للجاني. كما يجب أن يستعمل الجاني الخداع والأساليب الاحتيالية للاستيلاء على مال الغير لكي يتحقق فعل الاحتيال، أما إذا كان مالك المال هو يستخدم الخداع والأساليب الاحتيالية في سبيل استرداد ماله أو حقه فلا نكون

^١ محمد الشوابكة، "مرجع سابق"، ص ١٩٢.

^٢ ابتدع القضاء الفرنسي نظرية التسليم المعادل والتي اعتبر فيها أن مجرد القيد الكتابي لصالح أحد الأشخاص يعادل تسليمه المال. أيمن عبد الله فكري، "مرجع سابق"، ص ٧٠٤.

^٣ Crime du 10 de'c 1975, J.C.P. 1970-17977 nate Gassin.

أمام جريمة احتيال، فالمؤجر أو المودع أو الراهن الذي يسترد ماله بالخداع لا يرتكب جرم الاحتيال، وذلك لعدم توفر ركن أساسي من أركان قيام جريمة الاحتيال وهو الاستيلاء على مال الغير^١.

ويختلف الحال في حالة الدائن، إذ لا يعتبر الدائن مالكاً لشيء من أموال مدينه، فكل ما يملكه المدين يعتبر بالنسبة للدائن مملوكاً للغير، فإذا استولى بالخداع على مال مدينه فيعتبر محتالاً^٢.

وفي إطار جريمة الاحتيال المعلوماتي فإن هذا الركن يتوافر عندما يقوم الجاني بالاستيلاء على مال الغير عن طريق الاحتيال، أما الاستيلاء على البرامج والمعلومات فيحدث على الدعامة أو وسيط مخزن عليه معلومات أو برامج يصلح أن يكون محلاً للاحتيال، فالغرض من هذا الاحتيال هو الاستيلاء على المعلومات التي لا يمكن فصلها عن الدعامة أو الوسيط، وبذلك تنتقل حيازة المعلومة من مالكة الأصلي إلى حيازة الجاني، ويحدث ذلك أيضاً في حالة النسخ المكرر من النسخة الأصلية^٣.

فالمعلومات والبرامج تصلح لأن تكون محلاً للملكية، وفقاً لقانون حماية الملكية الفكرية، فقاعدة الحيازة في المنقول سند الحائز تنطبق على المعلومات والبرامج، بالإضافة على أن البرامج تعد ملكاً لمن ابتكرها^٤.

الفرع الثالث: أن يكون موضوع الاحتيال منقولاً. ٥

يعرف المنقول على أنه "كل ما يمكن تغييره من موضعه، أي يقبل الشيء النقل والحركة من مكانه، سواء أصابه تلف أم لم يصبه، وسواء كان جزءاً من العقار أم لم يكن"^٥.

^١ محمد طارق الخن، "مرجع سابق"، ص ١٤١.

^٢ محمود نجيب حسني، "مرجع سابق"، ص ٣٨٦.

^٣ محمد احمد طه، "مرجع سابق"، ص ٤٨٣.

^٤ هدى قشقوش، "مرجع سابق"، ص ٥٨.

^٥ علي القهوجي، "مرجع سابق"، ص ٦٦٨.

من خلال التعريف السابق بخصوص المنقول، فإن مفهوم السندات يدخل في إطار المال المنقول، ويقصد بالسندات "الصكوك أو المحررات ذات القيمة المالية، أي كل ورقة تحمل تعهداً أو إبراء"^١.

وتعد سندات الدين من قبيل التعهدات أما سندات المخالصة فهي تعتبر من الإبراء، فلا يقتصر مفهوم السند على موضوع السند ذات الطبيعة المادية، بل يمتد إلى التعهد أو الإبراء نفسه، كأن يحصل الجاني بطريق الخداع على تعهد أو سند في حيازة المجني عليه دون أن يحصل على السند ذاته، كأن يستطيع الجاني أن يثبت اسمه لدى المجني عليه أنه يستحق مالاً في ذمته، أو أن يحذف من دفتره أي المجني عليه مبلغاً كان ثابتاً في ذمة الجاني^٢.

وتتوثر بعض الأسئلة الموضوعية حول مدى اعتبار محل الاحتياال المعلوماتي عقار، ففي جريمة النصب مثلاً ينبغي أن يكون المحل منقولاً، أما في جريمة الاحتياال المعلوماتي من الناحية النظرية فإن العقار والمنقول يمكن أن يكون محلاً للنشاط الإجرامي، فالعبرة الأساسية هي التمكن من الحصول على المحل الإجرامي بوضع الشيء في متناول يد الجاني على سبيل التلاعب في البيانات والمعلومات التي تثبت ملكية العقار أو التي تحدد ثمنه أو تمكن من إنشاء حقوق عينية على العقار، في هذه الحالة يكون الاحتياال المعلوماتي^٣.

فإذا ما أُوهم الجاني عبر طرق احتيالية باستخدام تقنية المعلومات المجني عليه أن لديه أرصدة بنكية أو رصيد ائتماني مملوك له يستطيع من خلالها الوفاء بتسديد المبلغ المطلوب لتسجيل عقار باسمه، مما دفع المجني عليه بتسجيل هذا العقار باسم الجاني، وتبين بعد ذلك بأن الجاني لا يملك ثمن العقار أو أنه لا يملك رصيد ائتماني^٤.

أما التكييف القانوني للبرامج والمعلومات حول مدى اعتبارها منقولات أم عقار، فهي تعتبر من قبيل المنقولات والتبرير في ذلك أنه عند تشغيل الحاسوب تنتقل هذه المعلومات أو

^١ علي القهوجي، "مرجع سابق"، ص ٨٠٤.

^٢ محمود نجيب حسني، "مرجع سابق"، ص ٣٨٩.

^٣ سامر سلمان الجبوري، "مرجع سابق"، ص ١٠٤.

^٤ محمد طارق الخن، "مرجع سابق"، ص ١٤٤.

البرامج من ذاكرة الحاسوب إلى ذهن المتلقي، وهي عبارة عن إشارات إلكترونية تشبه التيار الكهربائي القابل للانتقال على الرغم من عدم حيازته المادية^١.

المطلب الثاني

موضوع تسليم المال في جريمة الاحتيال المعلوماتي

هناك تشابه بين مفهوم الاحتيال بصورته العامة والتي يقصد بها كل فعل يباشره المتهم بنفسه أو بغيره ويتوصل من خلاله إلى تسليم مال منقول مملوك للغير بدون وجه حق باستعمال الجاني مجموعة من الوسائل الخداعية التي نص على تجريمها القانون كالغش والخداع والنصب^٢، والتي يقع على إثرها المجني عليه في الخطأ، بينما الاحتيال بشقه الخاص وهو الاحتيال المعلوماتي فيقع عندما يتم تلاعب الجاني في البيانات والمعلومات المخزنة في نظام الحاسب الآلي أو في مكوناته وفقا لأساليب متعددة كإدخال بيانات غير صحيحة بهدف تحويل أموال الغير إليه أو تلاعب بالأرصدة من أجل منفعة خاصة^٣، وسيتم تقسيم المطلب إلى ثلاثة فروع هي:

الفرع الأول: موضوع التسليم في جريمة الاحتيال المعلوماتي.

الفرع الثاني: التسليم في جريمة الاحتيال المعلوماتي.

الفرع الثالث: موقف التشريعات العربية من موضوع التسليم في جريمة الاحتيال المعلوماتي.

الفرع الأول: موضوع التسليم في جريمة الاحتيال المعلوماتي.

^١ هدى قشقوش، "مرجع سابق"، ص ٥٦.

^٢ أحمد خليفة الملط، "مرجع سابق"، ص ٤٢٢.

^٣ محمد أحمد طه، "مرجع سابق"، ص ١٤٩.

إن التقارب بين أركان جريمة النصب في صورتها التقليدية والعامة التي تتمحور حول الاحتيال المعلوماتي خلقت مجموعة من الإشكاليات القانونية والفقهية في محاولة لفهم مدى الانطباق والتقارب بين النصوص المطبقة على كل حالة، فهل تتوافر أركان جريمة الاحتيال في الحالات التي يتم فيها التلاعب في البيانات والمعالجات آلياً أو في البرامج المعلوماتية الهادفة للاستيلاء على مال الغير؟ مثال قيام شخص بالتلاعب في البيانات المخزنة أو المدخلة للحاسب الآلي أو التلاعب في البرامج أو التلاعب في النبضات الإلكترونية المرسلة من الحاسب الآلي المركزي.

فما مدى وقوع فعل الاحتيال على نظام الحاسب الآلي الذي يدفعه للوقوع في فرضية التسليم؟

أشرنا إلى أن السلوك المادي لجريمة النصب يدور حول الكذب والخداع من قبل الجاني للاحتيال على المجني عليه للقيام بتسليمه مالا من أمواله، أي أن الخداع وقع من قبل إنسان لإنسان، ولكن هل يمكن تطبيقه في حالة كان الطرف الأول إنسان والطرف الثاني أنظمة الحاسوب الآلية؟

في هذه الحالة يصعب تطبيق أركان جريمة الاحتيال المعلوماتي لعدم صلاحية خضوع البرامج للنشاط الإجرامي للنصب، لكونه لا يوجد نشاط مادي يتحقق به التسليم والاستيلاء^١، وحتى لو تم افتراض عملية التسليم والاستيلاء في حالة الاحتيال المعلوماتي فإنه لا ينتج عنه حرمان المجني عليه من المعلومات التي نقلها بالقول بل ستظل تحت سيطرة من نقلها وفي حوزته وهو ما يعني أن ما سبق قوله يتفق مع طبيعة المعلومات والبرامج المعلوماتية في حين عدم اتفاقها مع جريمة النصب.

ويرى الفقه الفرنسي أن خداع الحاسب الآلي وسلب المال يتحقق بالطرق الاحتيالية بمفهومها المستقر في المادة (٤٠٥) من قانون العقوبات الفرنسي والتي نصت على أنه " كذب تدعمه أعمال مادية أو واقعية خارجية حيث يتوافر بالإضافة للكذب واقعة خارجية تسانده هي إبراز أو تقديم المستندات أو المعلومات التي تدخل في الحاسب الآلي بناء على ما وقع من

^١ علي حسن الطويلة، "مرجع سابق"، ص ١٨٢.

تلاعب في البيانات المخزنة أو البرامج المعلوماتية لكي يستولي على أموال الغير بدون وجه حق^١.

ويرى اتجاه من الفقه الفرنسي أن التلاعب في البيانات أو البرامج المخزنة داخل الحاسوب المؤدي إلى إلغاء رصيد مستحق على الجاني أو خلق أرصدة لمصلحته بمبالغ غير مستحقة له يتحقق فيها عنصر التسليم المقصود بجريمة الاحتيال وذلك باستنادهم على نظرية التسليم المعادل التي تم إرسائها من قبل محكمة النقض الفرنسي في قضية تتلخص وقائعها بأن شخص قدم إلى ضريبة المبيعات فواتير وهمية بهدف خصمها من الضرائب المستحقة عليه فقررت المحكمة أن مقدار الخصم يعادل مبلغ التسليم^٢.

الفرع الثاني: التسليم في جريمة الاحتيال المعلوماتي.

عُرف التسليم بأنه: "سلوك صادر عن خُدع بالاحتيال الواقع من الجاني، بمقتضاه ينقل المجني عليه إلى غيره المال موضوع الجريمة"، ولكن بالنظر إلى بعض الحالات الاحتيالية نجد أن الحاسب الآلي يقوم بفعل التسليم بمفهومه المادي لكونه ينطوي على تسليم يدوي كالجرائم الواقعة على البطاقات الائتمانية بصورة غير مشروعة سواء عن طريق الوفاء بواسطتها أو لسحب النقود منها، وتتم هذه الجريمة كما أسلفنا سابقاً من خلال الحصول على كلمة السر الموجودة في نظام الحاسب الآلي الواقع عليه الاحتيال^٣.

وهناك تسليم للمال يتم بصورة أخرى غير مادية ولا يتم النظر إليه على أنه واقعة مادية تتمثل في مناوله ترد على شيء ينقله المجني عليه من حوزته إلى غيره وهو المحتال، ولكن يفترض النظر إليه على أنه عمل قانوني عنصره إرادة المجني عليه وهي الخداع وليست المناولة سوى المظهر المادي لهذا العمل أو أثره، فإذا تم الأخذ بهذا المعنى للتسليم فلا نجد أي إشكال في موضوع الاحتيال المعلوماتي التي لا تتطلب التسليم المادي للمال محل النشاط الإجرامي،

^١ راجع في ذلك، محمد علي العريان، "الجرائم المعلوماتية"، دار الجامعة الجديدة، الإسكندرية، ٢٠١١، ص ١٤٨.

^٢ راجع في ذلك، علي حسن الطوالبة، "مرجع سابق"، ص ١٧٩.

^٣ بدر بن أحمد بن محمد الزهراني، "مرجع سابق"، ص ٨١.

والذي يمكن أن يكون التسليم على شكل عمليات حسابية يقوم بها الحاسب الآلي بحيث لا يصل الجاني للمال بصورة مباشرة^١.

ومما سبق يتبين إن جريمة الاحتيال المعلوماتي في صورتها التقليدية تعتبر من جرائم النصب فالتسليم لا يعني المناولة اليدوية فقط بل يكفي اتجاه الجاني في جريمة النصب والاحتيال لوضعه تحت تصرف الجاني نتيجة التأثير عليه بالوسائل والطرق الاحتيالية وهو ما ذهب إليه المشرع المصري في المادة (٣٣٦) عقوبات بأنه: توصل إلى الاستيلاء على نقود - أو عروض أو سندات دين أو سندات مخالصة أو أي متاع منقول - وهنا تم تقسيم النصب لمجموعتين المجموعة الأولى تضم الاموال المنقولة ذات القيمة الذاتية مثل النقود والعروض أما الثانية فتضم الأموال التي ليست لها قيمة ذاتية وإنما تستمد قيمتها من صلاحيتها للمطالبة بحق وهي سندات الدين والمخالصة، وهذا ما أثار مجموعة من الإشكاليات القانونية في مدى اعتبار الوقائع غير المادية نصباً، وهناك من يرى عدم صلاحية الأشياء التي تكون ذات قيمة معنوية لأن تكون محلاً للجريمة^٢.

ولكن في ذات الوقت يمكن تطبيق هذه المادة على المال المعلوماتي سواء كان هذا المال مالياً مادياً من شاشات واسطوانات وديسكات وأسلاك وكابلات وأجهزة وأدوات وشرائح إلكترونية وكهرومغناطيسية، أو كان معنوياً من بيانات ومعلومات وبرامج ونظم تطبيقية منسوخة على دعامات ممغنطة أو في شكل شحنات كهربية أو بطاقات مثقبة، فعملية الاحتيال هنا في الأصل تتم نتيجة خداع الحاسب الآلي لدفعه على تسليم المال المراد الاستيلاء عليه من أوراق أو سلع أو خدمات أو بقاء الجاني بالاستعانة بجهاز الحاسب الآلي لارتكاب جريمة من الجرائم الأخرى الاحتيالية كالنصب^٣. فالمال هنا في جريمة الاحتيال المعلوماتي يقصد به أي مال مملوك للغير سواء كانت له قيمة مادية أو معنوية وسواء كانت له قيمة في نظر كل الناس أو في نظر بعضهم.

وهنا يمكن القول أنه في حالة كانت جريمة الاحتيال بواسطة النظام المعلوماتي وسيلة من أجل السيطرة على مال الغير فهذا يمكن تطبيق التشريعات الخاصة بجريمة الاحتيال، أما إذا تمت الجريمة بواسطة المعلومات كوسيلة ضد جهاز المعلومات نفسه فهذا يمكن تطبيق قانون العقوبات على أساس أن المستهدف بجريمة النصب الآلة وليس الإنسان، مما أثار خلافاً فقهيًا

^١ سامر سلمان الجبوري، "مرجع سابق"، ص ١٠٢.

^٢ محمد أحمد طه، "مرجع سابق"، ص ١٥٢.

^٣ بلال أمين زين الدين، "مرجع سابق"، ص ١٥٤.

حول مدى صلاحية النصوص التقليدية المجرمة لجريمة الاحتيال لتجريم أفعال الاحتيال المعلوماتي.

الفرع الثالث: موقف التشريعات العربية من موضوع التسليم في جريمة الاحتيال المعلوماتي.

لقد حدد المشرع البحريني في المادة (٨) من القانون الخاص بجرائم تقنية المعلومات موضوع الاستيلاء وطبيعة المال المستولى عليه بالطرق الاحتيالية، فقد نصت على أن "يعاقب بالحبس من توصل دون مسوغ قانوني إلى الاستيلاء على مال مملوك للغير أو حصل على أية مزية لنفسه أو لغيره أو إلى توقيع سند أو إتلافه أو تعديله باتخاذ اسم كاذب أو صفة غير صحيحة أو بالاستعانة بطريقة احتيالية".

يتضح من نص المادة أن المشرع البحريني لم يفسر ما المقصود بالمال في مثل هذا الجرائم التي تقع باستخدام وسائل تقنية المعلومات، ولما كانت جريمة الاحتيال المعلوماتي نتيجتها الجرمية هي الاستيلاء على المال الذي لا يتسم بالمادية كالنقود الكتابية أو البنكية وجب الإلمام بمدى اعتبار النقود الكتابية أو البنكية من قبيل الأموال المادية.

في ذات السياق ذهب المشرع البحريني في قانون جرائم تقنية المعلومات لتوضيح مسألة المال المنقول وغير المنقول أي موضوع التسليم في المادة (٨) بقوله: "يعاقب بالحبس من توصل دون مسوغ قانوني إلى الاستيلاء على مال مملوك للغير أو حصل على أية مزية لنفسه أو لغيره أو إلى توقيع سند أو إلغائه أو إتلافه أو تعديله باتخاذ اسم كاذب أو صفة غير صحيحة أو بالاستعانة بطريقة احتيالية، وذلك من خلال أي فعل مما يلي:

أ- إدخال أو تعييب أو تعطيل أو إلغاء أو حذف أو تدمير أو تغيير أو تعديل أو تحريف أو حجب بيانات وسيلة تقنية المعلومات.

ب- القيام بأي تدخل في عمل نظام تقنية المعلومات.

كما نصت المادة (١١) من القانون الاتحادي رقم (٥) لسنة ٢٠١٢ على أنه "يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من استولى لنفسه أو لغيره بغير حق على مال منقول أو منفعة أو على سند أو توقيع هذا السند، وذلك بالاستعانة بأي طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلومات الكتروني أو إحدى وسائل تقنية المعلومات". أما المادة (١٢) من ذات القانون فنصت على أن: "يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين كل من توصل بغير حق، عن طريق استخدام الشبكة المعلوماتية أو نظام معلومات الكتروني أو إحدى وسائل تقنية المعلومات، إلى أرقام أو بيانات بطاقة ائتمانية أو الكترونية أو أرقام أو بيانات حسابات مصرفية، أو أي وسيلة من وسائل الدفع الإلكتروني.

وتكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة ألف درهم ولا تجاوز ثلاثمائة ألف درهم أو بإحدى هاتين العقوبتين، إذا قصد من ذلك استخدام البيانات والأرقام في الحصول على أموال الغير، أو الاستفادة مما تنتجه من خدمات. فإذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال مملوك للغير فيعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن مائتي ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين. ويعاقب بذات العقوبة المنصوص عليها في الفقرة السابقة كل من نشر أو أعاد نشر أرقام أو بيانات بطاقة ائتمانية أو الكترونية أو أرقام أو بيانات حسابات مصرفية تعود للغير أو أي وسيلة أخرى من وسائل الدفع الإلكتروني.

أما المشرع السعودي بالمادة (٤) من نظام مكافحة جرائم المعلوماتية السعودي فقد نص في المادة (٤) على أن: "يعاقب بالسجن مدة لا تزيد عن ثلاث سنوات وبغرامة لا تزيد عن مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا 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 تنتجه من خدمات. وجاءت المادة الثالثة عشر من القانون لتؤكد على جواز الحكم

بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصل عليها منها".

نلاحظ من خلال ما سبق التوسع في مفهوم الاحتيال المعلوماتي فلم يبق مرتكز على المال المنقول فقط بل أيضاً على البيانات والمستندات والخدمات.

وفيما يخص ممارسة الأفعال الاحتيالية على الأشخاص الطبيعية أو الاعتبارية فإن التساؤل يدور حول تعرض الحاسب الآلي نفسه لأفعال الاحتيال وإيقاعه في الغلط من عدمه؟

وهو ما ذهبت إليه التشريعات محل المقارنة بتشريعات مستحدثة تتناسب مع جريمة الاحتيال المعلوماتي وتطورها، في إطار النصوص التشريعية السابقة التي توسعت على من يقع عليه جريمة الاحتيال ليشمل إلى جانب الشخص الطبيعي الآلة، فلم ينع ذلك النقاش القائم بين مسألة خداع الإنسان أو الآلة مما يستوجب ضرورة حل هذا الإشكال بمجموعة من النصوص التفسيرية لتفادي التفسيرات الواسعة لها.

المطلب الثالث

الضرر في جريمة الاحتيال المعلوماتي

ثار خلاف سابقاً بين الفقهاء حول عنصر الضرر في كل من التشريع الفرنسي والمصري في جريمة الاحتيال من حيث وجوبه من عدمه، فهل هذا شرط لاعتبار الجريمة واقعة وضرورة أن يلحق المجني عليه بالضرر من استيلاء الجاني على أموال المجني عليه، أو أن الجريمة تتحقق حتى لو لم يتم عنصر الضرر؟ وهذا عنصر الخلاف بين الفقهاء.

كانت البداية الأولى للاختلاف الفقهي حول عنصر الضرر في جريمة الاحتيال، حيث يرى أغلب الفقه أنه يكفي أن يكون الضرر محتمل الوقوع في جريمة الاحتيال، ولا يفترض فيه قيام العدوان على ملكية الأفراد أو المساس بحرية الإرادة، فكل عدوان على ملكية الغير ومساس بحريته يعتبر من البديهي ضرراً، ولا داعي إلى أن يشترط ضرورة وجود نقص في أموال المجني عليه^١.

فقد نصت المادة (٣٣٦) من قانون العقوبات المصري على أن يكون الاحتيال للاستيلاء على عروض أو سندات ... أو أي متاع منقول ومثلها المادة (٤٠٥) من قانون العقوبات الفرنسي التي تطلبت استيلاء الجاني على كل ثروة الغير أو بعضها^٢.

وفي كلتا الحالتين انتقاص من ثروة المجني عليه حتى تقوم جريمة الاحتيال، أما إذا لم يكن هناك انتقاص للثروة فلا يتحقق الضرر وبالتالي تنتفي جريمة الاحتيال، وذهب البعض بالقول لا جريمة ولا عقاب إذا انتفى عنصر الضرر.

وذهب آخر وهو الراجح لدى القضاء الفرنسي إلى أن الاحتيال كالسرقة لا يتطلب أكثر من وقوع الاستيلاء على مال منقول مملوك للغير^٣، وأما الضرر فهو عنصر لصيق بالفعل ومفترض الوجود حيث يترتب على الاحتيال التأثير على إرادة المجني عليه وجعله يتصرف في ملكيته بالطريقة التي لا يريد، فالضرر المقصود به المساس بحقوق المجني عليه وعلى ماله

^١ أحمد خليفة الملط، "مرجع سابق"، ص ٤٢١.

^٢ بلال أمين زين الدين، "مرجع سابق"، ص ١٥٧.

^٣ بلال أمين زين الدين، "مرجع سابق"، ص ١٥٧.

إما بالانتقاص منه ويعرف بالضرر المادي أو التأثير عليه وهو يعرف بالضرر المعنوي، وما جاء في المادة (٣٣٦) والمادة (٤٠٥) هي نصوص عامة لا تتطلب ضرر معين بذاته كما لا تتطلب أكثر من انصراف إرادة الجاني إلى ارتكاب جريمة النصب حتى يتوضح الجانب المعنوي عن الجانب الموضوعي للجريمة^١.

أما أحكام المادة (٣١٣) من القانون الفرنسي الجديد لعام في تفسيره للنص فيما هو متعلق - بالضرر المتطلب - قد انحصر الخلاف الفقهي فيما إذا كان الضرر المتطلب يشكل عنصراً ومكوناً أساسياً للجريمة ينفصل عن غيره من العناصر الأخرى أم أنه يندمج مع العناصر الأخرى كالتسليم، كالقول بأن كل تسليم يتم بطريقة احتيالية يجب أن يحتوي على ضرر^٢.

ولكن المادة (٣١٣) في فقرتها الأولى فصلت هذه المسألة حيث أنه إذا لم يترتب على التسليم ضرر يقع على المجني عليه أو على غيره كما لم يتمكن المتهم من تحصيل الصك الذي حصل عليه من المجني عليه نتيجة طرق الاحتيال الممارسة عليه فلا يمكن القول في هذه الحالة أن التسليم قد يحتوي على ضرر، بينما عارض اتجاه هذا الموقف بقوله: "أن التسليم الناتج عن طرق احتيالية ينطوي في ذاته على الضرر المتطلب لأنه يشكل اعتداء على حرية إرادة المجني عليه، هذا الأمر دفع إلى تباين الأحكام الفرنسية الصادرة في هذا الاتجاه لتتبنى تارة هذا الرأي وتارة الرأي الآخر^٣.

فيما ذهب في بعض أحكامه أن التسليم الصادر عن الإرادة نتيجة لممارسة الطرق الاحتيالية حيالها لا يكون جريمة الاحتيال حيث لا يترتب عليه ضرر والذي يتمثل في سلب ثروة الغير^٤.

وفي هذا الإطار اتفق أغلب الفقهاء للاعتبارات العلمية المتعلقة بجريمة الاحتيال المعلوماتي ينبغي أن يكون الضرر محتملاً، لأن تسليم المال قد يكون محتملاً أيضاً، إذ قد يكون نتيجة تسليم المال بمقابل أو التوقيع على سند منشئ للالتزام وقد يتم التسليم نتيجة المقاصة أو بتبادل الدين الذي كان في ذمة المجني عليه^٥.

^١ بلال أمين زين الدين، "مرجع سابق"، ص ١٥٧.

^٢ سامر سلمان الجبوري، "مرجع السابق"، ص ١٠٧.

^٣ سامر سلمان الجبوري، "مرجع السابق"، ص ١٠٧.

^٤ سامر سلمان الجبوري، "مرجع السابق"، ص ١٠٧.

^٥ أحمد خليفة الملط، "مرجع سابق"، ص ٤٢١.

فالاحتيال المعلوماتي يختلف عن الاحتيال التقليدي فلا يتطلب في أغلب الحالات مجهوداً من قبل الجاني وهو ما يؤدي على الاخلال بمقتضيات العدالة طالما تم ارتباط الجريمة بتوافر ركنها المادي فقط. فيجب أن يترتب على فعل الاحتيال قيام المجني عليه بالاستيلاء على مال الغير بدون وجه حق إما باستخدام الحاسب الآلي أو تطبيقاته، أي أن يكون الحاسب الآلي أداة للاستيلاء على مال الغير، أو بواسطة الاستخدام التعسفي لبطاقات ممغنطة أو بطاقات الائتمان متى استخدمت كأداة لارتكاب الجريمة المعلوماتية، كقيام شخص بإدخال معطيات وهمية أو بتعديل البرامج أو خلق برامج احتيالية يترتب عليها وسيلة للاحتيال التي يمكن من خلالها الاستيلاء على أموال الغير، وهذا ما جاءت به الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المصادق عليها من قبل التشريع البحريني والمقارن لبيان الضرر الواقع في جريمة الاحتيال المعلوماتي بنص المادة (١١) على أنه: "التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير، عن طريق:

١- إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات.

٢- التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها.

٣- تعطيل الأجهزة والبرامج والمواقع الالكترونية".

ويتمثل عنصر الضرر والنتيجة الإجرامية في أن يدفع بالمجني عليه تسليم ماله أو جزء منه إلى الجاني تحت تأثير هذه الطرق والوسائل بغية الحصول على معلومات من الضحية. فقد حدثت مجموعة من الوقائع في هذا المجال، ومنها ما وقع في دولة الكويت إذ قام مبرمج يعمل لدى البنوك وحال تواجده نتيجة لعمله في أحد البنوك قام بعمل برنامج يعطي من خلاله أمراً بتحويل الأموال من حسابات العملاء المسجلة في الحاسب الآلي لصالح حسابات تابعة له ثم عاد لبريطانيا بعد انتهاء مدة عمله في الكويت، وقام بطلب لتحويل الأموال من الكويت لبريطانيا، وتم أمر التحويل، وحُولت كافة الأموال إلا أنه تم اكتشاف أمره لاحقاً وأنكر الواقعة وبرهن إنه لم يخالف القانون الكويتي ودفع بعدم الاختصاص^١.

خلاصة القول: يتضح أن معظم الآراء الفقهية المختلفة والتشريعات المقارنة محل الدراسة قد أجازت اعتبار البرامج والمعلومات من قبيل الأموال المادية وذلك انطلاقاً من عدة اعتبارات أهمها تلك التي استندت على موضوع القيمة الاقتصادية لهذه البرامج والمعلومات والتي اعتبرتها

^١ سامر سلمان الجبوري، "مرجع سابق"، ص ١٠٨.

محلاً للملكية والتي يقع الاعتداء عليها، بالإضافة إلى إمكانية إيقاع الحاسب الآلي لفعل الخداع واعتباره مجرد وسيط يدار من قبل المجني عليه وأي اعتداء على الحاسب هو بمثابة اعتداء على المجني عليه المالك لهذا الحاسب الذي يمتلك حقوق برمجته ، أما بالنسبة لركن التسليم ومدى جواز انطباقه على النقود الكتابية فذهبت معظم التشريعات وهذا إلى إمكانية تحقق فعل التسليم على هذه النقود في جريمة الاحتيال المعلوماتي وتعادل في ذلك تسليم الأموال العادية وهو ما عبر عنه الفقه الفرنسي بنظرية التسليم المعادل، وكذلك التشريع الفرنسي أقرت محكمة النقض الفرنسية نظرية التسليم المعادل، واعتبرت أن مجرد القيد الذي لا يقتضي تسليم شيء مادي أياً كان يعد من قبيل التسليم المعادل.

الفصل الثالث

الطبيعة الإجرائية لإثبات جريمة الاحتيال باستخدام
وسائل تقنية المعلومات

الفصل الثالث

الطبيعة الإجرائية لإثبات جريمة الاحتيال باستخدام وسائل تقنية المعلومات

تمهيد وتقسيم:

تعد جريمة الاحتيال المعلوماتي كغيرها من الجرائم التي لها أركان وعناصر، وتسير الدعوى الجنائية بالنسبة لها بذات المراحل التي تسير فيها الدعوى في الجرائم التقليدية، وتهدف الإجراءات الجنائية في جريمة الاحتيال المعلوماتي إلى فحص الأدلة القائمة على وقوع الجريمة ونسبتها إلى فاعلها، ومن أهم الإجراءات القانونية إجراءات التحري والتحقيق وفحص الأدلة كالمعينة والتفتيش والضبط. وتمتاز جريمة الاحتيال المعلوماتي بأن الأدلة التي قد يتركها الجاني تقع في بيئة إلكترونية، إذ تقوم على التلاعب في البيانات والبرامج، ويمتاز المجرم المعلوماتي بقدرته الهائلة على إخفاء جريمته والتلاعب بالأدلة، لذلك يجب على السلطات القضائية أن تتعامل مع هذه الجرائم بما يتناسب معها من أدلة الكترونية. فجريمة الاحتيال المعلوماتي تتطلب إجراءات خاصة متفق عليها من أجل حماية الدليل، ولكن الوسائل التي يتم فيها حفظ الأدلة واستنتاج هذه الأدلة تختلف عنها في الجرائم التقليدية. وتمتاز جريمة الاحتيال المعلوماتي بأنها حديثة النشأة إذ ترافق ظهورها بظهور الإنترنت ووسائل تقنية المعلومات، لذلك لجأت أغلب الدول حديثاً إلى سن قوانين تجرم هذه الجريمة وتوقع على مرتكبيها الجزاء المناسب، ومن خصائص جريمة الاحتيال أنها عابرة للحدود مما استدعى تظافر الجهود الدولية والوطنية لمواجهة هذه الجريمة وللإلمام أكثر بالإجراءات الجنائية لجريمة الاحتيال وللتعرف على مدى حجية الأدلة المستخرجة من البيئة المعلوماتية لها، وما مدى تظافر الجهود الدولية والوطنية في مواجهة جريمة الاحتيال المعلوماتي سنقسم الفصل إلى ثلاث مباحث وذلك على النحو الآتي:-

المبحث الأول: الإجراءات القانونية لإثبات جريمة الاحتيال باستخدام وسائل تقنية المعلومات.

