# الجريمة الإلكترونية في ميزان الفقه والقانون


**إعداد:**

**د. زينب طرقي العنزي**

**كلية الشريعة – جامعة الكويت**

بسم الله الرحمن الرحيم

**ملخص البحث:**

تطورت الظاهرة الإجرامية في العصر الحديث تطورًا ملحوظًا ومذهلا، سواء في شخصية مرتكبيها، أو أسلوب ارتكابها مع استخدام آخر ما توصلت إليه العلوم التقنية والتكنولوجية. وقد تميز القرن العشرون باختراعات هائلة على المستوى التقني، لعل من أهمها ظهور الحاسوب الالكتروني، ووجود ما يعرف بالإنترنت، وتعني شبكة الشبكات، أي: ربط شبكات الحاسوب الموجودة بعضها ببعض.

ومن هنا يمكن أن نعرف الجريمة الإلكترونية بأنها أعمال متعلقة بالكمبيوتر؛ لتحقيق مكاسب شخصية، أو مالية، أو ضرر، بما في ذلك أشكال الأفعال المتصلة بجريمة الهوية، وجرائم محتويات الكمبيوتر، أيضا تم تقسيم الجرائم بحسب كيفية ارتكابها إلى: جرائم بسيطة، يتكون الركن المادي لكل منها من فعل مادي واحد، مثل جرائم القتل، وجرائم اعتيادية، يتكون ركنها المادي من عدة أعمال مادية متماثلة، أي: أن الفعل بذاته لا يعد جريمة، ولكن الاعتياد على ارتكاب الفعل هو الجريمة، والمقصود تكرار الفعل المادي، والمجرم المعلوماتي هو شخص يختلف

عن المجرم العادي، فلا يمكن أن يكون هذا الشخص جاهلا للتقنيات الحديثة المعلوماتية.

هناك عدد من الأسباب التي يمكن حصرها كأسباب للجريمة الإلكترونية، منها ما يقع على مستوى كوني، ومنها ما يقع على مستوى مجتمعي، ومنها ما يقع على مستوى فردي أو شخصي.

ولذلك كان لا بد من وجود قانون صارم يحد من هذه التجاوزات الكبيرة، ولكن مع ضرورة الاحتفاظ بحق الفرد في إبداء رأيه، وخاصة فئة الشباب الذين يجدون مواقع التواصل الاجتماعي متنفسات لهم للتعبير عما يدور من حولهم من قضايا المجتمع الداخلي أو الخارجي.

**Summary:**

The criminal phenomenon has developed remarkably and surprisingly in the modern era; Whether in the personality of the perpetrators or the manner in which they were committed, with the use of the latest technical and technological sciences. The twentieth century was marked by tremendous inventions at the technical level, perhaps the most important of which is the emergence of the electronic computer. The existence of what is known as the Internet; Network of networks means the connection of existing computer networks to each other

Hence, we can define cybercrime as computer-related acts for personal or financial gain or harm, including forms of acts related to identity crime and computer content crimes. Also, crimes were divided according to how they were committed into: Minor crimes: The material element of each of them consists of a material act.

One is like murders, and ordinary crimes whose material component consists of several similar material acts, i.e., that the act itself is not considered a crime, but the habit of committing the act is the crime, and what is meant is the repetition of the material act and the information criminal is a person different from the ordinary criminal, so this cannot be The person is ignorant of modern informational technologies.

There are a number of reasons that can be enumerated as causes of cybercrime, some of which occur on a global level, some at a

societal level, and some of them occur on an individual or personal level.

Therefore, it was necessary to have a strict law that limits these major transgressions, but with the necessity to preserve the right of the individual to express his opinion, especially the group of young people who find social networking sites an outlet for them to express what is going on around them from the internal or external community issues.

**المقدمة:**

بسم الله، والحمد لله، والصلاة والسلام على رسول الله محمد بن عبد الله، وعلى آله، وصحبه، ومن والاه.

أما بعد:

فإن الإنسان يولد وهو على الفطرة السليمة التي لا تعرف الأذى أو الإجرام، وتسهم البيئة المحيطة به في تشكيل شخصيته والتأثير فيه، وقد يتعرض بعض الأشخاص لتأثير سلبي من قبل البيئة المحيطة بهم؛ مما يجعلهم ينحرفون نحو فعل السلوكيات غير الجيدة، وارتكاب الممارسات غير المقبولة بالنسبة لإنسان سوي؛ مما يقودهم إلى الجرائم.

لا أقصد الجريمة بالمفهوم العام، ولكن أود أن أسلط الضوء على بعض صورها الحديثة، ووسائل التواصل الاجتماعي، وهي الجريمة الإلكترونية أو المعلوماتية، وتشعبت أنواعها، فلم تعد تهدد العديد من الصالح التقليدية التي تحميها القوانين والتشريعات منذ عصور قديمة، بل أصبحت تهدد العديد من المصالح والمراكز القانونية التي استحدثتها التقنية المعلوماتية بعد اقترانها بثورتي الاتصالات والمعلومات.

فالمصالح التقليدية التي تحميها كل التشريعات والنظم القانونية منذ زمن بعيد بدأت تتعرض إلى أشكال مستحدثة من الاعتداء بواسطة هذه التقنية الحديثة، فبعد أن كان الاعتداء على الأموال يتم بواسطة السرقة التقليدية أو النصب، وكانت الثقة في المحررات الورقية يعتدى عليها بواسطة التزوير أصبحت هذه الأموال يعتدى

عليها عن طريق اختراق الشبكات المعلوماتية، وإجراء التحويلات الإلكترونية من أقصى مشارق الأرض إلى مغاربها في لحظات معدودة، كما أصبحت تلك الحقوق الثابتة في الأوعية الورقية يتم الاعتداء عليها في أوعيتها الالكترونية المستحدثة عن طريق اختراق الشبكات والأنظمة المعلوماتية دون الحاجة إلى المساس بأية وثائق أو محررات ورقية.

البحث في الجرائم الالكترونية أصبح حاجة ماسة في وقتنا الحالي بسبب الضرر الفادح لها، وكثرة من تضرر بسبب سوء استخدام هذه التقنية؛ فأوجب توعية المجتمع بالجريمة الإلكترونية، وأنواعها، وأسبابها، والتعريف بممارسات مجرمي الشبكة الإلكترونية، كل هذا من منظور الشرع والقانون، وتكييف هذه الممارسات فقهيا، وذكر بعض من مواد القانون المطابقة لها.

**أهمية البحث:**

تأتي أهمية البحث من خلال توعية الأفراد والمجتمع ورفع الضرر، "لا ضرر ولا ضرار".

أيضًا قلة الأبحاث في تلك النوعية من الجرائم دفعتني للبحث فيه لأهميته.

**سبب اختيار الموضوع:**

حداثة الموضوع، وانتشار الأخطار والأضرار المعلوماتية داخل المجتمع العربي والكويتي.

**خطة البحث:**

**المقدمة.**

**المبحث الأول:** تعريف الجريمة الإلكترونية.

**المبحث الثاني:** نشأة الجريمة الإلكترونية وصورها.

**الخاتمة:** النتائج.

**فهرس المراجع.**

## المبحث الأول

## تعريف الجريمة الإلكترونية

اختلفت الاجتهادات في ذلك اختلافا كبيرا، يرجع إلى سرعة وتيرة تطور التقنية المعلوماتية من جهة، وتباين الدور الذي تلعبه هذه التقنية في الجريمة من جهة أخرى، فالنظام المعلوماتي لهذه التقنية يكون محلًا للجريمة تارة، ويكون وسيلة لارتكابها تارة اخرى، فكلما كان البحث منصبًاعلى الجرائم التي ترتكب ضد النظام المعلوماتي انطلق التعريف من زاوية محل الجريمة بأنها الجريمة المرتكبة بالاعتداء على النظام المعلوماتي، أما إذا كان البحث منصبًا على دراسة الجرائم التي ترتكب باستخدام التقنية المعلوماتية ارتكز التعريف على الوسيلة وكان: "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي[1].

