جرائم الحاسوب والإنترنت

الجريمة المعلوماتية(*)

عرض وتحليل

إبراهيم عبد الموجود حسن

مركز المعلومات والتوثيق – اللجنة الاستشارية العليا

الديوان الأميرى – الكويت

فى كل سبق حضارى يحققه الإنسان لابد أن يصاحبه جوانب إيجابية مضيئة وأخرى سلبية مظلمة ، وهذا ما يحدث الآن بالنسبة لظاهرة الإنترنت ، والتى تعد بكل المقاييس إنجازاً حضارياً غير مسبوق فى سرعة وحرية تدفق المعلومات على نطاق العالم كله ، وبالرغم من كل الجوانب الإيجابية التى صاحبت الظاهرة . إلا أن جوانبها السلبية لم ينج منها الإنسان ، وأصبحت الجرائم التى ترتكب من خلالها أو بواسطتها نقطة سوداء فى الثوب ناصع البياض .

وهذه الجرائم – كطبيعة المعلومات نفسها – تعد جرائم بدون ملامح بارزة لا يستخدم فيها أسلحة أو تسفك فيها دماء ، وإنما هى جرائم عامدها العقل والتفكير تخطيطاً وتنفيذاً ، تماماً كالمرحلة الصناعية التى نعيشها والتى تعتمد فى الأساس على العقل والذهن والتفكير ألا وهى صناعة المعلومات ، وتبقى فى النهاية جريمة كبقية الجرائم المرتبطة بالتكنولوجيا المعاصرة مهما اختلفت الدواعى والأسباب .

والكتاب الذى نستعرضه فى هذه السطور . هو واحد من الكتب الصادرة حديثاً التى تتناول ظاهرة الاستخدام السئ وغير المشروع لشبكة الإنترنت والتى يعاقب عليها القانون ، والموضوع بلا شك من الموضوعات الجادة والمثيرة فى الوقت نفسه وذو جوانب عديدة قانونية واجتماعية واقتصادية وأخلاقية ، ولكنه ينطوى تحت ما يعرف حديثاً باسم «الجريمة المعلوماتية» :

وقد أحسن الباحث فى عرض عناصر الموضوع فجاءت بشكل واضح ومركز ومفهوم دون الاستغراق فى المسائل الفقهية والقانونية العويصة وبالرغم من أنه لم يتعد ٢٦٥ صفحة . واشتمل البحث على مقدمة وبابين :

(*) محمد أمين أحمد الشوابكة . جرائم الحاسوب والإنترنت: الجريمة المعلوماتية .– عمان : مكتبة دار الثقافة للنشر والتوزيع ، ٢٠٠٤ .– ٢٦٥ ص .

- **الباب الأول** : أهم جرائم الإعتداء على الأشخاص عبر الإنترنت ويشمل الفصل :

الفصل الأول : جرائم الذم والقدح والتحقير (القذف والسب) عبر الإنترنت .

الفصل الثانى : جرائم الإعتداء على حرمة الحياة الخاصة عبر الإنترنت .

الفصل الثالث : جرائم الإستغلال الجنسى للأطفال عبر الإنترنت .

- **الباب الثانى** : نوعية جرائم الإعتداء على الأموال عبر الإنترنت ويشمل الفصل :

الفصل الأول : سرقة المال المعلوماتى المعنوى عبر الإنترنت .

الفصل الثانى : التحويل الإكترونى غير المشروع للأموال عبر الإنترنت .

الفصل الثالث : إتلاف نظم المعلوماتية عبر الإنترنت .

تعريف الجريمة المعلوماتية :

فى مقدمة البحث التى شملت الصفحات ٧-٢٧ من الكتاب ، حدد الباحث موضوع بحثه بالجرائم المرتبطة بشبكة الإنترنت بوصفها نتاج المعلوماتية - وكأداة للربط والاتصال بين مختلف شعوب العالم ، فإنها تشكل أداة لإرتكاب الجريمة أو محلاً لها وذلك بإساءة استخدامها واستغلالها على نحو غير مشروع ، مما أدى إلى ظهور طائفة جديدة من الجرائم عرفت بالجريمة المعلوماتية . وعدد الباحث التعريفات الفقهية التى تناولت هذه الظاهرة ، والتى اختلفت ما بين تعريف ضيق وتعريف واسع . ومن بين التعريفات الواسعة للجريمة ما ذهب إليه بعض الفقهاء إلى القول بأن الجريمة المعلوماتية تتمثل فى :

«كل عمل أو امتناع يأتيه الإنسان إضراراً بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به باعتبارها من المصالح والقيم المتطورة التى تمتد مظلة قانون العقوبات لحمايتها» .

«كل فعل أو امتناع عمدى ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ، ويهدف إلى الاعتداء على الأموال المادية والمعنوية» .

وتبنـــى مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين تعريفاً جامعاً لجرائم الحاسب الآلى وشبكاته ، حيث عرف الجريمة المعلوماتية بأنها :

«أية جريمة يمكن ارتكابها بواسطة نظام حاسوبى أو شبكة حاسوبية ، أو داخل نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التى يمكن إرتكابها فى بيئة إلكترونية» .

وهذا التعريف فى رأى الباحث هو من أفضل التعريفات التى تناولت ظاهرة الإجرام المعلوماتى . إذ أنها تشمل كلا الجانبين المادى والمعنوى للحاسب الآلى ومنها شبكة الإنترنت ، وكذلك فإنه لا يقتصر على مجرد كون الحاسب الآلى وشبكاته محلاً للإعتداء بل أيضاً بوصفه وسيلة للإعتداء وإرتكاب الجرائم .

وبدوره قدم الباحث تعريفاً للجرائم المرتكبة عبر الإنترنت أو الجريمة المعلوماتية ، على أنها :

«كل إعتداء يقع على نظم الحاسب الآلى وشبكاته أو بواسطتها» .

النطاق القانونى للجريمة المعلوماتية :

تدخل الجرائم المرتكبة عبر الإنترنت فى نطاق دراسات القانون الجنائى الداخلى (الوطنى) والتى تقع فى صميم القسم الخاص لقانون العقوبات ، وحيث أنها من الجرائم ، يضيف الباحث ، التى تتخطى حدود الدولة الواحدة فهى تدخل أيضاً فى نطاق دراسات القانون الجنائى وتدخل كذلك فى عداد الجريمة المنظمة التى تقوم على أساس تنظيم هيكلى وتدرجى له صفة الاستمرارية لتحقيق مكاسب طائلة ، ونظراً لنمو وتزايد التجارة الإلكترونية عبر الشبكة من خلال المبادلات والمراسلات التجارية الإلكترونية فإن جرائم الإنترنت لصيقة الصلة بالقانون التجارى وبحركة التجارة العالمية الحديثة ، وكذلك ترتبط الجريمة بالقانون الدستورى حيث أدى تزايد إنتهاك الحقوق الأساسية والحريات الفردية للأفراد فى مجتمع المعلومات الإلكترونى والتى كفلتها القوانين الدستورية . كما ترتبط بالقانون الإدارى خاصة مع ظهور ونمو الحكومات الإلكترونية ، كذلك فإن ظهور العقود الإلكترونية e-contract واتمام عمليات البيع والشراء عن بعد ، تظهر إرتباط الموضوع بالقانون المدنى وبفروع القانون الخاص الداخلى والدولى ولاسيما بظهور التحكيم عن بعد أو التحكيم الإلكترونى e-arbitration ، كما لا يمكن تجاهل البعد الاقتصادى وارتكاب الجرائم عبر الإنترنت إذ قد تمارس خلالها أنشطة اقتصادية غير مشروعة ، والتى تندرج تحت ما يسمى بالاقتصاد الخفى ، وبصفة عامة – يضيف الباحث – فإن إساءة استخدام شبكة الإنترنت تتداخل مع جميع فروع القانون الداخلى والخارجى . غير أن أخطر ما جاءت به يبرز فى مواجهة القانون الجنائى الداخلى والدولى .