المبحث الثاني: الأدلة الجنائية في إثبات جريمة الاحتيال باستخدام وسائل تقنية المعلومات.

المبحث الثالث: الجهود الدولية والوطنية لمواجهة جريمة الاحتيال باستخدام وسائل تقنية المعلومات.

المبحث الأول

الإجراءات القانونية لإثبات جريمة الاحتيال باستخدام وسائل تقنية المعلومات

إن الإجراءات المتبعة في جريمة الاحتيال المعلوماتي من حيث إثباتها لا تختلف كثيراً عن الجرم التقليدي ، غير أن جريمة الاحتيال المعلوماتي ذات طبيعة خاصة بالنسبة لآلية تلقي البلاغات والشكاوى، وأيضاً فيما يخص إجراءات البحث والتحري عن الجريمة وأطرافها، وتتنوع وسائل جهاز الشرطة في مجال الضبط القضائي لمكافحة جريمة الاحتيال المعلوماتي، ويجب على جهاز الضبط القضائي أن يمتلك الخبرة الكافية للتعامل مع البيئة الرقمية التي تمتاز بها جريمة الاحتيال المعلوماتي.

حيث تعتمد هذه الجريمة على كيانات معنوية موجات -كهرومغناطيسية- في اقترافها، فمجرم البيئة الرقمية يعتمد على الجانب الفكري لا العضلي، كما يمتاز بالإلمام بالجوانب الفنية والتقنية في مجال الحاسب الآلي، فلديه القدرة على إخفاء الأدلة والتلاعب فيها، لذا يجب على السلطات المختصة أن تتعامل مع هذه الجرائم بما يتناسب معها من أدلة إلكترونية ورقمية.

ويتولى أفراد الضبط القضائي إجراءات مرحلة الضبط والتحري بتفويض من النيابة العامة حيث يعدون تابعين وخاضعين لإشرافها باعتبارهم مساعدين للقضاء بهدف البحث عن الجرائم ومرتكبيها تمهيداً لافتتاح الدعوى العمومية، ولالإلمام أكثر بإجراءات جمع الأدلة لجريمة الاحتيال المعلوماتي سنقسم المبحث إلى ثلاث مطالب على النحو الآتي:

المطلب الأول: البلاغ والشكوى في جريمة الاحتيال المعلوماتي.

المطلب الثاني: معاينة جريمة الاحتيال المعلوماتي.

المطلب الثاني: إجراءات التفتيش والضبط في جريمة الاحتيال المعلوماتي.

المطلب الأول

البلاغ والشكوى في جريمة الاحتيال المعلوماتي

يعتبر البحث والتحري بمثابة مجموعة من الإجراءات التي يقوم بها المتحري عبر الشبكة بواسطة التغطية الإلكترونية وكذلك على أجهزة الحاسب الآلي، وذلك للحصول على بيانات ومعلومات تعريفية أو توضيحية عن الأشخاص أو الأماكن والأشياء حسب طبيعتها لضبط الجرائم المعلوماتية أو الرقمية عبر الإنترنت، فإجراءات البحث والتحري عن الجريمة الرقمية من الإجراءات الاستدلالية والتي تتمثل في الإرشاد الجنائي عبر الإنترنت وبالمراقبة الإلكترونية للاتصالات للتقصي والكشف عن الجرائم، وضبط فاعليها والتحقيق معهم وتقديمهم للمحاكمة^١. وسيتم تقسيم المطلب الى فرعين على النحو الآتي:-

الفرع الأول: ماهية الشكاوى والبلاغات.

الفرع الثاني: البلاغ والشكوى عن جريمة الاحتيال المعلوماتي.

الفرع الأول: ماهية الشكاوى والبلاغات

إذا علم مأمورو الضبط القضائي بوقوع جريمة، سواء تحقق هذا العلم بطرق شخصية أو عن طريق شكوى مقدمة من المتضرر منها، أو عن طريق الإبلاغ عنها بأية طريقة أخرى، أن يقبلوا ما يرد إليهم من الإخبارات والشكاوى عن الجرائم التي تكون قد ارتكبت وبمارسوا مهامهم بجمع المعلومات الخاصة بالجريمة وإثباتها في محضر التحري، وعليهم تسجيل ملخص البلاغ فوراً في دفتر يعد لذلك بمركز الشرطة، على أن يتم إخطار النيابة العامة فوراً دون تأخير في الجنايات، ومحققي الشرطة في الجناح بوقوع تلك الجريمة^٢.

وفيما يخص البلاغ عن الجريمة فيقصد به إبلاغ السلطات المختصة من مأموري الضبط القضائي عن أن هناك شك أو خوف أو عزم أو اتفاق جنائي على ارتكاب جريمة، أو أن هناك

^١ عفيف كامل عفيفي، "جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية"، مكتبة الأهرام، القاهرة،

٢٠٠٠م، ص ٣٣٨.

^٢ فهد عبد الله العازمي، "الإجراءات الجنائية المعلوماتية"، رسالة دكتوراه، كلية القانون بجامعة عين شمس، كلية القانون، القاهرة، ٢٠١٢م، ص ١٧٠.

جريمة على وشك الوقوع أو وجود أدلة أو قرائن عن وقوع جريمة^١، أو أن هناك جريمة قد ارتكبت، أما الشكوى فهي البلاغ المقدم من المجني عليه أو المضرور من الجريمة للتعبير عن إرادته أمام السلطات المختصة^٢.

ويتم الإبلاغ بكافة الطرق التي توصل البيانات إلى الجهات المختصة، فيرد بصورة كتابية أو شفوية من قبل المجني عليه أو غيره مما شاهدوا الجريمة أو علموا بها وقد يقوم الجاني نفسه بالتبليغ عن جريمته فنكون هنا بصدد البلاغ المادي، أما إذا تم البلاغ بطريقة أخرى بواسطة البريد أو البرقية أو الاتصال أو النشر فهذا ما يصطلح عليه البلاغ المعنوي، أو قد يتم عن طريق الإنترنت وهو ما يطلق عليه البلاغ الرقمي^٣.

وينقسم البلاغ إلى بلاغ جوازي وبلاغ وجوبي، فالمقصود بالبلاغ الجوازي أن الأمر متروك للشخص للتبليغ عن الجريمة لا أحد يجبره على ذلك، أما الوجوبي فهو مفروض بقوة القانون على أشخاص معينين في حالة علمهم بوقوع الجريمة أن يقوم بإخبار السلطات المختصة حتى إن لم يكن متضرراً منها وله مصلحة من ورائها^٤.

^١ فهد عبد الله العازمي، "مرجع سابق"، ص ١٧٢.

^٢ جميل عبد الباقي الصغير، "الجوانب الإجرائية للجرائم المتعلقة بالإنترنت"، دار النهضة العربية، القاهرة، ٢٠٠١، ص ٦٥.

البلاغ يقدمه أي شخص علم بوقوع جريمة الاحتيال المعلوماتي، أما الشكوى فيقدمها الشخص المتضرر من جريمة الاحتيال المعلوماتي أي المجني عليه، ويختلف البلاغ عن الشكوى في عدة نقاط أهمها: أن الشكوى موجهة من المجني عليه أو وكيله ضد شخص معين ولا يشترط ذلك في البلاغ، كما ينقضي الحق في الشكوى بموت المجني عليه بالإضافة إلى توفر الأسباب التي تنقضي بها الدعوى الجنائية، أما البلاغ فلا ينقضي أبداً، وتقدم الشكوى في مدة زمنية معينة على عكس البلاغ الذي لا يكون له وقت محدد لتقديمه. أنظر محمد أحمد سلامة، "مرجع سابق"، ص ٤٨.

^٣ جميل عبد الباقي الصغير، "الجوانب الإجرائية للجرائم المتعلقة بالإنترنت"، دار النهضة العربية، القاهرة، ٢٠٠١، ص ٦٥.

البلاغ يقدمه أي شخص علم بوقوع جريمة الاحتيال المعلوماتي، أما الشكوى فيقدمها الشخص المتضرر من جريمة الاحتيال المعلوماتي أي المجني عليه، ويختلف البلاغ عن الشكوى في عدة نقاط أهمها: أن الشكوى موجهة من المجني عليه أو وكيله ضد شخص معين ولا يشترط ذلك في البلاغ، كما ينقضي الحق في الشكوى بموت المجني عليه بالإضافة إلى توفر الأسباب التي تنقضي بها الدعوى الجنائية، أما البلاغ فلا ينقضي أبداً، وتقدم الشكوى في مدة زمنية معينة على عكس البلاغ الذي لا وقت محدد لتقديمه. أنظر محمد أحمد سلامة، "مرجع سابق"، ص ٤٨.

^٤ هشام رستم، "مرجع سابق"، ص ١٦-١٧.

فيجب على مأمور الضبط القضائي إذا علم بوقوع الجريمة عن طريق الأخبار أو الشكوى أو أي طريق آخر أن يقوم بجمع المعلومات عن الجريمة ومرتكبيها، والحصول على جميع الإيضاحات المتعلقة بها، فقد يحصل على هذه المعلومات من مقدم الشكوى أو من الشهود أو من المشتبه به أو أي شخص لديه معلومات عن الجريمة، حيث يمكن إجراء بعض التحريات المبدئية لجمع أدلة الاتهام والتفتيش أو الضبط والتحقيق تساعد في الكشف عن الملابس والظروف المحيطة بالجريمة لتعقب الجناة والبحث عنهم لجمع الأدلة لإثبات ادانتهم^١.

الفرع الثاني: البلاغ والشكوى عن جريمة الاحتيال المعلوماتي

يصعب على الأشخاص العاديين الإبلاغ عن جريمة الاحتيال المعلوماتي نظراً لطبيعتها الخاصة التي لا تتوفر إلا في أشخاص على دراية كاملة بتقنية الحاسب الآلي وذلك لتحديد الفعل المشروع وغير المشروع^٢. أما بالنسبة لمستخدمي الإنترنت فيمكنهم الإبلاغ عن الأشخاص عن طريق الحاسب الآلي دون أن ينتقلوا إلى قسم الشرطة طالما أن رقم الكود (IP Adress) للحاسب الآلي الذي صدر عنه البلاغ موجود على شبكة الإنترنت^٣.

وعلى الهيئات المنوط بها متابعة التقارير والبلاغات والشكاوى المتعلقة بالجرائم المعلوماتية متابعة هذه البلاغات والشكاوى ودراستها والقيام بالتحري عنها بمجرد وصولها إلى الجهات المختصة سواء كانت محلية أو دولية، حيث يتم تسجيلها آلياً في قاعدة البيانات الخاصة للمراجعة الأولية من الناحيتين التقنية والقانونية، ويتم الإبلاغ عنها للأجهزة المختصة على المستوى المحلي والدولي، ويتم التصرف معها حسب التشريعات النافذة والتفاهات الدولية والإقليمية، وبعد التأكد من صحة ودقة الإجراءات في مرحلة تلقى البلاغات والتحقق من صحة المعلومات في مرحلة التقصي والاستدلال يتم تسجيل هذه الشكاوى وإعطائها رقم تسلسلي حتى يتسنى للمبلغ معرفة مستجدات التحقيقات، ومن عوامل نجاح سياسة القضاء على الجريمة المعلوماتية وفعالية مواجهتها هي حصر وتوثيق الشكاوى والبلاغات بشكل سليم، وذلك حتى

^١ مصطفى محمد موسى، "دليل التحري عبر شبكة الانترنت"، دار الكتب القانونية، القاهرة، ٢٠٠٥م، ص ٢٢.

^٢ راشد بشير راشد، "التحقيق الجنائي في جرائم تقنية المعلومات"، دراسة صادرة عن مركز الامارات للدراسات والبحوث الاستراتيجية، العدد ١٣١، ٢٠٠٨، ص ٤٨.

^٣ جميل صغير، "مرجع سابق"، ص ١٤.

يمكن المختصون من وضع الخطط والاستراتيجيات وتفعيل البرامج التي تهدف إلى مكافحة جريمة الاحتيال المعلوماتي بصفة خاصة والجريمة المعلوماتية بصفة عامة^١.

وتمر الإجراءات الخاصة بتلقي الشكاوى في جريمة الاحتيال المعلوماتي في مراحل مختلفة مروراً باستقبالها ودراستها والتحري حولها والتصرف فيها وفقاً للتشريعات النافذة وذلك للتأكد من صحتها لتبأشر الهيئات المختصة إجراءات التحري والتحقيق في هذه الجرائم، واعطائها الوصف القانوني وإعداد السجلات والاستمارات المنظمة لعملية تلقي البلاغات والشكاوى متضمنة البيانات الأساسية لكل جريمة والتي تشمل مرفقاتها أيضاً^٢.

ومما سبق يتبين بأن آلية تلقي البلاغات والشكاوى تمر بمراحل مختلفة وهي، مرحلة الاستقبال والتوثيق بمحضر التحري، ومرحلة جمع المعلومات والأدلة، ومرحلة إحالة البلاغات إلى الجهات المختصة بتطبيق القانون، ومرحلة المتابعة والتحقيق والمعاينة، وسماع الشهود، والخبرة.

كما يجب أن يتضمن البلاغ عدة عناصر وذلك لمساعدة رجال الضبط القضائي في تحديد معالم الجريمة الرقمية ووضع خطة للتعامل معها من الناحية الفنية والقانونية وهذه العناصر هي:

١- **تحديد مكان وقوع الجريمة:** على المبلغ أن يضمن بلاغه مكان وقوع الجريمة أي مكان وقوع الأفعال غير المشروعة، ووصفها ليتسنى لرجال الضبط القضائي الانتقال إليها وإجراء التحري عنها^٣.

٢- **تحديد نوع الجريمة:** لا يكفي للمبلغ أن يقوم بتحديد مكان وقوع الجريمة بل يجب أن يقوم بتحديد نوع الجريمة المرتكبة، ويحدد ما إذا كانت اعتداء على أموال أو تزوير^٤.

٣- **تحديد محل الجريمة:** يجب أن يقوم المبلغ بتحديد الحاسب الآلي التي وقعت عليه الجريمة، والموقع الذي استهدفه الاعتداء^٥.

^١ مصطفى موسى، "مرجع سابق"، ص ١٧٠.

^٢ فهد العازمي، "مرجع سابق"، ص ١٧٨.

^٣ انظر: خالد ممدوح إبراهيم، "فن التحقيق الجنائي في الجرائم المعلوماتية"، دار الفكر الجامعي، الإسكندرية، ط ١، ٢٠٠٩م، ص ١٥٧.

^٤ خالد ممدوح إبراهيم، "مرجع سابق"، ص ١٥٨.

^٥ فهد العازمي، "مرجع سابق"، ص ١٨٠.

ويرى الباحث أنه ليس بمقدور أي شخص الإبلاغ عن جريمة الاحتيال المعلوماتي ما لم تتوفر المعلومات الكاملة والمقدرة على استخدام الحاسب الآلي والتعامل مع تقنية المعلوماتية، وهذا بدوره ما يعتبر عائقاً أمام صعوبة ومكافحة جريمة الاحتيال المعلوماتي، فمعظم جرائم الاحتيال المعلوماتي تقيد ضد مجهول وذلك لصعوبة تحديد الجاني شخصياً في البلاغات، وبالرغم من إمكانية تحديد الحاسب الآلي التي وقعت من خلاله الجريمة من خلال البلاغات التي تصل إلى الجهات المختصة إلا أن ذلك لا يعني تحديد هوية الجاني، حيث قد ترتكب غالبية تلك الجرائم بمقاهي الانترنت.

فالمشرع البحريني في قانون جرائم تقنية المعلومات في المادة (٢٢) قد أقر بـسريان أحكام المرسوم بقانون رقم (٤٦) لسنة ٢٠٠٢ بإصدار قانون الإجراءات الجنائية وفق ما يتناسب مع جرائم تقنية المعلومات وبالقدر المناسب.

أما فيما يخص الجهة المختصة بتلقي البلاغات والشكاوى في البحرين فبموجب المرسوم الملكي رقم (١٠٩) للعام ٢٠١١ الصادر بشأن تعديل بعض أحكام المرسوم رقم (٦٩) للعام ٢٠٠٤م والقاضي بإعادة تنظيم وزارة الداخلية، أنه يتم إنشاء إدارة عامة لمكافحة الفساد والأمن الاقتصادي والإلكتروني والتي تندرج تحت مظلتها عدد من الإدارات الأمنية تهدف لحفظ دعائم الاقتصاد الوطني، ويدخل ضمن اختصاص هذه الإدارة متابعة البلاغات والشكاوى الخاصة بالجرائم الإلكترونية حيث يقدم البلاغ عبر موقع الإدارة الإلكتروني أو بواسطة الاتصال المباشر برقم الإدارة.

وفي دولة الإمارات العربية المتحدة يتم الإبلاغ عن الجرائم الإلكترونية بصفة عامة وذلك عبر الموقع الإلكتروني "لديوان المحاسبة" وهي خدمة إلكترونية تتيح الإبلاغ عبر الإنترنت، وهي متاحة لموظفي الحكومة الاتحادية وموردي الخدمات والسلع وتختص بالمسائل المتعلقة بالمؤسسات الاتحادية حصراً، وتتوفر الإرشادات الشاملة حول كيفية الإبلاغ عن الاحتيال، على الموقع الإلكتروني الخاص بالديوان، حيث يمكن للأفراد الإبلاغ عن حادثة الاحتيال عبر رسالة إلكترونية أو رسالة بريدية خطية^١.

ولم يرد نص واضح وصريح في القوانين المقارنة على الكيفية التي ترفع من خلالها الشكاوى في الجرائم المعلوماتي على وجه الخصوص، ولم تتضمن القوانين الخاصة بالجرائم الإلكترونية في دول المقارنة على كيفية التبليغ عن الشكاوى، فاقترنت آلية إجراء الشكاوى أو البلاغ حسب ما ورد في قانون الإجراءات الجنائية فيما يخص جمع الأدلة وإجراءات التبليغ أو الشكاوى عن هذه الجرائم.

^١ فهد العازمي، "مرجع سابق"، ص ١٩٣.

المطلب الثاني

معاينة جريمة الاحتيال المعلوماتي

أول خطوة في الكشف عن جرائم الاحتيال الإلكتروني على مستوى الضبطية القضائية هي مرحلة التحري، حيث يقصد بالتحري في مجال الضبط القضائي، البحث عن الجرائم المرتكبة والتحقق من صحة الوقائع المبلغة لضباط الشرطة القضائية، وجمع القرائن التي تفيد في حصول الواقعة أو نفي وقوعها^١.

لذلك فإن رجال الضبطية القضائية إذا أخطروا بجريمة من الجرائم، فإنهم يقومون بالإجراءات الأولية وهذه الإجراءات مرتبطة بالبحث والتحري والذي يعد كمرحلة تمهيدية للدعوى، هذه الإجراءات في حد ذاتها ضرورية، فكلما قرب الزمن بين الإجراء والجريمة كانت الأدلة واضحة أكثر وأسلم ولم يشبها أي تغيير أو تحريف ومن تم كانت أدعى للثقة^٢.

يقصد بإجراءات البحث والتحري في جريمة الاحتيال المعلوماتي "مجموعة الإجراءات التي يقوم بها المتحري عبر شبكة الإنترنت بواسطة التقنية الإلكترونية الرقمية وكذلك على أجهزة الحاسب الآلي، للحصول على بيانات ومعلومات تعريفية أو توضيحية عن الأشخاص أو الأماكن أو الأشياء حسب طبيعتها لضبط جرائم الكمبيوتر والإنترنت ولتحقيق الأمن الإلكتروني أو لأي غرض آخر"^٣.

إن خصوصية جريمة الاحتيال المعلوماتي، أبرزت مشكلة المكافحة الإجرائية للجريمة المعلوماتية خاصة من ناحية كيفية جمع الأدلة الإلكترونية ومدى حجيتها. وسيتم تقسيم المطلب إلى فرعين على النحو الآتي:-

الفرع الأول: ماهية المعاينة.

الفرع الثاني: الإجراءات الفنية والعملية للمعاينة.

^١ محمد ماجد ياقوت، "أصول التحقيق الإداري في المخالفات التأديبية"، دراسة مقارنة، منشأة المعارف، الإسكندرية، مصر، بدون سنة نشر، ص ٢٨٩.

^٢ محمد محدة، "ضمانات المتهم أثناء التحقيق"، الجزء الثالث، دار الهدى، عين مليلة، الجزائر، الطبعة الأولى، ١٩٩٢م، ص ١٠٥....

^٣ مصطفى موسى، "مرجع سابق"، ص ٢٢.

الفرع الأول: ماهية المعاينة

عند الحديث عن المكافحة الإجرائية للجريمة المعلوماتية، أول ما يجب دراسته هو معاينة مسرح الجريمة المعلوماتية: ويقصد بهذه الأخيرة رؤية العين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة^١، أو هي إثبات لحالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة وهي تتطلب أن ينتقل مأمور الضبط القضائي إلى مكان ما لمباشرتها لإثبات حالته وحالة ما قد يوجد فيه من أشخاص أو أشياء تفيد في إظهار الحقيقة للكشف عن الجريمة محل الإجراء^٢.

وهي إجراء جائز في كافة الجرائم، إلا أن غالبية التشريعات، تقصرها على الجنايات والجنح الهامة، بحيث تعد إجراءً وجوبياً في الجنايات وجوازياً في الجنح، وهي قد تتم في مكان عام أو مكان خاص، فإذا كانت في مكان عام؛ فمأمور الضبط القضائي لا يحتاج إلى إذن أو نذب سلطة تحقيق بإجرائها، أما إذا كانت بمكان خاص؛ فلا بد لصحتها، إما رضا حائز المكان أو وجود إذن مسبق من سلطة التحقيق بإجرائها^٣.

والهدف من إجراء المعاينة هو ضبط ما استعمل في ارتكاب الجريمة أو نتج عنها، ووضع الأختام في الأماكن التي أجريت فيها المعاينة، إذا وجدت آثار أو أشياء تفيد في الكشف عن الجريمة، كما يجوز لمأمور الضبط القضائي أن يعين حراساً على هذه الأماكن مع ضرورة إخطار النيابة العامة بهذه الإجراءات^٤.

وقد تكون المعاينة مرحلة من مراحل الاستدلال حيث يجب على مأمور الضبط القضائي الانتقال فوراً بدون تردد ولا تمهل إلى مكان ارتكاب الجريمة المعلوماتية لمعاينته ولعمل جميع التحريات اللازمة للمحافظة على الآثار والأدلة الالكترونية للجريمة التي يُخشى إخفاؤها، ولضبط ما يمكن أن يؤدي إلى إظهار الحقيقة، وإثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة، وأن يعرض الأشياء المضبوطة على الأشخاص المشتبه في مساهمتهم في الجريمة

^١ محمد زكي أبو عامر، "الإجراءات الجنائية"، دار الجامعة الجديدة، الطبعة الثامنة، ٢٠٠٨، ص ١٢٣.

^٢ نبيلة هروال، "الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات "دراسة مقارنة"، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م، ص ٢١٢.

^٣ عدنان زيدان، "الإجراءات الجنائية" في دولة الإمارات العربية المتحدة، الجزء الأول، مطبوعات كلية الشرطة، دبي، دون سنة نشر، ص ٢٧٣.

^٤ خالد ممدوح إبراهيم، "مرجع سابق"، ص ١٦١.

للتعرف عليها وكذا إخطار النيابة العامة فوراً بانتقاله، لكي تنتقل بدورها إلى محل الجريمة في حالة الجناية المتلبس بها^١.

وقد أشار المشرع البحريني إلى إجراء المعاينة في قانون الإجراءات الجنائية، وأشار إليها في قانون جرائم تقنية المعلومات على وجوب إجراء المعاينة وذلك بأمر من النيابة العامة^٢.

وأشار المشرع الإماراتي إلى إجراء المعاينة في قانون الإجراءات الجزائية^٣ للأماكن والأشخاص وكل ما يتعلق بالجريمة وكل ما يلزم في إثباتها، بالإضافة إلى ذلك فقد حدد من خلال نص المادة ذاتها أنه إذا لزم الأمر معاينة مكان أو أشخاص خارج دائرة اختصاص عضو النيابة أن يطلب تنفيذ هذا الإجراء من عضو النيابة المختص.

ولم يرد نص واضح وصريح من قبل المشرع السعودي على إجراء المعاينة فيما يخص نظام مكافحة الجرائم المعلوماتية واكتفى بالإشارة إلى إجراء المعاينة في نظام الإجراءات الجزائية السعودي^٤.

ومن خلال ما سبق يتضح بأن ثمة قصور من قبل المشرع في دول المقارنة، حيث لم يتطرق المشرع إلى إجراء المعاينة الخاصة بالجرائم المعلوماتية، واكتفى بالإشارة إلى المعاينة التقليدية التي أوردها في قانون الإجراءات الجزائية، وهذا ما يؤخذ عليه.

ويرى الباحث أن على المشرع أن يقوم بإضافة نصوص خاصة في القوانين المعنية بمكافحة الجريمة المعلوماتية يقوم من خلالها بالإشارة لوجوب إجراء المعاينة بشكل واضح وصريح يتضمن من خلالها الكيفية التي تتم فيها المعاينة وأن يحدد النيابة المختصة التي تقوم بإجراء المعاينة نظراً للطبيعة الخاصة لهذه الجرائم التي تتطلب المعرفة والإلمام وتوفر الخبرة الكاملة بالجهة المختصة بإجراء المعاينة.

^١ هلال البوسعيد، "الحماية القانونية والفنية لقواعد المعلومات المحوسبة"، دراسة قانونية وفنية مقارنة، دار النهضة العربية، ٢٠٠٩، ص ٢٤٥.

^٢ أنظر نص المادة (٥٠) من قانون الإجراءات الجنائية البحريني والمادة (٥٢) بشأن الجرائم المتلبس بها، قانون رقم (٤٦) لسنة ٢٠٠٢.

^٣ أنظر نص المادة (١٢) من قانون جرائم تقنية المعلومات البحريني.

^٤ أنظر نص المادة (٣٥) من قانون رقم (٣٥) لسنة ١٩٩٢م بشأن إصدار قانون الإجراءات الجزائية الإماراتي.

^٤ أنظر نص المادة (٢٧) من نظام الإجراءات الجزائية السعودي الصادر لعام (١٤٣٥).

الفرع الثاني: الإجراءات الفنية والعملية للمعاينة

في الجرائم التقليدية يوجد مسرح جريمة فعلي يحتوي على الآثار المادية للجريمة مما يتيح عملية التحفظ لهذه الآثار لمعاينتها تمهيداً لفحصها وبيان صحتها في الاثبات، أما في الجرائم المعلوماتية يختلف الحال، حيث من النادر أن يتخلف عن الجريمة آثار مادية فعلية، فقد تطول الفترة الزمنية بين وقوع الجريمة واكتشافها، مما قد يعرض الآثار الناتجة عن الجريمة للتلف أو المحو أو العبث بها، أو إمكانية التلاعب في البيانات عن بعد، أو محوها عن طريق التدخل من خلال وحدة طرفية من قبل الجاني^١.

ولمعاينة مسرح جريمة الاحتيال المعلوماتي، يجب التفريق بين حالتين:

أ - معاينة الجرائم الواقعة على المكونات المادية للحاسوب (Hardware) كشاشة العرض ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسوب ذات الطابع المادي المحسوس، فهي لا تثير أية مشكلة بحيث يمكن لمأمور الضبط القضائي معاينتها والتحفظ على الأشياء التي تعد أدلة مادية للكشف عن الجريمة^٢.

ب - معاينة الجرائم الواقعة على المكونات غير المادية أو بواسطتها (Software) كتلك الواقعة على برامج الحاسوب وبياناته، هذه المكونات تثير صعوبات عديدة تحول دون فاعلية المعاينة أو فائدته، وهذه الصعوبات، تتلخص فيما يلي:

١- قلة الآثار المادية المترتبة عن الجرائم التي تقع على المكونات غير المادية للحاسوب^٣.

٢- الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية التي غالباً ما تكون طويلة، وذلك بين اقتراف الجريمة والكشف عنها، الأمر الذي يمنح

^١ جميل الصغير، "مرجع سابق"، ص ٢٩.

^٢ عبد الفتاح بيومي حجازي، "الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت"، دار الكتب القانونية، ٢٠٠٤، ص ٥٩.

^٣ جميل الصغير، "مرجع سابق"، ص ٢٩.

فرصة لإحداث تغييرات أو العبث بالآثار المادية أو زوال بعضها، مما يؤدي إلى غموض الدليل المستقى من المعاينة^١.

كما يجب أن تقتصر مباشرة عملية المعاينة على مأموري الضبط وفئة الخبراء، ممن تتوافر فيهم الكفاءة العلمية والخبرة الفنية في مجال الحاسوب واسترجاع المعلومات، وممن تلقوا التدريب الكافي لمواجهة هذه النوعية من الجرائم، والتعامل مع أدلتها وما تخلفه من آثار على مسرح الجريمة، ففي فرنسا مثلاً، يقوم فريق مكون من ١٣ شرطي بالإشراف على تنفيذ المهمات التي يعهد بها إلى وكلاء النيابة والمحققين، وهم قد تلقوا تدريب متخصص إلى جانب اختصاصهم الأساسي في مجال التكنولوجيا الحديثة، وهم يقومون بمرافقة المحققين أثناء التفتيش، حيث يقومون بفحص كل جهاز وينقلون نسخة من الاسطوانة الصلبة وبيانات البريد الإلكتروني ثم يقومون بتحرير تقرير يرسل إلى القاضي الذي يتولى التحقيق^٢.

أما عن المعدات والبرامج، فهم يستخدمون برامج تستطيع استعادة المعلومات من على الأسطوانة الصلبة كما يمكنها قراءة الاسطوانات المرنة والصلبة التالفة، كما يوجد تحت تصرفهم برامج تمكنهم من قراءة الحاسبات المحمولة ومن المهم هنا أن يتم توثيق مسرح الجريمة ووصفه بكامل محتوياته بشكل جيد، مع توثيق كل دليل على حدة بما فيها الأدلة الرقمية، بحيث يتم توضيح مكان الضبط والهيئة التي كان عليها، ومن قام برفعه وتحريزه وكيف ومتى تم ذلك^٣.

وبالنسبة إلى مدى جواز إجراء المعاينة في الجرائم المعلوماتية، فيجوز للمحقق اللجوء لإجراء المعاينة متى رأى ضرورة لذلك^٤. والأصل في المعاينة في الدعوى حضور أطراف الدعوى، كما قد يقرر المحقق إجرائها دون حضور الأطراف، كما لا يلتزم المحقق بدعوة محامي المتهم للحضور، وأيضاً غياب المتهم عن إجراء المعاينة لا يؤدي إلى بطلانها، فالمعاينة كما ذكرنا سابقاً جوازية متروكة لتقدير المحقق سواء طلبها الخصوم أم لم يطلبوها^٥.

^١ هشام رستم، "مرجع سابق"، ص ٥٩.

^٢ نورة طرشي، "مكافحة الجريمة المعلوماتية"، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر ١، ٢٠١١-٢٠١٢، ص ١٣١.

^٣ هشام رستم، "مرجع سابق"، ص ٥٨.

^٤ نبيلة هروال، "مرجع سابق"، ص ٢١٨.

^٥ جميل عبد الباقي الصغير، "مرجع سابق"، ص ٢٦.

خلاصة لما سبق يتضح بأن المعاينة التقنية تساهم في الاستدلال على شهود الجريمة المعلوماتية والكيفية التي ارتكبت من خلالها، فهي وسيلة أساسية لتثبيت الحقائق اللازمة في التحقيق، كالتعرف على وقت ارتكابها والمكان التي ارتكبت به.