تجدر الإشارة أيضًا إلى أن أهم عوامل صعوبة الاتفاق على تعريف هو أن التقنية المعلوماتية أصبحت تحل محل العديد من التقنيات السابقة، كالهاتف، والفاكس، والتلفزيون، فالمسألة لم تقتصر على معالجة البيانات فحسب، بل تعدتها إلى وظائف عديدة، مثل وظيفة النشر والنسخ، وهو ما يحتم ضرورة التفرقة بين جرائم الإنترنت وشبكات المعلومات بالمعنى الفني عن بقية الجرائم الأخرى التي يستخدم فيها الإنترنت أو الحاسب الآلي كأداة لا ارتكابها.

يقصد بجرائم الإنترنت وشبكات المعلومات الدخول غير المشروع إلى الشبكات الخاصة، كالشركات، والبنوك، وغيرها، وكذلك الأفراد، والعبث بالبيانات الرقمية التي تحتويها شبكة المعلومات، مثل تزييف البيانات، أو إتلافها ومحوها، وامتلاك أدوات أو كلمات سرية لتسهيل ارتكاب مثل هذه الجرائم التي تلحق ضررًا بالبيانات والمعلومات ذاتها، وكذلك بالنسبة للبرامج والأجهزة التي تحتويها، وهي

(١) د. هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٢.

الجرائم التي تلعب فيها القنية المعلوماتية دورًا رئيسا في مادياتها، أو السلوك الإجرامي فيها.

أما الجرائم التقليدية الأخرى مثل غسيل الأموال، وتجارة المخدرات، والإرهاب، والدعارة، والاستخدام غير المشروع للكروت الإلكترونية، ودعارة الأطفال Pornography، وجرائم التجارة الإلكترونية، وكذلك جرائم السب والقذف فجرائم تستخدم التقنية المعلوماتية كأداة في ارتكابها، دون أن تكون جرائم معلوماتية بالمعنى الفني، وإن كان يطلق عليها الجرائم الإلكترونية[1].

**تعريف الجريمة لغة واصطلاحًا:**

**الفرع الأول: تعريف الجريمة لغة:**

إن الأصل الثلاثي لكلمة (جرم) يدل على أربعة أمور، هي: القطع، والكسب، والذنب، والجَسَد، أو قد يأتي بمعنى الجزاء على الفعل.

**الفرع الثاني: تعريف الجريمة اصطلاحا:**

إن تعريف الجريمة في اصطلاح الفقهاء له اتجاهان:

عام، وهو قولهم: "الجريمة هي: فعل ما نهى الله عنه وزجر، وعصيان ما أمر الله به".

وخاص، وهو قولهم: "الجريمة هي: محظورات شرعية، زجر الله –تعالى– عنها بحد أو تعزير"، أو الجزاء المقرر لمصلحة الجماعة على عصيان أمر الشارع.

**التعريف الدولي للجريمة الإلكترونية:**

تعتمد تعريفات الجريمة الإلكترونية في الغالب على الغرض من استخدام المصطلح:

– هناك عدد محدود من الأفعال ضد السرية والنزاهة، وتوافر بيانات الكمبيوتر، أو أنظمته تمثل جوهر الجريمة الإلكترونية.

---

(١) أ.د. صالح أحمد البربري – دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية – الموقعة في بودابست في ٢٠٠١/١١/٢٣ –www.arablawinfo.com – ص٢

– أعمال متعلقة بالكمبيوتر؛ لتحقيق مكاسب شخصية، أو مالية، أو ضرر، بما في ذلك أشكال الأفعال المتصلة بجريمة الهوية وجرائم محتويات الكمبيوتر لا تصلح بسهولة إلى الجهود للوصول إلى التعاريف القانونية للمصطلح الكلي.

**الفرع الثالث: أنواع الجريمة:**

جسامة العقوبة، والمتمثلة في جرائم الحدود، وجرائم القصاص والدية، وجرائم التعزير.

حسب قصد الجاني إلى: جرائم مقصودة، وغير مقصودة.

كما أن عامل الوقت مهم في تحديد أقسام الجريمة؛ فهناك الجريمة المتلبس بها، وهي التي تكتشف وقت ارتكابها، وجرائم غير متلبس بها، وهي التي مضى بين ارتكابها وكشفها زمن غير يسير.

ومن أقسام الجرائم أيضًا الجرائم الإيجابية التي تتكون من إتيان فعل منهي عنه، كالسرقة، والزنا، وجرائم سلبية، تتكون من الامتناع عن إتيان فعل مأمور به، مثل الامتناع عن أداء الشهادة.

كما تم تقسيم الجرائم بحسب كيفية ارتكابها إلى: جرائم بسيطة، يتكون الركن المادي لكل منها من فعل مادي واحد، مثل جرائم القتل، وجرائم اعتيادية، يتكون ركنها المادي من عدة أعمال مادية متماثلة، أي: أن الفعل بذاته لا يعد جريمة، ولكن الاعتياد على ارتكاب الفعل هو الجريمة، والمقصود تكرار الفعل المادي.

والجرائم المؤقتة التي تتكون من فعل، أو امتناع يحدث في وقت محدد، ولا يستغرق وقوعها أكثر من الوقت اللازم لوقوع الفعل، أو قيام حالة الامتناع، مثل: جريمة الرشوة، أما الجرائم المستمرة فهي التي تتكون من فعل أو امتناع قابل للتجدد أو الاستمرار، مثل: الامتناع عن إخراج الزكاة.

كما تنقسم الجرائم إلى: جرائم عادية، وجرائم سياسية.

## المبحث الثاني
## نشأة الجريمة الإلكترونية وصورها

**المطلب الأول: نشأة الجريمة الإلكترونية:**

تطورت الظاهرة الإجرامية في العصر الحديث تطورًا ملحوظًا ومذهلا، سواء في شخصية مرتكبيها، أو أسلوب ارتكابها مع استخدام آخر ما توصلت إليه العلوم التقنية والتكنولوجية.

وقد تميز القرن العشرون باختراعات هائلة على المستوى التقني، لعل من أهمها ظهور الحاسوب الإلكتروني، ووجود ما يعرف بالإنترنت، وتعني شبكة الشبكات، أي: ربط شبكات الحاسوب الموجودة بعضها ببعض.

وقد نشأ الإنترنت نشأة عسكرية عام ١٩٦٩ من أجل وزارة الدفاع الأمريكية " البنتاجون"، ثم سرعان ما تحول استخدامه إلى المجال التعليمي سنة ١٩٧٢، حيث أتيح استخدامه من قبل الجامعة الأمريكية، وأخذت استخدامات الانترنت تتطور فيما بعد.

**المطلب الثاني: سمات المجرم الإلكتروني:**

المجرم المعلوماتي هو شخص يختلف عن المجرم العادي، فلا يمكن أن يكون هذا الشخص جاهلا للتقنيات الحديثة المعلوماتية.

لقد تنوعت الدراسات التي تحدد المجرم، وشخصيته، ومدى جسامة جرمه كأساس لتبرير وتقدير العقوبة.

ويكمن السؤال في حالتنا تلك كيف يمكن تبرير العقوبة وتقديرها في حالة مجرم الكمبيوتر والإنترنت؟ وهل هناك نموذج محدد للمجرم المعلوماتي؟

بالتأكيد لا يمكن أن يكون هناك نموذج محدد للمجرم المعلوماتي، وإنما هناك سمات مشتركة بين هؤلاء المجرمين، ويمكن إجمال تلك السمات فيما يلي:

١ – مجرم متخصص: له قدرة فائقة في المهارة التقنية، ويستغل مداركه ومهاراته في اختراق الشبكات، كسر كلمات المرور، أو الشفرات، ويسبح في عالم الشبكات؛ ليحصل على كل غالٍ وثمين من البيانات والمعلومات الموجودة في أجهزة الحواسب ومن خلال الشبكات.

٢ – مجرم يعود للإجرام: يتميز المجرم المعلوماتي بأنه يعود للجريمة دائمًا، فهو يوظف مهاراته في كيفية عمل الحواسيب، وكيفية تخزين البيانات والمعلومات، والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات ومرات فقد لا يحقق جريمة الاختراق بهدف الإيذاء، وإنما نتيجة شعوره بقدرته ومهارته في الاختراق.

٣ – مجرم محترف: له من القدرات والمهارات التقنية ما يؤهله لأن يوظف مهاراته في الاختراق، والسرقة، والنصب، والاعتداء على حقوق الملكية الفكرية، وغيرها من الجرائم مقابل المال.