أهمية دراسة الجريمة المعلوماتية :

عدد الباحث الأسباب الهامة التى من أجلها قام بدراسة موضوع الجريمة المعلوماتية ، فذكر أن الجرائم المرتكبة عبر الإنترنت تعد من الموضوعات الحديثة التى فرضت نفسها على المستوى الوطنى والدولى على حد سواء ، والتى ينبغى على المشرع الجنائى مواجهتها بتشريعات حاسمة لمكافحتها وعقاب مرتكبيها ، وبيّن أنه من الناحية العملية فإن المعلوماتية تثير . باعتبارها علم المعالجة الآلية للبيانات، مشكلات قانونية عدة ، إذ يساء استخدامها لإرتكاب الجريمة من ناحية أو تكون محلاً للإعتداء عليها من ناحية أخرى ، مما يثير مسألة تكييف الإعتداء ، وما إذا كان يشكل جريمة أم لا ؟ ، بالإضافة إلى ما تثيره من مشكلة تحديد الاختصاص القضائى والقانونى الواجب التطبيق على الجرائم المرتكبة عبرها ، وعلاوة على ذلك فإن الإجراءات الجنائية المتبعة فى ملاحقة مرتكبى الجرائم المعلوماتية تثير الكثير من المشكلات القانونية بدءاً من مرحلة الاستدلال وجمع الأدلة . حتى صدور الحكم الجنائى ولا سيما فيما يتعلق بإثبات الجرائم المرتكبة عبر الإنترنت وصلاحية الدليل الرقمى digital evidence للإثبات ومدى شرعية الأدلة المتحصلة بواسطة الإنترنت وقبولها لدى القاضى الجنائى .

وتغدو أهمية الموضوع – كما يوضح الباحث – من كون المعلومة قوة ، وتمثل قيماً اقتصادية مستحدثة ، مما ينبغى معه إحقاق مبدأ الحق فى المعلومات ، وذلك بتحقيق التوازن بين الاستخدام الحر والكامل للمعلومات ، وبين الحقوق والحريات

والمصلحة العامة ، بحماية من تتعلق بهم المعلومات من المساس بشرفهم أو اعتبارهم أو حرمة حياتهم الخاصة ، أو استخدام هذه المعلومات على نحو غير مشروع فى إرتكاب جرائم الغش المعلوماتى ، وإذا كانت الدولة تكرس نظام الاقتصاد الحر القائم على حرية تداول السلع والخدمات ، فإن وجد التجريم يتغير مما يظهر أهمية الموضوع اقتصادياً .

واجتماعياً تؤثر ظاهرة الإجرام المعلوماتى سلباً على الطبقات الاجتماعية فتزيد الهوة بينها بمقدار ما تملك من المعلومات ، فيجد ذوى الياقات البيضاء الفضاء الإلكترونى Syper Space مناخاً مناسباً لهم لمباشرة أعمالهم ، وتجد العصابات الإرهابية شبكة الإنترنت خير وسيلة لبث ونشر أفكارها والتشجيع على القيام بأعمال إرهابية .

أما من الناحية النظرية فتبرز أهمية الدراسة – كما يؤكد الباحث – لمعرفة مدى كفاية النصوص الجنائية الحالية لمنع الجرائم المرتكبة عبر الإنترنت وردع مرتكبيها ، وهل المواجهة الجنائية هى الحل الأمثل ، أم يجب أن تكون الحل الأخير ، وهل تفى نصوص الإجراءات الجنائية فى تحقيق غايتها أم يلزم تعديل هذه النصوص بما يتواءم مع التعداد التقنى للمعلوماتية ؟ .

الجريمة في القانون المقارن :

اهتم المشرع المقارن بتجريم صور الإعتداء الناجمة عن المعالجة الآلية للبيانات والتى تنطبق بلا شك – على صور الإعتداء عبر شبكة الإنترنت ، حيث أصدر نصوصاً قانونية عدة تكفل الحماية الجنائية للحاسب الآلى وشبكاته :

- فقد أصدر المشرع الجنائى الفرنسى قانون العقوبات الجديد لسنة ١٩٩٢ والمعمول به منذ مارس ١٩٩٤ ، والذى جرم فيه صور الإعتداء الناجمة عن المعالجة الآلية للبيانات ، مما يسمح بانطباقه على الأفعال التى تقع على الإنترنت (كمحل للإعتداء) أو بواسطتها (كوسيلة للإعتداء) .
- وكذلك الأمر بالنسبة للمشروع الأمريكى فقد أصدر قوانين عدة فى مواجهة الجرائم المرتكبة عبر الإنترنت حيث أصدر قانون آداب الاتصالات عام ١٩٩٦ Communication decency Act (CDA) يجرم فيه القذف والسب عبر شبكة الإنترنت ، وكذلك يجرم التعرض للأخلاق والآداب العامة عبر الإنترنت ويكفل حماية الأطفال ضد الاستغلال الجنسى لهم ، ووسع نطاق الحماية بإصداره قانون حماية الأطفال على الخط العام ١٩٩٨ أو ما عرف بـ Child Online Protection Act (COPA) ، وفى إطار حماية حرمة الحياة الخاصة من الإعتداء عليها أصدر المشرع الأمريكى قانون الخصوصية Privacy Act (PA) عام ١٩٧٤ ، وقانون خصوصية الاتصالات الإلكترونية Electronic Communication Privacy Act (ECPA) عام ١٩٨٦ . وفى إطار حمايته للأموال المعلوماتية بجانبيها المادى والمعنوى ، أصدر المشرع قوانين متتالية بحيث تواكب التطور العلمى والتقنى فى مجال المعلوماتية وما استحدثته من مشكلات قانونية ، وكان ذلك بإصدار القانونى الفيدرالى لحماية أنظمة

الكمبيوتر (CSPA) عام ١٩٧٧ ، مروراً بقوانين السرقة الإلكترونية وقانون احتيال الأسلاك ، والقانون الفيدرالى للتجسس الاقتصادى Electronic Espiogne ACT (EEA) عام ١٩٩٦ ، وإنتهاء بالقانون الفيدرالى للغش وإساءة استخدام الكمبيوتر Computer Frud and Abuse Act (CFAA) .

- أما بالنسبة للمشرع الإنجليزى فقد بادر إلى مواجهة المشكلات القانونية الناجمة عن تطور تقنيات المعلوماتية فأفرد حماية خاصة للأطفال ضد الاستغلال الجنسى بقانون حماية الطفل لعام ١٩٧٨ (CPA) . وأصدر قانوناً خاصاً يتعلق بإساءة استخدام الكمبيوتر Computer Abuse Act (CAA) لعام ١٩٩٠ ، وكفل حماية الأفراد من مخاطر ثورة المعلومات فى قانون العدالة الجنائية والنظام العام لعام ١٩٩٤ (CJOPA) .