ويرى الباحث بأنه وبالرغم من خصوصية جريمة الاحتيال المعلوماتي وصعوبة تنفيذ المعاينة بها، إلا أنه قد تكون المعاينة حكمية، بحيث يمكن الولوج إلى الجهاز محل الجريمة دون الانتقال الفعلي لمعاينة ذلك الجهاز، وذلك من خلال الدخول إلى إليه، ومعاينته وتفتيشه من خلال البرامج المخصصة لذلك، وهو ما يؤدي إلى سرعة تنفيذ المعاينة دون الحاجة إلى الانتقال الفعلي للمعاينة.

المطلب الثالث

إجراءات التفتيش والضبط في جريمة الاحتيال المعلوماتي

إن الهدف من التفتيش هو حفظ الوسائط الالكترونية التي سجلت عليها البيانات لجمعها وتخزينها كالأقراص الممغنطة والاسطوانات، ومخرجات الحاسب الآلي المتعلقة بالجريمة، كما يفيد التفتيش في كشف الحقيقة ويكون محل التفتيش في الجرائم المعلوماتية البيانات المعالجة آلياً^١.

فكل ما يضبطه مأمور الضبط القضائي بعد عملية التفتيش من أشياء متعلقة بالجريمة هو الأثر المباشر للتفتيش، فالضبط إذن يعد أيضاً إجراء من إجراءات التحقيق في جريمة الاحتيال المعلوماتي؛ بوضع اليد على الشيء وحبسه والمحافظة عليه، للحصول على دليل لمصلحة التحقيق عن طريق إثبات واقعة معينة. وهو ما ستوضحه الدراسة في هذا الجزء منها وعليه سيقسم المطلب إلى ثلاث فروع وهي كالآتي:

الفرع الأول: تفتيش نظم المعلومات.

الفرع الثاني: تفتيش نظم الحاسوب المنطقية أو المعنوية.

الفرع الثالث: الضبط في جريمة الاحتيال المعلوماتي.

الفرع الرابع: التنصت والمراقبة الالكترونية.

الفرع الأول: تفتيش نظم المعلومات

عملية تفتيش نظم المعلومات تنصب على المكونات المادية بأوعيتها المختلفة، للبحث في أي شيء يتصل بجريمة معلوماتية ما للكشف عنها، يدخل في نطاق التفتيش التقليدي وفقاً للإجراءات القانونية المعمول بها، إلا أن هناك حالات خاصة للتفتيش في هذه المكونات، هي:

^١ فهد العازمي، "مرجع سابق"، ص ٢٧٥.

١ - الحالة الأولى: في حالة ما إذا كانت هذه المكونات موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته، فإنها تأخذ نفس الأحكام المقررة لتفتيش المسكن وبنفس الضمانات المقررة قانوناً في مختلف التشريعات^١.

وقد أشار المشرع البحريني في القانون رقم (٦٠) الخاص بجرائم تقنية المعلومات إجراء التفتيش الخاص بنظام تقنية المعلومات وأشترط بإذن التفتيش أن يكون مسبباً وصادراً من النيابة العامة، حيث أشار إلى تفتيش أنظمة البيانات المخزنة على وسيلة تقنية المعلومات، وفي الفقرة الثانية أمر بتفتيش الوسائط الخاصة بتخزين بيانات تقنية المعلومات^٢.

وقد أثير أمر التفتيش في الطعن رقم ١٩٧ لسنة ٢٠١٤ مملكة البحرين الذي ينعي الطاعن على الحكم المطعون فيه إذ دانه بجريمتي استعمال توقيع إلكتروني لغرض احتيالي، يعزي الطاعن وينفي جريمة الاحتيال وأن الحكم قد شابه قصور في التسبيب وأخطأ في تطبيق القانون وانطوى على خطأ في تطبيق القانون ذلك أنه دفع ببطلان القبض عليه لحصوله من غير مختص ودون إذن من النيابة العامة وبطلان أقواله بمحضر جمع الاستدلالات لصدورها عنه من غير حضور مترجم لكونه هندي الجنسية ولا يتحدث العربية، ولكن المحكمة اعتبرت تلك الأسباب غير سائغة، لكون الأدلة المقدمة يكفي للفصل في القضية، كما أن المحكمة في هذه المرحلة غير ملزمة بنذب خبير في الدعوى متى رأت من الأدلة المقدمة فيها ما يكفي للفصل فيها دون حاجة لذلك، وكان طلب الطاعن بنذب خبير لفحص المستندات الدالة على الواقعة لا يتجه إلى نفي الفعل المكون للجريمة ولا إلى استحالة حصول الواقعة بالصورة الواردة بالأوراق فإنه يعد دفاعاً موضوعاً لا تلتزم المحكمة بإجابته أو الرد عليه إذا الرد مستفاد من الحكم بالإدانة استناداً إلى أدلة الإثبات التي أوردها الحكم، لذلك اعتبر الطعن على غير أساس وتم رفضه موضوعياً^٣.

^١ محمد طارق الخن، "مرجع سابق"، ص ١٧٦.

^٢ نص المادة (١٥) الفقرة الأولى من القانون رقم (٦٠) الخاص بجرائم تقنية المعلومات البحريني على: للنيابة العامة أن تصدر أمراً مسبباً بالدخول على ما يلي وتفتيشه:

أ- نظام تقنية المعلومات المتصل بالجريمة أو أي جزء منه أو أية بيانات لوسيلة تقنية المعلومات مخزنة فيه.

ب- أي من وسائط تخزين بيانات وسيلة تقنية المعلومات التي من المحتمل ان يكون مخزناً عليها بيانات متصلة بالجريمة.

^٣ الطعن رقم ١٩٧ لسنة ٢٠١٤، جلسة ١٧ نوفمبر ٢٠١٤، منشور على الموقع الإلكتروني التالي:

<http://elb-iis-web-303033976.eu-west-1.elb.amazonaws.com/Taan/>

أما المشرع الإماراتي، فلم يورد نص واضح وصريح إلى آلية التفتيش في جرائم تقنية المعلومات واكتفى بإعمال النصوص المتعلقة بإجراء التفتيش الواردة في قانون الإجراءات الجزائية.

وكذلك المشرع السعودي ، لم يورد نص يوضح من خلاله الكيفية التي يتم من خلالها تفتيش نظام البيانات الخاص بتقنية المعلومات ولا حتى الوسائط التي قد يخزن عليها بيانات خاصة بالجرائم المتعلقة بالتقنية المعلوماتية، وهذا ما يؤخذ على المشرع السعودي، إذ اقتصر بالإشارة إلى إجراء التفتيش حسب ما ورد في نظام الإجراءات الجزائية ولم يراعي خصوصية جرائم تقنية المعلومات.

مما سبق يتضح أن المشرع البحريني قد وفق في تضمينه نصوص خاصة يبين من خلالها الآلية التي يتم من خلالها إجراء التفتيش على نظم المعلومات الخاصة بوسائل تقنية المعلومات والتي يخزن عليها البيانات حتى على الوسائط التي من الممكن أن تحتوي على بيانات خاصة بالجريمة المعلوماتية.

٢- الحالة الثانية: إذا كانت مكونات الحاسوب المادية منعزلة عن غيرها من أجهزة الكمبيوتر أو أنها متصلة بجهاز أو نهاية طرفية في مكان آخر كمسكن غير مسكن المتهم، بحيث إذا كانت هناك بيانات مخزنة في أوعية هذا النظام الآخر، فإن عملية الكشف تصبح صعبة جداً، وربما مستحيلة، لذلك حتى تتم عملية تفتيش هذه الأجهزة المرتبطة بأجهزة في أماكن أخرى، يتعين مراعاة القيود والضمانات التي يوجبها المشرع لتفتيش هذه الأماكن^١.

وقد أشار المشرع البحريني إلى إجراء التفتيش في هذه الحالة وبالكيفية التي يحددها القانون وفق ما جاء بالقانون رقم (٦٠) الخاص بجرائم تقنية المعلومات^٢. ولم يتطرق كل من المشرع الإماراتي والسعودي إلى هذه الحالة في إجراء التفتيش، وهذا ما يؤخذ عليهم، حيث من الممكن وبحسب طبيعة جرائم تقنية المعلومات أن تمتد آثار الجريمة إلى أنظمة معلوماتية أخرى فلا تقتصر الآثار على وسيلة تقنية المعلومات التي ارتكبت بواسطتها الجريمة أو عليها.

ويرى الباحث بأن المشرع البحريني قد أصاب الحقيقة في إقراره ضمن إطار قانون جرائم تقنية المعلومات هذه الحالة والتي تعتبر في رأي الفقه مسألة مختلف عليها كون الأنظمة الأخرى قد تقع خارج حدود الدولة وسيادتها وهذا ما يعتبر تعدي على سيادة الدولة، أو قد تقع في مكان

^١ نورة طرشي، "مرجع سابق"، ص ١١٥.

^٢ أنظر نص المادة (١٥) في فقرتها الثانية، من القانون رقم (٦٠) الخاص بجرائم تقنية المعلومات البحريني.

آخر من الدولة، مما يتطلب إصدار إذن بالتفتيش لهذه الأماكن، ولكن حرصاً على سرعة التحفظ على البيانات وضمان عدم التلاعب فيها أو اتلافها وجب على الجهات المختصة التحفظ على هذه البيانات بأسرع وقت ممكن فهنا قد وفق المشرع في هذا الإجراء وإن كان في بعض الحالات قد يتم انتهاك الخصوصية الشخصية ولكن يبرر ذلك الحرص على تحقيق الصالح العام.

وهذا ما حصل فعلاً في قضية تركيب أجهزة على الصراف الآلي لإستعمالها في الإستيلاء على مال الغير، فبعد العثور على المتهمين في منطقة مدينة عيسى عند الصراف الآلي الخاص ببنك الأهلي المتحد، وقد تم تفتيش المتهم الأول وعثر معه على كاميرات بعلبة بلاستيكية في جرابه الأيمن تم طلائها باللون الأزرق وهو لون البنك الأخير وبفتيش السيارة عثر على كاميرات رقمية وبطاقات وأسلاك، وبفتيش غرفة المتهمين بالفندق عثر على أسلاك وشاحن كهربائي وجهاز عبارة عن قطعة سوداء خاصة بالصراف الآلي، يتم من خلاله قراءة المعلومات الخاصة بعملاء البنك بعد توصيلها إلكترونياً^١.

خلاصة القول: لتفتيش الحاسب الآلي الذي له نهاية طرفية في دولة أجنبية، نصت بعض التشريعات على طريقة ثانية كإجراء للتحقيق في جريمة الاحتيال المعلوماتي وهذه الطريقة هي: التصنت والمراقبة الإلكترونية لشبكات الحاسوب ويقصد بهذه الطريقة -التصنت -مراقبة المحادثات التلفونية وتسجيلها بالنسبة للأحاديث الخاصة بشخص أو أكثر مشتبه فيه، ويعتقد بفائدة محادثته في الكشف عن الجريمة، وذلك عن طريق إخضاعها لنوع من الرقابة بقصد التعرف على مضمونها.

٣- الحالة الثالثة: إذا وجدت مكونات الحاسوب المادية (في حالة الحاسوب الآلي المحمول) في الأماكن العامة بطبيعتها كالمطاعم والسيارات العامة كسيارات الأجرة... الخ، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها في هذه الحالات، وقد اتفقت بعض التشريعات، كالتشريع الجنائي الكندي في المادة (٤٨٧) التي أجازت إصدار أمر قضائي لتفتيش وضبط أي شيء يؤدي للاعتقاد بأن الجريمة قد وقعت أو يشتبه في وقوعها، ونصت صراحة على إمكانية تفتيش مكونات الحاسوب المادية للكشف عن الجريمة المعلوماتية باتخاذ أي إجراء أو القيام بأي فعل لازم لجمع الأدلة والحفاظ عليها.

^١ الطعن رقم ٩٦ جنائي لسنة ٢٠٠٧، جلسة ٢٨ من إبريل لسنة ٢٠٠٨، منشور على الموقع التالي:

<http://elb-iis-web-303033976.eu-west-1.elb.amazonaws.com/Taan/>

الفرع الثاني: تفتيش نظم الحاسوب المنطقية أو المعنوية

يعرف الكيان المنطقي للحاسوب بأنه: "مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات"^١. وهو يشمل على جميع العناصر غير المادية اللازمة لتشغيل الكيان المادي كالبرامج ونظم التشغيل وقواعد البيانات ... الخ.

لقد ثار الخلاف في التشريع المقارن في مسألة ضبط وتفتيش المكونات المعنوية أو المنطقية للحاسوب، وتعددت الآراء في هذا الشأن؛ فذهب رأي إلى أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تقيد في الكشف عن الحقيقة، فإن هذا المفهوم يجب أن يمتد ليشمل البيانات الالكترونية، كالقانون الإجرائي اليوناني في نص المادة (٢٥١) التي تعطي لسلطات التحقيق إمكانية القيام بأي شيء يكون ضرورياً لجمع وحماية الدليل، تفسيراً لعبارة أي شيء بأنها تشمل ضبط البيانات المخزنة أو المعالجة آلياً أو إلكترونياً، بما فيها ضبط البيانات المخزنة في حاملات البيانات المادية، أو في الذاكرة الداخلية وذلك بإعطاء المحقق أمراً للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل للمحاكمة الجنائية، على أساس إنها كيانات يمكن قياسها بما إنها نبضات أو ذبذبات الكترونية قابلة لأن تسجل وتخزن على وسائط معينة يمكن قياسها^٢.

هناك بعض الحالات الخاصة يفرض التساؤل عن كيفية التعامل معها قانونياً في إجراءات ضبط المعلوماتية، والتي سنرى كيف تصدت لها القوانين المقارنة، بالحل كالتالي:

أولاً: مدى جواز الاطلاع على المحتويات المعلوماتية

يطرح في مجال التفتيش والضبط المعلوماتي في الجريمة المعلوماتية إشكال جواز أو عدم جواز اطلاع مأمور الضبط القضائي على المحتويات المعلوماتية، فجرى العمل في ألمانيا على أن سلطة الاطلاع على مطبوعات الحاسوب وحاملات البيانات تقتصر على المدعى العام فقط، ولا يكون لضباط الشرطة الحق في قراءة البيانات عن طريق تشغيل البرامج أو الوصول إلى البيانات المخزنة دون إذن من الشخص الذي له الحق في نقل هذه البيانات، لكن كل ما

^١ عفيفي كامل عفيفي، "جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون"، مرجع سابق، ص ٢٣٢.

^٢ أحمد عبد الله هلال، "تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتية"، دار النهضة العربية القاهرة، ٢٠٠٠، ص ٥٢.

يمكنهم هو مجرد فحص حاملات البيانات دون استخدام أي مساعدات فنية تطبيقاً لما جاء في القسم (١١٠) من قانون الإجراءات الألماني^١.

وقد أشار المشرع البحريني في نص المادة (١٨/٢) من القانون الخاص بجرائم تقنية المعلومات على ذلك، حيث جرم كل من يتم تكليفه بتسجيل البيانات أو أي إجراء متعلق باتصالات يتم إرسالها بواسطة نظام تقنية المعلومات بالكشف لأي شخص آخر عن هذه المعلومات ذات صلة بالجريمة أو الانتفاع بها بأي طريقة دون مسوغ في القانون، وذلك حرصاً على سرية المعلومات الشخصية للأفراد وللشخصيات المعنوية وضمان سرية التحقيقات وحفاظاً على هذه المعلومات^٢.

أما المشرع الإماراتي فقد أشار إلى السلطة المختصة في إثبات جرائم تقنية المعلومات وهي مأموري الضبط القضائي والذين يتم تعيينهم بقرار من وزير العدل، وذلك بموجب نص المادة (٤٩) من القانون الخاص بمكافحة جرائم تقنية المعلومات، ولم يتضمن القانون أي نصوص يفهم خلالها عدم التصرف بمخرجات التفتيش من بيانات لأي جهة كانت أو أشخاص دون مسوغ قانوني، وهذا ما يعتبر قصور من قبل المشرع الإماراتي، إذا يستوجب عليه أن يورد نصوص أكثر تفصيلاً وتوضيحاً وذلك تماشياً مع طبيعة الجريمة المعلوماتية وما يشوبها من إشكالات في مرحلة التحقيق.

وقد اكتفى المشرع السعودي إلى بيان الجهات المختصة بالتحقيق والادعاء بالجرائم المعلوماتية دون أن يتطرق المشرع إلى هذا الإجراء بنص صريح وفق ما جاء في نظام مكافحة جرائم تقنية المعلومات، كما أنه لم يشر إلى خصوصية حفظ المعلومات المستخرجة من البيئية الرقمية لكيانات وسائل تقنية المعلومات وهذا ما يعتبر قصور من قبل المشرع السعودي حيث يجب أن تكون هناك نصوص واضحة يحدد من خلالها ضرورة عدم التصرف فيما يتم التحفظ عليه من بيانات إلى بمسوغ قانوني.

ثانياً: حق المتهم في الصمت

يقصد بالحق في الصمت أن للشخص المتهم في جريمة ما مطلق الحرية في الكلام أو عدمه أو عدم الإجابة على الأسئلة الموجهة إليه من قبل مأمور الضبط القضائي القائم بالتحقيق

^١ نورة طرشي، "مرجع سابق"، ص ١٢٠.

^٢ نصت المادة (١٥) على "يحظر على من تم تكليفه وفقاً لأحكام الفقرة (١) من هذه المادة الكشف دون مسوغ في القانون لأي شخص آخر عن هذا التكليف أو بأية معلومات ذات صلة به أو الانتفاع بها بأية طريقة.

معه، لأنه غير ملزم بالكلام كما يجب أن يراعى أن رفضه الإجابة وصمته لا يجوز أن يؤخذان كقرينة ضده^١.

وذلك تطبيقاً للقاعدة الإجرائية العامة التي مفادها: "عدم إجبار الشخص على الكلام أمام أي جهة أو سلطة كحق من حقوق الإنسان"، والتي أوصى بها كل من المؤتمر الدولي السادس لقانون العقوبات المنعقد في روما سنة ١٩٥٣، والمؤتمر الدولي الذي نظمتها اللجنة الدولية لرجال القانون في أثينا في جوان لعام ١٩٥٥، كما حرصت معظم التشريعات الجنائية على النص صراحة على هذا الحق كالقانون الفرنسي في المادة (١١٤) قانون إجراءات جزائية لعام ١٩٩٤م والتي التي تلزم قاضي التحقيق أن ينبه المتهم عند حضوره أمامه لأول مرة إلى أنه حر في عدم الإدلاء بأي إقرار، وبثبت ذلك التنبيه في محضر التحقيق.

أما بالنسبة للشاهد المعلوماتي، نعلم أن الشهادة هي إثبات واقعة معينة من خلال ما يقوله أحد الأشخاص عما شهده أو سمعه أو أدركه بحواسه عن هذه الواقعة، كما يقصد بسماع الشهود السماح لغير أطراف الدعوى الجنائية بالإدلاء بما لديهم من معلومات أمام سلطات التحقيق، والشاهد المعلوماتي قد يكون شاهداً عادياً أو خبيراً في الدعوى القائمة، بالنسبة للشاهد العادي فهو ذلك الشخص الذي يقدم إلى القاضي معلومات حصل عليها بالملاحظة الحسية، أما الخبير فهو ذلك الشخص المختص الذي يقدم إلى القاضي تقارير وآراء توصل إليها بتطبيق قوانين علمية وأصول فنية.

وقد أكد المشرع البحريني على إلزام الشاهد على الجريمة بتقديم ما لديه من معلومات تفيد في كشف الحقيقة وبيان ملابساتها وفق ما جاء في قانون الإجراءات الجنائية^٢، قد ذهب كل من المشرع الإماراتي والسعودي إلى ما ذهب إليه المشرع البحريني بخصوص شهادة الشهود في الجرائم بصفة عامة وجريمة الاحتيال المعلوماتي على وجه الخصوص^٣.

ثالثاً: مدى جواز إجبار المتهم والشاهد المعلوماتي على الإدلاء ببيانات.

بالنسبة للمتهم المعلوماتي جرى العمل في الفقه والقانون في فرنسا حسب نص المادة (٢٧) من قانون الإجراءات الجزائية الفرنسي التي نصت على أنه: "من غير الممكن إجراء

^١ سامي صادق الملا، "اعتراف المتهم"، دار الفكر العربي، ط١، ١٩٩٨، ص ١٨٧ وما بعدها

^٢ أنظر المواد (٨٨-٩٥) من قانون الإجراءات الجنائية البحريني.

^٣ المواد (١١٤-١٢٥) من قانون الإجراءات الجزائية الإماراتي رقم (٣٥) لسنة ١٩٩٢، والمواد (٩٥-١٠٠) من نظام الإجراءات الجزائية السعودي الصادر لعام (١٤٣٥).

تفتيش المساكن وضبط الأشياء التي يمكن أن تكون متعلقة بالجريمة إلا بموافقة صريحة للشخص المراد تفتيش منزله أو أشياءه"، كما بينت الفقرة الثانية من نفس المادة، "بأن الموافقة يجب أن تكون صريحة لا ضمنية، وفي حالة رفض الموافقة الصريحة فإن ذلك يعني رفض ذوي الشأن"، ولذلك تعد الإجراءات باطلة وعلى هذا لا يجوز قانوناً إجبار المتهم على طباعة ملفات بيانات مخزنة داخل نظام المعالجة الآلية للمعلومات أو إلزامه بالكشف عن الشفرات أو كلمات السر خاصة بالدخول إلى هذه المعلومات أو إجباره على تقديم الأمر اللازم لوقف فيروس، تطبيقاً لمبدأ عدم جواز إلزام الشخص بتقديم دليل ضد نفسه سواء عن طريق الشهادة أو غيرها من عناصر الإثبات، إلا أن ذلك لا يمنع من إجباره على تسليم الشفرة الخاصة بالحاسوب الآلي المخزنة فيه البيانات محل الجريمة^١.

والشاهد المعلوماتي بنوعيه المذكورين سابقاً يلتزم بالكشف عن الشفرات أو كلمات السر التي يكون على علم بها، كما أنه يلتزم في بعض الدول الأوروبية بإجراء ما يسمى بإنعاش الذاكرة، بفحص الأماكن والمستندات التي توجد تحت سيطرته وذلك في كل من السويد وفنلندا والنرويج، أما في إنجلترا فالقانون الانجليزي الصادر عام ١٩٨٤ يعطي المحققين الحق في إلزام الغير بتمكين سلطات التحقيق الدخول إلى المعلومات المخزنة في الحاسوب الآلي أو الاطلاع عليها أو قراءتها، كما تسمح بعض التشريعات المقارنة في مجال التحقيق المعلوماتي الاستفادة من الشهود كخبراء أو كمساعدين للقضاء من تلقاء أنفسهم ودون حاجة لاستدعائهم^٢.

رابعاً: شروط التفتيش في جريمة الاحتيال المعلوماتي.

يشترط لإجراء التفتيش أن تتوفر فيه شروطاً معينة، وتنقسم هذه الشروط إلى شروط موضوعية وشروط شكلية، وهي كالتالي:-

الشروط الموضوعية للتفتيش في جريمة الاحتيال المعلوماتي.

ترتبط الشروط الموضوعية للتفتيش بسببه، فعدم توافر سبب التفتيش يؤدي إلى بطلانه بطلاناً مطلقاً، فالغاية من التفتيش هو ضبط الأشياء التي تفيد في الوصول إلى الحقيقة، فإذا التفتيش لا يعد وسيلة من وسائل التحري عن الجريمة، أي أن التفتيش ليس غاية بحد ذاته وإنما

^١ جميل عبد الباقي الصغير، "مرجع سابق"، ص ١٠٦.

^٢ محمد زكي أبو عامر، "مرجع سابق"، ص ٦٨.

هو وسيلة تتمثل فيما يمكن الوصول من خلاله إلى أدلة مادية تساهم في بيان وظهور الحقيقة، وبناء عليه فإن التفتيش الباطل ينتج آثاراً باطلة مما يترتب عليه بطلان الأدلة الناتجة عنه^١.

وعليه يمكن تناول الشروط الموضوعية كالتالي:

أ- السبب.

في كافة الجرائم يكون سبب التفتيش هو الكشف عن حقيقة تلك الجرائم والبحث في الأدلة للوصول إلى تحديد ما إذا كانت هذه الجريمة جنائية أو جنحة، بالإضافة إلى التعرف على كافة مفاصل الجريمة سواء تعلق ذلك بما تخلفه من آثار وأدلة وقرائن تساعد في الوصول إلى الحقيقة، وجريمة الاحتيال المعلوماتي يكون سبب التفتيش فيها الكشف عن الجناة الحقيقيين والمشاركين في هذه الجريمة، وذلك عن طريق توفر قرائن وأمارات تؤدي في النهاية للكشف عن الحقيقة، والتفتيش في جريمة الاحتيال المعلوماتي ينعقد بعد وقوع الجريمة فلا يجوز التفتيش لمجرد ورود معلومات تبين أو تشير إلى إمكانية وقوع الجريمة في المستقبل^٢.

ب- محل التفتيش.

المقصود بمحل التفتيش ذلك المكان الذي يحتفظ فيه الشخص للأشياء المادية التي تتضمن أسرارها، أما ما يحميه القانون من أسرار فهي تلك التي أدرجت محلها بحرمة، وفي جريمة الاحتيال المعلوماتي على الجهات المختصة حين استصدارها لإذن التفتيش أن تحدد محل التفتيش، والغرض منه، والتأكد من جواز تفتيش المحل، وإلا كان التفتيش باطلاً. ويكون الهدف من تفتيش المحل هو الحصول على الأدلة، فقد يكون محل التفتيش شخصاً أو مكاناً^٣.

وإذا كان محل التفتيش شخصاً فقد يكون من مستخدمي الحاسب الآلي أو من خبراءه، أو قد يكون من المحللين أو مهندسي الصيانة، أو من مديري أنظمة المعلومات، وهذا ما نصت عليه المادة (٦٦) من قانون الإجراءات الجنائية البحريني، والمادة (٥١) من قانون الإجراءات الجزائية الإماراتي^٤، والمادة (٤٢) من نظام الإجراءات الجزائية السعودي^٥.

^١ مصطفى موسى، "مرجع سابق"، ص ١٩٩.

^٢ عبد الله الكيتوب، "مرجع سابق"، ص ١٣٤.

^٣ عبد الفتاح حجازي، "مرجع سابق"، ص ٣٨٨.

^٤ قرار رقم (٣٥) لعام ١٩٩٢م، بشأن قانون الإجراءات الجزائية الإماراتي.

^٥ قرار رقم (١٢) الصادر في (١/٢٢/١٤٣٥هـ) بشأن نظام الإجراءات الجزائية السعودي.

وفي أثناء التفتيش إذا توافرت لدى أفراد الضبط القضائي قرائن قوية ضد شخص معين موجود في مكان التفتيش تفيد في كشف الحقيقة جاز لأفراد الضبط تفتيشه وهذا ما أكدته المادة (٦٨) من قانون الإجراءات الجنائية البحريني، والمادة (٥٧) من قانون الإجراءات الجزائية الاماراتي والمادة (٤٤) من نظام الإجراءات الجزائية السعودي.

والمقصود بالمكان كمحل للتفتيش في البيئة المعلوماتية هو المأوى أو مكان الإقامة وما يتعلق به من محلات يستخدمها الإنسان بصفة دائمة أو غير دائمة وسواء كانت ثابتة أو غير ثابتة، وذلك إذا وجدت فيها مكونات ومتعلقات خاصة بالحاسب الآلي مادية كانت أو منطقية رقمية أو شبكات اتصال خاص^١.

ج- السلطات المختصة بالتفتيش.

تعد مرحلة التفتيش من مرحلة التحقيق الابتدائي، فقد أوكل المشرع هذه المهمة لجهة قضائية لما لها من أهمية كبرى وذلك لتعلقها بحقوق وحريات الإنسان، ولحماية هذه الحقوق وضمان احترامها حرص المشرع على اسنادها للنيابة العامة وقاضي التحقيق وأجاز لهم أن يسندوا هذه المهمة كاستثناء لرجال الضبط القضائي.

وقد حدد المشرع البحريني السلطة المختصة بإجراء التفتيش في جريمة الاحتيال المعلوماتي وذلك وفق ما جاء في قانون جرائم تقنية المعلومات بنص المادة (١٥).

ويرى الباحث أن التفتيش بمثابة الوسيلة التي من خلالها يمكن ضبط الأشياء التي تعد تصبح بعد ذلك أدلة مادية تساهم في اثبات الجريمة والوصول إلى الحقيقة من خلالها، فهو مجرد وسيلة لا غاية.

الشروط الشكلية للتفتيش.

أ- يجب أن يكون الإذن بالتفتيش مكتوباً وأن يكون صريحاً في الدلالة على التفويض من مباشرة التفتيش فلا يجوز على الإطلاق أن يصدر شفاهية ولا يغني عن ذلك إقرار المحقق أمام المحكمة بأنه إذن شفوي بالتفتيش، فبالتالي يجب أن يكون أمر التفتيش ثابتاً بالكتابة حتى يكتسب قوته القانونية^٢.

^١ عدنان زيدان، "مرجع سابق"، ص ٣٠٠.

^٢ سعد سلامة، "دليل مأموري الضبط القضائي في كيفية تنفيذ الإذن بالتفتيش" مجلة مركز بحوث الشرطة، أكاديمية مبارك للأمن، العدد ٣٠، يوليو ٢٠٠٦م، ص ١٩٨.

ب- إجراء التفتيش بحضور أشخاص معينين بالقانون: من بين هذه الأشخاص المتهم والقائم بالتفتيش^١.

ت- إعداد محضر خاص بالتفتيش: ويكون بتكليف القائم بالتفتيش باصطحاب كاتب يحرر محضراً خاصاً بالتفتيش والضبط، تسجل فيه جميع وقائع التحقيق بالتفصيل، وذكر البيانات والأشياء والوثائق التي يتم ضبطها بكل أمانة ودقة وحرص.

أما فيما يخص التفتيش الخاص بجريمة الاحتيال المعلوماتي:

١- إجراءات تنفيذ تفتيش نظم الحاسوب الآلي وميعاده: لهذه الإجراءات خصوصية تتميز بها، وذلك لدقة التعامل مع الأجهزة والبرامج الموجودة عليها، ولكي تتم على أكمل وجه، يجب تحديد نوع النظام المراد تفتيشه، وبالتالي يجب أن يكون القائم بالتفتيش على علم بقدر كبير بعلوم الإعلام الآلي حتى يتسنى له معرفة نظم الحاسوب المراد تفتيشها، والاستعانة بخبراء النظام للاستعانة بهم في عملية إجراء التفتيش، ومعرفة إمكانية الحصول على كلمة السر والدخول للنظام المراد تفتيشه، ومعرفة مكان القيام بتحليل نظم الحاسوب الآلي^٢.

٢- بالإضافة إلى تحديد هوية أعضاء فريق التفتيش يجب على القائم بالتفتيش اتخاذ الخطوات التالية عند تنفيذ إذن التفتيش والتي تتلخص فيما يلي:

أ- تأمين حماية مسرح الجريمة، بضمان فصل القوة الكهربائية عن موقع المعاينة وأجهزة خدمة شبكة الإنترنت، لشل فاعلية الجاني في القيام بأي فعل من شأنه التأثير على آثار الجريمة.

ب- إبعاد المتهم عن مكان النظام إن كان قريباً منه.

ت- أخذ الحيطة لمنع تمكن المتهم من الدخول عن بعد للنظام المعلوماتي.

ث- الدخول إلى الموقع ببطء، لكيلا يتم تشويه أو إتلاف الدليل.

ج- عدم لمس لوحة المفاتيح، لأن ذلك قد يستلزم استخدام برامج أخرى احتيالية أو صعبة.

ح- يجب العناية بالملاحظات وكلمات السر ورموز الشفرة إلى غيرها من العمليات والإجراءات الفنية التي تساعد على الكشف عن الجريمة المراد إثباتها^٣.

^١ عبد الله الكيتوب، "مرجع سابق"، ص ١٣٩

^٢ نورة طرشي، "مرجع سابق"، ص ١٢٥.

^٣ عفيفي كامل عفيفي، "مرجع سابق"، ص ٦٥.