٤ – مجرم ذكى: حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطوير في الأنظمة الأمنية؛ حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب[1].

**المطلب الثالث: صور الجريمة الإلكترونية:**

إذا كانت الجرائم المعلوماتية لها صور متعددة بتعدد دور التقنية المعلوماتية من جهة، وتعدد صور الجرائم التقليدية من جهة أخرى؛ فإن ذلك لا يعني تناول هذا الموضوع بالطريقة المدرسية التقليدية التي تتمثل في سرد كل الجرائم التي يتناولها قانون العقوبات، بل يجب التعرض للحالات التي تثير مشكلة في تطبيق النصوص القانونية، إما لتعذر المطابقة بينها وبين النصوص التقليدية، أو بسبب الفراغ التشريعي لمواجهة هذه الجرائم، ولما كان المجال لا يتسع للحديث عن كل

(١) البحر، عبد الرحمن ( ١٩٩٩ ). معوقات التحقيق في جرائم الأنترنت. "رسالة ماجستير غير منشورة" الرياض: أكاديمية نايف العربية للعلوم الأمنية.

أنواع الجريمة المعلوماتية فقد تخيرنا أكثرها إثارة للمشكلات القانونية، وهي جرائم الاعتداء على الحياة الخاصة، وجرائم الأموال، وجريمة التزوير.

**أولًا: جرائم الاعتداء على الحياة الخاصة للأفراد:**

المقصود من التطرق لموضوع جرائم الاعتداء على الحياة الخاصة للأشخاص التعرض لتلك الجرائم التي يتعذر علينا مواجهتها بالنصوص التقليدية، فالاعتداء عليها يتم بواسطة هذه التقنية التي أدت إلى سلب مادية السلوك، ومناقشة الحالات التي تثير مشكلة في تطبيق النصوص التقليدية، وتكشف مدى الحاجة إلى التصدي التشريعي لهذا النوع من الجرائم، وهي جرائم الاعتداء على الحياة الخاصة.

يصعب بداية حصر عناصر الحق في الحياة الخاصة، فهي تتكون من عناصر ليست محل اتفاق بين الفقهاء، فيمكن القول بأنها تشمل حرمة جسم الإنسان، والمسكن، والصورة، والمحادثات، والمراسلات، والحياة المهنية(١).

أما علاقة الحياة الخاصة بالتقنية المعلوماتية فقد ظهرت أهميتها بانتشار بنوك المعلومات في الآونة الاخيرة لخدمة أغراض متعددة، وتحقيق أهداف المستخدمين في المجالات العلمية والثقافية والعسكرية(٢).

هكذا أصبحت الشبكات المعلوماتية مستودعا خطيرا للكثير من أسرار الانسان التي يمكن الوصول إليها بسهولة وسرعة لم تكن متاحة في ظل سائر وسائل الحفظ التقليدية، فأصبحت بنوك المعلومات أهم وأخطر عناصر الحياة الخاصة للإنسان في العصر الحديث.

---

(١) ممدوح خليل عمر – حماية الحياة الخاصة والقانون الجنائي – دار النهضة العربية، القاهرة ١٩٨٣، ص ٢٠٧.

(٢) أسامة عبد الله قايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات – دار النهضة العربية القاهرة، ١٩٩٤، ص ٤٨.

وقد كان ذلك في البداية بالنسبة للمعلومات التي يدلي بها بعض الأشخاص بإرادتهم الخاصة أثناء تعاملاتهم مع المؤسسات العامة والخاصة في البنوك والمؤسسات المالية، كمؤسسات الائتمان، وشركات التأمين، والضمان الاجتماعي وغيرها، فالبيانات الخاصة بشخصية المستخدم يمكن الوصول إليها عن طريق زيارة بعض المواقع على شبكة المعلومات؛ لأن شبكات الاتصال تعمل من خلال بروتوكولات موحدة تسهم في نقل المعلومات بين الأجهزة، وتسمى هذه البروتوكولات الخاصة، مثل بروتوكولات HITP الذي يمكن عن طريقها الوصول الى رقم جهاز الحاسب الشخصي، ومكانه، وبريده الإلكتروني، كما أن هناك بعض المواقع التي يؤدي الاشتراك في خدماتها إلى وضع برنامج على القرص الصلب للحاسب الشخصي، وهو ما يسمى cookies، وهدفه جمع معلومات عن المستخدمين.

بل إن اخطر ما في استخدام هذه الشبكة يتمثل في أن كل ما يكتبه الشخص من رسائل يحفظ في أرشيف خاص يسمح بالرجوع إليه، ولو بعد عشرين عاما(١).

ويظن الكثيرون أن الدخول باسم مستعار، أو بعنوان بريدي زائف لساحات الحوار ومجموعات المناقشة قد يحميهم ويخفي هويتهم، وفي الحقيقة إن مزود الخدمة، أو internet service provider (ISP) يمكنه الوصول إلى كل هذه المعلومات، بل يمكنه أيضا معرفه المواقع التي يزورها العميل.

وعلية فإن القوانين المقارنة اهتمت بهذه المسألة، واتجهت إلى تبني العديد من الضمانات التي يمكن تلخيصها فيما يلي:

(١) عبد الفتاح بيومي حجازي – صراع الكمبيوتر والإنترنت – في القانون العربي النموذجي، دار الكتب القانونية – القاهرة ٢٠٠٧، ص ٦٠٩.

١- مبدأ الإخطار العام: وهو أن يعلم الجمهور الهيئات التي تقوم بجمع هذه البيانات وتنوع المعلومات التي تقوم بتسجيلها[١]، فيجب أن تكون هناك قيود على إنشاء الأنظمة المعلوماتية المختلفة لمعالجة البيانات.

٢- شرعية الحصول على المعلومة: يجب أن يتم الحصول على المعلومة بطريقة تخلو من الغش والاحتيال، حيث تمنع المادة ٢٥ من القانون الفرنسي للمعلوماتية تسجيل أية معلومة إلا إذا كانت برضاء صاحب الشأن.

٣- التناسب بين المعلومات الشخصية المسجلة والهدف من ذلك التسجيل، فعلى الجهة الراغبة في إقامة أي نظام معلوماتي أن تحدد الهدف من إقامته[٢].

ولقد تضمنت بعض القوانين العربية العديد من النصوص والقواعد التي تحمي البيانات الشخصية، وتفرض عقوبات على إفشاء هذا النوع من البيانات، مثال ذلك الفصل العاشر من قانون التجارة الإلكترونية المصري الصادر سنة ٢٠٠٤، الذي نص على حماية سرية البيانات المشفرة، واحترام الحق في الخصوصية، وكذلك قانون التجارة الإلكترونية، وقانون التجارة والمعاملات الإلكترونية في إمارة دبي الصادر سنة ٢٠٠٢، وقانون التجارة الإلكترونية التونسي الصادر سنة ٢٠٠٠، وهو ما يعني أن المشرع الليبي تأخر كثيرا في اللحاق بهذا الركب، خاصة بعد أن صدر القانون العربي النموذجي لجرائم الكومبيوتر، والذي تم إعداده من قبل اللجنة المشتركة بين المكتب التنفيذي لمؤتمر وزراء العدل العرب والمكتب التنفيذي لمؤتمر وزراء الداخلية العرب تحت رعاية جامعة الدول العربية، وجرى إقراراه بوصفه منهجا استرشاديا، يستعين به المشرع الوطني عند إعداد تشريع في جرائم المعلوماتية.

---

(١) بدر سليمان لويس – أثر التطور التكنولوجي مع الحريات الشخصية في النظم السياسية، رسالة الدكتوراة – حقوق القاهرة، ١٩٨٢.

(٢) عبد الفتاح بيومي حجازي – المرجع السابق، ص ٦٢٠.

**ثانيًا: جرائم الاعتداء على الأموال:**

إذا كان قانون العقوبات الليبي شأنه شأن كل قوانين العقوبات الأخرى قد جرم الاعتداء على الأموال في صوره التقليدية، كالسرقة، والنصب، وخيانة الأمانة، واختلاس الأموال العامة؛ فقد كان ذلك في ظل عصر لا يعرف سوى النقود الورقية أو المعدنية، وما يحل محلها من صكوك أو أوراق مالية، كالكمبيالات، والسند الإذنى في عصر المصارف التقليدية ذات المقر المحدد مكانيا، وقد كان أقصى ما وصلت إليه من تقدم متمثلا في إجراء التحويلات المصرفية بإجراءات ورقية معقدة، ومقابل رسوم مالية معينة.