صور الجريمة المعلوماتية عبر الإنترنت :

استعرض الباحث بشئ من التفصيل صور الجرائم التى ترتكب عبر الإنترنت وذلك فى ضوء التشريعات المقارنة ، ولم يجد الباحث فى التشريعين الأردنى والمصرى – حتى لحظة إعداد دراسته – أية نصوص تجرم أو تحظر فعل الدخول غير المشروع إلى النظام المعلوماتى أو البقاء فيه بدون إذن – سواء كان هذا الفعل بقصد إرتكاب أية جريمة أم لا ؟ . وحدد الباحث صور الجرائم المرتكبة عبر الإنترنت بأنها تقوم أساساً على التلاعب بالبيانات والمعلومات والبرامج فيما عدا بعض الحالات . ويتم ذلك بالقيام بالمعالجة الآلية للبيانات بمحوها أو تعديلات أو تشويهها أو إلغائها أو تحويل مجراها .

وذكر الباحث أن الصورة الغالبة لتحقيق غاية (المجرم المعلوماتى) فى نطاق شبكة الإنترنت تتمثل فى فعل الدخول غير المشروع Unauthorized Access إلى النظام المعلوماتى أو البقاء فيه بدون إذن أو صلاحية ، وهو ما يعاقب فى التشريعات المتقدمة – ومن ثم قيام الجانى بإرتكاب فعله الذى يكون مجرّماً بنصوص عقابية أو لا يكون كذلك .

وبعد استعراض النصوص الواردة فى بعض التشريعات المقارنة والتى جرمت إساءة استخدام الحاسب الآلى وشبكاته العامة والخاصة ، وجد الباحث أن هنالك فرقاً بين فعل الدخول غير المشروع من ناحية وبين البقاء دون صلاحية من ناحية أخرى ، إذ أن البقاء داخل النظام المعلوماتى قد يكون نتيجة دخول مشروع أو نتيجة خطأ أثناء التجوال فى النظام ، وهما فى كلا الحالتين يقتضيان ضرورة توفر القصد الجنائى .

وتطرق الباحث إلى بعض المسائل الشيقة فى القانون الجنائى فذكر أن فعل الدخول غير المشروع إلى النظام المعلوماتى يعد من الجرائم الوقتية ، ولا يلزم توافر صفة خاصة فى مرتكبها أو الغاية من ارتكابها ، حيث يستوى الفاعل من الخبراء أو من الأفراد العاديين ، ويستوى كذلك أن يكون الدخول بهدف إرتكاب فعل غير مشروع أو لمجرد التسلية وحب الاستطلاع . وأيضاً تعد من قبيل الجرائم الشكلية التى يكتمل شكلها القانونى بمجرد تحقق السلوك الإجرامى دون تطلب عنصر آخر فى الركن المادى للجريمة . ويتحقق فعل البقاء بمجرد التواجد

المعنوى أو الإلكترونى داخل نظام المعالجة الآلية للمعلومات بدون إذن أو تصريح بذلك بما يؤدي إلى اختلاس وقت النظام متخذاً بذلك صورة الجريمة المستمرة ، وكذلك تتحقق الجريمة سواء كان الدخول إلى النظام المعلوماتى بطريق الخطأ أو الصدفة ، أو تم الدخول والبقاء فى النظام بشكل مشروع ولكن تجاوز الفاعل الوقت المحدد أو المسموح به أو الغرض الأساسى المصرح به للدخول خلافاً لإدارة صاحب الشأن المسيطر على هذا النظام.

ومن جانبه طرح الباحث مسألة فنية هامة وهى هل يشترط لقيام جريمة الدخول غير المشروع أن يكون النظام محمياً بتجهيزات أمنية إلكترونية تمنع الوصول إلى النظام كجدران النار أو ضرورة توافر كلمة مرور ، أو وجود إنذار لمنع الدخول غير المشروع ؟! .

ذهب الرأى الغالب – والبحث يؤيده – إلى عدم ضرورة وجود نظام أمن إلكترونى لكى تقوم الجريمة – وطبقاً لهذا الرأى فإن نظام الأمن لا يكون له إلا دوراً واحداً ، وهو إثبات سوء نية من قام بإنتهاك النظام والدخول بطريقة غير مشروعة ولكن القصد الجنائى يمكن إثباته بطريقة أخرى . بينما يرى البعض الآخر ضرورة وجود نظام أمنى لتجريم فعل الدخول إلى النظام المعلوماتى إذ يقتضى المنطق والعدالة توافر مثل هذا الشرط ، فوجود نظام حماية يمكن اعتباره إلتزاماً مفروضاً بنص القانون على كل من يقوم بإدارة نظام معلوماتى ، ومن ثم يفترض أن تقع الجريمة على نظام لا يجوز سوى لأشخاص محددة الدخول إليه .

وفيما إذا كان فعل الدخول غير المشروع إلى نظام المعلومات أو البقاء فيه بدون إذن يشكل تعداداً مادياً للجرائم أم أنه يشكل جريمة واحدة ؛ ذكر الباحث أقوال الفقهاء فى هذا الصدد . فمنهم من اعتبره جريمة واحدة نظراً لأن الجانى أراد بالدخول غير المشروع البقاء داخل النظام ، بينما ذهب البعض الآخر إلى تحقق الاجتماع المادى للجرائم بين جريمتى الدخول غير المشروع إلى النظام المعلوماتى والبقاء فيه مدة من الوقت ، ولكن ثار الخلاف بينهم حول تحديد الفترة التى تنتهى فيها جريمة الدخول لتبدأ بعدها جريمة البقاء غير المشروع .

وفيما يتعلق بكون جريمة الدخول إلى النظام المعلوماتى أو البقاء فيه بطريق غير مشروع من الجرائم العمدية أم لا ؟ فذكر الباحث أنها من الجرائم المادية التى تقوم بالقصد الجنائى أى بتوافر العلم والإرادة ، مضيفاً أنه يكفى أن يعلم الجانى أن يدخل إلى نظام معلوماتى خاص بالغير وأنه يتجول فيه دون أن يكون له الحق فى ذلك ، وينتفى القصد الجنائى إذا دخل المستخدم إلى النظام بطريق الخطأ لأن ذلك يعد جهلاً بالوقائع ، ولكنه يسائل جنائياً إذا دخل بطريق الخطأ إلى نظام معلوماتى ومع ذلك ظل متجولاً داخل النظام مع علمه بذلك .

اهم جرائم الإعتداء الواقعة عبر الإنترنت :

ونمضى مع الباحث فى بحثه الشيق والممتع وننتقل خلال عرضه الأساسى لأهم الجرائم الواقعة عبر شبكة الإنترنت ، والذى ركز فيه على فكرتين أساسيتين :

الأولى : فى حالة ما إذا كانت الشبكة أداة إيجابية لإرتكاب الجريمة ، أي كوسيلة تسهل للمجرم المعلوماتى تحقيق غايته الإجرامية ، ويرى الباحث فى ذلك أغلب صور جرائم الإعتداء على الأشخاص التى يتصور وقوعها على الشبكة .

الثانية : فى حالة ما إذا كانت الشبكة أداة سلبية لإرتكاب الجريمة أى محلاً لها إذ يكون هدف المجرم البيانات والمعلومات المخزنة والمنقولة عبر قنوات الإنترنت المفتوحة (العامة) أو المغلقة (الخاصة) من خلال إختراق الحواجز وجدران النار، ويرى فيها الباحث صور جرائم الإعتداء على الأموال مقتصراً على الجانب غير المادى (المعنوى) للأموال المعلوماتية .