وفي نطاق تفتيش نظم الحاسوب، نجد أن أغلب التشريعات الإجرائية لم تحدد مدة معينة لتنفيذ إجراء التفتيش ما عدا البعض منها كالتشريع الانجليزي الذي حدد مهلة الشهر الواحد من تاريخ إصدار الإذن كما أنها تختلف في الزمن الذي يجري فيه التفتيش أو تحديد المدة التي يجري فيها، غير أن الرأي الغالب في مجال تفتيش النظم المعلوماتية هو عدم تقييد المحقق بمدة زمنية معينة، بل يجب تركها للسلطة التقديرية له، لأن الوقت الذي تكثر فيه الجرائم المعلوماتية هو ليلاً، لسهولة الاتصال ومجانيته في ذلك الوقت في بعض الحالات، وأيضاً لسهولة الدخول إلى المواقع المستهدفة بالفعل الإجرامي لقلة المستخدمين في هذا الوقت. والجدير بالذكر هنا أن الكثير من التشريعات قد تبنت إمكانية التفتيش دون الحصول على إذن في حالات الضرورة، وذلك لتقوية الفرصة أمام الجاني لمحو الدليل، ولكي تتمكن أيضاً الجهات المعنية من الحصول على الدليل، وهذا ما اخذ به المشرع البلجيكي في قانون تحقيق الجنايات البلجيكي الصادر في ٢٣ نوفمبر لعام ٢٠٠٠م، والذي أجاز أيضاً إمكانية امتداد التفتيش إلى نظام معلوماتي آخر غير مكان التفتيش الأصلي وهذا ليس مطلقاً إنما مقيد بشروط معينة يمكن إجمالها في الحصول على الأدلة التي تكون معرضة للإتلاف والتدمير^١.

وكذلك فعل المشرع الأمريكي حيث أجازت المادة (٤١a) من قانون الإجراءات الجنائية الفيدرالي الأمريكي، وأقرت الاتفاقية الأوروبية الخاصة بالجرائم المعلوماتية ذلك متى كانت المعلومات المخزنة بحاسوب غير حاسوب المتهم، والتي يتم الدخول إليها من خلال الحاسب الأصلي محل التفتيش^٢.

الفرع الثالث: الضبط في جريمة الاحتيال المعلوماتي

يعرف الضبط على أنه وضع اليد على شيء يتصل بجريمة وقعت، ويفيد في كشف الحقيقة عنها وعن مرتكبها^٣. فالضبط هو الوسيلة القانونية التي تضع بواسطتها السلطة المختصة المختصة يدها على جميع الأشياء التي وقعت على الجريمة، أو نتجت عنه، أو استعملت لاقتوافها، وعليه يكون الضبط أثراً مباشراً للتفتيش باعتبار أن التفتيش هو ضبط الأدلة أو الأشياء التي تفيد في إظهار الحقيقة في الجريمة، فالضبط هو نتيجة للتفتيش، وقد يقع الضبط استناداً لأسباب أخرى كالمعاينة^٤. فبطان التفتيش يؤدي إلى بطلان الضبط^١.

^١ فهد العازمي، "مرجع سابق"، ص ٢٧٨-٢٨٣.

^٢ عبد الله الكيتوب، "مرجع سابق"، ص ١٤٥.

^٣ عبد الفتاح حجازي، "مرجع سابق"، ص ٢٠٧.

^٤ عبد الله الكيتوب، "مرجع سابق"، ص ١٤١.

ويعرف الضبط على أنه ضبط الأدلة المادية للكشف عن الجريمة، ويكون ذلك بوضع اليد على الدلائل المادية المخزنة فيها البيانات الإلكترونية والمعلومات التي تتصل بالجريمة، كما يستخدم في ضبط الجريمة المعلوماتية برامج خاصة من أجل الولوج إلى البيانات المراد ضبطها إلى جانب وضع اليد على الدلائل المادية^٢.

تتوقف طبيعة الضبط على الكيفية التي يتم بها وضع اليد على الشيء المضبوط، أي أن إذا كان الشيء المضبوط في حيازة الشخص وتم ضبطه فيكون هنا الضبط إجراء تحقيق، أما إذا كان بمثابة الاستيلاء عليه دون الاعتداء على حيازة قائمة فيكون إجراء استدلال^٣.

والضبط في جريمة الاحتيال المعلوماتي هو وضع اليد على الدلائل المادية المخزنة فيها البيانات الإلكترونية والمعلومات التي لها علاقة بالجريمة والتي تفيد في الوصول إلى الحقيقة وعن مرتكبها^٤، ويستخدم لذلك وسائل غير تقليدية وهي البرامج التي تساعد في الولوج من أجل الحصول على البيانات المراد ضبطها ووضع اليد عليها^٥.

أولاً: ضبط المكونات المادية في جريمة الاحتيال المعلوماتي.

يدور هنا الحديث على الأدلة المادية التي يجوز ضبطها في الجريمة المعلوماتي والتي لها قيمة في اثبات جريمة الاحتيال المعلوماتي ونسبتها للمتهم وهي:

أ- **المخرجات والمستندات الورقية:** كثير من جرائم الاحتيال المعلوماتي ما تترك وراءها قدر كبير من الأوراق والمستندات الرسمية منها والخاصة، ولكن وجود الحاسب الآلي يتيح إمكانية حفظ هذه المعلومات على الحاسب نفسه^٦.

ب- **جهاز الحاسب الآلي:** يجب أن يتم تحديد الحاسب التي تمت من خلاله الجريمة أو التي وقعت عليها الجريمة، والخبير في مجال الحواسيب الإلكترونية يستطيع التعرف على الحاسب ومكوناته وكيفية التعامل معه، وتتمثل مكونات الحاسب في وحدة المعالجة المركزية ولوحة المفاتيح والشاشة، ومع ظهور وسائل تقنية جديدة صغيرة الحجم كالهاتف النقال واللابتوب فإن هذه الأجهزة يجب ضبطها وتحريزها ككتلة واحدة^٦.

^١ عبد الفتاح حجازي، "مرجع سابق"، ص ٢٠٧.

^٢ مصطفى موسى، "مرجع سابق"، ص ٢٠٨.

^٣ طارق الخن، "مرجع سابق"، ص ٢٩١.

^٤ خالد ممدوح إبراهيم، "مرجع سابق"، ص ٢٠.

^٥ خالد ممدوح إبراهيم، "مرجع سابق"، ص ٢٧٦.

^٦ خالد إبراهيم، "مرجع سابق"، ص ٢٧٦.

ت-الأقراص المغناطيسية: وهي الأقراص التي تحتوي على بيانات ومعلومات هائلة الحجم وقد تكون في مكان لا يوجد فيه الحاسب الآلي الخاص بالجريمة إلا أن المعلومات المخزنة عليها قد تفقد في مراحل التحقيق في الجريمة وقد توجد بأعداد كبيرة في الشركات والبنوك وتكون مغلفة بأغلفة توضح محتويات كل منها^١.

ث-الأشرطة الممغنطة: وهي عبارة عن شرائط ممغنطة تستخدم عادة للحفظ والتخزين وقد تكون في مكان آمن بعيد عن الحاسب الآلي^٢.

ج- المودم: وهي أجهزة يمكن من خلالها اتصال أجهزة الحاسب الآلي ببعضها البعض^٣.

ح- الطابعات: وتنقسم إلى نوعين منها العادية وأخرى التي تعمل بتقنية الليزر، والأجهزة الحديثة التي يمكن تخزين المستندات والمعلومات التي تمت طباعتها^٤.

وقد أعطى المشرع البحريني الحق للنيابة العامة بإجراء الضبط والتحفظ على بيانات وسيلة تقنية المعلومات المخزنة على النظام أو أي جزء منه أو من المخزنة على وسائط تخزين وسيلة تقنية المعلومات^٥.

وهنا أراد المشرع البحريني من رجال الضبط القضائي إحاطة مكان الجريمة والتحفظ على كل ما له صلة بالجريمة أو كل ما من شأنه أن يصلح بأن يكون دليلاً على الجريمة بالإضافة إلى التحفظ على كافة الوسائط التي قد تكون لها بالجريمة كتخزين معلومات أو برامج مساعدة.

^١ طارق الخن، "مرجع سابق"، ص ٢٩٣.

^٢ عبد الله الكيتوب، "مرجع سابق"، ص ١٤٦.

^٣ فهد العازمي، "مرجع سابق"، ص ٣٠٤.

^٤ فهد العازمي، "مرجع السابق"، ص ٣٠٤.

^٥ نص المادة (1/16) الفقرة الأولى من قانون رقم (٦٠) لسنة ٢٠١٤ البحريني، " للنيابة العامة الضبط والتحفظ على بيانات وسيلة تقنية المعلومات التي يتم الدخول إليها استناداً إلى أحكام...."

أ- الضبط والتحفظ على نظام تقنية المعلومات، أو أي جزء منه، أو أي من وسائط تخزين بيانات وسيلة تقنية المعلومات.

ب- استنساخ بيانات وسيلة تقنية المعلومات والاحتفاظ بالنسخة.

ت- المحافظة على سلامة بيانات وسيلة تقنية المعلومات.

ث- رفع بيانات وسيلة تقنية المعلومات من نظام تقنية المعلومات الذي تم الدخول إليه أو جعل الدخول إليها غير متاح.

واكتفى المشرع الإماراتي والسعودي بإعمال النصوص الخاصة لإجراء الضبط في قانون الإجراءات الجزائية، حيث لم يرد نص يحدد من خلاله كيفية إجراء الضبط في القوانين الخاصة بمكافحة الجريمة المعلوماتية.

ثانياً: ضبط المكونات المعنوية في جريمة الاحتيال المعلوماتي.

وإجراء الضبط في مجال الفضاء الإلكتروني متعلق بضبط الأدلة المتحصل عليها من التفتيش، وهي البيانات المعلوماتية وتعد مراقبة المكالمات السلكية واللاسلكية تحت رقابة القضاء وذلك لضبط ما يفيد في كشف الحقيقة أحياناً^١.

ونظراً لأن الضبط في جريمة الاحتيال المعلوماتي محله البيانات المعالجة إلكترونياً، فقد تواجه صعوبات وتثار هنا إشكالية مفادها، هل من الممكن وضع اليد على شيء غير مادي؟

وللإجابة على هذه الإشكالية هناك اتجاهين تشريعيين، وهما:

١- **الاتجاه الأول:** وهو الاتجاه الذي رفض أن تكون بيانات الحاسب الآلي محلاً

للضبط، لعدم اتسامها بالمادية، ولا يمكن ضبطها إلا بعد نقلها على كيانات مادية ملموسة، وقد أخذ بهذا الاتجاه المشرع الألماني^٢.

٢- **الاتجاه الثاني:** والذي أجاز ضبط البيانات المعالجة إلكترونياً، وبرر ذلك بإمكانية

تسجيل وحفظ البيانات على وسائط مادية مما يتيح نقلها وبثها وإعادة انتاجها، وقد أيد هذا الاتجاه كل من المشرع الكندي والأمريكي، وجاء ذلك في المادة (٧/٢٩) من قانون الإثبات الكندي حيث نصت على أن "تفتيش وضبط الدفاتر والسجلات الخاصة بمؤسسة مالية، يقتصر على تفتيش المكان بغرض تفقده أو أخذ نسخة من المواد المكتوبة، يستوي في ذلك أن تكون السجلات مكتوبة أم في شكل إلكتروني"^٣.

وحسناً ما ذهب إليه الدكتور علي الطوالة في مسألة ضبط الكيانات المعنوية للحاسب الآلي من خلال الاتجاه الأول المقنع وهو متى تم نقلها أو تحويلها على كيانات مادية ملموسة كطباعتها على الورق وضبطها بذلك^٤.

^١ خالد ممدوح إبراهيم، "مرجع سابق"، ص ٢٧٤.

^٢ هشام رستم، "الجوانب الإجرائية للجرائم المعلوماتية"، مرجع سابق، ص ٩٤.

^٣ هشام رستم، "مرجع سابق"، ص ٩٥.

^٤ علي حسن الطوالة، "التفتيش الجنائي على نظم الحاسوب والانترنت"، الطبعة الأولى ٢٠١٠م، ص ١٤٩.

ويرى الباحث إلى أنه لا خلاف على ذلك ما دام هناك تشريعات قننت في موادها إجراءات الضبط على الكيانات المعنوية للحاسب الآلي مثلما ذهب إليه المشرع البحريني والإماراتي والسعودي في القوانين ذات الصلة.

الفرع الرابع: التنصت والمراقبة الإلكترونية

يعد التنصت والمراقبة لشبكات الحاسب الآلي من إجراءات التحقيق في جريمة الاحتيال المعلوماتي، وبغض النظر عما يثيره هذا الإجراء من جدل حول انتهاك حرمة الحياة الخاصة للأفراد إلا أن معظم التشريعات أخذت بهذا الإجراء وعدته من قبيل إجراءات التحقيق.

أولاً: ماهية التنصت والمراقبة الإلكترونية.

تعرف المراقبة الإلكترونية بأنها "وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه، يقوم بها مراقب إلكتروني يتمثل في مأمور ضبط قضائي ذو كفاءة عالية تتماشى مع نوع جريمة الاحتيال المعلوماتي، مستخدماً في ذلك التقنية الإلكترونية وعبر شبكات الإنترنت، ومن خلال مراقبة أحد الهكرة ممن قام باختراق الحاسب الآلي الخاص بالمجني عليه، أو يقوم بإعداد صندوق بريد إلكتروني مستنسخ لمراقبة المشتبه فيه"^١.

وتقوم عملية المراقبة الإلكترونية وفق آلية ووسيلة معينة وهي التنصت على الشبكات ومراقبتها وتتم عملية التنصت بالتمركز في مكان معين داخل شبكة الاتصالات، ويجري من خلالها تسجيل وحفظ البيانات المتبادلة بين الأنظمة المعلوماتية^٢.

فالمراقبة الإلكترونية هي عملية مراقبة شبكة الاتصالات ويقوم من خلالها المراقب بجمع البيانات والمعلومات عن المشتبه فيه سواء كان شخصاً أو مكاناً أو شيئاً حسب طبيعته مترتب ذلك بالزمن والتاريخ، ويهدف من وراء هذه المراقبة تحقيق غرض أمني أو أي غرض آخر^٣.

^١ نبيلة هروال، "مرجع سابق"، ص ١٩٩.

^٢ عبد الله الكيتوب، "مرجع سابق"، ص ١٤٧.

^٣ مصطفى موسى، "المراقبة الإلكترونية عبر شبكة الإنترنت دراسة مقارنة" بين المراقبة الأمنية التقليدية والإلكترونية"، الكتاب الخامس، دار الكتب والوثائق القومية المصرية، ٢٠٠٣م، ص ١٩٢.

ثانياً: طبيعة التنصت والمراقبة الإلكترونية في جريمة الاختيال المعلوماتي.

بالرغم من الجدل الذي يثيره إجراء التنصت والمراقبة الإلكترونية والمتمثل في رأي الفقه كونه يمثل اعتداء على الحياة الخاصة للأفراد؛ إلا أن معظم التشريعات أقرت هذا الإجراء ككاشف للحقيقة في جريمة الاختيال المعلوماتي، فقد أجاز المشرع الفرنسي في قانونه الخاص بالإجراءات الجزائية المعدل لعام ١٩٩٢م اعتراض الاتصالات البعيدة بما في ذلك شبكات تبادل المعلومات، وكذلك فعل المشرع الهولندي الذي أعطى لقاضي التحقيق الحق بأن يأمر بالتنصت على شبكات الاتصالات إذا كانت هناك جرائم خطيرة تستدعي هذا الإجراء^١.

إلا أن ذلك لم يمنع من الاختلاف الفقهي حول إمكانية تسجيل هذه المعلومات، حيث يرى جانب من الفقه أن يقتصر هذا الإجراء على المراقبة فقط دون جواز التسجيل^٢.

وقد أجاز المشرع البحريني إجراء التنصت والمراقبة على المحادثات والمراسلات السلوكية واللاسلكية بنص المادة (٩٣) من قانون الإجراءات، واشترط لذلك إذن من قاضي المحكمة الصغرى، كما أن المشرع أعطى الحق في تسجيل هذه المحادثات إذا استدعت الضرورة لذلك وقد حدد مدة إجراء المراقبة بثلاثين يوماً قابلة للتجديد لأكثر من مرة^٣.

ولا بد أن يكون الأمر بالمراقبة مسبباً، حتى نضمن عدم تجاوز الحدود المنصوص عليها في الدستور، والتي يكفل حماية الحياة الخاصة للمواطنين كافة، ويبقى تقدير مدى جدية التحريات وكفايتها لإصدار الإذن بالمراقبة، هو من المسائل الموضوعية التي يوكل الأمر فيها إلى سلطة التحقيق (النائب العام)^٤.

ويتفق الباحث مع ما ذهب إليه المشرع البحريني، لأن الطبيعة التي تمتاز بها جريمة الاختيال المعلوماتي، تقتضي إجراء المراقبة بالكيفية التي أوردها المشرع، وذلك للحيلولة دون محو الأدلة أو إتلافها، وللمحد من انتشار هذه الجريمة، فتعتبر المراقبة من أهم إجراءات التحقيق في مجال المعلوماتية، ولكن يجب أن يكون هذا الإجراء وفق القانون.

^١ خالد ممدوح إبراهيم، "مرجع سابق"، ص ٢٠٨.

^٢ راجع في ذلك عبد الفتاح حجازي، "مرجع سابق"، ص ٣٧٤.

^٣ مرسوم بقانون رقم (٤٦) لسنة ٢٠٠٢ بإصدار قانون الإجراءات الجنائية البحريني.

^٤ علي حسن الطوالة، "مرجع سابق"، ص ٢٣٣.

وقد أشار المشرع الإماراتي إلى جواز إجراء المراقبة من قبل المحقق دون إعطائه سلطة تسجيل ما تم مراقبته^١، إلا أنه بالإمكان التغلب على هذه الإشكالية وذلك بإفراغ ما تم مراقبته بمحضر رسمي كتابي على غرار محاضر التحقيق، ويتم توثيق ما تمت مراقبته من مكالمات ومحادثات وبيانات.

وقد ذهب المشرع السعودي إلى ما ذهب إليه المشرع البحريني من حيث جواز إجراء المراقبة على المحادثات والمراسلات السلكية واللاسلكية واشترط أن يتم ذلك بموافقة قاضي التحقيق وذلك وفق ما جاء في نظام الإجراءات السعودي^٢.

خلاصة القول إن المشرع في دول المقارنة ذهب إلى ما ذهبت إليه معظم التشريعات بإقرارها إجراء المراقبة الإلكترونية وفق ما نص عليه القانون، حيث يتطلب ذلك بأخذ الإذن من قبل الجهات المختصة بالتحقيق للقيام بالمراقبة على المحادثات والمراسلات سلكية كانت أو لاسلكية، وقد حددت المدة القانونية لإجراء المراقبة ومع إمكانية تجديد هذه المدة حسب الضرورة.

ويرى الباحث أن إجراء المراقبة الإلكترونية عملية ضرورية في جريمة الاحتيال الإلكتروني وقد وفق المشرع في دول المقارنة بجواز إجراءه، وذلك لتمكين جهات التحقيق من استخراج الأدلة وضبطها مما يدعم في إبراز الحقيقة المرجوة.

^١ نص المادة (٧٥) من قانون الإجراءات الجزائية الإماراتي رقم (٣٥) لعام ١٩٩٢م، على "العضو النيابة العامة أن يفتش المتهم... وأن يراقب المحادثات السلكية واللاسلكية متى استوجبت مقتضيات التحقيق ذلك".

^٢ المادة (٥٦) من نظام الإجراءات الجزائية السعودي رقم (١٢) الصادر في (٢٢/١/١٤٣٥هـ)، نصت على "الرئيس هيئة التحقيق والادعاء العام أن يأمر بضبط الرسائل والخطابات والمطبوعات والطرود، وله أن يأذن بمراقبة المحادثات الهاتفية وتسجيلها، متى كان لذلك فائدة في ظهور الحقيقة في جريمة وقعت، على أن يكون الإذن مسبباً ومحددًا بمدة لا تزيد على عشرة أيام قابلة للتجديد وفقاً لمقتضيات التحقيق".

المبحث الثاني

الأدلة الجنائية في إثبات جريمة الاحتيال باستخدام وسائل تقنية المعلومات

إن ما ينطبق من أدلة جنائية في الجرائم التقليدية تصلح للتطبيق في مجال التحقيق وإثبات الجريمة ذات الطابع التقني والمعلوماتي.

ولكن هذه الأدلة تبدو قاصرة أمام الجرائم المعلوماتية بوجه عام وجريمة الاحتيال المعلوماتي على وجه الخصوص، نظراً للخصوصية التي تتمتع بها هذه الجرائم كما بينها سابقاً، فالمجرم المعلوماتي يمتلك المقدرة على إخفاء آثار الجريمة مما يصعب إثباتها واكتشافها، وهنا يبرز دور المحقق في مجال جريمة الاحتيال المعلوماتي في استخراج الدليل الإلكتروني الرقمي وهذا الدليل خاص بالجرائم المعلوماتية، ولا بد في مثل هذه الجرائم وأثناء مراحل التحقيق الاستعانة بالمعلومات والمصادر والعناوين التي تحتويها النظم المعلوماتية.

ومن هنا تأتي أهمية موضوع حجية الأدلة الرقمية الناتجة عن الحاسوب في إثبات جريمة الاحتيال المعلوماتي، ويبرز معها كفاءة المحقق الجنائي والذي يلعب الدور الرئيسي في تتبع آثار جريمة الاحتيال المعلوماتي والذي يحاول المجرم المعلوماتي إخفاؤها قدر الإمكان، ولأن هذه الآثار يمكن أن تُخفى أو تُتلف بشكل متعمد وغير متعمد، حيث يمكن لمجرم محترف أن يستخدم وسائل تكنولوجية وتقنية متقدمة قادرة على إخفاء هذه الآثار بالكامل، كما يمكن لمحقق جنائي لا يمتلك الخبرة الكافية أن يتلف هذه الأدلة أثناء عملية التحقيق الجنائي وبالتالي يصعب نسبتها لشخص معين، وللتعرف أكثر على الدليل الرقمي ومدى حجيته في مجال الإثبات لجريمة الاحتيال المعلوماتي وسيتم تقسيم هذا المبحث كالتالي:

المطلب الأول: دور الأدلة التقليدية في إثبات جريمة الاحتيال المعلوماتي.

المطلب الثاني: الدليل الرقمي ودوره في إثبات جريمة الاحتيال المعلوماتي.

المطلب الثالث: مدى قبول الأدلة الرقمية كأدلة إثبات جريمة الاحتيال المعلوماتي.

المطلب الأول

دور الأدلة التقليدية في إثبات جريمة الاحتيال المعلوماتي

لا يقتصر الإثبات الجنائي في جريمة الاحتيال المعلوماتي على الأدلة المستحدثة فقط، فقد تكون للأدلة التقليدية دور في عملية الإثبات لهذه الجريمة، وإن لم تكن بنفس القوة التي تتصف بها الأدلة المستحدثة، وهذا ما سنبينه خلال هذا الجزء من الدراسة، وسيتم تقسيم المطلب إلى أربعة فروع على النحو الآتي:

الفرع الأول: الشهادة.

الفرع الثاني: القرينة.

الفرع الثالث: الاعتراف.

الفرع الرابع: الخبرة.

الفرع الأول: الشهادة

تُعرف الشهادة على إنها إجراء من إجراءات التحقيق، فهي المعلومات التي تتعلق بالجريمة التي يدلي بها الشاهد أمام سلطة التحقيق، وهي السبيل العادي للإثبات الجنائي^١.

وعُرفت على أنها "إذن أو تقرير يصدر عن شخص في شأن واقعة عاينها بحاسة من حواسه^٢، ومصدر الشهادة هو الحقيقة نفسها، فلا يمكن أن تكون الشهادة رأي أو معتقد^٣.

أما عن الشاهد في جريمة الاحتيال المعلوماتي، فيشترط في الشاهد هنا أن يكون من أصحاب الخبرة والتخصص في تقنية المعلومات والحواسيب الآلية، والتي يمتلك معلومات هامة لازمة للدخول إلى نظام المعالجة الآلية للبيانات^٤. وعليه فإن الشاهد قد يكون القائم على تشغيل الحاسوب أو المبرمج أو المحلل أو مهندسو الصيانة والاتصال أو مدير النظام نفسه^٥.

^١ عبد الفتاح حجازي، "مرجع سابق"، ص ٣٣٤.

^٢ محمود نجيب حسني، "مرجع سابق"، ص ٤٤١.

^٣ يونس العرب، "مرجع سابق"، ص ٩٤٩.

^٤ عبد الفتاح حجازي، "مرجع سابق"، ص ٣٣٩.

^٥ خالد ممدوح إبراهيم، "مرجع سابق"، ص ٢٦٥.

وعن رأي الفقه في مدى جواز إجبار الشاهد على الشهادة؟ فقد انقسم الفقه إلى اتجاهين، أما الأول فأخذ بعدم إكراه الشاهد على تقديم المعلومات كإفشاء كلمات المرور أو شفرات النظام وهذا ما أخذ به المشرع في كل من تركيا وألمانيا، والاتجاه الآخر وهو السائد في كل من فرنسا وهولندا وانجلترا فهو يأخذ بمبدأ إلزام الشاهد بالإدلاء ما يملك من كلمات السر والشفرات الخاصة^١.

وعليه يجب على الشاهد في جريمة الاحتيال المعلوماتي أن يلتزم بالآتي:

- ١- إعلام الجهات المختصة بالتحقيق عما يملك من معلومات تفيد القضية^٢.
- ٢- يجب أن تكون المعلومات التي يقدمها الشاهد تتسم بالسهولة والبساطة وبعيدة عن التعقيد والغموض^٣.
- ٣- أن تتسم المعلومات بالدقة والتحديد إلى جانب الصدق والأمانة، وأن يبين الشاهد معلوماته على يقين لا على الخداع والتزوير^٤.

خلاصة لما سبق يتضح بأن الشاهد في جريمة الاحتيال المعلوماتي يلعب دوراً في كشف حقيقة الجريمة الواقعة أمامه شريطة أن يكون على دراية بالتقنية الحديثة، وأن يكون من أهل الاختصاص في مجال تقنية المعلومات.

يؤيد الباحث الرأي القائل بضرورة إفصاح الشاهد عما لديه من معلومات، ولا يجب أن يخفيها، وهذا تماشياً مع مقتضيات الحاجة إلى مكافحة جريمة الاحتيال المعلوماتي، نظراً للمخاطر الناجمة عن جريمة الاحتيال المعلوماتي، فعلى الشاهد أن يقدم كل ما لديه من معلومات ولو كانت بسيطة وذلك لتمكين جهات التحقيق من الوصول إلى الحقيقة.

الفرع الثاني: القرينة

تعرف القرينة على أنها: استنتاج الواقعة المطلوب إثباتها من واقعة أخرى قام عليها الدليل^٥، وتعرف أيضاً على أنها "استنتاج واقعة مجهولة من أخرى معلومة تتحد معها في

^١ طارق الخن، "مرجع سابق"، ص ٣٠٦.

^٢ أحمد هلاي، "التزام الشاهد بالإعلام في الجرائم المعلوماتية دراسة مقارنة"، دار النهضة العربية، القاهرة، ط١، ١٩٩٧، ص ٢٥.

^٣ عبد الفتاح حجازي، "مرجع سابق"، ص ٣٤٦.

^٤ أحمد هلاي، "مرجع سابق"، ص ٦٣.

^٥ محمود نجيب حسني، "مرجع سابق"، ص ٤٨٧.

العلّة"^١، وللقرائن دور في إثبات جريمة الاحتيال المعلوماتي وذلك عبر تتبع عنوان (IP) الخاص بالحاسب الآلي والوصول إليه فذلك يعتبر قرينة على مالك الحاسوب، بالرغم من عدم كفايتها كدليل إدانة^٢.

وقد يستنتج القاضي بعض القرائن على المتهم كاستخدامه بنفس أسلوب الاحتيال في عمليات سابقة أصبحت مكشوفة لدى الجهات المختصة.

الفرع الثالث: الاعتراف

يعرف الاعتراف على أنه إقرار المدعى على نفسه بصدور الواقعة الجرمية عنه^٣. وليس للاعتراف شكل معين فقد يرد شفويًا أو كتابيًا ويصح أن يكون مقروء أو مسموع أو مرئي، كما يجب أن يتوفر في الاعتراف شروطه وهي أن يصدر من شخص مدرك وواعي، بالإضافة إلى أن يكون صادر عن الإرادة الحرة.

وعن الاعتراف في جريمة الاحتيال المعلوماتي، فبعد أن تنازل الاعتراف عن مكانته كسبباً للأدلة، نظراً للإشكاليات العدة التي واجهته، كأن يعترف أكثر من شخص على ارتكاب الجريمة، أو كأن يصدر الاعتراف عن شخص ليس له علاقة بالجريمة وذلك للتستر على الفاعل الأصلي للجريمة، فهذا ما قد يرد على جريمة الاحتيال المعلوماتي أيضاً، مثل ما إذا وقعت جريمة استيلاء على بطاقة إئتمان، وقام أكثر من شخص بالاعتراف بالجريمة^٤.

فهنا يجب أن يتم اللجوء إلى التأكد من تطابق أقوال الجاني مع الطريقة التي استخدم فيها جريمة الاحتيال المعلوماتي، ويتم مطابقة ما يصدر من أقوال من قبل الجاني مع ما يمكن تحليله من أفعال بالتعرف على طريقة الاختراق التي تمت والآلية التي اتبعتها في تحويل الأموال^٥.

ويرى الباحث ضرورة الأخذ بالاعتراف في صورته العملية لكي يتم إقراره كدليل إثبات في جريمة الاحتيال المعلوماتي ولا يمكن أن يكون الاعتراف بصورته التقليدية دليل كافٍ في إثبات جريمة الاحتيال المعلوماتي.

^١ عمر أبو بكر يونس، "مرجع سابق"، ص ٩٣٦.

^٢ طارق الخن، "مرجع سابق"، ص ٣١٤.

^٣ عمر أبو بكر يونس، "مرجع سابق"، ص ٩٤١.

^٤ طارق الخن، "مرجع سابق"، ص ٣١٩.

^٥ عمر أبو بكر يونس، "مرجع سابق"، ص ٩٤٧.

الفرع الرابع: الخبرة

تعرف الخبرة على أنها "إبداء رأي فني من قبل شخص مختص فنياً في شأن واقعة ذات أهمية في الدعوى الجزائية"^١. والخبرة الوسيلة الوحيدة لتحديد التفسير الفني للأدلة أو الدلائل بالاستعانة بالمعلومات العلمية، وتتميز على باقي أدلة الإثبات التقليدية في أنها تقوم على الرأي الفني للخبير لتحديد قيمتها في الإثبات^٢.

والخبرة في جريمة الاحتيال المعلوماتي تلعب دوراً رئيسياً، وتعد من أهم طرق الإثبات للجريمة، فإذا كان الحديث يدور على وجوب أن تتمتع سلطات التحقيق في المجال المعلوماتي بالخبرة اللازمة في مجال تقنية المعلومات لتستطيع القيام بأعمالها، ولما كان الشاهد في هذه الجريمة يجب أن تتوفر لديه المعرفة بالتقنية الحديثة وأن يكون قادراً على استخدام هذه التقنية^٣.

فمن هنا يتضح دور الخبرة في الإثبات حتى أصبح البعض يطلق عليها بالمعلوماتية الشرعية والتي يقصد بها "العملية التي يقوم بها الخبراء التقنيون بهدف الوصول إلى الأدلة الرقمية بالجريمة، من أجل كشف غموضها وتوضيحها، كما أن البعض لا يشترط مسألة التخصص في الدراسة في هذا المجال، فيكفي المعرفة التقنية العالية نتيجة الممارسة والخبرة، فالقدرة على التعامل مع التقنية الحديثة بغض النظر عما إذا كان الشخص من دارسي هذه التقنية أم لا، فالأمر يتطلب هنا المهارة والموهبة في استعمال وسائل تقنية المعلومات"^٤.