فإذا كان الركن المادي للسرقة المتمثل في الاختلاس يمكن أن يطبق على التحويلات المالية غير المشروعة التي تتم عبر المصارف التقليدية فذلك لأن جريمة السرقة من الجرائم ذات القالب الحر، لم يحدد المشرع شكل السلوك الإجرامي لها، يمكن أن يتم بأي فعل يؤدي إلى حرمان المجني عليه من المال المنقول، وإدخاله في حيازة الجاني، كذلك الحال بالنسب لجريمة النصب، حيث يتحقق السلوك الإجرامي لها بالاستيلاء على أموال الآخر بالطرق الاحتيالية، فهل ينطبق ذلك على جرائم السرقة والاحتيال التي ترتكب عن طريق التقنية المعلوماتية؟

**الوسائل الفنية للتحويل الإلكتروني للأموال:**

يتم التحويل غير المشروع للأموال بعدة وسائل يصعب حصرها لسرعة وتيرة التطور في هذا المجال، لكن يمكن الاشارة إلى أكثرها انتشارًا:

١- استخدام برامج معده خصيصا لتنفيذ الاختلاس: أشهر هذه الوسائل هو تصميم برامج معينة تهدف إلى إجراء عمليات التحويل الآلي من حساب إلى آخر، سواء أكان ذلك من المصرف نفسه، أم من حساب أخر في مصرف آخر، على أن يتم ذلك في وقت معين يحدده مصمم هذا البرنامج، وأشهر هذه الوقائع قيام أحد العاملين بمركز الحاسبات المتعاقد مع مصرف الكويت التجاري لتطوير أنظمة

المعلومات بالاستيلاء على مبالغ طائلة من المصرف بعد أن تمكن من اختيار خمسة حسابات راكدة في خمسة فروع محلية للمصرف، وأعد لها برنامجا، تمثلت مهمته في تحويل مبالغ معينة من هذه الحسابات إلى حسابات أخرى فتحت باسمه في الفروع نفسها، على أن تتم عملية التحويل أثناء وجوده بالطائرة في طريقة إلى المملكة المتحدة عائدا إلى بلاده بعد انتهاء عقد عمله، ثم فتح حسابات أخرى فور وصوله وطلب من المصرف تحويل هذه المبالغ إلى حساباته الجديدة في بريطانيا(١).

كما توجد برامج أخرى تقوم بخصم مبالغ ضئيلة من حسابات الفوائد على الودائع المصرفية بإغفال الكسور العشرية، بحيث يتحول الفارق مباشرة إلى حساب الجاني؛ لأنها برامج تعتمد على التكرار الآلي لمعالجة معينة، ومما يؤدي إلى صعوبة اكتشاف هذه الطريقة رغم ضخامة المبلغ هو أن هذه الاستقطاعات تتم على مستوى آلاف الأرصدة في وقت واحد مع ضآلة المبلغ المخصوم من كل حساب على حده بحيث يصعب أن ينتبه إليه العميل(٢).

٢- التحويل المباشر للأرصدة: يتم ذلك عن طريق اختراق أنظمة الحاسب وشفرات المرور، أشهرها قيام أحد خبراء الحاسب الآلي في الولايات المتحدة باختراق النظام المعلوماتي لأحد المصارف، وقيامه بتحويل ١٢ مليون دولار إلى حسابه الخاص في ثلاث دقائق فقط، وعادة ما يتم ذلك أيضا عن طريق إدخال معلومات مزيفة، وخلق حسابات ومرتبات وهمية، وتحويلها إلى حساب الجاني، ويمكن ان يتم التحويل المباشر أيضا عن طريق التقاط الإشعاعات الصادرة عن الجهاز إذا كان النظام المعلوماتي متصلا بشبكة تعمل عن طريق الأقمار

---

(١) هشام فريد رستم – قانون العقوبات مخاطر المعلومات مكنة الآلات الحديثة، أسيوط، ١٩٩٢، ص ٨١.

(٢). Pit Man –third edition–Introduction to computer law –David Bainbridge ٢٣٧p ١٩٩٦publishing

الصناعية، فهناك بعض الأنظمة الى تستخدم طابعات سريعة تصدر أثناء تشغيلها إشعاعات إليكترومغناطيسية، ثبت أنه من الممكن اعتراضها والتقاطها أثناء نقل الموجات وحل شفراتها بواسطة جهاز خاص لفك الرموز، وإعادة بثها مرة أخرى بعد تحويرها[1]. وهو ما نصت عليه اتفاقية بودابست في المادة ٥.

٣- التلاعب بالبطاقات المالية: لقد ظهرت أولى محاولات هذا النوع من الاحتيال بالتقاط الأرقام السرية لبطاقات الائتمان وبطاقات الوفاء المختلفة من أجهزة الصرف الآلي للنقود إلى أن ظهرت الصرافة الآلية Electronic Banking، والنقود المالية digital Cash.

أما جرائم الاعتداء على هذه البطاقات فتتمثل في استخدامها من قبل غير صاحب الحق بعد سرقتها، أو بعد سرقة الارقام السرية الخاصة بها، وهو ما يتم عن طريق اختراق بعض المواقع التجارية التي يمكن أن تسجل عليها أرقام هذه البطاقات.

وفي هذا النوع من الاعتداءات لا نجد صعوبة في تطبيق نصوص جرائم السرقة والنصب عليها، سواء تم ذلك عن طريق سرقة البطاقة نفسها، أو عن طريق سرقة الرقم السري واستخدامه استخداما غير مشروع للتحايل على المؤسسات المالية، وصرف هذه المبالغ، خاصة أن النموذج التجريمي لجريمة النصب لم يشترط في الوسائل الاحتيالية أن تكون مرتكبة ضد الإنسان، فيكفي أن ترتكب هذه الوسائل الاحتيالية ضد الآلة، ما دامت تؤدي إلى الحصول على نفع غير مشروع؛ إضرارا بالآخر، وهو ما نصت عليه المادة ٤٦١ ع.

٤- جرائم الاعتداء على أجهزة الصرف الآلي للنقود: تثور هذه المشكلة في حالة استخدام الجهاز لصرف ما يتجاوز الرصيد الفعلي إذا تم ذلك بواسطة العميل صاحب البطاقة، فالمسألة هنا لا تعدو أن تكون مسألة مديونية بين المؤسسة

(١) محمد سامي الشوا، ثورة المعلومات وبعكسها على قانون العقوبات، دار النهضة العربية، القاهرة، ١٩٩٤، ص ٧٠-٧٢ وما بعدها.

المالية والعميل، ولا يمكن تكييفها بأنها سرقة طبقا للمادة ٤٤٤ع؛ لأن الاستيلاء على المبلغ لم يتم دون رضاء المؤسسة المالية، طالما أن هذه الأخيرة تعلم بأن الجهاز غير مرتبط بسقف حساب العميل حتى لا يتجاوزه.

٥- جرائم الاستيلاء على النقود الإلكترونية: يمكن تعريف النقود الإلكترونية Electronic Cash بأنها "قيمة نقدية مخزنة على وسيلة إلكترونية مدفوعة مقدمًا، وغير مرتبطة بحساب مصرفي، تحظى بقبول غير من قام بإصدارها، وتستعمل كأداة دفع". وتتمثل أهم عناصرها في أن قيمتها النقدية تشحن على بطاقة بلاستيكية، أو على القرص الصلب للحاسب الشخصي للمستهلك، فهي تختلف عن البطاقات الائتمانية؛ لأن النقود الإلكترونية يتم دفعها مسبقًا، بالإضافة إلى أنها ليست مرتبطة بحساب العميل، فهي أقرب إلى الصكوك السياحية منها إلى بطاقة الائتمان، أي: أنها استحقاق عائم على مؤسسة مالية، يتم بين طرفين، هما: العميل، والتاجر، دون الحاجة إلى تدخل طرف ثالث كمصدر هذه النقود مثلًا[١]، فهي مجموعة من البروتوكولات والتوقيعات الرقمية التي تتيح للرسالة الإلكترونية أن تحل فعليا محل تبادل العملات النقدية[٢]، ومن هذه البطاقات ما يعمل عن طريق إدخالها إلى المركز الخاص بالمعاملة المصرفية لدى البائع أو الدائن، حيث تم انتقال البيانات الاسمية من البطاقة إلى الجهاز الطرفي للبائع تحول عليه نتائج عمليات البيع والشراء إلى البنك الخاص بالبائع[٣].