فى الفصل الأول من الباب الأول عرض الباحث لجرائم الذم والقدح والتحقير عبر الإنترنت ، والتى تتنوع صورها (المبحث الأول) بتنوع الغرض من استخدام الإنترنت والطريقة التى تستخدم بها ، فقد يكون الذم والقدح ... وجاهياً ، عبر خطوط الاتصال المباشر ، أو يكون كتابياً أو قد يكون غيابياً، أو قد يكون بواسطة المطبوعات ، وجميع هذه الصور ترتكب عبر الشبكة من خلال المبادلات الإلكترونية الكتابية أو الصوتية أو الفيديوية ، وهى أما أن تكون بين طرفيات إنترنت متصلة (الحواسيب) ، وأما أن تكون بواسطة طرفيات إنترنت منفصلة، (مستقلة) .

وعلى هذا الأساس قسم الباحث هذا المبحث إلى مطلبين :

فى المطلب الأول عدد الباحث عدة فروع يمكن خلالها استخدام الشبكة فى الإعتداء على الأشخاص بالذم والقدح والتحقير مثل البريد الإلكترونى حيث يستطيع الجانى من خلال هذه الوسيلة أن يسند مادة معينة إلى شخص ما قد يكون معين بذاته وهى الصورة الغالبة – أو غير معين ، بحيث تنال من شرفه أو كرامته أو تعرض إلى بغض الناس واحتقارهم . ولا يلزم أن تكون هذه المادة جريمة تستلزم العقاب . وقد يقوم الجانى بالاعتداء على كرامة الغير أو شرفه أو اعتباره – ولو فى معرض الشك والإستفهام ، من دون بيان مادة معينة، فإذا ما استخدم الجانى البريد الإلكترونى للقيام بالأفعال السابقة عُد مرتكباً لجريمة الذم والقدح .

واعتبر الفرع الثانى شبكة الويب العالمية (WWW) احدى الوسائل التى يتخذها المجرم المعلوماتى كوسيلة من وسائل الذم والقدح ، وذلك من خلال إسناد مادة كتابية ، صوتية ، فيديوية صوتية (سمع بصرية) تسئ إلى أحد الأشخاص ومن شأنها أن تنال من شرفه أو كرامته أو تعرضه إلى بغض الناس واحتقارهم ، وهو غالباً ما يتخذ صورة الذم والقدح الخطى بواسطة المطبوعات ، حيث أنه من خلال صفحات الويب يتم نشر وإذاعة وتوزيع الكتابات أو الرسوم أو الصور والإستهزائية أو مسودات الرسوم (قبل أن تزين) والمكاتيب المفتوحة وبطاقات البريد التى تسيئ إلى المعتدى عليه .

وبالرغم من الاختلافات الناتجة عن اعتبار المواقع على شبكة الويب مواقع خاصة تقتصر على الاستخدام الشخصى وبالتالى تنتفى المسؤولية عن مضمون صفحات الويب الخاصة ، أم بغرض عرضها على الغير وبالتالى قيام المسؤولية الجنائية

عن الأنشطة المادية لجريمة الذم والقدح ... ، إلا إن الأنشطة المادية لهذه الجرائم قد تمارس عبر الإنترنت من خلال شبكة الويب العالمية مما يثير مسألة تنازع الاختصاص القضائى بين بلدان عدة تجيز حرية التعبير عن الرأى ولا تعد بعض الأفعال من قبيل أفعال الذم والقدح والتحقير وبين بلدان أخرى تسعى إلى تطبيق قوانينها المحلية على كل ما يمكن أن يمس حرية الأفراد أو شرفهم واعتبارهم .

وفى الفرع الثالث جاءت مجموعات الأخبار News Groupes كإحدى الرسائل التى تستخدم ضمن نطاق الشبكة فى الذم والقدح ، فيكون الذم والقدح وجاهياً متى كان كل من الجانى والمجنى عليه يتبادلون الرسائل عبر مجموعات الأخبار أو فى صدد تعليقهم ومشاركتهم على موضوع معين ، وتتحقق علانية الفعل حيث أن كل المشتركين فى مجموعات الأخبار يمكنهم أن يروا ما يرد من رسائل وتعليقات حول الموضوع الذى اختاروه لمناقشتهم حيث أن المعلومات لا تصل إلى المشترك إلا فى حالة ما إذا كان هذا الشخص متداخلاً فى الشبكة ، ويضيف الباحث أن كل صور الذم والتحقير يمكن أن تتحقق من خلال هذه الوسيلة.

وفى الفرع الرابع وردت غرف المحادثات والدردشة Chat Rooms كإحدى الوسائل المستخدمة فى الشكبة ، وتتخذ صورة الذم والقدح فى غرف المحادثات والدردشة ، الصورة الخطية بشكل رئيسى .

أما فى المطلب الثانى والخاص بالمراسلات الإلكترونية عبر طرفية إنترنت منفصلة فتمثل كل تقنية علمية حدثية غير الحاسوب تسمح بصورة مباشرة أوغير مباشرة بالتبادل الإلكترونى للبيانات (EDI) وهو ما يعرف بتسمية الشريك الإلكترونى E-epartner ، فلم تعد الثورة الرقمية – كما يوضح الباحث ، مقصورة على التبادل الإلكترونى للبيانات عبر الشبكات المحلية أو حتى فى نطاق الشبكة العالمية بين الحواسيب فقط ، بل أصبح من الممكن الدخول إلى شبكة الإنترنت والانتفاع من الخدمات المتاحة وإجراء المبادلات الإلكترونية من خلال أجهزة الهواتف الخلوية ، ويمكن من خلال الهاتف النقال Cellular استقبال أو إرسال البيانات على شكل رسائل قصيرة ، كما يمكن إرسال بيانات أو رسائل البيانات على شكل رسائل قصيرة ، كما يمكن إرسال بيانات أو رسائل منها إلى أى بريد إلكترونى ، وكذلك يمكن الاتصال بأى موقع على الشبكة للاستفسار عن أية معلومات يريدها المستخدم ، وكذلك يمكن إجراء التحويلات الإلكترونية للأموال من هذه الطرفية ، وكذلك كله وفقاً لما تتيحه خدمة بروتوكول التطبيق اللاسلكى (WAP) . والهاتف النقال شأنه شأن الإنترنت – قد يساء استخدامه فى غير الغرض الذى خصص من أجله لإقتراف أفعال مختلفة تكون مجرّمة أو غير مجرّمة وذلك وفقاً للتفسيرات المختلفة للنصوص التقليدية .

ويشير الباحث إلى حالتين لإرتكاب جرائم الذم والقدح من خلال تلك الطرفيات : الأولى تتعلق بالرسائل الإلكترونية المتضمنة مواد القدح ... من شبكة الإنترنت بواسطة خدماتها المتاحة إلى الهاتف النقال . سواء كانت رسائل كتابية أو رسوم أو صور أو محادثات صوتية أى (الرسائل السمع بصرية) ، والحالة الثانية تتعلق بالرسائل الإلكترونية

من الهاتف النقال إلى شبكة الإنترنت من خلال خدماتها المتاحة (البريد الإلكترونى أو شبكة الويب أو غرف المحادثة أو مجموعات الأخبار ... إلخ) .