ويرى الباحث أن الخبرة تلعب دوراً أساسياً ورئيسياً في إثبات جريمة الاحتيال المعلوماتي، ولا بد من ذلك اشتراط أن تكون جهات التحقيق والشهود من أصحاب الخبرة في مجال التقنية الحديثة، فالخبير وحده هو القادر على استخراج الأدلة وإثبات وقوع الجريمة، وتعيين الأسلوب التي وقعت به الجريمة، كما يمكن للخبير أن يقوم بإرجاع البيانات التي تم حذفها أو إتلافها، بالإضافة أن خصوصية الجريمة المعلوماتية تتطلب التعامل معها بالخبرة والمهارة اللازمة لاستخراج الأدلة، ولا يتطلب لذلك أن يكون الخبير ممن درسوا مجال تقنية المعلومات، فيكفي أن يكون من أصحاب المهارة والمقدرة على استخدام الحاسب الآلي بشكل يخول لهم أن يكون من أصحاب الخبرة.

^١ محمود نجيب حسني، "مرجع سابق"، ص ٣٢٥.

^٢ عبد الفتاح حجازي، "مرجع سابق"، ص ٣٢١.

^٣ عبد الله الكيتوب، "مرجع سابق"، ص ١٦٧.

^٤ عمر أبو بكر يونس، "مرجع سابق"، ص ١٠٢٤.

المطلب الثاني

الدليل الرقمي ودوره في اثبات جريمة الاحتيال المعلوماتي

إن الدليل الرقمي من الأدلة الجنائية التي ظهرت مع ظهور الجرائم المعلوماتية، وأصبحت ضرورة ملحة فرضتها الحاجة إلى أدلة تنتمي للبيئة التي ترتكب فيها أو من خلالها هذه الجرائم وأصبح هناك اعتراف قانوني بهذه الأدلة، وممارسة فعلية للاستفادة منها، إلا أن هناك بعض التخوف والتردد عند اثبات جرائم المعلوماتية، والأخذ بالدليل الرقمي، إضافة إلى وجود بعض الضوابط الإجرائية والتقنية التي تحكم عملية استنتاج الدليل وتقديمه للجهات المعنية، وسنستعرض الدليل الرقمي من خلال فرعين كالآتي:

الفرع الأول: تعريف الدليل الرقمي.

الفرع الثاني: نطاق عمل الدليل الرقمي في الإثبات الجنائي.

الفرع الأول: تعريف الدليل الرقمي

قد تعددت التعاريف التي قيلت بخصوص الدليل الرقمي وتباينت بين التوسيع والتضييق، ويرجع ذلك إلى البيئة التي ينشأ فيها الدليل الرقمي أو المجال الذي يستخدم فيه هذا الدليل، فقد عرّف الدليل من منظور تقني بحت، وعُرف أيضاً من منظور قانوني مركزاً على إجراءات استخلاصه ومدى اعتماده كوسيلة إثبات لدى مختلف التشريعات، وبشكل عام فقد اعتمد تعريف الدليل الرقمي على الجانب الشكلي دون الإجرائي، وجعل من محل استخلاصه "الحاسب الآلي" أساساً لتعريفه، ومن هذه التعريفات نجد الآتي:

يُعرف على أنه "كل بيانات يمكن إعدادها أو تخزينها في شكل رقمي بحيث تُمكن الحاسوب من إنجاز مهمة ما"^١.

أما المنظمة العالمية لدليل الكمبيوتر (IOCE) فعرفته على أنه "المعلومات ذات القيمة المختلفة والمخزنة أو المنقولة في صورة رقمية"^٢.

^١ عمر أبو بكر يونس، "مرجع سابق"، ص ٩٦٩.

^٢ مصطفى موسى، "مرجع سابق"، ص ٢١٣.

وهناك من عرّفه على أنه "الدليل الذي يجد لنفسه أساساً في العالم الافتراضي ويقود إلى الجريمة"^١. ويعرف أيضاً على أنه "معلومات مخزنة أو منقولة بشكل يمكن قبوله في المحكمة"^٢.

وعرف على أنه "الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال أو الرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون"^٣.

وتعرف الأدلة الرقمية أيضاً على أنها "معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحاسوبية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جانٍ أو مجني عليه"^٤.

ويعرف الدليل الرقمي أيضاً على أنه "الدليل الذي يجد له أساساً في العالم الافتراضي، ويقود إلى الجريمة، وهو ذلك الجزء المؤسس على الاستعانة بتقنية المعلومات، والذي يؤدي إلى إقناع قاضي الموضوع بثبوت ارتكاب شخص ما لجريمة عبر الإنترنت"^٥.

وبناء على ما سبق من تعريفات للدليل الرقمي يمكن لنا تعريف الدليل الرقمي بأنه الدليل المشتق من أو بواسطة النظم البرمجية المعلوماتية للحاسوب، أو شبكات الاتصال من خلال إجراءات قانونية وفنية لتقديمها إلى القضاء بعد تحليلها علمياً باستخدام برامج وتطبيقات خاصة وتفسيرها في شكل نصوص مكتوبة، أو رسومات أو صور أو أشكال وأصوات لإثبات الجريمة، ولتقرير البراءة أو الإدانة.

^١ عمر أبو بكر يونس، "مرجع سابق"، ص ٩٦٩.

^٢ طارق الخن، "مرجع سابق"، ص ٣٤٠.

^٣ أحمد فتحي سرور، "الوسيط في قانون الإجراءات الجنائية"، دار النهضة العربية، القاهرة، ط ٢، ١٩٨١م، ص ٤١٨.

^٤ طارق الخن، "مرجع سابق"، ص ٢٣٤.

^٥ ممدوح عبد المطلب، "البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت"، دار الكتب القانونية، القاهرة، مصر، ٢٠٠٦م، ص ٨٨.

الفرع الثاني: نطاق عمل الدليل الرقمي في الإثبات الجنائي

إن الجرائم المعلوماتية تختلف عن الجرائم التقليدية في طريقة الحصول على الدليل، حيث إن هذه الأخيرة يتم استخلاص الدليل منها بواسطة رجل الشرطة الذي ينتقل إلى مسرح الجريمة ليقوم بوصف كل شيء وصفاً دقيقاً موضعاً مكان الدليل والشكل الذي وجد عليه وكل ما يتعلق به حسبما يشاهده أمامه، ثم يتم تصوير الدليل المادي فوتوغرافياً وكذلك حركياً عن طريق كاميرا الفيديو، وبعدها يتم تحريز الدليل في حرز خاص موضعاً به نوعه ومكان العثور عليه واسم من قام بتحريزه وينقل إلى المختبر الجنائي لاستكمال فحصه وإصدار تقرير فني يوضح به جميع ما يتوصل إليه من نتائج.

كذلك فإن الأمر لا يختلف كثيراً بالنسبة للدليل الرقمي في الجريمة المعلوماتية الذي يمر بمرحلة التحريز ثم التحليل ثم التقديم والعرض، ففي مرحلة التحريز يتم المحافظة على جميع القيم الرقمية بنسخ جميع أجزاء القرص الصلب سواء ما يحتوي منها على معلومات أو الفارغة، لأن الخبير في هذه المرحلة لا يعرف أي المعلومات سيتم استخدامها، وبعدها يتم فحص البيانات التي تم نسخها بتحديد نوعية الدليل، ثم يقدم الدليل ويعرض على المحقق للاستعانة بها في عملية الإثبات.

وقد أشار المشرع البحريني إلى اعتماد إقرار الدليل الرقمي في الجرائم المعلوماتية وقد أكد ذلك حيث وضح من خلالها أن طريقة جمع الأدلة في جرائم تقنية المعلومات قد تكون بصورة إلكترونية إذ يسري ذلك على كافة الجرائم التي وردت في القانون الخاص بجرائم تقنية المعلومات، بالإضافة إلى أن ذلك لم يقتصر على اعتماد الدليل الرقمي فقط على الجرائم المعلوماتية إنما أيضاً يتم اعتماده في أي جريمة إذا تعلق إثباتها إلكترونياً^١.

وهنا قد وفق المشرع البحريني وهذا تأكيداً منه على مشروعية الدليل الرقمي في مجال جرائم تقنية المعلومات وإعمالاً منه لمبدأ حرية الإثبات الذي يأخذ به قانون الإجراءات الجنائية والذي من خلاله يعطي كافة الأطراف في الدعوى بتقديم الأدلة التي من شأنها أن تساعد في الوصول إلى الحقيقة، مع إعطاء القاضي حرية الاقتناع بهذه الأدلة حسب ما يتنامى لديه من قناعة بهذه الأدلة.

ولم ينص كل من المشرع الإماراتي والسعودي في نص صريح على الأخذ بهذا الدليل واقتصر بالإشارة للأخذ بمبدأ حرية الإثبات المستوحى من نصوص قانون الإجراءات الجزائية،

^١ تنص المادة (١١) الفقرة الثالثة من قانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات في مملكة البحرين على: تسري أحكام هذا الفصل على ما يلي: "جمع الأدلة التي تكون في صورة إلكترونية والمتعلقة بأي جريمة.

وهذا ما يعتبر قصور لدى المشرع الإماراتي والسعودي ، حيث يجب أن تتضمن القوانين الخاصة بجرائم تقنية المعلومات لكيفية التي يتم فيها استنتاج الدليل الرقمي والآلية التي يتم من خلالها استخراجها عبر إجراءات التفتيش والضبط والتحفيز والمعاينة.

ومن الملاحظ أن جريمة الاحتيال المعلوماتي بالرغم من شدة صلتها بالدليل الرقمي إلا أن إثباتها لا يقتصر عليه، فمن الممكن أن يتم إثباتها بأدلة الإثبات التقليدية كالشهادة والاعتراف وغيرها^١، ولذلك فإن التلازم بين مشكلة الدليل الرقمي وإثبات جريمة الاحتيال المعلوماتي ليس له فعالية هنا، فجريمة الاحتيال المعلوماتي وإثباتها تثير إشكاليات أخرى لا شأن لها بالدليل الرقمي، فإذا كانت غاية الدليل عموماً هي إثبات الجريمة ونسبتها إلى مرتكبها، فإن هذا الدليل لا يكون قاصراً^٢، لأنه إذا اقتصر على مجرد إثبات وقوع الجريمة دون تحديد مقترفها، إذ مع ذلك تصح تسميته كدليل، وتبدو أهمية هذا النوع من الأدلة بالنسبة لجريمة الاحتيال المعلوماتي لصعوبة إثبات وقوعها عادة^٣.

لذلك فإن تحليل الدليل الرقمي يتطلب التفسير للآثار الالكترونية وتقييمها، وهو يشكل القاعدة الأساسية للاستنتاجات فيما بعد، فيتحمل خبراء التحقيق الإلكتروني أن يقدروا ويصفوا درجة اليقين في استنتاجاتهم لتمكين المحققين فيما بعد من وضع القيمة الحقيقية للدليل الذي تم تقديمه من قبلهم، لأن قوة الدليل تعتمد على خبرة المحققين الذين يعملوا في الغالب تبعاً لمنهجية واحدة، كما أن تعقيد قضايا المعلوماتية وتفرعها يضيفان صعوبة أخرى في الوصول إلى قطعية الدليل^٤.

يتضح أن العلاقة بين نطاق العمل بالدليل الرقمي من جهة وجريمة الاحتيال المعلوماتي من جهة أخرى هي علاقة تلازم، لأن الدليل الرقمي أصبح ضرورة ملحة فرضتها الحاجة من خلال الأدلة التي تنتمي إلى البيئة التي ترتكب فيها.

^١ على محمود حمودة، "الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي"، بحث مقدم ضمن أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، نظمته شرطة دبي، في الفترة من ٤ افريل إلى ٦ افريل عام ٢٠٠٣م، دبي ص ٢٢.

^٢ طارق الجملي، "الدليل الرقمي في مجال الإثبات الجنائي"، ورقة عمل مقدمة للمؤتمر المغاربي الأول للمعلوماتية المنعقد في الفترة (٢٨-٢٩ / أكتوبر ٢٠٠٩) تنظمه أكاديمية الدراسات العليا، طرابلس، ص ٥.

^٣ عفيفي كامل، "جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية" ودور الشرطة والقانون، "مرجع سابق"، ص ٣٤٤.

^٤ فهد العازمي، "مرجع سابق"، ص ٣٧٠.

المطلب الثالث

مدى قبول الأدلة الرقمية كأدلة إثبات جريمة الاحتيال المعلوماتي

يمتاز الدليل الرقمي بخصائص ومميزات تميزه عن سائر الأدلة المادية والعلمية والفنية، فلا شك بأن الدليل الرقمي كلما أحيط بمجموعة من الشروط والضمانات ووسائل التوثيق التي تكفل سلامة المعلومات والبيانات والدلائل المقروءة والمحلاة إلكترونياً المنقولة والمثبتة عبر الوسائل والأجهزة الالكترونية وسلامة ودقة صحة نسبتها إلى صاحبها، يثير مجموعة من المشاكل والصعوبات القانونية المتمثلة حول مدى شمولية الأدلة الرقمية بالقوانين والأنظمة والتشريعات الصادرة بشأن الأدلة المادية الأخرى، وسيتم تقسيم المطلب على النحو الآتي:-

الفرع الأول: شروط قبول الدليل الرقمي.

الفرع الثاني: حجية الأدلة الرقمية.

الفرع الثالث: سلطة القاضي في قبول الأدلة الرقمية.

الفرع الأول: شروط قبول الدليل الرقمي

إن الأدلة المتحصل عليها من الآلة تثير إشكالية عدم قبولها لدى القضاء نتيجة عدم تعبيرها عن الحقيقة نظراً لما يمكن أن تخضع له طرق الحصول عليها من التعرض للتزييف أو التحريف أو الأخطاء المتعددة وسرعة إتلافها أو تغييرها.

لذلك يتعين على القاضي لقبول هذه الأدلة كأساس تستند إليه الحقيقة في الدعوى العمومية سواء أكان الحكم فيها بالإدانة أو بالبراءة بتوافر بعض الشروط أهمها ما يلي:

أولاً: أن تكون الأدلة يقينية.

يجب أن تكون الأدلة يقينية غير قابلة للشك، ويستوجب ذلك الاقتراب من الحقيقة الواقعية قدر المستطاع وأن تبتعد عن الظنون والتخمينات، ووفقاً لذلك يجب أن تكون مخرجات الوسائل الإلكترونية من مخرجات ورقية وإلكترونية أو مخرجات مادية كالأقراص المغنطة أو مصغرات فيلمية أن تخضع لتقدير القاضي الجنائي^١.

^١ فهد العازمي، "مرجع سابق"، ص ٣٨٨.

يبدو من ذلك أن قناعة القاضي تلعب دور أساسي ورئيسي في إصدار الحكم وفقاً لما يجريه من تحقيقات ولا يشاركه في ذلك أحد، ولكن هذه الصفة المطلقة لا تعني أن يأخذ القاضي برأي الخبير متى اقتنع بهذا الرأي ولكن يجب عليه أن يبين أسباب اقتناعه بهذا الرأي وذلك لاعتبار رأي الخبير من الأدلة المقدمة أمامه^١.

وأكدت بعض النصوص القانونية في الولايات المتحدة الأمريكية على أن النسخ المستخرجة من البيانات التي يحتويها الحاسوب تعد من أفضل الأدلة المتاحة للإثبات الجنائي لهذه البيانات، وبالتالي يتحقق مبدأ اليقين لهذه الأدلة، وتنص القواعد الفيدرالية على أن: الشرط الأساسي للتوثيق أو التحقق من صحة أو صدق الدليل، كشرط مسبق لقبوله، هو أن يفي بأمانة أو بيئة كافية لأن تدعم اكتشاف (أو الوصول) إلى الأمور التي تتصل بالموضوع بما يؤيد الادعاءات أو المطالبة المدعى بها^٢.

ويشترط القانون الفرنسي في المخرجات الإلكترونية أن تكون يقينية حتى يمكن الحكم من الإدانة ذلك أنه لا محل لدحض قرينة البراءة وافترض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين^٣.

ثانياً: مناقشة الأدلة الرقمية

يتعين مناقشة الدليل الرقمي تطبيقاً لمبدأ شفوية المرافعة، فإذا كانت مخرجات الوسائل الإلكترونية تعد أدلة إثبات قائمة في أوراق الدعوى في جريمة الاحتيال المعلوماتي، فإنه يجب مناقشتها أمام الحضور، ويترتب على ذلك أن هذه المخرجات سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسوب، أم كانت بيانات مدرجة في حاملات، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية، تكون محلاً للمناقشة عند الاعتماد عليها كأدلة إثبات أمام المحكمة^٤، وبناءً على ذلك يجب أن يتم مناقشة الدليل الرقمي بحضور كافة الخصوم، ويجب على الخبير أن يقوم بقراءة تقريره أمام الحضور وذلك إعمالاً لقاعدة أن القاضي لا يمكن

^١ أحمد هاللي، "مرجع سابق"، ص ١١٥.

^٢ سعيد عبد اللطيف حسن، "إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت"، دار النهضة العربية، القاهرة، ط ١، ١٩٩٩م، ص ١٥٩.

^٣ المادة (٤٢٧) من قانون الإجراءات الجنائية الفرنسي.

^٤ أحمد هاللي، "مرجع سابق"، ص ٢٣.

أن يبني حكمه إلا بناءً على ما توافر من أدلة في القضية، كما يجب على القاضي أن يقوم بمناقشة الخبر الصادر عنه التقرير^١.

إن الأدلة التي يتم الحصول عليها من خلال بيئة تكنولوجيا المعلومات يجب أن تعرض في الجلسة وذلك بصفة مباشرة أمام القاضي، كذلك الشهود يجب أن يعيدوا أقوالهم أمام المحكمة، والخبراء في مجال التقنية المعلوماتية باختلاف تخصصاتهم أيضاً^٢.

وللقاضي أن يبني حكمه على الأدلة التي وردت في التحقيقات الأولية طالما كان الدليل أو الإقرار المطروح أمام المحكمة تمت مناقشته في جلسات سابقة واهتدى القاضي إلى اقتناعه به وكان مدون في محضر التحقيق حتى دون أن يسمعه، فالقاضي غير ملزم بتسبيب طرحه لبعض الأدلة أو الأخذ ببعضها الآخر^٣.

ثالثاً: مشروعية الأدلة الرقمية.

الإدانة في أي جريمة لا بد أن تكون مبنية على أدلة مشروعة وتم الحصول عليها وفق قواعد الأخلاق والنزاهة واحترام القانون، ويجب أن تكون الأدلة الرقمية قد تم الحصول عليها من الوسائل الإلكترونية بصورة مشروعة وغير مخالفة لأحكام الدستور ولا القانون.

فمبدأ المشروعية في الدليل الرقمي تتطلب ضرورة صحة إجراءات الحصول على هذه المخرجات بما يتفق مع القواعد القانونية والأنظمة الثابتة في وجدان المجتمع المتحضر، فمشروعية الدليل الرقمي تتطلب صدقه في مضمونه، وعلى ذلك يجب أن تكون إجراءات جمع الأدلة المستخرجة من البيئة الإلكترونية ضمن الإطار العام الذي حدده القانون وإلا فإن الدليل المستمد بطريق مخالف للأحكام الواردة في الدستور يكون باطلاً بطلاناً مطلقاً لتعلقه بالنظام العام، ويجوز لكل ذي مصلحة التمسك به كما أن للمحكمة أن تقضي به من تلقاء نفسها، فإذا شاب البطلان القواعد الإجرائية التي تنظم كيفية الحصول عليها، فإنها باطلة ولا تصلح لأن تكون أدلة تبني عليها الإدانة في المواد الجنائية^٤.

^١ محمد فهمي طلبة، "فيروسات الحاسب الآلي وأمن البيانات"، مطابع الكتاب المصري الحديث، القاهرة، ١٩٩٢م، ص ٣١.

^٢ محمد فهمي طلبة، "مرجع سابق"، ص ١٩.

^٣ هلاي أحمد، "مرجع سابق"، ص ١٠٩.

^٤ هلاي أحمد، "مرجع سابق"، ص ١٢١.

فلا يحكم القاضي بناءً على معلوماته الشخصية، أو على ما رآه بنفسه، فعقيدة القاضي واقتناعه بالإدانة يجب أن تستمد من مخرجات الحاسب الآلي، وذلك إعمالاً للقاعدة القانونية والتي مفادها ألا يحكم القاضي إلا بناءً على التحقيقات^١، كما أنه لا يجب على القاضي أن يحكم بناءً على إجراء شابه البطلان كدليل ناتج من الحاسب الآلي^٢.

الفرع الثاني: حجية الأدلة الرقمية

الحجية تعني الوصف الثابت بحكم الشرع يلحق مضمون الحكم القضائي أو الأمر القضائي فيه ويكون غير قابل للمناقشة فيه مرة أخرى^٣.

ومعنى الحجية عند فقهاء القانون "هي حجية الشيء المحكوم فيه أو عدم نقضه، وهو أن القاضي إذا عرضت منازعه أمامه في موضوع ما وتنازع الخصوم فيه، وفحص القاضي أدلة كل خصم ومستنداته ووزنها، وثم قال كلمته الفاصلة في موضوع هذه الدعوى فلا يجوز لأي من الخصوم أن يعيدوا عرض النزاع ثانية لمناقشة ما سبق الفصل فيه^٤.

وقد اختلفت الأنظمة المقارنة في تقديرها لحجية الدليل الرقمي، ومصدر هذا الاختلاف مرتبط بتنوع أنظمة الإثبات الجنائي في الأنظمة المقارنة، فالدول التي تأخذ بمبدأ حرية الإثبات وحرية القاضي في تقدير الأدلة، لا تثار لديها إشكالية تتعلق بمدى قبول الأدلة الرقمية في الإثبات الجنائي، إذ أنها تقوم في الأساس على حرية القاضي وأطراف الدعوى في تقديم ما لديهم من أدلة، وهذا هو المبدأ في النظام اللاتيني في معظم دول أوروبا والدول العربية^٥.

فقد نص قانون الإجراءات الجنائية الفرنسي في المادة (٤٢٧) على أن "المالم يرد نص مخالف، جواز إثبات الجرائم بجميع طرق الإثبات ويحكم القاضي بناءً على اقتناعه الشخصي"^٦.

^١ مأمون سلامة، "مرجع سابق"، ص ٧٣٢.

^٢ مأمون سلامة، "مرجع سابق"، ص ٧٣٢.

^٣ هدى قشقوش، "مرجع سابق"، ص ٧١.

^٤ حسن الحمادي، "عقود وخدمات المعلومات، دراسة في القانون المصري والفرنسي"، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط١، ٢٠٠٣، ص ٧١.

^٥ فهد العازمي، "مرجع سابق"، ص ٤٠١.

^٦ خالد العتيبي، "الجوانب الإجرائية في الجرائم المعلوماتية: دراسة مقارنة"، مكتبة القانون والاقتصاد، الرياض، ص ١٤٩.

وأشار المشرع المصري في قانون الإجراءات الجنائية بنص المادة (٢٩١) إلى الأخذ بمبدأ حرية الإثبات والتي جاء فيها "للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازماً لظهور الحقيقة"^١.

أما الأنظمة التي تأخذ بنظام الإثبات المختلط القائم في تحديد القانون للأدلة المقبولة في الإثبات الجنائي فهي تترك للقاضي في نطاق الأدلة حرية التقدير، كالقانون الياباني الذي حصر طرق الإثبات المقبولة في أقوال المتهم، وأقوال الشهود، والقرائن، والخبرة، وأيضاً المشرع التشيلي الذي حصر طرق الإثبات في شهادة الشهود، وتقارير الخبراء، والمعاينة والمستندات الرسمية والعرفية، والاعتراف، والأدلة الظرفية، فإنه في ظل هذا التحديد يمكن أن يكون الدليل الرقمي مقبولاً في مجال الإثبات الجنائي وذلك استناداً إلى تقرير خبير يقدمه بشأن الدليل الرقمي^٢.

فبالنظر إلى الدليل الرقمي في الأنظمة التي تأخذ بالنظام المختلط متاح، ويتوقف ذلك على دور الفقه في إعمال الدليل الرقمي، حيث يشترط في هذه الأنظمة أن يتم إخراج الدليل الرقمي في صورة مادية ليتسنى اعتماده وتوثيقه والأخذ به في المحكمة، فالسجلات الإلكترونية مغناطيسية يمكن استخدامها كدليل إذا ما تم تحويلها إلى صورة مرئية ومقروءة عن طريق طباعة هذه السجلات وهذا ما أخذ به المشرع الياباني، وأيضاً يمكن أن يكون الدليل الرقمي مقبولاً في المحكمة كدليل كتابي أو مستندي بعد طباعته^٣.

وفي الدول التي تأخذ بالنظام المقيد كنظام معتمد في المسائل الجنائية، والتي يحدد فيها المشرع أدلة الإثبات التي يجب على القاضي أن يتقيد فيها ويقدر قيمتها، فإن اعتماد الأدلة الرقمية في هذه النظام يتطلب أن يتدخل المشرع^٤.

فقد ذهب المشرع البريطاني إلى إقرار قانون الشرطة والإثبات الجنائي لسنة ١٩٨٤م والذي حدد فيه قبول مخرجات الحاسوب والإنترنت كأدلة إثبات في المواد الجنائية. وفي الولايات المتحدة الأمريكية تناولت بعض القوانين حجية الدليل الرقمي والذي نص عليه قانون الحاسوب لعام ١٩٨٤م الصادر في ولاية (إيوا)، والذي جاي فيه أن مخرجات الحاسوب تكون مقبولة بوصفها أدلة إثبات بالنسبة للبرامج والبيانات المخزنة فيه (المادة ١٦/٧١٦/١٦)، وأيضاً قانون

^١ قانون الإجراءات الجنائية المصري، قانون رقم (٩٥)، لسنة ٢٠٠٣.

^٢ عفيفي كامل عفيفي، "مرجع سابق"، ص ٣٧٣. أنظر أيضاً: هلاي أحمد، "مرجع سابق"، ص ٦٤.

^٣ عائشة بن قارة، "حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن"، دار الجامعية الجديدة، ٢٠١٠، ص ١٨٠.

^٤ فهد العازمي، "مرجع سابق"، ص ٤٠٤.

الإثبات الصادر عام ١٩٨٣م في ولاية كاليفورنيا وجاء فيه أن النسخ المستخرجة من البيانات التي يحتويها الحاسوب تكون مقبولة بوصفها أفضل الأدلة المتاحة لإثبات هذه البيانات^١.

وذهبت التشريعات محل المقارنة كالتشريع البحريني والإماراتي والسعودي في موضوع حجة الأدلة الرقمية كإثبات إلى اعطاء سلطة للقاضي مطلق الحرية في أن يصل إلى الحقيقة من أي دليل قانوني مهما كان نوعه، ويأخذ من الأدلة ما يراه مناسب ويقتنع به؟

الفرع الثالث: سلطة القاضي في قبول الأدلة الرقمية

تحدد سلطة القاضي الجنائي في قبول الدليل الرقمي حسب طبيعة نظام الإثبات السائد، ومع تطور دور الإثبات العلمي مع ظهور الدليل الرقمي جعل القاضي يضطر للتعامل مع الأدلة المستحدثة بغية اكتشاف الجرائم، ونتيجة لذلك فإن القاضي غير مقيد بالأدلة التي يقدمها أطراف الدعوى لأن من حقه أن يبادر بنفسه لاتخاذ جميع الإجراءات بحثاً عن الأدلة اللازمة لتكوين قناعته، وفي سبيل ذلك له أن يوجه أوامر إلى مزود خدمة الإنترنت من أجل جمع الأدلة الرقمية كعناوين المواقع التي اطلع عليها المتهم، والحوارات التي شارك فيها، والرسائل التي أرسلها واستقبلها، كما له أن يأمر مشغل النظام بتقدير المعلومات اللازمة لاختراق النظام والولوج إلى داخله، كالإفصاح عن الكلمات السرية والشفرات الخاصة بتشغيل البرامج المختلفة، وله أن يأمر بتفتيش الحاسب الآلي^٢.

وللقاضي الجنائي التحقق وفق التشريعات من قبول الدليل الرقمي ومدى صحته ومصداقيته، فالقاعدة السائدة في التشريعات الجزائية فيما يتعلق بالإثبات أن للقاضي الحرية الكاملة في الاقتناع بما يقدم لديه من أدلة في أي مرحلة من مراحل التحقيق والمحاكمة^٣، هذا ما نصت عليه المادة (٤٢٧) من قانون الإجراءات الفرنسي رقم (٩٤-٦٥٣) لعام ١٩٩٤م، ولكن هذه الحرية في الاقتناع ليست على إطلاقها إذ على القاضي أن يقوم بتبرير استبعاده لأدلة والأخذ بأدلة بعينها، وعليه يكون للقاضي كامل الحرية في تقدير الأدلة المعروضة أمامه في الدعوى وله أن يفاضل بين جميع الأدلة فيأخذ بما يطمئن إليه من أدلة ويستبعد عما لا يطمئن إليه من أدلة أخرى^٤.

^١ هلاي أحمد، "مرجع سابق"، ص ٥٧.

^٢ عائشة بن قارة، "مرجع سابق"، ص ١٩٤.

^٣ خالد العتيبي، "مرجع سابق"، ص ١٥٠.

^٤ هلاي أحمد، "مرجع سابق"، ص ٥٥-٧٥.

وللقاضي الجنائي له الحرية في تقدير جمع أدلة الدعوى الجنائية بغض النظر عن مصدرها الذي استمدت منه طالما كانت مشروعة ويستوي في ذلك الدليل الجنائي التقليدي والدليل الرقمي، فباب الإثبات مفتوح أمام القاضي حيث يأخذ بالدليل الذي يطمئن له وجدانه ويستبعد الدليل الذي يدور حوله الشك^١.

كما يجب أن تكون عقيدة القاضي واقتناعه بالأدلة الرقمية قد استمدت من مخرجات إلكترونية طرحت بالجلسة لأن القاعدة هي ألا يحكم القاضي إلا بناءً على التحقيقات التي تحصل بالطرق والشروط القانونية وليس بناءً على معلوماته الشخصية أو على ما قد رآه بنفسه أو حقيقة في غير مجلس القضاء كما ينبغي أن يؤسس القاضي حكمه على دليل ناتج من الحاسب الآلي^٢.

إن الأدلة الرقمية تخضع لحرية القاضي في الاقتناع الذاتي، بحيث يمكن أن يطرح مثل هذه الأدلة - رغم قطعيتها من الناحية العلمية - عندما يجد أن الدليل الرقمي لا يتسق منطقياً مع ظروف الواقعة وملابساتها^٣.

والقاضي الجنائي له مطلق الحرية في أن يصل إلى الحقيقة من أي دليل قانوني مهما كان نوعه، بما في ذلك الدليل الرقمي الذي يعد من قبيل القرائن: إلا أنه يشترط في هذا الدليل أن يتوفر فيه ما يلي^٤:

١- القيمة العلمية القاطعة للدليل.

٢- الظروف والملابسات التي وجد فيها الدليل.

حيث أن القاضي لا يتناول في تقديره إلا للأدلة العلمية القاطعة، والدليل الرقمي يقوم على أسس علمية دقيقة، ولا يمكن للقاضي مناقشة الحقائق العلمية الثابتة.

^١ عفيفي كامل عفيفي، "مرجع سابق"، ص ٣٧٤.

^٢ اشد البلوشي، ورقة عمل حول الدليل في الجرائم المعلوماتية مقدمة إلى المؤتمر الدولي حول "حماية المعلومات والخصوصية في قانون الإنترنت"، برعاية الجمعية الدولية لمكافحة الإجرام السيبراني بفرنسا، القاهرة، ٢٠٠٨م، ص ٣٥.

^٣ على الطوالبة، "مرجع سابق"، ص ٢٠١.

^٤ للمزيد أنظر، على الطوالبة، "مرجع سابق"، ص ٢٠٢.

وفيما يتعلق بالظروف والملابسات التي وجد فيها الدليل، فإنها تدخل في نطاق تقديره الشخصي لأنها من طبيعة عمله، فللقاضي الجزائي أن يطرح الدليل المستخرج من الحاسوب عندما يجد أن وجوده لا يتفق منطقياً مع ظروف الواقعة، فمجرد توفر الدليل العلمي لا يعني أن يحكم القاضي مباشرة، دون البحث بالظروف والملابسات^١.

وقد أعطى المشرع البحريني الحق للقاضي بأن يحكم في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته^٢.

ووافقه المشرع الإماراتي إذ أعطى للقاضي الحرية في الاقتناع والأخذ بأي دليل طرح أمامه في الدعوى لينتقي منها حسب العقيدة التي تكونت^٣.