---

(١) محمد إبراهيم محمد الشافعي، النقود الإلكترونية، مجلة الأمن والحياة، أكاديمية الشرطة، دبي، س ١٢، ع١، يناير، ٢٠٠٤، ص١٤٢-١٤٨.

(٢) منير الجنبيهي – ممدوح الجنبيهي – البنوك الالكترونية ط ٢ – ٢٠٠٦ دار الفكر الجامعي – الإسكندرية، ص٤٧.

(٣) عبد الفتاح بيومي حجازي – صراع الكمبيوتر والإنترنت – في القانون العربي النموذجي، دار الكتب القانونية – دار للنشر والبرمجيات – القاهرة ٢٠٠٧، ص ٦٠٩.

**التكييف القانوني لهذه الأنماط من السلوك:**

ولقد تدخل القانون العربي النموذجي بالنص مع تجريم الصور السابقة والاستيلاء على الأموال، فنص في المادة ٦ على أنه كل من استخدم بطاقة ائتمانية للسحب الالكتروني من الرصيد خارج حدود رصيده الفعلي أو باستخدام بطاقة مسروقة، أو تحصل عليها بأية وسيلة بغير حق، أو استخدام أرقامها في السحب، أو الشراء، وغيرها من العملات المالية مع العلم بذلك يعاقب بالحبس الذي لا تقل مدته عن( )، وبالغرامة ( ). وهو ما يعني أن هذا النص قاصر على توفير الحماية لغيرها من البطاقات لتقدير الدولة.

أما اتفاقية بودابست السابق الإشارة اليها فقد نصت المادة ٨ منها، والخاصة بالتحايل المرتبط بالحاسب computer related frau على معاقبة أي شخص يتسبب بأية خسائر مادية للغير عن طريق تعديل، أو محو، أو إيقاف لأي بيانات مخزنة في أي نظام معوماتي، أو عن طريق أي تدخل فيه، وبذلك تتوافر الحماية الجنائية اللازمة للأموال في مواجهة السلوك المرتكب بالحاسب الآلي.

إذا كانت جرائم الأموال المرتكبة بواسطة الحاسب الآلي تواجه فراغا تشريعيا في الكويت فإن المشكلة الحقيقة في نظرنا بالنسبة لهذه الجرائم لا تتمثل في الفراغ التشريعي بقدر ما هي كامنة في طرق ضبطها وإثباتها، وهو ما يرجع الى افتقاد الآثار التقليدية التي قد تتركها أية جريمة في الجريمة المعلوماتية، فالبيانات يتم إدخالها مباشرة في الجهاز دون أن تتوقف على وجود وثائق أو مستندات؛ لأنه كثيرا ما يكون هناك برامج معدة ومخزنة سلفا على الجهاز، ولا يكون عليه سوى إدخال البيانات في الأماكن المعدة لها، كما هو الحال بالنسبة للمعاملات المصرفية والمؤسسات التجارية الكبرى، ويمكن في هذه الفروض اقتراف جرائم الاختلاس والتزوير فتفقد الجريمة آثارها التقليدية[1].

(١) عبد الفتاح بيومي حجازي – جرائم الكمبيوتر والإنترنت – دار الكتب القانونية – القاهرة، ٢٠٠٥، ص ٤٢.

فالجريمة المعلوماتية ترتكب في مسرح خاص يتمثل في عالم افتراضي مفرغ cyberspace، وهو ما يختلف كليا عن المسرح الذي ترتكب فيه الجرائم في صورتها التقليدية، حيث تطبق القواعد العامة لانتداب الخبراء في اقتفاء آثار الجناة الذين يرتكبون جرائم تتكون من سلوك مادي ملموس، وله محل مادي ملموس أيضا، مما لا يتناسب ونوع الخبرة المطلوبة لمعاينة المسرح السيبيري للجريمة المعلوماتية المرتكبة في الفضاء الإلكتروني.

فالخبرة المطلوبة للتحقيق في الجريمة المعلوماتية يجب أن تكون على درجة عالية من الكفاءة العلمية أو العملية أيضا، وهو ما يوجب أن يكون الخبير في الجريمة المعلوماتية ملما بأدق تفاصيل تركيب الحاسب، وعمل الشبكات المعلوماتية، والأماكن المحتملة للأدلة، كالمواضع التي يمكن أن تحتفظ بآثار الاختراق وتوقيته، والبرامج المستخدمة في أية عملية تمت أثناء الاختراق، بالإضافة إلى إمكانية نقل الأدلة الى أوعية أخرى دون تلف.

يجب الإشارة أيضا إلى أن ملاحقة الجرائم المعلوماتية لا يتطلب رفع كفاءة الخبراء فقط، بل إنها تحتاج إلى رفع كفاءة مأموري الضبط القضائي بصفة عامة؛ لأن مأمور الضبط القضائي أول شخص يكتشف الجريمة ويتصل بمسرحها، والمسئول الأول عن التحفظ على أي أثر يتركه الجاني بعد ارتكابه للجريمة؛ مما يستوجب أن يكون المتعامل الأول مع النظام المعلوماتي على درجة من الكفاءة، تسمح له بالتحفظ على هذه الأدلة؛ لأن أي خطأ في التعامل الأولى مع هذه الأجهزة قد يؤدي إلى محو الأثر أو الأدلة.

أما اتفاقية بودابست السابق الاشارة اليها فقد أشارت في القسم الإجرائي منها في المادة ١٦ إلى أنه (على الدول الأعضاء العمل على تطبيق أنظمة فنية لحماية البيانات المخزنة مع إلزام العاملين في أي نظام معلوماتي بحفظ كل العمليات المنطقية التي تجري على الأجهزة لمدة لا تقل على ٩٠ يوما)، وهو ما يعني أن الاتفاقية تشترط مستوى معينًا للكفاء الفنية في العمل بهذه التقنية، مما

يعني أننا نحتاج إلى برنامج وطني متكامل لرفع مستوى كفاءة العمل بهذه التقنية قبل الحديث عن إمكانية تطبيق هذه المعاهدة.

**ثالثًا: جريمة التزوير:**

نصت المادة ٣٤١ع على أنه يعاقب بالحبس مدة لاتقل عن ثلاث سنوات كل موظف يضع أثناء ممارسة مهامه وثيقة مزورة في كليتها، أو جزء منها، أو زور وثيقة صحيحة.

ما يهمنا في هذا الصدد محل جريمة التزوير؛ لأن هذه الأخيرة من الجرائم ذات القالب الحر التي لم يحدد المشرع فيها شكلا معينا للسلوك الإجرامي فيه، لكنه حدد محل هذا السلوك بالوثيقة دون أن يعرفها أو يحدد مضمونها، تاركا للفقه والقضاء هذه المهمة.

فالوثيقة هي مجموعة من المعاملات والرموز التي تعبر تعبيرا اصطلاحيا عن مجموعة مترابطة من الأفكار والمعاني الصادرة عن شخص أو أشخاص معينين، وتكمن القيمة الحقيقية لها ليس في مادتها أو ما تحتويه، بل تكمن فيما لهذا التعبير من دلالة اجتماعية(١).

فجوهر جريمة التزوير هو الإخلال بالثقة العامة التي أراد المشرع حمايتها في هذه الوثيقة؛ لما لها من آثار قانونية باعتبارها وسيلة للإثبات(٢).

ولما كان ذلك فإن قوة الوثيقة في الإثبات هى جوهر الحماية الجنائية لها، ومن هنا ذهبت بعض الآراء الفقهية الى أن كل مادة تصلح للاثبات يجوز أن تكون محلا للتزوير مهما كان شكلها أو مساحتها، ولا أهمية للمادة المستعملة في

---

(١) محمود نجيب حسني – شرح قانون العقوبات – القسم الخاص – الجرائم المضرة بالمصلحة العامة – دار النهضة العربية – القاهرة ١٩٧٢، ص ٣٢٢.