جرائم الإعتداء على الحياة الخاصة عبر الإنترنت :

أما فى الفصل الثانى المتعلق بجرائم الإعتداء على حرمة الحياة عبر الإنترنت فقد جاءت مباحثه كما يلى :

- **المبحث الأول** : أثر ميكنة المعلومات وخدمات الإنترنت على الحياة الخاصة ، وقد بين العلاقة ما بين المعلومات والحياة الخاصة للأفراد وأثر خدمات الإنترنت عليها من خلال نواح مختلفة تتمثل فى :

١ - طبيعة المعلومات المتعلقة بالحياة الخاصة :

يثور التساؤل فى هذا الصدد حول ماهية المعلومات التى تعرض خصوصية الأفراد فى إطار مجتمع المعلومات الإلكترونية للإنتهاك ؟ فهل كل معلومة يتم تداولها عبر شبكة الإنترنت تثير مسألة الخصوصية الشخصية ؟ وكذلك هل يعتبر الرضاء بإعطاء بيانات شخصية لأحد المواقع أو الجهات رضاء بتداول هذه المعلومات ؟ .

يجيب الباحث أن الأمر يصدق فى حالة المساس بالمعلومات المتعلقة بأفراد معرّفين مما يؤدى إلى المساس بخصوصياتهم فتكون بذلك المعلومة اسمية إذ أنها تسمح بالتعرف على الشخص محل هذه المعلومة بطريقة مباشرة أو غير مباشرة .

وقد تكون المعلومة موضوعية لا تعكس آراء شخصية أو تكون ذاتية تحمل رأياً ذاتاً عن الغير ، أما المعلومات الإسمية المخزنة فى بنوك المعلومات فهى التى تمس الحياة الخاصة للأفراد والحق فى الخصوصية المعلوماتية ، وتعرف هذه البيانات بأنها البيانات الشخصية التى تتعلق بالحق فى الحياة الخاصة للمرء كالبيانات الخاصة بحالته الصحية والمالية والوظيفية والمهنية والعائلية عندما تكون هذه البيانات محلاً للمعالجة الآلية .

٢ - موضوع حماية الحياة الخاصة :

كون الحق فى المعلومات يصلح لأن يكون محلاً للحقوق الشخصية والمالية فإنه يجب أن تحمى خصوصية الأفراد بقوانين حديثة وذلك بالتخلى عن حرفية النص الجنائى فيما يتعلق بالحماية الجنائية للحق فى الخصوصية وعن العناصر المبهمة المكونة للجريمة للحفاظ قدر الإمكان على خصوصية المعلومات الخاصة بالأفراد من مخاطر الإنترنت واستخداماتها والتى غدت تقدماً للوسائل القامعة للحرية الفردية فى حالة ما إذا أسيء استخدامها .

٣ - الاتجاهات المختلفة حول مشروعية بنوك المعلومات [المتعلقة ببيانات الافراد الخاصة] :

بيّن الباحث الآراء المؤيدة والمعارضة لمشروعية استخدام بنوك المعلومات والتى جرت فى اتجاهين رئيسيين : **الأول** : يرى أن بنوك المعلومات لا تشكل تهديداً للحق فى حرمة الحياة الخاصة ، **أما الإتجاه الثانى** وصد الغالب فيرى أن استخدام بنوك المعلومات يمثل خطراً على الحياة الخاصة .

٤ - اثر البيانات الإسمية المخزنة في بنوك المعلومات في مواجهة أجهزة الدولة :

والسؤال المثار هنا هو هل يحق للدول ممثلة بحكوماتها أن تكون بمنأى عن البيانات الشخصية لمواطنيها ، وهل تشكل أفعال التخزين للبيانات التى تقوم بها الحكومات إنتهاكاً صريحاً لخصوصيات الأفراد ولا سيما مع بدء ما يعرف بالحكومة الإلكترونية ؟ .

٥ - اثـــر المعلومـــات وخدمـــات الإنترنت علـــى خصوصيات المستهلكين :

تتطلب عمليات التبادل الإلكترونى للبيانات فى مضمار التجارة الإلكترونية معرفة بعض البيانات الشخصية والتى تسمح بالتعرف على الشخص بشكل أوفى ، وقد تمتد هذه البيانات إلى معرفة أرقام بطاقات الإئتمان لإتمام عمليات الشراء والتعاقد وهذه بدورها تشكل أكثر البيانات الشخصية عرضة للإعتداء سواء بالحصول عليها عن طريق الاحتيال أو بسرقة أرقام هذه البطاقات خلال الفجوات غير الآمنة فى قنوات الإنترنت ، ونظراً لتزايد حجم التجارة الإلكترونية عبر الشبكة برزت الدعوة إلى حماية خصوصية المستهلك لتوطيد الثقة والأمان لمستخدمى الشبكة ولا سيما وان تجارة جمع البيانات الشخصية أصبحت شيئاً مألوفاً وفق تقنيات ملفات الكوكيز Cokies .

وإزاء رواج سوق الحياة الخاصة على الإنترنت تغدو الحاجة – كما يؤكد الباحث – ملحة لتنظيم أوجه الحماية للمستهلكين المتعاملين بالتجارة الإلكترونية بقوانين حديثة تكفل لهم خصوصياتهم كالتى فرضتها بعض التشريعات فى كندا على سبيل المثال ، كما لوحظ فى إطار شبكة العمل – حجز لمحات عن حياة الأشخاص ونظام حياتهم واختيارات التسوق لديهم مما ساعد على تركيز الصناعة وفق احتياجات التسوق ودون الأخذ بعين الاعتبار خصوصية المستهلك .

٦- اثـــر المعلومـــات علـــى العلاقـــة بـين الحرية والمسؤولية :

إذا كان الحصول على المعلومات هو الغاية النهائية من استخدام شبكة الإنترنت سواء بإرسال أو نقل هذه المعلومات إما ليحصل عليها المتلقى كمعلومات نهائية أو ليدفع بها كمدخلات إلى نظام معالجة أخر ، فإن ما يمكن إثارته فى هذا الصدد يكمن فى العلاقة ما بين الحرية والمسؤولية أى حق الفرد فى ممارسته حريته من ناحية ومسؤوليته تجاه ما تواضع عليه المجتمع فى إطار فكرة النظام العام من ناحية أخرى . وإذا كانت البيانات الشخصية المتصلة بالحياة الخاصة للفرد غالباً ما يقدمها الشخص بنفسه أو قد تتوصل الهيئات إليها بوسيلة أو بأخري فإن تهديد الحرية الشخصية يثور إذا أفشيت هذه المعلومات دون موافقته ، أو إذا نشرت البيانات الشخصية بصورة مغايرة عن تلك التى سبق وأن تم نشره بها أو فى حالة الخطأ والتحوير فى المعلومات التى تسجل عن الشخص .

أما المبحث الثانى فى هذا الفصل فجاء عنوانه: موقف الأنظمة القانونية المختلفة من حماية الحياة الخاصة فى مواجهة نظم المعلومات وجاء فى تمهيد ومطلبين :

ويذكر الباحث أن صور إنتهاك الخصوصية فى مجال نقل البيانات فى شبكة لا تتمتع بأمان كامل أو مطلق لسرية ما ينقل عبرها من بيانات فإن إمكانية مراقبة أو اعتراض وتفريغ الرسائل المتبادلة عن طريق البريد الإلكترونى والتوصل بطريق غير مشروع إلى ملفات تخص الآخرين أصبح عرضة للعديد من الانتهاكات مما يثير التساؤل حول الجهود المبذولة فى مواجهة خطر إنتهاك خصوصيات الأفراد والتى أصبحت تزداد بازدياد مستخدمى ومشتركى الشبكة والمتعاملين مع نظم المعلومات ، ويري الباحث أن إعطاء قدر من تنظيم التدابير الوقائية لمستخدمى ومشتركى الشبكة فيما يتعلق بخصوصياتهم أقل بكثير من ترك الأمور دون حد أدنى من الرقابة والتنظيم .