وقد تبنى المشرع السعودي مبدأ حرية القاضي بالاقتناع وبالحكم في الدعوى وأن ينتقي من الأدلة ما يراه مناسباً^٤.

ويرى الباحث أن التشريعات المقارنة اعطت للقاضي الحق في أن يستمد قناعته من أي دليل يطمئن إليه ما لم ينص القانون على غير ذلك، فالسلطة الواسعة التي أقرها القانون للقاضي الجنائي تخوله بأن يأخذ من الأدلة ما تطمأن لها عقيدته وترتاح لها قناعته.

^١ هلاي أحمد، "مرجع سابق"، ص ٤٧.

^٢ تنص المادة على (٢٥٣) من قانون جرائم تقنية المعلومات البحريني على "يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته...".

^٣ نص المادة (٢٠٩) من القانون الاتحادي رقم (٢) لسنة ٢٠٠٦ على "يحكم القاضي حسب القناعة التي تكونت لديه...".

^٤ تنص المادة (١٩٧) من نظام مكافحة جرائم المعلوماتية السعودي على "تستند المحكمة في حكمها إلى الأدلة المقدمة إليها أثناء نظر القضية، ولا يجوز للقاضي أن يقضي بعلمه ولا بما يخالف علمه.

المبحث الثالث

الجهود الدولية والوطنية لمواجهة جريمة الاحتيال باستخدام وسائل تقنية المعلومات

إن مكافحة جريمة الاحتيال المعلوماتي على وجه الخصوص والجرائم المعلوماتية بشكل عام، يستوجب أن يكون في المجال الدولي والوطني، إذ لن يكون له أي تأثير يذكر إلا إذا كان هناك تعاوناً ودولياً ووطنياً على أكبر قدر من التنسيق والتعاون، وعليه يمكننا القول إن أي مجهود أو إجراءات قد تقوم بها أيًا من الدول على مستوى العالم لن يأتي بأي نتائج ملموسة تحد من ارتكاب تلك النوعية من الجرائم، فتلك الجرائم لها طابع خاص تتسم به هو أنها (جرائم عابرة للحدود)، فقد ترتكب جريمة الاحتيال المعلوماتي داخل الدولة ولكن آثارها لا تتحصر داخل هذا الإقليم، ومن ثم تمتد آثارها إلى إقليم دول أخرى مما يستوجب التنسيق والتعاون بين كافة الدول للحيلولة دون انتشار هذه الجرائم ومكافحتها، إذا قد تنامي لدى الأسرة الدولية ضرورة مواجهة هذه الجرائم لما لها من خطر يطل كافة قطاعات الدولة الاقتصادية منها والأمنية.

وبناءً عليه فإن التعاون والتضامن الوطني والدولي أمر هام جداً في مجال مكافحة جرائم الإنترنت وبدون هذا التعاون الوطني والدولي لن يكون هناك أي أثر لأي مجهود تقوم به أي من الدول بمفردها نظراً لأنه سيكون عديم الفائدة وبلا أثر تقريباً ولن يؤد إلى الحد من ارتكاب تلك الجرائم المسماة بالجرائم "العابرة للحدود" وعليه فسوف يكون تناولنا لمكافحة الجرائم المعلوماتية من خلال التركيز على التعاون الوطني والدولي والعناصر الذي يركز عليها هذا التعاون. وسيتم تقسيم هذا المبحث إلى ثلاث مطالب على النحو الآتي:-

المطلب الأول: مكافحة جريمة الاحتيال المعلوماتي على المستوى الدولي.

المطلب الثاني: مكافحة جريمة الاحتيال المعلوماتي على المستوى الوطني لدول المقارنة.

المطلب الثالث: صعوبات مكافحة جريمة الاحتيال المعلوماتي على المستوى الدولي والوطني.

المطلب الأول

مكافحة جريمة الاحتيال المعلوماتي على المستوى الدولي

إن التطور العلمي في المجال التقني واستحداث وسائل تقنية المعلومات وما يطرأ على هذه الوسائل من تطور أفرز لدى المجتمعات نوع جديد من الجرائم نتيجة إساءة استخدام هذه الوسائل، فعلى الصعيد الأمني يجب التعاون الدولي، حيث لكي يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدر من الأمن والنظام، وتشكل الجريمة إحدى القضايا الرئيسية في الكثير من دول العالم، وتشغل بال الحكومات والمختصين والأفراد على حد سواء، ولقد أثبت الواقع العملي أن الدولة - أي دولة - لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس لكافة ميادين الحياة^١.

وقد يحدث أن ترتكب جريمة في إقليم دولة معينة ويكون مرتكب هذه الجريمة أجنبياً، وتخضع هذه الجريمة للاختصاص الجنائي للدولة الأولى استناداً إلى مبدأ الإقليمية، وتخضع كذلك اختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبه الإيجابي، وقد تكون الجريمة المرتكبة على إقليم الدولة من الجرائم التي تهدد أمن وسلامة دولة أخرى، فتخضع للاختصاص الجنائي الإقليمي من جهة، كما تخضع للاختصاص الدولة المجني عليها استناداً إلى مبدأ الاختصاص العيني من جهة أخرى، كما تثار أيضاً فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية، كما لو قام الجاني ببيث المعلومات الغير مشروعة أو الصور الإباحية من إقليم دولة معينة وتم الاطلاع عليها في دولة أخرى^٢.

فوفقاً لمبدأ الإقليمية فإن الاختصاص الجنائي والقضائي يثبت لكل دولة من الدول التي مستها الجريمة، سواء تلك التي وقع فيها الفعل الإجرامي "فعل البث" أو تلك التي حدثت نتيجة الفعل فيها "تلقي الصور غير المشروعة" الأمر الذي أطاح بمبدأ عدم جواز محاكمة الشخص عن الفعل الواحد أكثر من مرة، وهو أحد المبادئ الأساسية التي يقوم عليها القانون الجنائي^٣.

^١ عمر ابو بكر يونس، "مرجع سابق"، ص ٣٧٠.

^٢ عمر ابو بكر يونس، "مرجع سابق"، ص ٣٧١.

^٣ منير محمد الجنيهي، "جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها"، دار الفكر الجامعي، ٢٠٠٦م، ص ٥١٠.

وسنتناول الجهود الدولية لجريمة الاحتيال المعلوماتي من خلال ما يلي:

الفرع الأول: التعاون الشرطي الدولي.

الفرع الثاني: التعاون القضائي الدولي.

الفرع الثالث: الاتفاقيات والمعاهدات الدولية في مجال مكافحة جرائم الإنترنت.

الفرع الأول: التعاون الشرطي الدولي

البدايات الأولية للتعاون الدولي الشرطي ترجع إلى عام ١٩٠٤ عندما تم إبرام الاتفاقية الدولية الخاصة بمكافحة الرقيق الأبيض بتاريخ ١٨ / ٥ / ١٩٠٤ والتي نصت في مادتها الأولى على، تعهد كل الحكومات المتعاقدة بإنشاء أو تعيين سلطة لجمع المعلومات الخاصة باستخدام النساء والفتيات لغرض الدعارة في الخارج، ولهذه السلطة الحق في أن تخاطب مباشرة الإدارة المماثلة لها في كل الدول الأطراف المتعاقدة، بعد ذلك أخذ التعاون الشرطي الدولي بأخذ صورة المؤتمرات الدولية، أولها وأسبقها تاريخياً كان مؤتمر موناكو "١٤ - ١٨ / ٤ / ١٩١٤م" والذي ضم رجال الشرطة والقضاء والقانون من (١٤) دولة، وذلك لمناقشة ووضع أسس التعاون الدولي في بعض المسائل الشرطية، خاصة فيما يتعلق بمدى إمكانية إنشاء مكتب دولي للتسجيل الجنائي وتنسيق إجراءات تسليم المجرمين، إلا أنه ونتيجة للحرب العالمية الأولى لم يحقق المؤتمر أي نتائج عملية تذكر^١.

يجب تدعيم التعاون بين سلطات البوليس في الدول المختلفة بناء على اتفاقيات دولية، حيث يستهدف ذلك تأكيد وتشجيع التعاون بين سلطات البوليس في الدول الأطراف على نحو فعال يحقق مكافحة الجريمة، وذلك بتجميع بيانات ومعلومات متعلقة بالمجرم المعلوماتي والجريمة من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنضمة، وتبادل المعلومات والبيانات فيما بينها، والتعاون في ضبط المجرمين بمساعدة أجهزة الشرطة الوطنية في الدول الأطراف ومدها بالمعلومات المتوفرة لديها على إقليمها^٢.

^١ كوثر مازوني، "الشبكة الرقمية وعلاقتها بالملكية الفكرية"، دار الجامعة الجديدة، طبعة ٢٠٠٨م، ص ٦١٠-٦١١.

^٢ هدى قشقوش، "مرجع سابق"، ص ٨٢-٨٣.

أي أن عضو الانتربول لا يقوم بنفسه بإجراء القبض على المتهم، بل أن هذا العمل منوط بجهاز الشرطة الوطنية في الدولة التي يتواجد المجرم في إقليمها، الأمر الذي يؤكد على احترام مبدأ السيادة الوطني^١.

تبدل الشرطة جهود في الدول المتقدمة في مكافحة الجرائم المعلوماتية وتحاول جاهدة تطوير أدائها لملاحقة التطور في تلك الجرائم على درجة عالية من التقنية، ومن هذه الدول الولايات المتحدة، والسويد، ودول الاتحاد الأوروبي^٢.

وتعد الولايات المتحدة الأمريكية من أولى الدول التي واجهت الجرائم المعلوماتية، وذلك بالنص على مواجهتها تشريعياً بإنشاء إدارة متخصصة لمتابعة الجرائم المعلوماتية بمكتب التحقيقات الفيدرالية (F.B.I)، والذي يضم بداخله مجموعة من الأشخاص المدربين على كيفية متابعة تلك الجرائم والتحري عنها وضبطها والمحافظة على ما يتم تحصيله من أدلة.

فكان أسلوب عمل إدارة مكافحة جرائم المعلومات في الـ (F.B.I) كالتالي:

١- منذ تلقي الأخطار بوقوع الجريمة، يتم الانتقال إلى مكان ارتكاب الجريمة، ثم يتم الحصول على كافة المعلومات عن أسلوب العمل، والتي تفيد في كشف الجريمة وتحديد مرتكبها.

٢- يقوم الفريق المكلف بالبحث والتحري بتنظيم العمل داخله من خلال:

أ- تنظيم عملية الاتصال بين الأعضاء المختلفين للفريق، ويتم وضع خطة بحثية مكتوبة توضح دور كل فرد في الفريق وكيفية التنسيق بينهم.

ب- يقوم الفريق بعملية البحث في الأنواع المختلفة من السجلات والتسجيل والتي لها صلة بالقضية، والتي تتضمن بعض المعلومات الهامة.

٣- يتم الاستعانة بعملية المراقبة لتحديد الشخص المشتبه به سواء كان من داخل المؤسسة أو المنشأة.

٤- يتم تصوير الأرقام المسلسلة للأجهزة وأرقام النموذج ومخطط بيان التوصيلات^٤.

^١ كوثر مازوني، "مرجع سابق"، ص ٣٥١.

^٢ فهد العازمي، "مرجع سابق"، ص ٥٥٦.

^٣ فهد العازمي، "مرجع سابق"، ص ٥٦٠.

^٤ منير الجنبهي، "مرجع سابق"، ص ٦٢٠.

- ٥- يتم تسجيل كافة المعلومات المسلسلة للأجهزة وأرقام النموذج التي تم العثور عليها في أي من الوسائط المتعددة أو وحدات التسجيل الداخلية عند بداية ونهاية التحريات، لإثبات عدم حدوث أي تلف لأي دولة.
- ٦- يتم تصوير كافة ما تعرضه شاشات الكمبيوتر.
- ٧- يتم التمييز بين كافة الأدلة بحيث يمكن تجميع كافة كابلات الأجهزة الأخرى.
- ٨- يتم تدوين وتسجيل كافة الوسائط المتعددة التي يتم العثور عليها في موقع ارتكاب الجريمة.

وفي أعقاب أحداث الحادي عشر من سبتمبر ٢٠٠١، بدأ مكتب التحقيقات الفيدرالي في فتح آفاق جديدة تمكنه من مراقبة الاتصالات الإلكترونية، لذلك فقد طلب مكتب الـ (F.B.I) من الشركات تغيير أنظمتها لزيادة دقة عمليات التضييق، وإعطاء مساحة واسعة من الحرية لمراقبة الاتصالات الصوتية المرسلة عبر شبكة الإنترنت، مع تأكيد إدارة الشرطة الأمريكية بأنها سوف تحرص دائماً على أن تكون التدخلات عند حالة الطوارئ فقط^١.

الفرع الثاني: التعاون القضائي الدولي

يلعب القضاء في أي دولة دوراً هاماً في مواجهة حالات التعدي الآثم الماس بمصالح المجتمع وأفراده على حد سواء وذلك من خلال تطبيق القوانين وتفسيرها بما يتفق مع الغاية من سنّها والمصالح التي تبقى حمايتها، فمن الرؤى البعيدة تصور أن يكون للقضاء دوراً وقائياً مشابهاً لدور الشرطة في مكافحة الجرائم إلا أنه في الواقع يلعب دوراً هاماً في ردع كل من تسول له نفسه في الاعتداء على المصالح الاجتماعية والاقتصادية محل الحماية القانونية^٢.

ومما لا شك فيه أن القاضي الجنائي يلعب دوراً هاماً من خلال دوره في محور التقدم التقني وما ينتج عنه باعتباره متفهم جيداً لدوره ولما يملكه من سلطة أوسع من نظيره في القضاء المدني حيث أن الحماية القانونية لن تأتي إلا من خلال قاضي قادر على إدراك ذلك وخاصة مع

^١ محمد عبيد الكعبي، "الجرائم الناشئة عن الاستخدام الغير مشروع بشبكة الإنترنت"، دار النهضة العربية، الطبعة الثانية، ٢٠٠٩م، ص ٥٩١.

^٢ سليمان أحمد فضل، "مرجع سابق"، ص ٤٢٠.

صدور قوانين خاصة تتطلب الإلمام ببعض المعرفة الفنية وأنظمتها وما يستخدم في هذا المجال^١.

وتكمن الصعوبة في الجرائم التي يستخدم فيها الحاسب في مسألتين هامتين:

تتمثل الأولى في تقييم أدلة الجريمة بواسطة قاضي جنائي في ضوء أنظمة الإثبات السائدة.

والثانية: تتمثل في التكيف القانوني للأفعال المستحدثة بواسطة التشريعات التجريبية الحديثة والخاصة بهذه الجرائم والتي تختلف كثيراً عن نظيرتها في المجال التقليدي^٢.

إن التعاون القضائي الدولي يوفق بين الدول واستقلال كل دولة في ممارسة اختصاصها الجنائي على حدود إقليمها، وبين ضرورة ممارسة حقها في العقاب وبدون هذا التعاون فلا يمكن للدولة من الناحية العملية إقرار حقها في العقاب، ومن هنا فإن التعاون الدولي تحتّمه الضرورة العملية لسببين:

الأول: تقييد سلطات الدولة بحدود إقليمها، فقانون العقوبات يمكنه التصدي في نطاق تطبيقه ما لا يتجاوز حدود إقليم الدولة، إلا أنه لا يمكنه مباشرة الإجراءات خارج حدود الدولة للإقليم الوطني لها وفقاً لمبدأ سيادة الدولة الأجنبية الأخرى^٣.

الثاني: لا يمكن تطبيق قانون العقوبات بدون قانون إجراءات جنائية^٤.

الفرع الثالث: الاتفاقيات والمعاهدات الدولية في مجال مكافحة جرائم الإنترنت

مكافحة الجرائم المعلوماتية لن يكون له تأثير يذكر إلا إذا كان هناك تعاوناً دولياً على أكبر قدر من التنسيق والتعاون، وعليه يمكن القول بأن أي مجهود أو إجراءات لأي من الدول على مستوى العالم لن يأتِ بأي نتائج ملموسة تحد من ارتكاب تلك النوعية من الجرائم إلا من خلال تعزيز التعاون على المستوى الدولي^٥.

^١ حسين بن سعيد الغافري، "السياسة الجنائية في مواجهة جرائم الإنترنت"، دار النهضة العربية، القاهرة، ٢٠٠٩م، ص ٦٤٣.

^٢ فتوح الشاذلي، "جرائم الكمبيوتر"، منشورات الحلبي، ٢٠٠٣م، ص ٣٤٩.

^٣ هدى قشقوش، "مرجع سابق"، ص ٨٧.

^٤ هلاي أحمد، "مرجع سابق"، ص ٥٢١.

^٥ سليمان فضل، "مرجع سابق"، ص ٥١٢.

والاتفاقيات الدولية هي وحدها الأداة التي يمكن أن تتبع عنها الالتزامات بين الدول، من ثم فإنه بدون الاتفاقية الدولية وخارج الشروط التي تنص عليها لا يمكن للدولة أن تعتمد على مساعدة الدولة المطلوب منها، على أن كل ما كان ملزماً يظل مع ذلك ممكناً وفقاً لما ينص عليه القانون الداخلي في كلا من الدولتين^١.

إن المعاهدات الدولية هي الأساس الذي يركز عليه التعاون الدولي في مجال مكافحة الجرائم المعلوماتية، وقد تم عقد العديد من المعاهدات الدولية التي تعمل على التعاون في مجال مكافحة الجرائم المعلوماتية. ومن هذه المعاهدات:

أولاً: معاهدة بودابست لمكافحة جرائم الإنترنت

ثانياً: توصيات المجلس الأوروبي بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات^٢.

أولاً: معاهدة بودابست لمكافحة جرائم الإنترنت.

شهدت العاصمة المجرية بودابست في ٢٣/١١/٢٠٠١م ميلاد أولى المعاهدات الدولية التي تكافح جرائم الإنترنت "internet crimes" وتبلور التعاون والتضامن الدولي في محاربتها ومحاولة الحد منها خاصة بعد أن وصلت تلك الجرائم إلى حد خطير أصبح يهدد الأشخاص والممتلكات، ويُعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال تكوين تضامن دولي مناهض لتلك الجرائم التي تتم عبر شبكة الإنترنت واستخدامها سيء^٣.

وبناءً عليه، فقد وقعت تلك المعاهدة ٢٦ دولة أوروبية بالإضافة إلى كندا وجنوب أفريقيا والولايات المتحدة الأمريكية. وللمعاهدة أهمية كبيرة في توفير أسس الأمن العام، فبعد التوقيع على تلك المعاهدة دولياً والتي تهدف إلى توحيد الجهود الدولية في مجال مكافحة جرائم الإنترنت "internet crimes" انتقلت من مرحلة ابتدائية كانت تتمثل في محاولات التسلل البريئة التي كان يقوم بها الهواة في الأغلب الأعم من الحالات ودون أي فرض إجرامي إلى مرحلة

^١ عفيفي كامل عفيفي، "مرجع سابق"، ص ٢٨٦.

^٢ منير الجنيبي، "مرجع سابق"، ص ٥٣١.

^٣ كوثر مازوني، "مرجع سابق"، ص ٦٤٠.

جديدة يقوم بها محترفون على أعلى درجة من التخصص وتتمثل في الاحتيال والاختلاس وجرائم تهديد الحياة وهي قضايا تعرض حياة وممتلكات الكثير من رواد شبكة الإنترنت للخطر^١.

إن الخلاف الوحيد بين الدول الموقعة على الاتفاقية هو مجال محاربة العنصرية فالدول الأوروبية تعتبر أن التحريض على الكراهية العنصرية هي جريمة، ومن المعروف أن هذه الجريمة يعاقب عليها القانون الدولي، وبالتالي فلا بد أن تنص الاتفاقية على لزوم العمل على إزالة تلك المواقع التي تعمل على التحريض على الكراهية العنصرية، ومسألة القائمين عليها على أساس أنهم يرتكبون جريمة يعاقب عليها القانون الأوروبي^٢.

تناولت معاهدة بودابست الجرائم التي تعتبر من أكثر الجرائم انتشاراً على مستوى العالم مثل الإرهاب الإلكتروني، وتزوير بطاقات الإئتمان ودعارة الأطفال، كما حددت المعاهدة أفضل الطرق الواجب اتباعها في التحقيق في جرائم الإنترنت، وتعاهدت الدول الموقعة بالتعاون الوثيق من أجل محاربتها، كما تحاول إقامة توازن بين الاقتراحات التي تقدمت إلى أجهزة الشرطة والقلق الذي عبرت عنه المنظمات المدافعة على حقوق الإنسان، والصناعات المعينة ومزودي خدمات الإنترنت.

ويرى الباحث أن تلك المعاهدة التي لا غرض لها إلا احترام حقوق الإنسان والحد من تعرضه للكلم الهائل من الجرائم التي ترتكب عبر شبكة الإنترنت لا تتعارض بأي حال من الأحوال مع الإعلان العالمي لحقوق الإنسان الذي يعد الأساس في تقرير حريات الأشخاص.

ثانياً: توصيات المجلس الأوروبي.

نظراً للتطور السريع في مجال تكنولوجيا الكمبيوتر والإنترنت وشهود الدولة الأوروبية بأهمية إعادة النظر في الإجراءات الجنائية في هذا المجال. فقد أصدر المجلس الأوروبي التوصية رقم ١٣١٩٥ في سبتمبر ١٩٩٥م في شأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات لحث الدول الأعضاء بمراجعة القوانين الجنائية الوطنية لتلاءم التطور في هذا المجال^٣.

^١ محمد الكعبي، "مرجع سابق"، ص ٦١٢.

^٢ مصطفى محمد موسى، "أساليب إجرامية بالتقنية الرقمية ومكافحتها"، مطابع الشرطة، ط ١، ٢٠٠٣م، ص ٥٨١.

^٣ حسين الغفاري، "مرجع سابق"، ص ٧١١.

إن أهم ما ورد في توصية المجلس الأوروبي هو^١:

- ١- أن توضح القوانين إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحويها المعلومات أثناء انتقالها.
- ٢- أن تسمح الإجراءات الجنائية لجهة التفتيش بضبط برامج الكمبيوتر والمعلومات الموجودة بالأجهزة وفقاً لذات الشروط الخاصة بالتفتيش العادي.
- ٣- تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة في مجال تكنولوجيا المعلومات.
- ٤- يجب إلزام العاملين بالمؤسسات الحكومية والخاصة التي توفر خدمات الاتصال بالتعاون مع سلطات التحقيق لإجراء المراقبة والتسجيل.
- ٥- يتعين تعديل القوانين الإجرائية بإصدار أوامر لمن يحوز معلومات (برامج - بيانات) تتعلق بأجهزة الكمبيوتر وتسليمها.
- ٦- يجب أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة. يتعين عندئذ أن تسمح السلطة الأخيرة بإجراء التفتيش والضبط^٢.

ويرى الباحث أن مكافحة الجرائم المستحدثة تقتضي إذاً توحيد التشريعات المختلفة من ناحية، وأن يكون نظام الإثبات بالدليل الإلكتروني واحداً بين الدولة التي وقعت فيها الجريمة من ناحية، والدولة التي يقيم المتهم فيها وتتولى المحاكمة عنها من ناحية أخرى، لذلك لابد أن يكون هناك تعاون دولي يتفق مع هذه الطبيعة للجرائم، والتي تتميز بطابع خاص يقتضي أن تكون هناك ردود فعل سريعة.

ومما سبق يتضح أن مكافحة جرائم الإنترنت على المستوى الدولي تقتضي توثيق روح التعاون بين الأنظمة القانونية الداخلية وتقليل المغالاة في إقامة القطيعة بينها، وهذا التعاون القانوني فيما بين الدول لا ينال من سيادة الدولة، بل على العكس، فإن انعدام التعاون وتضامن الدول يعمق أوجه الاختلاف والتباعد بين الأنظمة العقابية مما يساعد على تزايد الجرائم العابرة للحدود ومنها جرائم الإنترنت وسهولة انتقال المجرمين عبر الدول.

ويعد التعاون الشرطي الدولي والتعاون القضائي الدولي وأيضاً الاتفاقيات والمعاهدات الدولية من أهم صور التعاون الدولي في مجال الجرائم التي تتعدى الحدود ومنها جريمة الاحتيال المعلوماتي^١.

^١ مصطفى موسى، "مرجع سابق"، ص ٥٢١.

^٢ هلاي أحمد، "مرجع سابق"، ص ٦٣٠.

المطلب الثاني

مكافحة جريمة الاحتيال المعلوماتي على المستوى الوطنية لدول المقارنة

لاحظ المشرع منذ فترة في القانون المقارن خطورة بعض أفعال الاعتداء على أجهزة الحاسب وبرامجها وقواعد البيانات، فتدخل لتوفير حماية جنائية لها، والحقيقة أن الاعتداء على مواقع الإنترنت وصحائفها لا يخرج عن كونه أحد التطبيقات السابقة والتي يمثل اعتداء على أنظمة الحاسب حيث يستخدم في إعداد هذه البرامج في أجهزة الكمبيوتر وبرامجها المختلفة، فيقابل التطور في المجال التكنولوجي سواء من ناحية الحياة العامة أم الخاصة واعتماد الجميع عليه في سائر شؤونهم واستغلال الجناة لتلك التقنية لارتكاب جرائمهم، هذا التطور المتلاحق في مجال المعلومات لا يقابله بذات الدرجة تطور في النصوص القانونية من أجل مواجهته^١.

إن القانون الجنائي بنصوصه الحالية لا يكفي لإمكانية مواجهة تلك الصور المستحدثة من الجرائم، حيث يتطلب بغالبية النصوص الصفة المادية في الشيء محل ارتكاب الجريمة، وهذا مختلف مع طبيعة الجريمة المعلوماتية، وبالتالي تخرج تلك الصور من تحت طائلة العقاب، ونتيجة لذلك بات متطلباً من الأجهزة الجنائية الإجرائية في ممارستها لحق المجتمع في الذود عن كيانه ضد الإجرام أن تتعامل مع أشكال غير محسوسة من الأدلة، وهو ما ألقى بظلاله على أساليب كشف الجرائم المعلوماتية، وعمليات البحث الجنائي والتحقيق ومنظومة التدريب المتخصص اللازم لإكساب المهارات المطلوبة للتعامل مع هذه الجرائم وصولاً إلى الحقيقة بشأنها^٢. فبدأت أغلب البلدان في تنظيم تشريعاتها لمواجهة النمط الجديد من الجرائم، والذي ظهر مصاحباً لاستخدام الحاسب الآلي، وقد ذهب في هذا الاتجاه كل من أنظمة دول المقارنة، بعدما تنامي لديها الشعور بضرورة إقرار قوانين خاصة تنظم من خلالها هذا النوع من الجرائم. وسيتم تناول ذلك من خلال تقسيم هذا المطلب إلى الآتي:-

الفرع الأول : جهود مملكة البحرين في مكافحة جريمة الاحتيال المعلوماتي.

الفرع الثاني: جهود دولة الامارات العربية المتحدة في مكافحة جريمة الاحتيال المعلوماتي.

الفرع الثالث: جهود المملكة العربية السعودية في مكافحة جريمة الاحتيال المعلوماتي.

^١ كوثر مازوني، "مرجع سابق"، ص ٥٦١.

^٢ منير الجنيهي، "مرجع سابق"، ص ٤٢٠-٤٢١.

^٣ منير الجنيهي، "مرجع سابق"، ص ٥٢٠.

الفرع الأول: جهود مملكة البحرين في مكافحة جريمة الاحتيال المعلوماتي

كانت أولى محاولات المشرع البحريني للتصدي لجرائم الحاسب الآلي من خلال ما صدر بموجب مرسوم بقانون رقم (١٠) لسنة ١٩٩٣ بشأن حقوق المؤلف، وقد ورد ضمن هذه القانون نص خاص بحماية برامج الحاسب الآلي.

وقد أقر المشرع البحريني قانون جرائم تقنية المعلومات رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات. وجاء هذا القانون بمثابة خطوة هامة في مواجهة ظاهرة انتشار الجرائم الإلكترونية، فقد تم تحديد المفاهيم ذات العلاقة بالجرائم المعلوماتية، كما تضمن القانون العقوبات الواقعة على مرتكبي هذه الجرائم بالتفصيل، بالإضافة إلى تحديد الآليات التي من خلالها تتم إجراءات البحث والتحري الخاصة بهذه الجرائم.

أما فيما يخص الجهة المختصة بالتحري والمتابعة والكشف عن الجرائم الإلكترونية فقد تم تحديدها بموجب المرسوم الملكي رقم (١٠٩) للعام ٢٠١١ الصادر بشأن تعديل بعض أحكام المرسوم رقم (٦٩) للعام ٢٠٠٤م والقاضي بإعادة تنظيم وزارة الداخلية، حيث جاء فيه إنشاء إدارة عامة لمكافحة الفساد والأمن الاقتصادي والإلكتروني والتي تتدرج تحت مظلتها عدد من الإدارات الأمنية تهدف لحفظ دعائم الاقتصادي الوطني، ويدخل ضمن اختصاص هذه الإدارة متابعة البلاغات والشكاوى الخاصة بالجرائم الإلكترونية، حيث يقدم البلاغ عبر موقع الإدارة الإلكتروني أو بواسطة الاتصال المباشر برقم الإدارة.

وتختص الإدارة المشار إليها بمكافحة جميع الجرائم الإلكترونية من سرقة واختراق للبريد الإلكتروني والإساءة والتشهير والسب أو الابتزاز باستخدام وسائل إلكترونية وتتعقبها وكشفها وذلك لما تشكله من خطورة على أمن الفرد والمجتمع، وتحرص الادارة على تزويد العاملين فيها بأحدث الأجهزة الفنية لمساعدتهم في الحصول على المعلومات دقيقة وزيادة الإنتاجية، بالإضافة إلى التدريب المستمر للكوادر الفنية وعقد الندوات والمؤتمرات المتخصصة وإقامة الدورات وورش العمل في مجال مكافحة الجرائم التي تختص بها الإدارة.

وتحرص إدارة مكافحة الجرائم الإلكترونية للسعي من الحد من جرائم الشبكة العنكبوتية من خلال إنفاذ القانون والعمل على الوقاية من هذه الجرائم، كما أنها المسؤولة عن تنفيذ الاستراتيجيات في مجال مكافحة جرائم الحاسوب في مملكة البحرين وحل المسائل القانونية والتحقيق في الجرائم التي أثارها الكمبيوتر والاتصالات السلكية واللاسلكية والتكنولوجيات

المستحدثة؛ وكذلك إحالة القضايا للنياية العامة، بالإضافة إلى التعليق واقتراح التشريعات، والشروع والمشاركة في الجهود الدولية لمكافحة الجريمة الحاسوبية^١.

ولا شك أن التغيرات الناجمة عن استخدامات التقنيات الحديثة من أجهزة حاسبات وشبكات معلومات كان لها تأثيرها الواضح على الأوضاع الأمنية بصورة شاملة ومؤثرة، كل ذلك وضع الأجهزة الأمنية في تحدي واضح نحو حماية المجتمع من سلبيات وسوء استخدام شبكة المعلومات العالمية الإنترنت، ونتيجة لذلك بدأت أجهزة الشرطة البحرينية والجهات ذات الاختصاص بهذا الشأن في انتهاج أسلوب مميز في التقدم العلمي والتكنولوجي ومواكبة التطور واللاحق بالمسيرة العلمية من خلال الاعتماد على التقنيات الحديثة لمواجهة الصور المستحدثة من الإجراء المعلوماتي وعلى رأسها جرائم الإنترنت^٢، والسعي إلى الحد من الجرائم الإلكترونية وحماية المجتمع من الآثار السلبية لهذه الآفة، بالإضافة إلى استغلال عامل الوقاية في الحد من هذه الجرائم من خلال التوعية الفعالة والمستمرة لجميع مكونات المجتمع لتقادي الوقوع ضحية لهذا النوع من الجرائم^٣.