(٢) محمد سامي الشوا – ثورة المعلومات وانعكاساتها على قانون العقوبات – دار النهضة العربية – القاهرة ١٩٩٤، ص ١٥٥.

الكتابة، يستوى أن تكون مصنوعة من خشب أو جلد[١]، فإذا كانت فكرة التوسع في مفهوم الوثيقة مطروحة في الفقة الجنائي قبل ظهور جرائم المعلوماتية فإن هذا التوسع يبدو أكثر إلحاحا في ظل الفراغ التشريعي لمواجهة جرائم التزوير المرتكبة بواسطة الحاسب الآلي، إلا أن هذا الاتجاه واجه نقدًا شديدًا، حيث ذهب جانب من الفقة الفرنسي قبل صدور القانون رقم ١٩ لسنة ١٩٨٨ الخاص بالغش المعلوماتي إلى رفض اعتبار التعبير الواقع على الأسطوانات الممغنطة تزويرًا، استنادا إلى اعتبارين: أولهما انتفاء الكتابة؛ لان التغيير انصب على نبضات إلكترومغناطيسية، والثاني هو عدم التيقن من صلاحيتها في الإثبات[٢].

يؤيد هذا الرأي قياس ذلك على انتفاء التزوير في التغيير الذي يطرأ على الصوت المسجل، والعلة هي انعدام عنصر الكتابة، بالإضافة إلى أن النبضات الإلكترومغناطيسية تمثل جزءا من ذاكرة الآلة أو برنامج تشغيلها، وهو ما يمكن أن يتحقق معه معه الإتلاف أو التقليد إذا توافرت شروطهما، وقد بدأ الفكر القانوني الحديث يقبل فكرة الوثيقة الإلكترونية استنادا إلى أن المادة التي تصنع منها الوثيقة ليست عنصرا فيها.

إن مجاراة التقدم العلمي والتكنولوجي تتطلب تجاوز المفهوم التقليدي للوثيقة أو حصره في الورق المكتوب، ويمكن لنا في هذه الحالة أن نجد سندا لهذه الفكرة ومنطلقا لها أن المشرع المدني في الأصل رغم أخذه بمبدأ سيادة الدليل الكتابي على غيره من طرق الإثبات فإنه أورد عليه بعض الاستثناءات، فقبل الإثبات بالبينة فيما كان يجب إثباتها كتابة في حالات حددتها المواد ٣٨٧ ، ٢٨٩، ٣٩١ من القانون المدني الليبي، وهي اتفاق الأطراف على الإثبات بالبينة، أو وجود مانع يحول دون الحصول على الدليل الكتابي، فإذا اتفق الأطراف على الإثبات بالبينة

(١) حسن صادق المرصفاوي – قانون العقوبات الخاص – منشأة المعارف – الاسكندرية، مصر، ١٩٩١، ص ١١٦.

(٢) محمد سامي الشوا – المرجع السابق، ص ١٥٥.

يكون على القاضي أن يعتد بها؛ استنادا إلى عدم تعلق القواعد الموضوعية في الإثبات بالنظام العام، مما يمكن القول معه بإمكانية اتفاق الأطراف على الإثبات بالوسائل الإلكترونية، وهو ما يعد إيذانا ببداية عصر الوثائق الإلكترونية.

**موقف الشريعة الإسلامية من جرائم الحاسب الآلي والإنترنت:**

من مقاصد الشريعة الاسلامية في أحكامها رعاية المصالح، ودرء المفاسد، فكل مافيه مصلحة معتبر شرعًا، وكل ما فيه مفسدة غير معتبر شرعًا، وعلى ذلك فكل ما يؤدي إلى المفاسد يكون منهيًا عنه، ولا شك أن الجرائم بجميع أنواعها يترتب عليها مفسدة؛ وبالتالي فعلها يكون محرمًا شرعًا، وهذه الجرائم أفردها الفقهاء في عصر تدوين الفقه، ونصوا على أحكامها، وفي هذا العصر ظهرت جرائم كثيرة مرتبطة بالتقدم في جميع المجالات التقنية في مجال الحاسب الآلي والإنترنت، وعَرَّفت الشريعة الإسلامية الجريمة بأنها: "محظورات شرعية زجر الله عنها بحد أو تعزير "[1].

وتعرّف جرائم الحاسب الآلي والإنترنت بأنها: "ذلك النوع من الجرائم التي تتطلب إلمامًا خاصًا بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها، ومقاضاة فاعليها "( ٢٨ ).

كما يمكن تعريفها بأنها "الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني" (٢٩ ).

وهناك من عرّفها بأنها "أي عمل غير قانوني يستخدم فيه الحاسب كأداة، أو موضوع للجريمة" ( ٣٠ ).

وفي كل الأحوال فجريمة الحاسب الآلي "لا تعترف بالحدود بين الدول، ولا بين القارات، فهي جريمة تقع في أغلب الأحيان عبر حدود دولية كثيرة "(٣١).

(١) الماوردي، محمد حبيب. الاحكام السلطانية. (القاهرة: دار التراث العربي، ١٤٠٧هـ)، ١٩.

وتعد جريمة الإنترنت من الجرائم الحديثة التي تُستخدم فيها شبكة الإنترنت كأداة لارتكاب الجريمة، أو تسهيل ارتكابها (Vacca , 1996 ).

وأطلق مصطلح جرائم الإنترنت (Internet Crimes) في مؤتمر جرائم الإنترنت المنعقد في أستراليا للفترة من ١٦ – ١٩٩٨/٢/١٧م (٣٢).

**أما التعريف الإجرائي لدراسة الباحث فتُعَرَّفُ جرائم الإنترنت بأنها:** جميع الأفعال المخالفة للشريعة الإسلامية، وأنظمة المملكة العربية السعودية، المرتكبة بواسطة الحاسب الآلي، من خلال شبكة الإنترنت، ويشمل ذلك: الجرائم الجنسية، والممارسات غير الأخلاقية، وجرائم الاختراقات، والجرائم المالية، وجرائم إنشاء أو ارتياد المواقع المعادية، بالإضافة للمواقع التي تنشر الأفكار المنحرفة، وتشجع على الكراهية، والعنف، وارتكاب الجرائم.

**فماهي حدود الحماية الجنائية للحياة الخاصة في القانون الجنائي الكويتي؟**

الجرائم والعقوبات التي ينص عليها قانون الجرائم الالكترونية الكويتي:

• يتم معاقبة كل من يدخل بشكل غير مشروع أو قانوني إلى أي جهاز حاسوب، أو شبكة معلوماتي، أو نظام معلوماتي بالحبس لمدة ستة أشهر مع دفع غرامة تبلغ من ٥٠٠ إلى ٢٠٠٠ دينار كويتي، أو إحدى هاتين العقوبتين، وذلك وفقا للمادة رقم ٢ من قانون جرائم تقنية المعلومات.

• يتم عقوبة كل من يدخل إلى جهاز حاسب آلي، أو نظام معلوماتي، أو شبكة معلوماتية بطريقة غير مشروعة، ويقوم بإلغاء، أو حذف، أو تدمير، أو إعادة نشر للبيانات، أو المعلومات الخاصة بتلك الأنظمة – بالحبس لمدة سنتين، مع دفع غرامة من ٢٠٠٠ إلى ٥٠٠٠ دينار كويتي، أو إحدى هاتين العقوبتين، أما إذا كانت تلك البيانات أو المعلومات شخصية فتتعدى العقوبة إلى الحبس لمدة ثلاث سنوات، مع دفع غرامة من ٣٠٠٠ إلى ١٠,٠٠٠ دينار كويتي، وذلك وفقا للمادة رقم ٢ من قانون جرائم تقنية المعلومات.

• إذا تم الدخول إلى أحد الأنظمة الإلكترونية بهدف الحصول على بيانات أو معلومات حكومية وسرية يتم معاقبة الفاعل بالحبس لمدة عشر سنوات، مع دفع غرامة من ٥٠٠٠ إلى ٢٠,٠٠٠ دينار كويتي، أو إحدى هاتين العقوبتين، وذلك وفقا للمادة رقم ٣ من قانون جرائم تقنية المعلومات.