وفى المبحث الثالث من هذا الفصل تناول الباحث الحماية الجنائية لمعالجة البيانات الإسمية عبر الإنترنت فى التشريع الفرنسى ، وجاء هذا المبحث فى تمهيد وخمسة مطالب :

يقول الباحث فرض المشرع الفرنسى حماية جنائية للبيانات الشخصية فى مواجهته نظم المعلومات ، وذلك بالقانون الصدار فى ٦ يناير ١٩٧٨ والمسمى بقانون نظم المعالجة الرقمية والحرية Informatique Et Biberte وقد قصر المشرع نطاق حماية البيانات على الأشخاص الطبيعية دون المعنوية حيث استهل نصوص قانونه بمبدأ أساسى وهو أن المعالجة الإلكترونية للبيانات يجب أن لا تحمل تعدياً على حصانة الفرد ولا على حقوق الإنسان وعلى حياته الخاصة أو حرياته الفردية والعامة ، ولاسيما وان القانون يهدف إلى تحقيق التوازن ما بين الاستخدام الحر والكامل للمعلوماتية من ناحية ولحماية المواطن فى إطار نظام ديمقراطى حر من ناحية أخرى ، وكانت المطالب الخمسة كما يلى :

المطلب الأول : جريمة المعالجة الإلكترونية للبيانات الشخصية دون ترخيص .

المطلب الثانى : جريمة التسجيل غير المشروع للبيانات الإسمية .

المطلب الثالث : جريمة الحفظ غير المشروع للبيانات الإسمية .

المطلب الرابع : جريمة الانحراف عن الغرض أو الغاية من المعالجة الإلكترونية للبيانات الإسمية .

المطلب الخامس : جريمة الإفشاء غير المشروع للبيانات الإسمية .

الفصل الثالث تناول فيه الباحث جرائم الاستغلال الجنسى للأطفال عبر الإنترنت وعرض لصور التعرض للآداب والأخلاق العامة فى التشريع الأردنى ثم ألقى الضوء على الجرائم المخلة بالآداب والأخلاق العامة فى التشريع المقارن وبصفة خاصة جرائم الاستغلال الجنسى للأطفال عبر الإنترنت ، وندعو القارئ إلى قراءة هذا الفصل الهام دون التطرق لتفاصيله .

الباب الثاني : نوعية جرائم الإعتداء على الأموال عبر الإنترنت :

فى التمهيد استعرض الباحث إشكالية المعلومات الإلكترونية باعتبارها أموالاً يحق حمايتها

واختلاف نظرة التشريعات إليها وفقاً للمفهوم المادى والمنقول للأموال .

ويرى الباحث أن التقدير القانونى للأموال المادية والمعنوية يجب – فى حالة التقنية الرقمية – أن يكون مختلفاً وذلك من جانبين :

١ – إذا كانت طبيعة الأموال المادية يستأثر بها شخص محدد وعلى نحو مطلق فإن المعلومات هى مال شائع ومن ثم يجب أن تكون من حيث المبدأ حرة لا تتمتع بحماية الحقوق الاستئثارية التى تقتصر على الأموال المادية .

٢ – يجب أن لا ينظر إلى حماية المعلومات بوصفها مصالح إقتصادية بل أيضاً بوصفها تمثل مصالح الأشخاص الذين تأثروا لفحوى هذه المعلومات .

ويرى الباحث أنه إذا كان موضوع الإعتداء على الأموال فى نطاق المعالجة الآلية للمعلومات ينصب على الحاسب الآلى ذاته وما يرتبط به من أسلاك وما يتصل به من ملحقات فإنه هنا لا يثير أية صعوبة فى تطبيق النصوص الجزائية التقليدية ، كون الأمر يتعلق بمال مادى منقول وفقاً للمفهوم الدارج ، أما إذا وقع الاعتداء على ما يتعلق «بفن الحاسب الآلى» من برمجيات Software ونظم فإن النصوص التقليدية تأتى قاصرة عن حمايتها لما لهذا المال من طابع خاص غير تقليدى .

واستعرض الباحث نوعية هذه الجرائم فى ثلاثة فصول على النحو التالية :

١ – سرقة المال المعلوماتى المعنوى (اللامادى).

٢ – التحويل الإلكترونى غير المشروع للأموال.

٣ – إتلاف النظم المعلوماتية .

جاء الفصل الأول فى عدة مباحث : المبحث الأول : الطبيعة القانونية للمال المعلوماتى محل السرقة ، وقسمه إلى مطلبين : الأول : وضع المسألة فى القانونين الأردنى والمصرى ، والثانى : وضع المسألة فى التشريع المقارن . أما المبحث الثانى : أنماط سرقة المال المعلوماتى المعنوى فجاء فى تمهيد ومطلبين :

ذكر الباحث أن المال المعلوماتى المخزن فى قواعد البيانات والمتبادل عبر خطوط شبكة الإنترنت يتمثل فى البيانات والمعلومات اللامادية فإن تلك البيانات هى هدف الجانى وغايته فإذا ما اختلست تلك المعلومات بطريقة أو بأخرى فإن ذلك يمثل إعتداء على البيانات وسبباً موجباً لقيام وصف السرقة أو الاحتيال أو إساءة الائتمان وذلك حسب طبيعة الاختلاس وفيه الجانبى .

وفى المطلبين تناول الباحث أنماط سرقة المال المعلوماتى المعنوى :

١ – الالتقاط غير المشروع للبيانات ويشمل عدة فروع : أسلوب التجسس المعلوماتى ، أسلوب الخداع ، تقنية تفجير الموقع المستهدف .

٢ – سرقة منفعة الحاسب الآلى ويقصد بها استخدامه لأغراض شخصية أو تجارية بدون علم مالكه أو حائزه القانونى مثل سرقة الخدمات المعلوماتية أو سرقة الوقت ... إلخ . ويشمل عدة فروع : موقف الفقه من وصف السرقة ،

وصف الاحتيال (النصب) ، وصف إساءة الائتمان (خيانة الأمانة) ، موقف القضاء ، موقف التشريع .

أما الفصل الثانى : التحويل الإلكترونى غير المشروع للأموال ، فبعد أن استعرض الباحث فى التمهيد الطرق الملتوية وغير المشروعة للتحويل الإلكترونى للأموال والتى تتم من قبل مغامرين محترفين سواء من داخل البنوك ذاتها أو من خارجها ، طرح تساؤلاً مفاده هل يمكن تطبيق النصوص التقليدية المتعلقة بجريمتى الاحتيال وإساءة الائتمان على عمليات التحويل الإلكترونى غير المشروع للأموال رغم عدم وجود إعتداء مادى ملموس ؟

وللإجابة عن هذا التساؤل عرض فى دراسته لثلاثة مباحث :

١ – الاحتيال (النصب) فى نطاق المعلوماتية.

٢ – الإحتيال باستخدام بطاقات الدفع الإلكترونى عبر الإنترنت .