كما أسست الجهات المختصة في المملكة مركز الاستجابة لطوارئ الحاسب الآلي لأول مرة في مملكة البحرين عام ٢٠١٢ بالشراكة مع مجموعة من الشركات البريطانية والأمريكية والهندية، ومن أهداف المركز^٤:

- ١- تقديم خدمة كشف البرمجيات الضارة وتحديد مواقعها.
- ٢- توفير تنبيهات مبرمجة ومتعمقة تفيد توفير القدرة وسرعة القرار.
- ٣- تمكن المنظمات من تعزيز أعمالها ضد العدوى الخبيثة وضمان سمعة مدوناتها.
- ٤- يقدم الفريق خدماته التجارية في مملكة البحرين ودول مجلس التعاون الخليجي.

ويرى الباحث أن المشرع البحريني وبالرغم من إدراجه لقانون جرائم تقنية المعلومات وإعماله، إلا أن هناك بعض القصور، إذ على المشرع أن يحدد الجهة المختصة وأفراد هذه الجهة لكي يكونوا على قدر من الكفاءة والعلم بأنظمة وبرامج الحاسوب، والتي تكون ذات مقدرة عالية في هذا المجال والذي يخول لها كافة أعمال التحقيق من معاينة وتفتيش ضبط... الخ،

^١ أنظر موقع إدارة مكافحة الجرائم الإلكترونية عبر الإنترنت <http://www.acees.gov.bh>

^٢ مصطفى موسى، "مرجع سابق"، ص ٤٤٠.

^٣ أنظر موقع إدارة الجرائم الإلكترونية عبر الإنترنت <http://www.acees.gov.bh>

^٤ للمزيد أنظر مركز الاستجابة لطوارئ الحاسب الآلي على الموقع الإلكتروني www.cert.org/incident.

فطبيعة هذه الجرائم يسهل فيها محو الدليل أو اتلافه، مما يتطلب من الجهة التي تنتقل وتجرى أعمال التحقيق تكون من أصحاب الاختصاص في التقنية العالية.

الفرع الثاني: جهود دولة الإمارات العربية المتحدة في مكافحة جريمة الاحتيال المعلوماتي

بدأت محاولات المشرع الإماراتي في مواجهة جرائم المعلوماتية في العام ١٩٩٢م، فأصدر المشرع الإماراتي القانون الاتحادي رقم (٤٠) لسنة ١٩٩٢م في شأن المصنفات الفكرية وحقوق المؤلف، وقد شمل هذا القانون برامج الحاسب الآلي بالحماية. وأصدرت الإمارات في العام ٢٠٠٢م قانون التوقيع الإلكتروني والتجارة^١.

وتعتبر دولة الإمارات المتحدة من أوائل الدول العربية التي تصدر قانون خاص بجرائم تقنية المعلومات، حيث أقر المشرع الإماراتي قانون مكافحة جرائم تقنية المعلومات وذلك بموجب مرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢م. والذي تضمن تعريفاً لبعض المفاهيم ذات الصلة بالمعلوماتية، كما شمل كافة العقوبات للجرائم الواردة على التقنية المعلوماتية.

وما يؤخذ على هذا القانون عدم إلمامه وشموليته لإجراءات البحث والتحري والتحقيق في الجرائم المعلوماتية، حيث قام المشرع بإعمال قوانين البحث والتحري والتحقيق وفق قواعد تقليدية حسب ما جاء في قانون الإجراءات الجزائية.

ولمواجهة الجرائم المعلوماتية فقد أنشأت دولة الإمارات العربية المتحدة مركز الاستجابة لطوارئ الحاسب الآلي، فقد قامت هيئة تنظيم الاتصالات في الإمارات بإنشاء هذا المركز لتحسين معايير وممارسات المعلومات وحماية البنية التحتية لتقنية المعلومات من مخاطر اختراقات الإنترنت^٢.

ومن المهام المنوطة بهذا المركز دعم البنية التحتية للاتصالات ونظم المعلومات والمحافظة عليها من تهديدات الجرائم الأمنية على الإنترنت، كما ويقوم المركز ببناء ثقافة أمانة ومحمية في مجال جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة، ومن الأهداف التي يسعى المركز إلى تحقيقها هي^٣:

^١ عبد الله العازمي، "مرجع سابق"، ص ٦٩٩.

^٢ راجع في ذلك الموقع الإلكتروني لمركز الاستجابة لطوارئ الحاسب الآلي بدولة الإمارات العربية المتحدة www.aeccert.ae/about-us-ar.p

^٣ مجمع البحوث والدراسات، "مرجع سابق"، ص ٨٠.

- ١- تعزيز قانون مكافحة جرائم تقنية المعلومات والمساعدة في استحداث قوانين جديدة.
- ٢- تعزيز الوعي حول أمن المعلومات على مستوى الدولة.
- ٣- بناء خبرات وطنية في مجال أمن المعلومات وإدارة الطوارئ وتحري الأدلة في الحسابات.
- ٤- إنشاء مركز اتصالات موثوق للإبلاغ عن جرائم تقنية المعلومات في الدولة.
- ٥- إنشاء مركز وطني لجمع المعلومات عن التهديدات والمخاطر وجرائم تقنية المعلومات.
- ٦- تشجيع وإنشاء ومساعدة فرق الاستجابة لحوادث أمن الحسابات، في القطاعات المختلفة.

وفي الإمارات يتم الإبلاغ عن الجرائم المعلوماتية بصفة عامة وذلك عبر الموقع الإلكتروني لديوان المحاسبة وهي خدمة إلكترونية تتيح الإبلاغ عبر الإنترنت، وهي متاحة لموظفي الحكومة الاتحادية وموردي الخدمات والسلع وتختص بالمسائل المتعلقة بالمؤسسات الاتحادية حصراً، وتتوفر الإرشادات الشاملة حول كيفية الإبلاغ عن الاحتيال، على الموقع الإلكتروني الخاص بالديوان، حيث يمكن للأفراد الإبلاغ عن حادثة الاحتيال عبر رسالة إلكترونية أو رسالة بريدية خطية^١.

الفرع الثالث: جهود المملكة العربية السعودية في مكافحة جريمة الاحتيال المعلوماتي

لقد أقر المشرع السعودي نظام مكافحة جريمة المعلوماتية بموجب المرسوم الملكي رقم (٧) بتاريخ ١٤٢٨/٣/٨هـ، وذلك تماشياً لمتطلبات المرحلة التي ازدادت فيها الجريمة المعلوماتية انتشاراً، ولمواجهة المخاطر الناجمة عن هذه الجرائم قام المشرع السعودي بإصدار هذا القانون.

وقد أنشأت الجهات المختصة في السعودية المركز الوطني الإرشادي لأمن المعلومات: فريق الاستجابة لطوارئ الحاسب الآلي، وتم تم إنشاء هذا لمركز بواسطة هيئة الاتصالات وتقنية المعلومات السعودية، ويهدف للكشف عن التهديدات والمخاطر، منع الاختراقات والانتهاك للأمن السيبراني والتنسيق والاستجابة للمعلومات عن حوادث الأمن السيبراني على مستوى المملكة^٢.

^١ عبد الله العازمي، "مرجع سابق"، ص ١٩٣

^٢ مجمع البحوث والدراسات، "الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها"، بحث مقدم لأكاديمية السلطان قابوس لعلوم الشرطة، في العام ٢٠١٦م، ص ٨٣.

وتم إنشاء هذا المركز ليكون بمثابة المرجع بشأن أمن المعلومات في المملكة العربية السعودية، ويسعى المركز من خلال برامجه إلى^١:

- ١- زيادة مستوى الوعي بأمن المعلومات في المملكة العربية السعودية.
- ٢- تنسيق الجهود الوطنية نحو ترقية أفضل ممارسات الأمن السيبراني وخلق الثقة بين مجتمع المعلومات.
- ٣- المساعدة على التصدي لهجمات وحوادث أمن المعلومات في المملكة.
- ٤- أن يكون المركز المرجعية الأساسية في مجال أمن المعلومات بالنسبة لمجتمع المعلومات في المملكة العربية السعودية.
- ٥- بناء القدرات والمواهب البشرية في مجال أمن المعلومات في المملكة العربية السعودية.
- ٦- توفير بيئة موثوقة للتعاملات لبناء الثقة والتعاون مع الجمهور ومع مجتمع المعلومات في المملكة.

ويرى الباحث وبالرغم من أن الأنظمة القانونية لدول المقارنة تشمل على قوانين خاصة بالجرائم المعلوماتية، إلا أنها بحاجة إلى زيادة الخبرة وتفعيل التعاون الدولي والتنسيق على أعلى المستويات لمواجهة الجرائم المعلوماتية، بالإضافة لذلك يجب أن تقوم الدول المعنية بضرورة تأهيل وإعداد رجال ضبط قضائي متخصصين في مجال التقنية المعلوماتية واعتمادهم كخبراء في هذا المجال.

^١ الموقع الإلكتروني للمركز الوطني الارشادي لأمن المعلومات بالمملكة العربية السعودية:

المطلب الثالث

صعوبات مكافحة جريمة الاحتيال المعلوماتي على المستوى الدولي والوطني

في عالم مزدحم بشبكات اتصالية دقيقة ومتطورة تتغل وتشغل البيانات والمعلومات من مناطق متباعدة باستخدام تقنيات لا تكفل لها أمناً متكاملاً، ويتاح في ظلها التلاعب عبر الحدود بتلك المعطيات المنقولة أو المخزنة، مما قد يسبب لبعض الدول أو الأفراد أو الشركات أضرار فادحة، يغدو عندها التعاون الدولي واسع المدى في مكافحة الجرائم المعلوماتية ومن بينها جريمة الاحتيال المعلوماتي أمراً محتماً.

ومع ضرورة هذا التعاون والمناداة، إلا أنه ثمة صعوبات ومعوقات تقف دون تحقيقه وتجعله صعب المنال ومن خلال هذا الفرع سوف نحاول جاهدين أن نبرز أهم تلك الصعوبات وكيفية مواجهتها، وسيتم تقسيم هذا المطلب إلى ثلاث فروع على النحو الآتي^١:

الفرع الأول : صعوبات مكافحة جريمة الاحتيال المعلوماتي على المستوى الوطني.

الفرع الثاني: صعوبات مكافحة جريمة الاحتيال المعلوماتي على المستوى الدولي.

الفرع الثالث: كيفية القضاء على صعوبات مكافحة جريمة الاحتيال المعلوماتي.

الفرع الأول: صعوبات مكافحة جريمة الاحتيال المعلوماتي على المستوى الوطني

تتميز جرائم الإنترنت بمجموعة من الخصائص التي تؤدي إلى صعوبة التعامل معها وضبطها، حيث تواجه الأجهزة الأمنية عند مواجهتها لجريمة الاحتيال المعلوماتي على المستوى الوطني العديد من الصعوبات أهمها:

أولاً: إجماع الكثير من الجهات عند الإبلاغ عن تلك الجرائم:

فتمحصر أكثر الجهات وخاصة البنوك أو المؤسسات الادخارية على عدم الكشف عما تعرضت له، وعدم بيان عجزها عن تحقيق الأمان الكافي للمعلومات لأصول الأموال التي تتعامل معها، فتكتفي الجهة عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عما تعرضت له من جرائم للسلطات المختصة، تجنباً للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها، وبالتالي

^١ أحمد فضل، "مرجع سابق"، ص ٤٣٥.

يجب تحديث الأساليب الإجرائية في مواجهة الجرائم المعلوماتية واستكمالها على نحو يكفل استجابتها بشكل كافٍ، حيث يضمن تعويض الأفراد لحقوقهم وحياتهم دون التعرض لخطر المتطلبات العملية الإثباتية في مجال تقنية المعلومات والاتصالات^١.

ثانياً: عدم كفاية القوانين القائمة.

يقابل التطور في المجال التكنولوجي سواء من ناحية الحياة العامة أم الخاصة واعتماد الجميع عليه في سائر شئونهم استغلال الجناة لتلك التقنية في ارتكاب جرائمهم، وهذا التطور المتلاحق في مجال المعلومات لا يقابله بذات الدرجة تطور في النصوص القانونية، كما سبق دراسته من خلال المواجهة التشريعية لهذه الجرائم^٢.

فالقانون الجنائي بنصوصه الحالية لا يكفي لإمكانية مواجهة تلك الصور المستحدثة من الجرائم، حيث تتطلب غالبية النصوص الصفة المادية في الشيء محل ارتكاب الجريمة مما يتنافى مع الطبيعة المعلوماتية، وبالتالي تخرج تلك الصور من تحت طائلة العقاب.

أما بالنسبة للدول التي سنت في تشريعاتها الداخلية قوانين خاصة لجرائم تقنية المعلومات، فإن هذه القوانين لا زال يكتنفها القصور في بعض نصوصها، وهذا ما بدا واضحاً من خلال الدراسة التي بينت كيف أن التشريع الإماراتي والسعودي لم يتضمن إجراءات خاصة بالتفتيش والضبط في مجال الجرائم المعلوماتية بالرغم من إصدار هذه الدول لقوانين تقنن من خلالها الجرائم المعلوماتية.

ثالثاً: صعوبة إثبات الجريمة المعلوماتية والتحقيق فيها.

تتمثل هذه الصعوبات فيما يلي^٣:

- أ- انعدام الأثر المادي، حيث أن الجريمة لا يتخلف عنها أي أثر كتابي، بالإضافة إلى إمكانية قيام الجاني بتدمير أدلة الإدانة في ثوانٍ قليلة.
- ب- غياب الدليل المرئي.
- ت- إعاقة الوصول إلى الدليل بوسائل الحماية الفنية.
- ث- ضخامة البيانات المتعين فحصها.

^١ أحمد فضل، "مرجع سابق"، ص ٤٣٦.

^٢ حسين الغفاري، "مرجع سابق"، ص ٧١٥.

^٣ مصطفى موسى، "مرجع سابق"، ص ٥٢١.

- ج- الإحجام عند الإبلاغ عن جرائم الحاسب حفاظاً على ثقة العملاء.
- ح- نقص خبرة رجال الشرطة وجهات الادعاء والقضاء.
- خ- إمكانية ارتكاب هذا النوع من الجرائم خلال مسافات بعيدة قد تصل إلى دول وقارات.

الفرع الثاني: صعوبات مكافحة جريمة الاحتيال المعلوماتي على المستوى الدولي

التعاون الدولي بكافة صوره في مجال مكافحة ومواجهة الجرائم المعلوماتية وإن كان يعد مطلباً تسعى إلى تحقيقه أغلب الدول إن لم يكن كلها، ثمة صعوبات ومعوقات أهمها ما يلي:

أولاً: مشكلة الاختصاص في الجرائم المعلوماتية

الجرائم المعلوماتية من أكبر المشاكل التي تثير مسألة الاختصاص على مستوى محلي أو دولي ولا توجد أي مشكلة بالنسبة للاختصاص على المستوى الوطني أو المحلي حيث يتم الرجوع إلى المعايير المحددة قانوناً لذلك.

ولكن المشكلة تثار بالنسبة للاختصاص على المستوى الدولي حيث اختلاف التشريعات والنظم القانونية والتي قد ينجم عنها تنازع في الاختصاص بين الدول بالنسبة للجرائم المعلوماتية التي تتميز بكونها عابرة للحدود.

فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استناداً إلى "مبدأ الإقليمية" وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ "الاختصاص الشخصي"، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل عند إذن في اختصاصها استناداً إلى "مبدأ العيني"^١.

ثانياً: الصعوبات الخاصة بالمساعدات القضائية الدولية^٢.

نعلم أن الأصل بالنسبة لطلبات الإنابة الدولية والتي تعد من أهم صور المساعدات القضائية الدولية في المجال الجنائي أن تسلم بالطرق الدبلوماسية وهذا بالطبع يجعلها تتسم بالبسط والتعقيد، والذي يتعارض مع طبيعة الإنترنت وما تتميز به من سرعة، هو الأمر الذي

^١ هلاي أحمد، "مرجع سابق"، ص ٣٥٠.

^٢ حسين الغفاري، "مرجع سابق"، ص ٦٥٧.

انعكس على جرائم المتعلقة بالإنترنت، كذلك من الصعوبات الكبيرة في مجال المساعدات القضائية الدولية المتبادلة التباطؤ في الرد، حيث أن الدولة متلقية الطلب غالباً ما تكون متباطئة في الرد على الطلب سواء بسبب نقص الموظفين المدربين أو نتيجة الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد الاستجابة وغيرها من الأسباب.

ثالثاً: الصعوبات الخاصة بالتعاون الدولي في مجال التدريب.

تتمثل في عدم رغبة بعض القيادات الإدارية في بعض الدول في التدريب لاعتقادهم بدوره السلبي في تطوير العمل من خلال تطبيق ما تعلمه المتدربون في الدورات التدريبية وما اكتسبوه من خبرات، ومن الصعوبات أيضاً التي قد تهدد التعاون في مجال التدريب ما يتعلق بالفروق الفردية بين المتدربين وتأثيرها على عملية الاكتساب للمهارات المستهدفة بقوة تامة ومتكافئة لدى مختلف الأفراد المتدربين. أيضاً من الصعوبات التي قد تؤثر على العملية التدريبية على التعامل الدولي فيها ما يتعلق بالملامح العامة المميزة للبيئة التدريبية، من حيث عدم قدرتها على تمثيل الواقع العملي لبيئة العمل الطبيعية تمثيلاً تاماً ومتقناً، سواء بشأن ما يدور بها من وقائع وملابس وإجراءات، أو ما يتم فيها من نشاطات لا تبلغ حد التطابق مع طبيعة المهام التي سيؤديها المتدربون في بيئة العمل الطبيعية^١.

الفرع الثالث: كيفية القضاء على صعوبات مكافحة جريمة الاحتيال المعلوماتي

تعد الجرائم المعلوماتية صوراً إجرامية مستحدثة من الجرائم العابرة للحدود الوطنية في عالم ذابت فيه الفواصل وتلاشت الحدود، مما جعل من السهولة ارتكاب الجرائم عبر شبكة الإنترنت، ليس فقط على المستوى الوطني، بل وعلى المستوى الدولي.

وللقضاء على هذه الصعوبات التي تواجه مكافحة جرائم الإنترنت دولياً، فقد نادى العديد من الدول ومنها اليابان بضرورة التعاون الدولي المشترك في إطار مواجهة هذه الجرائم، مع الإشارة إلى أهمية وجود تشريع قضائي محلي خاص بكل دولة يعالج مثل هذه الجرائم، على أن يراعي هذا التشريع إمكانية استغلال سمة عبر الوطنية لتلك الجرائم، مع اقتراحها ما يسمى بالتحقيق الدولي المشترك لهذه الجرائم، بحيث يمكن من خلال إرسال معلومات مفصلة عن تلك الجريمة إلى أي من الدول مطالبتها باتخاذ الإجراءات القضائية المناسبة.

^١ أحمد فضل، "مرجع سابق"، ص ٤٥٠.

فيما يتعلق بالصعوبة الأولى التي تواجه مكافحة جرائم الإنترنت على المستوى الدولي فالنسبة لمشكلة الاختصاص في الجرائم المعلوماتية فيها حاجة ملحة إلى إبرام اتفاقيات دولية ثنائية كانت أو جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي خاصة بالنسبة للجرائم المتعلقة بالإنترنت، بالإضافة إلى تحديث القوانين الجنائية الموضوعية فيها والإجرائية بما يتناسب مع التطور الكبير التي تشهده تكنولوجيا المعلومات والاتصالات^١.

أما ما هو متعلق بالصعوبات الخاصة "بالمساعدات القضائية" الدولية والتباطؤ في الرد فإننا نجد أن الحاجة الملحة إلى إيجاد وسيلة أو طريقة تتسم بالسرعة تسلم من خلالها طلبات الإنابة كتعيين سلطة مركزية مثلاً أو بالسماح بالاتصال المباشر بين الجهات المختصة في نظر مثل هذه الطلبات لنقضي على مشكلة البطء والتعقيد في تسليم طلبات الإنابة.

هذا بالفعل ما أوصى به مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية الذي انعقد في بانكوك في الفترة من ١٨ - ٢٥/٤/٢٠٠٥م حيث أكد على ضرورة تقدير فعالية السلطات المركزية المعنية الضالعة في أعمال المساعدة القانونية المتبادلة وإقامة قنوات مباشرة للاتصال فيما بينها بقيمة ضمان تنفيذ الطلبات في الوقت المناسب^٢.

ويرى الباحث أن ما يتعلق بالصعوبات التي تواجه التعاون الدولي في "مجال التدريب" فإنه يمكن التغلب عليها بإجراء المزيد من الحملات التوعوية للتبئية بمخاطر الجرائم المعلوماتية والأضرار التي تسببها وبأهمية تدريب رجال العدالة الجزائية على مواجهتها، كما أنه وبالمزيد من التنسيق مع الأجهزة المعنية بتدريب رجال تنفيذ القانون إيجاد برامج تدريبية مشتركة تناسب جميع الجهات، هذا بالإضافة إلى قيام بعض العمليات المشتركة والتي من شأنها صقل مهارات القائمين على مكافحة تلك الجرائم وتقريب وجهات النظر من شأنها.

^١ حسين الغفاري، "مرجع سابق"، ص ٦٧٠.

^٢ هلاي أحمد، "مرجع سابق"، ص ٦٣١.

خاتمة

من خلال دراستنا لجريمة الاحتيال المعلوماتي باستخدام وسائل تقنية المعلومات توصلنا إلى جملة من النتائج سواء من خلال تحليل موضوع جريمة الاحتيال أو من خلال تحليل القوانين الخاصة بمكافحة جريمة الاحتيال المعلوماتي والذي يستخلص منها الباحث بعض النتائج العملية، بالإضافة إلى إبداء الآراء التي تصب في سد بعض الثغرات والتي تصنف كنقص في بعض القوانين العربية وتأتي في سياق المعالجة لهذه القوانين، بالإضافة إلى بعض التوصيات التي تأتي في سياق دعم وتطوير بعض القطاعات المختصة بمواجهة لجريمة الاحتيال المعلوماتي.

أولاً: الاستنتاجات.

١. إن الجرائم المرتكبة بوسائل تقنية المعلومات من الجرائم المستجدة والمستحدثة التي تهدد المجتمعات المعاصرة نتيجة سرعة انتشارها، وسهولة القيام بها، وحجم الخسائر الناجمة عن ارتكابها وصعوبة إثباتها. في ظل اعتبار وسيلة تقنية المعلومات محدد من محددات تطور المجتمعات والدول وهو المحدد الاستراتيجي للبناء الثقافي والتطور الاقتصادي.

٢. تعد جريمة الاحتيال المعلوماتي صورة من صور الجرائم الواقعة باستخدام تقنية المعلومات، فهي حديثة بأسلوب ارتكابها كما أن نتائجها وأهدافها أيضاً لا تخلو من الحداثة، فاستخدام التقنية الحديثة أفسح المجال أمام مستخدمي هذه التقنية بالطرق السلبية أن يقوموا بعمليات الاحتيال باستخدام وسائل تقنية المعلومات.

٣. في إطار جريمة الاحتيال المعلوماتي يجب أن يكون الجاني على قدر كبير من الإلمام بتقنية الحاسب الآلي وكيفية استخدامه والإحاطة بنظمه وبرامجه وكيفية تسخيرها للوصول إلى تحقيق النتيجة المرجوة، فتتصب تلك الجريمة على البيانات المخزنة في النظام الممثلة لأموال أو أصول أو خدمات، يهدف الجاني منها تحقيق مكاسب أو مزايا.

٤. وتمتاز جريمة الاحتيال المعلوماتي بأن الأدلة التي قد يتركها الجاني تقع في بيئة إلكترونية إذ إنها تقوم على التلاعب في البيانات والبرامج، ويمتاز المجرم المعلوماتي بقدرته الهائلة على إخفاء جريمته والتلاعب بالأدلة.

٥. تنصب أغلب وسائل الاحتيال المعلوماتي على التلاعب في المعلومات والبيانات التي يتم إدخالها للحاسب الآلي، وتظهر هذه الوسيلة عند إدخال بيانات مختلفة أو محرفة في النظام المعلوماتي، مما يدفع لتغيير البيانات الصحيحة المدخلة أو الجميع بينهما وهي الطريقة الأسهل لمرتكبي الجرم الاحتيالي.

٦. تتعدد انواع الوسائل التي تستخدم في التقنية المعلوماتية في عالمنا المعاصر فهي تتنوع بتنوع نوع الجريمة المرتكبة، وهذا ما يميز الجرائم باستخدام وسائل تقنية المعلومات عن الجرائم التقليدية، حيث تتدخل التكنولوجيا بصورها المتعددة في هذه الوسائل والتي يترتب عنها النتيجة الجريمة لهذه الأفعال وتتخذ وسائل تقنية المعلومات أنواع متعددة.

٧. تعتبر بطاقات الائتمان من أشهر الوسائل التي تتعرض للاحتيال باستخدام وسائل تقنية المعلومات، وهي ليست بعيدة عن صور احتيال البيانات الشخصية والبريد الإلكتروني، فهذه الصور مترابطة في الهدف وهو الاحتيال على الأشخاص لسرقة الأموال أو استخدام هذه البيانات في سرقتها، والبطاقات الائتمانية ذات طبيعة خاصة تختلف عن الأوراق المالية الأخرى، لذا انعكست الجرائم الواقعة عليها بطبيعة خاصة تميزها عن الجرائم الأخرى، وانتشار استخدام البطاقات الائتمانية من خلال شبكة الإنترنت أدى لظهور جرائم التسلل للسطو عليها على اعتبار أنها نقود إلكترونية، وهو أمر بالنسبة للمتسلل غير ذات صعوبة فمثلاً يستطيع المحتالون سرقة المئات من أرقام البطاقات وبيعها للآخرين، وتتم هذه العملية من خلال الحصول على كلمات السر المدرجة في أجهزة الكمبيوتر الخاصة بالمجني عليه.

٨. في الجرائم التقليدية يوجد مسرح جريمة فعلي يحتوي على الآثار المادية للجريمة مما يتيح عملية التحفظ لهذه الآثار لمعاينتها تمهيداً لفحصها وبيان صحتها في الإثبات، أما في الجرائم المعلوماتية يختلف الحال، حيث من النادر أن يتخلف عن الجريمة آثار مادية فعلية، فقد تطول الفترة الزمنية بين وقوع الجريمة واكتشافها، مما قد يعرض الآثار الناتجة عن الجريمة للتلف أو المحو أو العبث بها.

٩. إن الخبرة تلعب دور أساسي ورئيسي في إثبات جريمة الاحتيال المعلوماتي، ولا أدل من ذلك اشتراط أن تكون جهات التحقيق والشهود من أصحاب الخبرة في مجال التقنية الحديثة، فالخبير وحده هو القادر على استخراج الأدلة وإثبات وقوع الجريمة، وتعيين الأسلوب التي وقعت به الجريمة، كما يمكن للخبير أن يقوم بإرجاع البيانات التي تم حذفها أو إتلافها، بالإضافة إلى أن خصوصية جريمة الاحتيال المعلوماتي تتطلب التعامل معها بالخبرة والمهارة اللازمة لاستخراج الأدلة، ولا يتطلب لذلك أن يكون الخبير ممن درسوا مجال تقنية المعلومات، فيكفي أن يكون من أصحاب المهارة والمقدرة على استخدام الحاسب الآلي بشكل يخول لهم أن يكون من أصحاب الخبرة.

١٠. يمتاز الدليل الرقمي بخصائص ومميزات تميزه عن سائر الأدلة المادية والعلمية والفنية، فلا شك من أن الدليل الرقمي كلما أحيط بمجموعة من الشروط والضمانات ووسائل التوثيق التي تكفل سلامة المعلومات والبيانات والدلائل المقروءة والمحلاة إلكترونياً المنقولة والمثبتة عبر الوسائل والأجهزة الإلكترونية وسلامة ودقة صحة نسبتها إلى صاحبها، يثير مجموعة من الصعوبات القانونية حول مدى شمولية الأدلة الرقمية بالقوانين والأنظمة والتشريعات الصادرة بشأن الأدلة المادية الأخرى.

١١. يلعب القضاء في أي دولة دوراً هاماً في مواجهة حالات التعدي الآثم الماس بمصالح المجتمع وأفراده على حد سواء، وذلك من خلال تطبيق القوانين وتفسيرها بما يتفق مع الغاية من سنّها والمصالح التي تبقى حمايتها.

١٢. إن قانون العقوبات بنصومه الحالية لا يكفي لإمكانية مواجهة تلك الصور المستحدثة لجريمة الاحتيال المعلوماتي، حيث تتطلب غالبية النصوص الصفة المادية في الشيء محل ارتكاب الجريمة مما يتنافى مع طبيعة جريمة الاحتيال المعلوماتي، وبالتالي تخرج تلك الصور من تحت طائلة العقاب، ونتيجة لذلك بات متطلباً من الأجهزة الجنائية الإجرائية في ممارستها لحق المجتمع في الذود عن كيانه ضد الإجرام أن تتعامل مع أشكال غير محسوسة من الأدلة، وهو ما يلقي بظلاله على أساليب كشف تلك الجريمة، وعمليات البحث الجنائي والتحقيق ومنظومة التدريب التخصص اللازم لإكساب المهارات المطلوبة للتعامل مع هذه الجرائم وصولاً إلى الحقيقة بشأنها.

ثانياً: التوصيات.

يوصي الباحث بالتوصيات الآتية:-

١. ضرورة أن تتضمن قوانين جرائم تقنية المعلومات على مواد يتم من خلالها إيضاح إجراءات التحقيق كالمعاينة والتفتيش والضبط، وذلك لإزالة اللبس في تفسير إجراءات التحقيق التي جاءت في قوانين الإجراءات الجنائية، وذلك للخصوصية التي تمتاز بها الجريمة المعلوماتية بشكل عام وجريمة الاحتيال المعلوماتي على وجه الخصوص.
٢. ضرورة أن تتضمن القوانين الخاصة بالجرائم تقنية المعلومات على نصوص واضح وصريحه على الكيفية التي ترفع من خلالها الشكوى لجريمة الاحتيال المعلوماتي على وجه الخصوص، حيث لم تتضمن القوانين الخاصة بالجرائم تقنية المعلومات على كيفية التبليغ عن الشكوى، فاقترنت على آلية إجراء الشكوى أو البلاغ حسب ما ورد في قانون الإجراءات الجنائية عن كل الجرائم.
٣. يجب تحديد النيابة المختصة التي تقوم بإجراء المعاينة نظراً للطبيعة الخاصة لهذه الجرائم التي تتطلب المعرفة والإلمام وتوفر الخبرة الكاملة بالجهة المختصة بإجراء المعاينة.
٤. إشراك القضاة وأعضاء النيابة العامة وأعضاء الضبط القضائي بدورات متخصصة بالنظر في قضايا المعلوماتية وذلك لتأهيلهم فنياً وتقنياً وتعزيز التعاون المشترك في مجال القضاء بهذا الخصوص.
٥. التوصية بإنشاء محاكم مختصة بالنظر في الجرائم المعلوماتية.
٦. ضرورة تكثيف الجهود الدولية والإقليمية لمواجهة جريمة الاحتيال المعلوماتي وذلك بإبرام اتفاقيات دولية تختص بمكافحة هذه الجرائم عبر التعاون المشترك على المستوى الإقليمي والدولي.

٧. ضرورة إنشاء جهاز مختص ومستقل لمتابعة ومراقبة جرائم الاحتيال المعلوماتي في مملكة البحرين يعمل بالتنسيق مع كافة قطاعات الدولة، ويكون أفراد هذا الجهاز من ذوي الخبرة والتخصص وينفرد وحده برصد جرائم الاحتيال المعلوماتي واكتشافها.

٨. العمل على زيادة الوعي المجتمعي بالنشر في وسائل الاعلام والمناهج التعليمية في الجامعات والمدارس لبيان مخاطر جريمة الاحتيال المعلوماتي وتوضيح كيفية الإبلاغ عنها وعدم التستر على الجناة.

قائمة المراجع

أولاً: المعاجم اللغوية - ومن كتب الفقه:

١. ابن منظور، "لسان العرب المحيط"، الجزء ١ دار اللسان العربي، بيروت، بدون سنة طبع.
٢. ابن منظور، "لسان العرب"، دار المعارف للنشر، القاهرة، ط ١.
٣. أحمد بن تيمية، "الفتاوي الكبرى"، تحقيق ممد عبد القادر عطا، دار الكتب العلمية، بيروت، ط ٣، ١٤٢٥هـ، ٩٩/٣.