• إذا كان مخترق أحد الأنظمة الحكومية السرية قد عمل على إلغاء البيانات، أو إتلافها، أو تدميرها، أو نشرها، أو تعديلها، فستصل عقوبته إلى الحبس عشر سنوات، مع دفع غرامة مالية قدرها ٥٠٠٠ إلى ٢٠,٠٠٠ دينار، أو إحدى هاتين العقوبتين، وذلك وفقا للمادة رقم ٣ من قانون جرائم تقنية المعلومات.

• جريمة تزوير أي مستندات، أو إتلافها، أو تزوير سجلات إلكترونية، أو توقيعات إلكترونية، أو نظام إلكتروني، أو موقع إلكتروني – تقع عقوبة على فاعلها بالحبس لمدة ثلاث سنوات، مع دفع غرامة وقدرها ٣٠٠٠ إلى ١٠,٠٠٠ دينار كويتي، أو إحدى هاتين العقوبتين، وذلك وفقا للمادة رقم ٣ من قانون جرائم تقنية المعلومات.

• أما جريمة التزوير على أي مستندات، أو بيانات حكومية، أو بنكية، تقع عقوبة على فاعلها بالحبس لمدة سبع سنوات، مع دفع غرامة مالية قدرها ٥٠٠٠ إلى ٢٠,٠٠٠ دينار كويتي، أو إحدى هاتين العقوبتين، وذلك وفقا للمادة رقم ٣ من قانون جرائم تقنية المعلومات.

• إذا وقعت جريمة تزوير على مستندات إلكترونية، أو إتلافها، وتكون خاصة بالفحوصات الطبية، أو التشخيص، أو العلاج الطبي، سوف تقع عقوبة على فاعلها بالحبس ثلاث سنوات، مع دفع غرامة مالية قدرها ٣٠٠٠ إلى ١٠,٠٠٠ دينار كويتي، أو إحدى هاتين العقوبتين، وذلك وفقا للمادة رقم ٣ من قانون جرائم تقنية المعلومات.

• من يقوم بتهديد، أو ابتزاز شخص ما لحمله على فعل، أو الامتناع عنه– يتم معاقبته بالحبس لمدة ثلاث سنوات، مع دفع غرامة من ٣٠٠٠ إلى ١٠,٠٠٠ دينار

كويتي، أو أي من إحدى العقوبتين، وذلك وفقا للمادة رقم ٣ من قانون جرائم تقنية المعلومات.

• من يقوم بتهديد شخص بالقتل، أو بما يمس كرامة الشخص، أو يخدش شرفه، أو اعتباره، يتم معاقبته بالحبس لمدة خمس سنوات، مع دفع غرامة قدرها ٥٠٠٠ إلى ٢٠,٠٠٠ دينار، أو أي من إحدى العقوبتين، وذلك وفقا للمادة رقم ٣ من قانون جرائم تقنية المعلومات.

• يتم الحبس لمدة سنتين مع غرامة قدرها ٢٠٠٠ إلى ٥٠٠٠ دينار كويتي، أو أي من إحدى العقوبتين، لكل من قام بتعطيل، أو إعاقة الوصول إلى موقع، أو الدخول إلى الأجهزة والبرامج، أو مصادر البيانات بشكل متعمد، وذلك وفقا للمادة رقم ٤ من قانون جرائم تقنية المعلومات.

• إذا قام شخص بالتنصت، أو الاعتراض، أو الالتقاط بشكل متعمد عن أي من المرسلات عن طريق شبكة المعلومات، أو أي وسيلة من وسائل تقنية المعلومات– يتم معاقبته بالحبس لمدة سنتين، مع دفع غرامة من ٢٠٠٠ إلى ٥٠٠٠ دينار كويتي، وذلك وفقا للمادة رقم ٤ من قانون جرائم تقنية المعلومات.

• يتم الحبس سنتين مع دفع غرامة قدرها ٢٠٠٠ إلى ٥٠٠٠ لكل من يقوم بإنشاء موقع، أو نشر، أو إنتاج، أو إعداد، أو إرسال، أو تخزين لمعلومات، أو بيانات بهدف الاستغلال، أو التوزيع، أو العرض على أشخاص آخرين، وذلك وفقا للمادة رقم ٤ من قانون جرائم تقنية المعلومات.

• جريمة التحريض على أعمال منافية للأخلاق، كالدعارة، والفجور، أو المساعدة عليها، يتم حبس فاعلها لمدة سنتين مع دفع غرامة قدرها ٢٠٠٠ إلى ٥٠٠٠ دينار كويتي، أو أي من إحدى العقوبتين، وفقا للمادة رقم ٤ من قانون جرائم تقنية المعلومات.

• يتم معاقبة كل من يقوم باستخدام أي من وسائل تقنية المعلومات، أو الشبكة المعلوماتية بهدف التوصل إلى أرقام، أو بيانات خاصة ببطاقة ائتمانية، أو أي من

البطاقات الإلكترونية ذات الصلة، بالحبس لمدة سنة مع دفع غرامة قدرها من ١٠٠٠ إلى ٣٠٠٠ آلاف دينار كويتي، أو أي من إحدى العقوبتين، وفي حال استخدام تلك البيانات لسرقة أموال أصحابها أو للتمتع بخدمات البطاقة، يتم معاقبة الفاعل بالحبس لمدة ثلاث سنوات، ودفع غرامة لا تقل عن ٣٠٠٠ دينار، ولا تتعدى الـ ١٠,٠٠٠ دينار، أو أي من هاتين العقوبتين، وذلك وفقا للمادة رقم ٤ من قانون جرائم تقنية المعلومات.

• من ينشئ موقعا إلكترونيا، أو ينشر معلومات عن طريق الإنترنت، أو أي وسيلة من وسائل تقنية المعلومات، وكان هدفه الاتجار بالبشر، أو تسهيل التعامل فيهم، أو الترويج للمخدرات، أو ما شابه- يعاقب بالحبس لمدة سبع سنوات، مع دفع غرامة قدرها من ١٠,٠٠٠ إلى ٣٠,٠٠٠ دينار كويتي، وذلك وفقا للمادة رقم ٨ من قانون جرام تقنية المعلومات.

• كل من يقوم باستخدام شبكة الإنترنت، أو أي من وسائل تقنية المعلومات لغسيل الأموال، أو تحويل أموال غير مشروعة، أو نقلها، أو بإخفاء مصدرها غير المشروع، أو قام باكتسابها، أو استخدامها، أو حيازتها، وكان على علم بأنها أموال غير مشروعة- يتم حبسه لمدة عشر سنوات مع دفع غرامة وقدرها ٢٠,٠٠٠ إلى ٥٠,٠٠٠، أو إحدى هاتين العقوبتين، وذلك وفقا للمادة رقم ٩ من قانون جرائم تقنية المعلومات.

• من يقوم بإنشاء موقع إلكتروني تابع لمنظمة إرهابية، أو لشخص إرهابي، أو نشر أي معلومات عن إحداهما عبر الإنترنت، أو بأي وسيلة من وسائل تقنية المعلومات، حتى إذا كانت تحت أسماء مستعارة؛ لتسهيل عملية الاتصال بقيادات تلك المنظمة، أو أعضائها، أو الترويج لأفكارها، أو تمويلها، أو لنشر معلومات عن كيفية تصنيع المتفجرات والأجهزة الحارقة، أو أي من الأدوات التي تستخدم في العمليات الإرهابية- يتم معاقبته بالحبس لمدة عشر سنوات، مع دفع غرامة مالية

قدرها ٢٠,٠٠٠ إلى ٥٠,٠٠٠ دينار، أو إحدى هاتين العقوبتين، وذلك وفقا للمادة رقم ١٠ من قانون جرائم تقنية المعلومات.

**المطلب الثاني: أسباب الجريمة الإلكترونية:**

هناك عدد من الأسباب التي يمكن حصرها كأسباب للجريمة الإلكترونية، منها ما يقع على مستوى كوني، ومنها ما يقع على مستوى مجتمعي، ومنها ما يقع على مستوى فردي أو شخصي.