٣ – إساءة الائتمان فى نطاق المعلوماتية .

فى المبحث الأول أورد الباحث تعريفاً للإحتيال المعلوماتى Informatics Fraud بأنه «كل سلوك احتيالى يرتبط بعملية التحسيب الإلكترونى بهدف كسب فائدة أول مصلحة مالية» . وأوضح أن هذا التعريف يشمل كل ضروب غش الحاسوب والمتمثلة بالإعتداء على المعطيات المخزنة فى النظام المعلوماتى والمتبادلة عبر قنوات النظام بما تمثلها من أموال وخدمات بغرض الحصول على منفعة مادية . واستعرض ما جاء بقانون المعاملات الإلكترونية الأردنى رقم ٨٥ لعام ٢٠٠١ وما جاء فيه بخصوص الاحتيال المعلوماتى . كما بيّن الطرق الاحتيالية المستخدمة فى الحصول على الأموال المعلوماتية ممثلة بالمعلومات المخزنة فى الحاسب ، وقد طرح تساؤلاً حول ما إذا كان الاحتيال على الحاسب الآلى يدخل ضمن مفهوم جريمة الاحتيال أم لا ؟ وهل تعتبر النقود الكتابية أو البنكية من قبيل الأموال المادية التى يرد عليها الاستيلاء فى إطار المعلوماتية ؟ .

أجاب الباحث عن هذا التساؤل فى مطلبين ، الأول منهما هو الاحتيال على النظام المعلوماتى وفيه بيّن درجات الاختلاف بين الفقهاء فى هذا الصدد فقد ذهب جانب منهم إلى القول بأن التلاعب فى البرامج والبيانات والتغيير فيها بما يترتب عليه إيهام المجنى عليه بصحتها ما يجعله يسلم بها ، يعد من أحد أساليب التحايل ، وحسب هذا الإتجاه فإن الحاسوب ليس سوى مجرد وسيط للتحايل .

بينما ذهب البعض فى الفقه الفرنسى إلى أن غش أنظمة الحاسوب وخداعها للاستيلاء على الأموال تتحقق فى صفة الطرق الإحتيالية وبالتالى قيام جريمة الإحتيال ، بينما ذهب البعض الآخر إلى القول بعدم تحقق واقعة الاحتيال على الحاسوب الآلى ونظامه المعلوماتى وان استخدام وسائل الغش والخداع فى أنظمة الحاسب للاستيلاء على الأموال لا تدخل ضمن نطاق الطرق الاحتيالية وحجتهم فى ذلك ما بينته الأحكام الفرنسية التى تنطوى بالضرورة على وجود علاقة مباشرة بين شخصين المخادع والمخدوع وهو ما ينتفى فى هذه الحالة .

أما فيما يتعلق بمسلك التشريعات فى مدى تحققه ممارسة أفعال الاحتيال على الحاسب الآلى وإيقاعه فى الغلط فقد تباينت فى ثلاث إتجاهات :

- **الأول** : تستلزم تشريعات هذا الإتجاه لقيام جريمة الاحتيال أن يكون المخدوع شخصاً معنوياً (إنسان) ومن ثم لا يتصور – وفقاً لهذا الإتجاه – خداع الحاسب الآلي بوصفه آلة ، وبالتالى عدم انطباق نصوص جريمة الاحتيال التقليدية على خداع الحاسب ونظامه المعلوماتى لإفتقاره لأحد العناصر الضرورية .
- **الثانى** : يرى إمكانية تطبيق النصوص الخاصة بجريمة النصب على الاحتيال المعلوماتى ومنها تشريعات دول الأنجلوسكسون .
- **الثالث** : يطبق القوانين الخاصة بالغش فى مجال البريد والتلغراف والبنوك أيضاً على الاتفاق الجرمى لأغراض إرتكاب الغش على حالات النصب المعلومات ومنها تشريعات الولايات المتحدة الأمريكية .

وفى المطلب الثانى خلص الباحث إلى أن معظم تشريعات الدول ذهبت إلى عدم اعتبار النقود الكتابية بمثابة مال مادى بل بوصفها من قبيل الديون والتى يستحيل أن تكون محلاً للاختلاس أو السرقة ، وعلى النقيض منها ، فى عدد محدود من الدول ، فإن هنالك تشريعات ذهبت إلى جواز اعتبار النقود الكتابية – على الرغم من طابعها غير المحسوس – من قبيل الأموال التى تصلح لأن تكون محلاً لجرائم السرقة والاحتيال (النصب) وإساءة الائتمان (خيانة الأمانة) .

فى المبحث الثانى من هذا الفصل : الاحتيال باستخدام بطاقات الدفع الإلكترونى عبر الإنترنت ، فى التمهيد عرف بمفهوم نظام بطاقة الدفع الإلكترونى وطرق الاحتيال التى يرتكبها البعض باستخدام إمكانية تخليق أرقام البطاقات الائتمانية بواسطة برامج تشغيل تتيح إمكانية تخليق أرقام بطاقات بنك معين من خلال تزويد الحاسب الرقم الخاص بالبنك مصدر البطاقة ، علاوة على إمكانية التقاط هذه الأرقام عبر قنوات الإنترنت المفتوحة واستخدامها بطريقة غير مشروعة فى عمليات التسوق عبر الشبكة ، بحيث يتم خصم قيمة السلع من العملاء الشرعيين لهذه البطاقات .

وقد عرض الباحث لمسألة الاعتداء على البيانات السرية الخاصة ببطاقات الدفع الإلكترونية فى مطلبين : الأول : الغش باستخدام بيانات بطاقة الائتمان من قبل حاملها الشرعى ، والثانى : الغش باستخدام بيانات بطاقة الائتمان بواسطة الغير .

فى البحث الثالث من هذا الفصل : جريمة إساءة الائتمان فى نطاق المعلوماتية ، تساءل الباحث فى التمهيد حول إمكانية انطباق النصوص الخاصة بجريمة إساءة الائتمان فيما إذا ارتكبت فى نطاق المعلوماتية ؟ وأجاب عن تساؤله فى ثلاثة مطالب : الأول : محل جريمة إساءة الائتمان ، والثانى: الركن المادى للجريمة عبر الإنترنت ، والثالث: الركن المعنوى للجريمة عبر الإنترنت .

فى الفرع الأول من المطلب الأول ذكر الباحث أنه إذا كانت الأموال المعلوماتية كالبيانات والمعلومات والبرامج تتمتع بطبيعة ذاتية غير ملموسة (معنوية) فإن النصوص الجزائية تأتى قاصرة عن حماية الأموال المعلوماتية اللامادية من الاستيلاء

عليها ، غير أنه أردف أن بعض الأشياء اللامادية تصلح لأن تكون موضوعاً لجريمة خيانة الأمانة ، وذلك بالإشارة إلى نص المادة ٤٢٢ ع أردنى والمادة ٣٤١ ع مصرى لكونهما بمثابة بضائع أو أنها تدخل فى مفهوم الكتابات مشتملة على شيك أو مخالصة (إبراء) .