ثانياً: المراجع العامة:

١. أحمد عوض بلال، "الإثم الجنائي"، دار النهضة العربية، القاهرة، ٢٠٠٣م.
٢. أحمد فتحي سرور، "الوسيط في قانون الإجراءات الجنائية"، دار النهضة العربية، القاهرة، ط ٢، ١٩٨١م.
٣. أشرف توفيق شمس الدين، "شرح قانون العقوبات" النظرية العامة للجريمة والعقوبة"، دار النهضة العربية، القاهرة، ٢٠٠٩م.
٤. آمال عبد الرحيم عثمان، "شرح قانون العقوبات"، دار النهضة، القاهرة، ٢٠٠١م.
٥. بوحنية قوي، "الاتصالات الإدارية داخل المنظمات المعاصرة"، ديوان المطبوعات الجامعية، الجزائر، ٢٠١٠م.
٦. ربيع أنور فتح الباب، "النظم السياسية (السلطة، الدولة، الحكومة صورها وأساليبها)"، دار نصر للطباعة الحديثة، القاهرة، ٢٠٠٣م.
٧. سامي صادق الملا، "اعتراف المتهم"، دار الفكر العربي، ط ١، ١٩٩٨م.
٨. شمس الدين ابن القيم، تحقيق وضبط عبد الرحمن وكيل، "إعلام الموقعين عن رب العالمين"، دار إحياء التراث العربي، بيروت، د.ط، ١٤١٣هـ، ٣٠٤/٣.
٩. عبد العظيم مرسي وزير، "شرح قانون العقوبات"، دار النهضة العربية، القاهرة، ١٩٩٣م.
١٠. علي إبراهيم الخضر، "إدارة الأعمال الدولية"، دار رسلان للطباعة والنشر والتوزيع، ٢٠١٠م.

١١. علي القهوجي، "شرح قانون العقوبات" القسم الخاص"، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٣م.
١٢. علي حسين الخلف وسلطان عبد القادر الشاوي، "المبادئ العامة في قانون العقوبات"، مطابع الرسالة، الكويت، ١٩٨٢م.
١٣. فخري عبد الرزاق الحديثي، "شرح قانون العقوبات"، القسم العام، بغداد، ١٩٩٢م.
١٤. فضيل دليو، "تاريخ وسائل الاتصال"، مطبعة crita copy، قسنطينة، الجزائر، ٢٠٠٦م.
١٥. فوزية عبد الستار، "شرح قانون العقوبات" القسم الخاص"، دار النهضة العربية، القاهرة، ١٩٨٢م.
١٦. مأمون سلامة، "شرح قانون الإجراءات الجنائية"، دار الفكر العربي، القاهرة، ١٩٨١م.
١٧. محمد زكي أبو عامر، "الإجراءات الجنائية"، دار الجامعة الجديدة، ط ٨، ٢٠٠٨م.
١٨. محمد علي جعفر، "قانون العقوبات" القسم الخاص"، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، ٢٠٠٦م.
١٩. محمد ماجد ياقوت، "أصول التحقيق الإداري في المخالفات التأديبية"، دراسة مقارنة، منشأة المعارف، الإسكندرية، بدون سنة نشر.
٢٠. محمد محدة، "ضمانات المتهم أثناء التحقيق"، الجزء الثالث، دار الهدى، عين مليلة، الجزائر، ط ١، ١٩٩٢م.
٢١. محمود حسني، "جرائم الاعتداء على الأموال في قانون العقوبات اللبناني"، منشورات الحلبي الحقوقية، ط ٣، ١٩٩٨م.
٢٢. محمود نجيب حسني، "جرائم الاعتداء على الأموال في قانون العقوبات اللبناني"، دار النهضة العربية، القاهرة، ١٩٨٤م.
٢٣. مصطفى هرجة، "النصب وخيانة الأمانة وأحكام الشيك"، دار الثقافة للطباعة والنشر، القاهرة، ١٩٨٩م.

ثالثاً: المراجع المتخصصة:

١. أحسن أبو سقيعة، "الجرائم ضد الأشخاص والجرائم ضد الأموال"، دار هومة، الجزائر، ٢٠٠٨م.
٢. أحمد خليفة الملط، "الجرائم المعلوماتية -دراسة مقارنة"، كلية الحقوق جامعة القاهرة، أطروحة دكتوراه منشورة، ٢٠٠٥م.
٣. أحمد عبد الله هلالي، "تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي"، دار النهضة العربية القاهرة، ٢٠٠٠م.
٤. أحمد عبدالله هلالي، "التزام الشاهد بالإعلام في الجرائم المعلوماتية" دراسة مقارنة"، دار النهضة العربية، القاهرة، ط١، ٢٠٠٦م.
٥. أحمد محمود مصطفى، "جرائم الحاسبات الآلية في التشريع المصري" دراسة مقارنة"، دار النهضة العربية، القاهرة، ٢٠١٠م.
٦. أيمن عبد الحفيظ، "الاتجاهات الفقهية والأمنية لمواجهة الجرائم المعلوماتية"، دون دار نشر، ٢٠٠٥م.
٧. أيمن عبد الله فكري، "الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية"، مكتبة القانون والاقتصاد، الرياض، ط١، ٢٠١٥م.
٨. إيهاب السنباطي، "موسوعة الإطار القانوني للتجارة الإلكترونية"، دار النهضة العربية، القاهرة، ٢٠٠٧م.
٩. باسل عبد الله الضمور، "غسل الأموال في المصارف -دراسة مقارنة"، مكتبة القانون والاقتصاد، الرياض، ط١، ٢٠١٣م.
١٠. بشار دودين، "الإطار القانوني للعقد المبرم عبر شبكة الإنترنت"، دار الثقافة للنشر والتوزيع، عمان، ط١، ٢٠٠٦م.
١١. بلال أمين زين الدين، "جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشرعية الإسلامية"، دار الفكر الجامعي، الإسكندرية، ط١، ٢٠٠٨م.
١٢. جميل عبد الباقي الصغير، "الجوانب الإجرائية للجرائم المتعلقة بالإنترنت"، دار النهضة العربية، القاهرة، ٢٠٠١م.

١٣. حسن الحمادي، "عقود وخدمات المعلومات، دراسة في القانون المصري والفرنسي"، دار الثقافة للنشر والتوزيع، عمان، الطبعة الأولى، ٢٠٠٣م.
١٤. حسين بن سعيد الغافري، "السياسة الجنائية في مواجهة جرائم الإنترنت"، دار النهضة العربية، القاهرة، ٢٠٠٩م.
١٥. خالد السيد محمد عبد المجيد موسى، "إبرام عقد العمل الإلكتروني دراسة مقارنة"، مركز الدراسات العربية للنشر والتوزيع، مصر، الجيزة، ط١، ٢٠١٨م.
١٦. خالد العتيبي، "الجوانب الإجرائية في الجرائم المعلوماتية: دراسة مقارنة"، مكتبة القانون والاقتصاد، الرياض، ٢٠١١م.
١٧. خالد ممدوح إبراهيم، "فن التحقيق الجنائي في الجرائم المعلوماتية"، دار الفكر الجامعي، الإسكندرية، ط١، ٢٠٠٩م.
١٨. رياض فتح الله بصله، "جرائم بطاقات الائتمان دراسة معرفية تحليلية لمكوناتها وأساليب تزييفها وطرق التعرف عليها"، دار الشروق، ط١، ١٩٩٥م.
١٩. ساري محمد الخالد، "اتجاهات في أمن المعلومات وأمانها-أهمية تقنيات التعمية (الشفرة)"، مكتبة العبيكان للنشر، ط١، ٢٠١٨م.
٢٠. سامر سلمان الجبوري، "جريمة الاحتيال الإلكتروني دراسة مقارنة"، مكتبة زين الحقوقية، ط١، ٢٠١٨م.
٢١. سعيد عبد اللطيف حسن، "اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت"، دار النهضة العربية، القاهرة، ط١، ١٩٩٩م.
٢٢. سليمان أحمد فضل، "المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية"، القاهرة، ٢٠٠٧م.
٢٣. سمير دنون، "العقود الإلكترونية في إطار تنظيم التجارة الإلكترونية"، المؤسسة الحديثة للكتاب، لبنان، ط١، ٢٠١٢م.
٢٤. ضرغام جابر عطوش آل مواش، "جريمة التجسس المعلوماتي -دراسة مقارنة"، المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع، ط١، ١٤٣٨ - ٢٠١٧م.
٢٥. عائشة بن قارة، "حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن"، دار الجامعية الجديدة، ٢٠١٠م.

٢٦. عبد الحسن الحسيني، "القاموس الموسوعي في المعلومات والاتصالات المعلوماتية القانونية"، مكتبة صادر، بيروت، ط١، ٢٠٠٤م.
٢٧. عبد الحميد بسيوني، "طرق وبرامج الهاكرز وقرصنة المعلومات"، دار الكتب العلمية، للنشر والتوزيع، القاهرة، ٢٠١٣.
٢٨. عبد العال الديري، محمد صادق إسماعيل، "الجرائم الإلكترونية - دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت"، المركز القومي للإصدارات القانونية، القاهرة، ط١، ٢٠١٢م.
٢٩. عبد الفتاح حجازي، "الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت"، دار الكتب القانونية، ط١، ٢٠٠٥.
٣٠. عبد الفتاح مراد، "شرح جرائم الكمبيوتر والإنترنت"، دار الكتب والوثائق المصرية، دون سنة نشر.
٣١. عبد القادر أحمد محمد الصباغ، "قيد الأوراق المالية في البورصة دراسة مقارنة بين النظامين المصري والسعودي"، المركز العربي للنشر والتوزيع، مصر، ٢٠١٨م.
٣٢. عبد القادر عبد الحافظ الشخيلي، "جرائم الاحتيال المعاصرة"، جامعة نايف العربية للعلوم الأمنية، الرياض، ط١، ٢٠٠٥م.
٣٣. عبد الكريم خالد الردايدة، "الجرائم المستحدثة واستراتيجية مواجهتها"، دار ومكتبة الحامد للنشر والتوزيع، عمان، ط١، ٢٠١٣م.
٣٤. عبد الله بن جهيم الزمامي، "غسل الأموال في المملكة العربية السعودية دراسة مقارنة"، مكتبة القانون والاقتصاد للنشر والتوزيع، ط١، ٢٠١٠م.
٣٥. عبد الله سيف الكيتوب، "الأحكام الإجرائية لجريمة الاحتيال المعلوماتي"، دار النهضة العربية، القاهرة، ٢٠١٣م.
٣٦. عصمت عبد المجيد بكر، "دور التقنيات العلمية في تطوير العقد"، دار الكتب العلمية، لبنان، ٢٠١٥م.
٣٧. عفيف كامل عفيفي، "جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية"، مكتبة الأهرام، القاهرة، ٢٠٠٠م.

٣٨. عفيفي كامل عفيفي، "جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون"، منشورات الحلبي الحقوقية، بيروت ٢٠٠٣م.
٣٩. علي جبار صالح الحسيناوي، "جرائم الحاسوب والإنترنت"، دار اليازوري العلمية للنشر والتوزيع، ٢٠١١م.
٤٠. علي حسن الطوالبة، "التفتيش الجنائي على نظم الحاسوب والإنترنت"، الطبعة الأولى ٢٠١٠م.
٤١. علي حسن الطوالبة، "الجرائم الالكترونية"، جامعة العلوم التطبيقية - جامعة البحرين، مؤسسة فخراوي للدراسات والنشر - البحرين، ط ٢، ٢٠٠٩م.
٤٢. علي مؤيد سعيد، "التحويل الالكتروني للأموال دراسة مقارنة"، البنك المركزي العراقي، قسم إدارة الموارد البشرية، ٢٠١٣.
٤٣. عمر أبو بكر يونس، "الجرائم الناشئة عن استخدام الإنترنت (الأحكام الموضوعية والجوانب الإجرائية)"، دار النهضة العربية، ٢٠٠٤.
٤٤. عمر بن يونس، "الجرائم الناشئة عن استخدام الإنترنت"، دار النهضة العربية، القاهرة، ط ١، ٢٠٠٤م.
٤٥. عوض منصور محمد أبو النور، "مقدمة في علم الحاسب الالكتروني وبرمجة بيسك"، دار الأمل، إربد، الأردن، ط ٥، ١٩٩٦م.
٤٦. غادة نصار، "الإرهاب والجريمة الإلكترونية"، العربي للنشر والتوزيع، القاهرة، ط ١، ٢٠١٧م..
٤٧. فتوح الشاذلي، "جرائم الكمبيوتر"، منشورات الحلبي، ٢٠٠٣م.
٤٨. كوثر فرام، "الجريمة المعلوماتية على ضوء العمل القضائي المغربي"، المعهد اعالي للقضاء، وزارة العدل، ٢٠٠٩م.
٤٩. كوثر مازوني، "الشبكة الرقمية وعلاقتها بالملكية الفكرية"، دار الجامعة الجديدة، طبعة ٢٠٠٨م.
٥٠. محمد أبو بكر محمد سلامة، "موسوعة جرائم المعلوماتية"، منشأة المعارف، الإسكندرية، ٢٠٠٦م.

٥١. محمد أحمد طه، "المواجهة التشريعية لجرائم الكمبيوتر والإنترنت دراسة مقارنة"، دار الفكر والقانون للنشر والتوزيع، ٢٠١٦-٢٠١٧م.
٥٢. محمد الشوابكة، "جرائم الحاسوب والإنترنت- الجريمة المعلوماتية"، دار النهضة العربية، القاهرة، ط١، ٢٠٠٧م.
٥٣. محمد الهادي، "تكنولوجيا المعلومات وتطبيقاتها"، دار الشروق، القاهرة، ١٩٨٩م.
٥٤. محمد أمين أحمد الشوابكة، "جرائم الحاسوب والإنترنت"، مكتبة دار الثقافة والتوزيع، عمان، ط١، ٢٠٠٤.
٥٥. محمد جلال عبد الرحمن، "الجرائم الإلكترونية في الفقه الإسلامي والقوانين المقارنة" "دراسة مقارنة"، مكتبة القانون والاقتصاد، الرياض، ط١، ٢٠١٥م.
٥٦. محمد حماد مرهج الهيبي، "الجريمة المعلوماتية نماذج من تطبيقاتها -دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني"، دار الكتب القانونية، ٢٠١٤م.
٥٧. محمد حماد مرهج الهيبي، "الحماية الجنائية لبطاقات الإئتمان الممغنطة"، دار الكتب القانونية، مصر، ٢٠٠٩م.
٥٨. محمد سالم الزعبي، "الجرائم الواقعة على السمعة عبر تقنية المعلومات الإلكترونية"، المجلس الوطني للإعلام، الإمارات، ط١، ٢٠١٤.
٥٩. محمد سامي الشوا، "ثورة المعلومات وانعكاساتها على قانون العقوبات"، دار النهضة العربية، القاهرة، ١٩٩٣م.
٦٠. محمد صادق إسماعيل، "الجرائم الإلكترونية -دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت"، المركز القومي للإصدارات القانونية، القاهرة، ط١، ٢٠١٢.
٦١. محمد طارق الخن، "جريمة الاحتيال عبر الإنترنت" الأحكام الموضوعية والأحكام الإجرائية"، منشورات الحلبي الحقوقية، بيروت، ط١، ٢٠١١م.
٦٢. محمد عبد الله أبو بكر سلامة، "موسوعة جرائم المعلوماتية - جرائم الكمبيوتر والإنترنت"، منشأة المعارف، الإسكندرية، ٢٠٠٦م.

٦٣. محمد عبيد الكعبي، "الجرائم الناشئة عن الاستخدام الغير مشروع بشبكة الإنترنت"، دار النهضة العربية، ط٢، ٢٠٠٩م.
٦٤. محمد علي العريان، "الجرائم المعلوماتية"، دار الجامعة الجديدة، الإسكندرية، المكتبة القانونية، ٢٠٠٤م.
٦٥. محمد علي العريان، "الجرائم المعلوماتية"، دار الجامعة الجديدة، الإسكندرية، ٢٠١١م.
٦٦. محمد علي قطب، "الجرائم المعلوماتية وطرق مواجهتها"، الجزء الثاني، وزارة الداخلية، الأكاديمية الملكية للشرطة، مارس ٢٠١٠م.
٦٧. محمد فهمي طلبة، "فيروسات الحاسب الآلي وأمن البيانات"، مطابع الكتاب المصري الحديث، القاهرة، ١٩٩٢م.
٦٨. محمد كمال محمود الدسوقي، "الحماية الجنائية لسرية المعلومات الإلكترونية -دراسة مقارنة"، دار الفكر والقانون للنشر والتوزيع، ط١، ٢٠١٥.
٦٩. محمد محرم علي، "جريمة النصب والاحتيال والتجارة الإلكترونية"، دار النهضة العربية، القاهرة، ١٩٩٨م.
٧٠. محمد نصر محمد، "الوسيط في الجرائم المعلوماتية"، مركز الدراسات العربية للنشر والتوزيع، ط١، ٢٠١٥.
٧١. مروة زين العابدين صالح، "الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني"، مركز الدراسات العربية للنشر والتوزيع، مصر-الجيزة، ط١، ٢٠١٦م.
٧٢. مروة شبل عجيزة، خالد بطي الشمري، "التسويق الإلكتروني في العالم العربي"، دار النشر للجامعات، مصر، ط١، ٢٠١٢.
٧٣. مصطفى محمد موسى، "أساليب إجرامية بالتقنية الرقمية ومكافحتها"، مطابع الشرطة، ط١، ٢٠٠٣م.
٧٤. مصطفى محمد موسى، "دليل التحري عبر شبكة الانترنت"، دار الكتب القانونية، القاهرة، ٢٠٠٥م.

٧٥. مصطفى موسى، "المراقبة الالكترونية عبر شبكة الإنترنت "دراسة مقارنة" بين المراقبة الأمنية التقليدية والالكترونية"، الكتاب الخامس، دار الكتب والوثائق القومية المصرية، ٢٠٠٣م.
٧٦. ممدوح عبد المطلب، "البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت"، دار الكتب القانونية، القاهرة، ٢٠٠٦م.
٧٧. منير محمد الجنيهي، "جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها"، دار الفكر الجامعي، ٢٠٠٦م.
٧٨. مي عبد الله، "نظريات الاتصال"، دار النهضة العربية، بيروت، ٢٠٠٦م.
٧٩. نائلة قورة، "جرائم الحاسب الآلي الاقتصادية"، منشورات الحلبي الحقوقية، بيروت، ط١، ٢٠١٢م.
٨٠. نبيلة هروال، "الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات "دراسة مقارنة"، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م.
٨١. ندى محمود ذنون، "عقد الاشتراك بخدمات الاتصالات (دراسة مقارنة)"، رسالة ماجستير، جامعة الموصل، ٢٠٠٩م.
٨٢. نوفل الصفو ومحمد عزت فاضل، "جرائم تقنية المعلومات المخلة بالأخلاق العامة - دراسة مقارنة"، مكتبة السنهوري، بيروت، ٢٠١٧م.
٨٣. هدى قشقوش، "جرائم الحاسب في التشريع المقارن"، دار النهضة العربية، القاهرة، الطبعة الأولى، ١٩٩٢م.
٨٤. هشام محمد رستم، "قانون العقوبات ومخاطر تقنية المعلومات"، مكتبة الآلات الحديثة، القاهرة، ١٩٩٤م.
٨٥. هشام محمد فريد رستم، "الجوانب الإجرائية للجرائم المعلوماتية"، مكتبة الآلات الحديثة، أسيوط، ط١، ١٩٩٤م.
٨٦. هلال البوسعيدي، "الحماية القانونية والفنية لقواعد المعلومات المحوسبة" دراسة قانونية وفنية مقارنة"، دار النهضة العربية، ٢٠٠٩م.

رابعاً: الرسائل العلمية:

١. اياد حسين عباس العزاوي، جريمة الاختتيال في القانون العراقي، دراسة مقارنة، رسالة ماجستير مقدمة إلى كلية القانون والسياسة جامعة بغداد، ١٩٨٨.
٢. بدر بن أحمد بن محمد الزهراني، "جريمة الاختتيال الإلكتروني في النظام السعودي - دراسة مقارنة"، جامعة نايف العربية للعلوم الأمنية، الرياض، رسالة ماجستير، ١٤٣٦ - ٢٠١٥م.
٣. درار نسيم، "الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني - دراسة مقارنة"، جامعة أبو بكر بلقايد، الجزائر، أطروحة دكتوراه، ٢٠١٥ - ٢٠١٦م.
٤. سامر سلمان الجبوري، "جريمة الاختتيال المعلوماتي"، رسالة ماجستير، جامعة النهرين، ١٤٣٥ - ٢٠١٤م.
٥. سعيد نعيم، "آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري"، رسالة ماجستير، جامعة الحاج لخضر، باتنة، ٢٠١٣م.
٦. صخير يوسف، "الجريمة المرتكبة عبر الإنترنت"، جامعة مولود معمري، الجزائري، رسالة لنيل شهادة الماجستير، ٢٠١٣م.
٧. عبد الله دغذ العجمي، "المشكلات العملية والقانونية للجرائم الإلكترونية" - دراسة مقارنة، جامعة الشرق الأوسط، رسالة ماجستير، ٢٠١٤م.
٨. فهد عبد الله العازمي، "الإجراءات الجنائية المعلوماتية"، رسالة دكتوراه، كلية القانون بجامعة عين شمس، كلية القانون، القاهرة، ٢٠١٢م.
٩. معتوق عبد اللطيف، "الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن"، رسالة ماجستير، ٢٠١١ - ٢٠١٢م.
١٠. نورة طرشي، "مكافحة الجريمة المعلوماتية"، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر، ٢٠١١ - ٢٠١٢م.
١١. يوسف خليل يوسف العفيفي، "الجرائم الإلكترونية في التشريع الفلسطيني - دراسة تحليلية مقارنة"، الجامعة الإسلامية، غزة، رسالة ماجستير، ١٤٣٥ / ٢٠١٣م.

خامسا: البحوث العلمية:

١. أبو الوفا محمد أبو الوفا إبراهيم، "المسؤولية الجنائية عن الاستخدام غير المشروع لبطاقة الائتمان في القانون المقارن والفقه الإسلامي"، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون لكلية الشريعة والقانون وغرفة تجارة وصناعة دبي والذي عقد في دولة الإمارات العربية المتحدة للفترة من ١٠ - ١٢/٥/٢٠٠٣، ٢٠٠٣ م.
٢. أشد البلوشي، "ورقة عمل حول الدليل في الجرائم المعلوماتية مقدمة إلى المؤتمر الدولي حول "حماية المعلومات والخصوصية في قانون الإنترنت"، برعاية الجمعية الدولية لمكافحة الاجرام السيبري بفرنسا، القاهرة، ٢٠٠٨ م.
٣. خالد حامد مصطفى، "المسؤولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل الاجتماعي"، مجلة رؤى استراتيجية، مركز الإمارات للدراسات والبحوث الاستراتيجية، المجلد الأول، العدد ٢، مارس ٢٠١٣.
٤. خالد ممدوح العزي، "الجرائم المالية الإلكترونية الجرائم المصرفية انموذجا"، مركز جيل البحث العلمي، المؤتمر الدولي الرابع عشر، طرابلس ٢٤-٢٥ مارس ٢٠١٧ م.
٥. ذياب موسى البداينة، "دور الأجهزة الأمنية في مكافحة جرائم الإرهاب المعلوماتي"، الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية، المنعقدة بكلية التدريب قيم البرامج التدريبية، القنيطرة، المملكة المغربية، أيام ٩-١٣، ابريل ٢٠٠٦ م.
٦. راشد بشير راشد، "التحقيق الجنائي في جرائم تقنية المعلومات"، دراسة صادرة عن مركز الإمارات للدراسات والبحوث الاستراتيجية، العدد ١٣١، ٢٠٠٨.
٧. رضا أحمد المزغني، "أساليب وصور الاحتيال المنظم"، جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث قسم الندوات واللقاءات العلمية، ندوة نظمت بالمنصورة بتاريخ ١٨-٢٠-٢٠٠٧ حول العلاقة بين جرائم الاحتيال والإجرام المنظم.
٨. طارق الجملي، "الدليل الرقمي في مجال الإثبات الجنائي"، ورقة عمل مقدمة للمؤتمر المغاربي الأول للمعلوماتية المنعقد في الفترة (٢٨-٢٩ / أكتوبر ٢٠٠٩) تنظمه أكاديمية الدراسات العليا، طرابلس.

٩. على محمود حمودة، "الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات

الجنائي"، بحث مقدم ضمن اعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، نظمتها شرطة دبي، في الفترة من ٤ أفريل إلى ٢٦ أفريل عام ٢٠٠٣م.

١٠. مجمع البحوث والدراسات، "الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها"، أكاديمية السلطان قابوس لعلوم الشرطة، سلطنة عمان، ٢٠١٦م.

١١. هدى حامد قشقوش، "الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني"، بحوث مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، من ١-٣ مايو ٢٠٠٠م، ط٢.

١٢. يونس العرب، "ورقة عمل بعنوان "التشريعات والقوانين المتعلقة بالإنترنت في الدول العربية"، مقدمة إلى مؤتمر ومعرض التكنولوجيات المصرفية العربية والدولية، اتحاد المصارف العربية، الأردن، ٢٨-٢٩ تشرين أول ٢٠٠٢م.

سادسا: الدوريات والمقالات:

١. سعد سلامة، "دليل مأموري الضبط القضائي في كيفية تنفيذ الإذن بالتفتيش" مجلة

مركز بحوث الشرطة، أكاديمية مبارك للأمن، العدد ٣٠، يوليو ٢٠٠٦م.

٢. شاهر فلاح العرود وطلال حمدون شكر، "جودة تكنولوجيا المعلومات وأثرها في كفاءة التدقيق الداخلي في الشركات الصناعية والخدمية المساهمة العامة الأردنية"، المجلة الأردنية في إدارة الأعمال، المجلد ٥، العدد ٤، ٢٠٠٩ م.

٣. طالب محمد جواد عباس، عبد الجبار ضاحي عواد، "جرائم تقنية المعلومات وإثباتها"، مجلة كلية الرافدين الجامعية للعلوم، العدد ٢٨، السنة الثالثة عشر، ٢٠١١م.

٤. عائشة البريملي، "تقنية البلوتوث (الإيجابيات -المخاطر -الحلول) دراسة ميدانية"، شرطة الشارقة - مركز بحوث الشرطة، الإمارات، ٢٠٠٦م.

٥. عبيد صالح حسن، "سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية"، مجلة الفكر الشرطي، المجلد الرابع والعشرون، العدد ٩٥، أكتوبر ٢٠١٥م.

٦. عدنان زيدان، "الإجراءات الجنائية" في دولة الإمارات العربية المتحدة، الجزء الأول، مطبوعات كلية الشرطة، دبي، دون سنة نشر.
٧. كامل فريد السالك، "الجريمة المعلوماتية"، الجمعية السورية للمعلوماتية، حلب، محاضرة أُلقيت في مؤتمر الجمعية السورية للمعلوماتية، ٢٠٠٠م.
٨. لورنس سعيد الحوامة، "الجرائم المعلوماتية أركانها وآلية مكافحتها -دراسة تحليلية مقارنة"، مجلة الميزان للدراسات الإسلامية والقانونية، جامعة العلوم الإسلامية العالمية، ٢٠١٦-٢٠١٧.
٩. ليندة عبد الله، "تبييض الأموال عن طريق الاعتماد المستندي للأموال"، مجلة جيل للبحث العلمي، عدد خاص عن اعمال المؤتمر الدولي الرابع عشر، طرابلس ٢٤-٢٥ مارس ٢٠١٧م.
١٠. محمد الهيتي، "جريمة الدخول إلى النظام الآلي لمعالجة المعطيات عن طريق الغش - دراسة في ضوء التشريع الفرنسي"، مجلة النهرين، العراق، المجلد ٩، العدد ١٥، شباط، ٢٠٠٦م.
١١. نوفل علي عبد الله، ومحمد عزت، "جريمة إنشاء موقع أو نشر معلومات مخلة بالآداب العامة بوسائل تقنية المعلومات"، مجلة الراافدين للحقوق، المجلد ١٢، العدد ٤٤، ٢٠١٠.
١٢. هشام محمد رستم، "الجرائم المعلوماتية، أصول التحقيق الجنائي الفني"، مجلة الأمن والقانون، دبي، العدد ٢، ١٩٩٩م.
١٣. هلال البياتي، وعبد الستار الكبيسي، وعوني الفخري، "تدوة القانون والحاسوب"، سلسلة المائدة الحرة، رقم (٣٧)، بيت الحكمة، بغداد، مطبعة اليرموك، ١٩٩٩م.

سابعاً: المراجع الأجنبية:

1. Advantages and disadvantages of electronic payment systems, unichange.me.
2. Apwg, Phishing Activity Trends Report, 1st Quarter 2018, Unifying The Global Response To Cybercrime, Published July 31, 2018. [Http://Docs.Apwg.Org/Reports/Apwg_Trends_Report_Q1_2018.Pdf](http://Docs.Apwg.Org/Reports/Apwg_Trends_Report_Q1_2018.Pdf)
3. Crime du 10 de'c 1975, J.C.P. 1970-17977 nate Gassin.
4. Gaston Stefanie, G. Levasseur, B Baulac, dreuit penal general D 15, Dolla, 2 1995.

https://unichange.me/articles/advantages_of_electronic_payment_systems.

5. Pradel et Feuillard, Les infraction commises au money de l'ordinateur Rev, de La pen crim 1985.
6. Rika Butler, "A framework of anti-phishing measures aimed at protecting the online consumer's identity", The Electronic Library, Vol. 25 Issue: 5, 2007. <https://www.researchgate.net/publication/220677176/download>.

Abstract

A Cybercrime is a kind of crime committed by using information technology. The potential seriousness of this crime lies in its adverse effect on the economic activities and the national economy as a whole. It takes place at the Electronic Fund Transfer System (EFTS), bank deposits, Electronic money or e-money, due to the magnitude and scope of financial trading through EFTS, and thereby reducing distances to allow carrying out cross-border fraud in several countries.

Such systems are recognized as a means of saving time to finalize transactions and remittances, as well as theft by fraudulent means in just a few seconds.

Technically and broadly speaking, automated processing system and computer data stored therein are being tampered with .There is an array of technical methods used in the manipulation of computer data for fraudulent purposes , more importantly is tampering with any data entered in the computer , software and remote database access , and this can be done in several ways: entry of synthetic or artificial data and damage and deletion of information already stored in the computer.

As regards infringement of information system software, such programs or operating systems are being modified or some programs are being manufactured for use in the process of fraud.

The key purpose of the fraud is to seize third-party movable property with the intention of owning the same by means of tampering with data and information to obtain funds and assets owned by third parties .the most vulnerable data to

manipulation are related to receivables, bank deposits, credit cards, balance sheet results and accounts.

The key feature of cybercrime is that the evidence left by the hacker is located in an electronic environment, based on manipulation of data and programs, and potential hacker hide their crimes and tamper with evidence, so the judicial authorities must deal with these crimes based on the electronic or digital evidence.

Therefore, most systems of comparative countries such as Bahraini, Emirati, Saudi lawmakers have enacted laws to combat this crime and the perpetrators to be punished in proportion to the nature of such crimes.

Hence, the study has recommended that some articles of the Anti-Cybercrime Laws in Bahrain, UAE and Saudi Arabia shall be included by defining “cybercrime” and explicitly providing for the place and subject matter of this crime, which leaves no room for interpretation and difference. The Anti-Cybercrime Laws in Bahrain, UAE and Saudi Arabia shall include articles setting out the procedures governing investigation such as inspection, search and seizure in order to avoid any misinterpretation of procedures stated in the laws of criminal procedure, and due to the specificity of cybercrime in general, and the crime of cyberfraud in particular.

UNIVERSITY OF BAHRAIN

College of Law



Department Of Public Law

FRAUD CRIME USING IT IN THE BAHRAINI COMPARED LEGISLATION

" A Comparative Study "

A Thesis Submitted in Partial Fulfillment of the Requirements for the Master
Degree in Public Law

Submitted by

Khaled ali salman

University number:20150045

Supervised by

Dr. Adel Hamed Bashir

Associate Professor of the Administrative Law

Kingdom of Bahrain

December 2019