كما أن أسباب الجريمة الإلكترونية تتفاوت وفق نوعها، ونوع المستهدف، ونوع الجاني، ومستوى تنفيذه (فردي، مجتمعي، كوني)، فجرائم الشباب والهواه والصغار تختلف عن أسباب جرائم المحترفين، وتختلف وفق هدفها: سرقة، أو معلومات، أو تجارة بالمعلومات، أو شخصية الخ.

**الفرع الأول: خصائص الجريمة الإلكترونية:**

– تتّسم بسهولة الوقوع في فخها؛ حيث إنّ غياب الرقابة الأمنية يسهم في انتشارها، وتسهيل ذلك.

– الضرر الناجم من الجرائم الإلكترونية غير قابل للقياس؛ إذ إنّها تخلق أضرارًا جسيمة.

– صعوبة الكشف عن مرتكب الجريمة إلا بأساليب أمنية وتقنية عالية.

– سلوك خارج عن المألوف وغير أخلاقي مجتمعيًّا.

– ذات عنف وجهد أقل من الجرائم التقليديّة.

– جريمة غير مقيّدة بزمان ومكان؛ إذ تمتاز بالتباعد الجغرافيّ، وعدم تقيدها بالتوقيت الزمنيّ.

– سهولة إخفاء آثار الجريمة والأدلة التي تدلّ على الجاني؛ نظرًا للترميز والتشفير الذي يحدث على الرموز المخزّنة على وسائط التخزين الممغنطة.

**الفرع الثاني: معالجة الجريمة الإلكترونية:**

– رسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الإنترنت؛ إذ يستلزم التدخل الحكومي والدولي؛ نظرًا للخطورة الجسيمة للأمر.

– الاعتماد على أساليب وتقنيات متطوّرة للتمكن من الكشف عن هوية مرتكب الجريمة والاستدلال عليه بأقل وقت ممكن.

– توعية الأفراد ونصحهم لماهية الجرائم الإلكترونية، وكل ما يترتب عليها من مخاطر.

– الحرص على الحفاظ على سرية المعلومات الخاصة بالعناوين الإلكترونية، كالحسابات البنكية، والبطاقات الائتمانيّة، وغيرها.

– عدم الكشف عن كلمة السر نهائيًا، وتغييرها بشكل مستمر، واختيار كلمات سر صعبة.

– تجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي وأجهزة الحاسوب.

– تجنّب تحميل أي برنامج مجهول المصدر.

– استمرارية تحديث برامج الحماية الخاصة بأجهزة الحاسوب ومنها، MCafee, Norton.

– تأسيس منظمة خاصة لمكافحة الجرائم الإلكترونية والحد منها.

– المسارعة في الإبلاغ للجهات الأمنية فور التعرض لجريمة إلكترونية.

– مواكبة التطورات المرتبطة بالجريمة الإلكترونية، والحرص على تطوير وسائل مكافحتها.

– استخدام برمجيات آمنة ونظم تشغيل خالية من الثغرات.

– الحرص على استخدام كلمات سرية للوصول إلى البرامج الموجودة على جهاز الحاسوب.

– عدم ترك جهاز الحاسوب مفتوحًا.

– فصل اتصال جهاز الحاسوب بشبكة الإنترنت في حال عدم الاستخدام.

– أخذ الحيطة والحذر، وعدم تصديق كل ما يصل من إعلانات، والتأكد من مصداقيتها عن طريق محركات البحث الشهيرة.

– وضع الرقم السري بشكل مطابق للمواصفات الجيدة التي تصعّب من عملية القرصنة عليه من هذه المواصفات، بأن يحتوي على أكثر من ثمانية أحرف، وأن يكون متنوع الحروف، والرموز، واللغات إلخ.

– يفضل تغيير كلمة المرور الخاصة بك بصفة دورية.

– لا تضع معلومات علي الإنترنت لا تحب أن يراها الجميع من تعرفهم ولا تعرفهم، وتذكر أنه بمجرد أن تضع معلومات علي الإنترنت لن تتمكن أبدا من ارجاعها مرة أخرى، حتى لو قمت بحذفها.

– معلوماتك الخاصة (اجعلها خاص)، إن معلوماتك الخاصة مثل اسمك بالكامل، ورقم هاتفك، ورقم الهوية، ورقم بطاقتك الائتمان، وأيضا عنوانك بالتفصيل هي معلومات خاصة، يجب أن لا تتاح للجميع علي الإنترنت، لأي شخص لا تعرفه، فلا تفصح له عنها، أو تضعها علي أي موقع لا تثق به.

## الخاتمة

**النتائج:**

لم تتوقف الجريمة الإلكترونية عند حد اختراقات الأجهزة أو الحسابات، بل أصبحت الميديا الجديدة وسيلة مهمة تستخدمها المنظمات الإرهابية في نشر أفكارهم المسمومة، وتحريضهم عبر إغواء الشباب، وتضليلهم فكريا من خلال حسابات وهمية يختلقونها عبر مواقع التواصل الاجتماعي، ويحاولون من خلالها استمالة الشباب للتغرير بهم؛ ولذلك كان لا بد من وجود قانون صارم يحد من هذه التجاوزات الكبيرة، ولكن مع ضرورة الاحتفاظ بحق الفرد بإبداء رأيه، وخاصة فئة الشباب الذين يجدون مواقع التواصل الاجتماعي متنفسا لهم للتعبير عما يدور من حولهم من قضايا المجتمع الداخلي أو الخارجي.

لذا وجب علينا التنويه وعمل الأبحاث اللازمة للحد من هذه الجرائم؛ لكي تساعد المجتمع والأفراد في عدم الوقوع في تلك الجرائم.

**Results**

Cybercrime did not stop at the limit of hacking devices or accounts, but the new media became an important means used by terrorist organizations to spread their poisoned ideas and incite them by seducing young people and misleading them intellectually through fake accounts they created through social networking sites and trying to win over young people to deceive them, and therefore it was not There must be a strict law that limits these major transgressions, but with the necessity of preserving the right of the individual to express his opinion, especially the group of young people who find social networking sites an outlet for them to express what is going on around them from the internal or external community issues.

Therefore, we must note and do the necessary research to reduce these crimes in order to help society and individuals not to fall into these crimes.

## فهرس المراجع


١- أسامة عبد الله قايد – **الحماية الجنائية للحياة الخاصة وبنوك المعلومات** – دار النهضة العربية، القاهرة، ١٩٩٤.

٢- البحر، عبد الرحمن ( ١٩٩٩ ). **معوقات التحقيق في جرائم الإنترنت.**" رسالة ماجستير غير منشورة" الرياض: أكاديمية نايف العربية للعلوم الأمنية.

٣- حسن صادق المرصفاوي – **قانون العقوبات الخاص** – منشأة المعارف – الاسكندرية، مصر، ١٩٩١.

٤- د. أحمد السيد عفيفي – **الأحكام العامة للعلانية في قانون العقوبات – دراسة مقارنة** – ٢٠٠١ – ٢٠٠٢– دار النهضة العربية، القاهرة.

٥- د. جميل عبد الباقي الصغير – **الإنترنت والقانون الجنائي** – دار النهضة العربية –٢٠٠١.

٦- عبد الفتاح بيومي حجازي – **جرائم الكمبيوتر والإنترنت** – دار الكتب القانونية – القاهرة، ٢٠٠٥.

٧- عبد الفتاح بيومي حجازي – **جرائم الكمبيوتر والإنترنت** – في القانون العربي النموذجي، دار الكتب القانونية – القاهرة، ٢٠٠٧.

٨- فتوح الشاذلي – **القانون الدولي الجنائي** – دار المطبوعات الجامعية – الاسكندرية – ٢٠٠١.

٩- فهد بن عبدالله اللحيدان، **الإنترنت، شبكة المعلومات العالمية** – الطبعة الأولى– الناشر غير معروف – ١٩٩٦.

١٠- الماوردي، محمد حبيب. **الأحكام السلطانية.** (القاهرة: دار التراث العربي، ١٤٠٧هـ).

١١- مبدر سليمان لويس – **أثر التطور التكنولوجي مع الحريات الشخصية في النظم السياسية**، رسالة الدكتوراة – حقوق القاهرة.

١٢- محمد إبراهيم محمد الشافعي، **النقود الإلكترونية**، مجلة الأمن والحياة، أكاديمية الشرطة، دبي، س ١٢، ع١، يناير، ٢٠٠٤.