أما فى الفرع الثانى من هذا المطلب فقد ذكر أن مفهوم المال المنقول يثير صعوبات جمة فى نطاق المعلوماتية بما يتعلق بالبيانات والبرامج والمعلومات فيما إذا أمكن اعتبارها من المنقولات وبالتالى تصلح لانطباق النصوص المتعلقة بإساءة الائتمان عليها ، أم أنها لا تعد كذلك وبالتالى لا تصلح محلاً للجريمة ، ويرى الباحث أن النصوص المتعلقة بجريمة إساءة الائتمان فى القانون الأردنى والقانون المصرى – تنطبق فى نطاق المعلوماتية على أموالها المادية والتى تعتبر أموالاً منقولة ، كالمعدات والأجهزة والدعامات المحتوية على المعلومات والبرامج، أما فيما يتعلق بالأموال المعلوماتية المعنوية (غير المحسوسة) فإن النصوص تأتي قاصرة عن حمايتها . وقد فرق الباحث بين مخرجات الحاسب الآلى الورقية – مثل التقارير والشيكات ، والمخرجات اللاورقية أو الإلكترونية كالأشرطة المغناطيسية والأقراص المغناطيسية ، وما بين مخرجات وحدة العرض المرئى (VDV) ووحدة المعالجة المركزية (CPU) ، وما ينطبق عليها من أن تكون محلاً لجريمة إساءة الإئتمان أو عدمه فى النصوص التشريعية .

وفى المطلب الثانى من هذا البحث الركن المادى لجريمة إساءة الائتمان عبر الإنترنت ناقش الباحث عدة فروع : الفعل الإجرامى وهل يمكن تحققه عبر شبكة الإنترنت والمعلوماتية ، وتناول فى هذا الصدد فعل الإختلاس والتبديد والاستعمال ووقوع هذا الفعل على مال منقول ملك للغير بالإضافة إلى توافر التسليم وأن يكون هنالك ضرر ، وهو ما يحققه النشاط المادى للجريمة فى نطاق المعلوماتية ، وخلص إلى أنه لا يكفى لتوافر الركن المادى فى جريمة إساءة الائتمان الإعتداء على ملكية الغير بالاختلاس أو الاستعمال أو التبديد ولكنه يلزم أن يكون هنالك ضرر لحق بالمجنى عليه .

أما المطلب الثالث : الركن المعنوى لجريمة إساءة الائتمان عبر الإنترنت فذكر الباحث أنه فى إطار المعلوماتية فإن القصد الجنائى يتحقق ويتوافر فيما لو أؤتمن الجانى على برامج أو اسطوانات مسجل عليها البرامج أو المعطيات لنسخها وإعادتها إلى أصحابها فيقوم بالتلاعب فى تلك البرامج والمعطيات التى يأذن بالدخول إليها والتعامل معها بحكم عمله وبغير حيازتها إلى حيازة كاملة تؤدى إلى الإضرار بالمجنى عليه مع توافر علمه بذلك .

وفى الفصل الثالث من الباب الثانى : جريمة إتلاف نظام المعلوماتية عبر الإنترنت بيّن أن جريمة الإتلاف فى نطاق المعلوماتية يقع بالإعتداء على الوظائف الطبيعية للحاسب وذلك بالتعدى على البرامج Logical والبيانات Data المخزنة والمتبادلة بين الحواسيب وشبكاتها الداخلية (المحلية) أو العالمية (الإنترنت) ، وذلك بطريق التلاعب بالبيانات سواء بإدخال معلومات مصطنعة أو بإتلاف المعلومات

المخزنة والمبادلة عبر الشبكة العالمية بمحوها أو تعديلها أو تغيير نتائجها أو بطريقة التشويش على النظام المعلوماتى بما يؤدى إلى إعاقة سير عمل النظام الآلى بصوره المختلفة ، وقد يكون الإتلاف للبرامج والبيانات بمحوها كلية أو تدميرها إلكترونياً أو تشويهها على نحو فيه إتلاف بما يجعلها غير صالحة للاستعمال .

وتأخذ جريمة الإتلاف فى نطاق المعلوماتية أما صورة الإتلاف المادى، وذلك بالاعتداء على المكونات المادية للحاسب (أجهزة العتاد) ، وهنا لا تثار أية عقبة قانونية فى تطبيق النصوص التقليدية الخاصة بجريمة الإتلاف على مثل هذه الاعتداءات. إذ ينصب الاعتداء فى هذا الإطار على مال مادى للغير ، وكذلك يتخذ الإتلاف صورة الإعتداء على البرامج أو البيانات والمعلومات المخزنة فى قواعد الحاسب والمتبادلة بين الحواسيب عبر قنوات الاتصال فى شبكة الإنترنت – سواء تم ذلك بمحوها أو تعديلها أو تغيير نتائجها مما يثير التساؤل عن مدى انطباق النصوص التقليدية المنوطة بجرعة الإتلاف على حماية البيانات والمعلومات اللامادية فى إطار الشبكة .

أجاب عن هذا التساؤل فى مبحثين : الأول : إتلاف المال المعلوماتى المادى ، والثانى : الاعتداء على سير نظام المعالجة الآلية للبيانات (إتلاف المال المعلوماتى المعنوى) .

ويتضح أن النصوص التشريعية تغطى مجال المبحث الأول ، ولكن بالنسبة للمال المعلوماتى المعنوى فهى مازالت قاصرة فى هذا الصدد فى وطننا العربى ، وان كانت بعض التشريعات الأجنبية قد أضفت حماية على هذه الأموال من الاعتداء عليها بالإتلاف ، مثل القانون الأمريكى «قانون الاحتيال وإساءة استخدام الكمبيوتر لعام ١٩٩٦ ، وكذلك التشريع الفرنسى فى قانون العقوبات ١٩٩٢ والمعمول به منذ عام ١٩٩٤ والذى فرق ما بين الاعتداء على سير عمل النظام المعلوماتى بإعاقته أو إفساده أو تعطيله وبين الاعتداء عليه بإتلاف البيانات والمعلومات وعرض الباحث للمسألتين فى مطلبين :

١ – إعاقة سير العمل فى نظام المعالجة الآلية للبيانات وذلك يتمثل فى فعل يسبب تباطؤ عمل النظام أو إرباكه مما يؤدي إلى تغير فى حالة عمل النظام على نحو يصيبه بشلل مؤقت ، مثل تعديل البرامج أو عمل برنامج احتيال أو من خلال إجراء التحويلات الإلكترونية كإغراق موقع على الشبكة بالرسائل الإلكترونية مما يؤدى إلى شله ، واستعرض الباحث التشريعات الأمريكية والفرنسية والأردنية التى تجرم هذا الفعل .

٢ – فى المطلب الثانى عدد الباحث صور الاعتداء على البيانات داخل نظام المعالجة الآلية للبيانات والتى تأخذ الصور التالية :

أ – ان يتم محو البيانات والمعلومات كلية أو بتدميرها إلكترونياً .

ب – أن يتم تشويه المعلومة أو البرنامج عن طريق تعديل البيانات أو تعديل طرق معالجتها أو وسائل إنتقالها .

وتتنوع أساليب الإتلاف التى قد تكون نتيجة فعل الدخول غير المشروع إلى النظام المعلوماتى أو البقاء فيه بدون إذن ، أو تكون نتيجة استخدام الطرق التقنية والفنية كاستخدام فيروسات الحاسب الآلى . وفى نهاية بحثه دعا الباحث إلى ضرورة تخلى المشرع العقابى فى الوطن العربى عن حرفية النص الجنائى التقليدى وتبنيه مفهوماً أشمل للمال المنقول بحيث يشمل الأموال المعلوماتية المعنوية غير المحمية والتى أضحت تشكل نواة المجتمع الإلكترونى الحديث .