أخطر مظاهر جرائم الإحتيال الإلكتروني التي يستخدمها المُحتال المعلوماتي

د. كريم معروف، دكتوراه في قانون جنائي، جامعة غليزان، الجزائر.

البريد الإلكتروني: karimmaarouf001@gmail.com

الملخص:

يوجد العديد من أشكال الإحتيال الإلكتروني المنتشرة في العالم عبر الفضاء الإلكتروني أو من خلال البطاقات الممنغطة، والتي تختلف صورها وأشكالها حسب طبيعة كل مجتمع ودولة، ودرجة تطور ها في مجال تكنولوجيا الإعلام والإتصال، فمثلا مظاهر الإحتيال الإلكتروني التي يستعملها المُحتال المعلوماتي في الدول الديمقراطية والمتطورة في المجال التكنولوجي تختلف عن مظاهر الإحتيال الإلكتروني التي يستعملها المُحتال المعلوماتي في الدول النامية.

من بين أخطر صور الإحتيال الإلكتروني هو الإحتيال الذي يقع بواسطة بطاقات الإئتمان الممغنطة مثل إستخدام بطاقات إئتمان مسروقة أو مفقودة أو مزورة، والإحتيال الذي يقع في مجال التجارة الإلكترونية مثل الإيهام بوجود مشروع كاذب أو الغش بإتخاذ إسم كاذب أو صفة غير صحيحة، وأيضا من صور الإحتيال الإلكتروني التي يستعملها المُختال المعلوماتي الإحتيال عبر الرسائل النصية والإحتيال بجمع التبرعات الخيرية.

الكلمات المفتاحية:

الإحتيال الإلكتروني، المُحتال المعلوماتي ، الجرائم الإلكترونية، بطاقة الإئتمان الممغنطة، البطاقات المزورة، المواقع الإلكترونية المزيفة، الغش والخداع. .

The Most Dangerous Manifestations of Electronic Fraud Crimes Used By The Electronic Fraudster

abstract

There are many forms of electronic fraud spread in the world through cyberspace or through covered cards, whose forms and forms vary according to the nature of each society and country, and the degree of their development in the field of information and communication technologies, for example, the manifestations of electronic fraud used by the information fraudster in democratic and technologically developed countries differ from the manifestations of electronic fraud used by the information fraudster in developing countries.

One of the most dangerous forms of electronic fraud is fraud that occurs by fraudulent credit cards, such as the use of stolen, lost or forged credit cards, and fraud that occurs in the field of e-commerce, such as the illusion of the existence of a false project or fraud by taking a false name or an incorrect characteristic, and also from the forms of electronic fraud used by the information fraudster, fraud via SMS, and fraud by collecting charitable donations.

Keywords,

fraud, fraud, cyber fraud, cybercrime, covered credit card, fake cards, fraudulent websites. Cheating and deception.

مقدمة:

على ضوء التطور التكنولوجي الحديث الذي نعيشه وتطور المعاملات المالية إنتشرت في الفترات الأخيرة عمليات الإحتيال الإلكتروني في العديد من المجتمعات وقع ضحيته الكثير من الضحايا من طرف عصابات تتاجر بأحلام الناس عن طريق منحهم وعودا بالثراء السريع، ووجود العديد من المُحتالين الذين يترصدون ضحاياهم عبر مواقع التواصل الإجتماعي والأنترنيت عن طريق وسائل منمقة تخبرهم بالفوز بجوائز مالية.

ويعتبر الإحتيال الإلكتروني من أكثر الجرائم تطورا ويستخدم المُحتالون حيلا وأساليب تتناسب وتتلاءم مع التطورات الحديثة، وظهرت طرق مختلفة للإحتيال عبر مواقع التواصل الإجتماعي والأنترنيت يقوم من خلالها المُحتالون بتمرير أعمالهم الإحتيالية تحت غطاء وهمي بأن أعمالهم مشروعه وعرفت حالات الإحتيال الإلكتروني في المجتمعات العربية إرتفاعا كبيرا ويواصل المُحتالون إستغلال الطمع والجشع والجهل ونقص الخبرة لدى الضحايا وإبتكار أساليب إحتيالية متنوعة ومختلفة يوما بعد يوم.

وقد إستهدفت عمليات الإحتيال الإلكتروني جميع الأعمار والمستويات وفي جميع الدول والمجتمعات تقريبا وإستغل المُحتالون التكنولوجيا الحديثة والمنتجات والخدمات المستجدة في إنشاء سيناريوهات لقصص وهمية يمكن تصديقها، وحسب الأبحاث والدراسات والإحصائيات في الدول والمجتمعات العالمية فإن عدد ضحايا الإحتيال الإلكتروني يزداد كل يوم وأغلبهم من الباحثين عن الثراء السريع والذين سقطوا فرائس سهلة لمُحتالين يمتلكون وسائل في الفضاء الإلكتروني بحيث يلعب المُحتالون على غرائز الجشع والطمع لدى شريحة واسعة وكبيرة من الناس تبحث عن الأموال والجوائز.

أسباب اختيار الموضوع

الأسباب الذاتية التي دفعتنا للتطرق لموضوع مكافحة مظاهر الإحتيال الإلكتروني هو الرغبة في الإطلاع على المواضيع الحديثة والمستجدة ورفع الرصيد المعرفي والثقافي حول المسائل المتعلقة بالجرائم المستحدثة والمتعلقة بالجرائم السيبرانية والمعلوماتية.

أما الأسباب الموضوعية التي دفعتنا لاختيار الموضوع محل المعالجة هو أن قضية الإحتيال الإلكتروني من القضايا والمسائل المتعلقة بأحداث الساعة، فالمُحتال لم يعد يعتمد على إستعمال الأساليب التقليدية والكلاسيكية في الإطاحة بالضحايا، ومع التطور التكنولوجي أصبح المُختال يستعمل أساليب إحتيالية تتماشى مع الواقع وما فرضه من تطور في المجال المعلوماتي، إضافة إلى أن جرائم الإحتيال الإلكتروني تمس أمن وإستقرار المجتمعات خاصة وأنها تزعزع الثقة بين المواطن ومسؤوليهم ومدى قدرتهم على حمايته وحماية ممتلكاته، وأصبح المُحتالون يرتكبون جرائمهم ويصطادون الضحايا بكل سهولة ويفرون من العقاب ومن المحاسبة والمتابعة الجزائية وعدم قدرة الأجهزة الأمنية والقضائية على القبض عليهم وتقديمهم للعدالة من أجل محاكمتهم، وعليه يجب تطوير السياسة الجنائية العربية لتتلاءم مع الأساليب الإحتيالية للمُحتالين.

أهمية الدراسة

تكمن أهمية هذا الموضوع محل المعالجة و الدراسة في كونه من المواضيع التي لها تأثير فعال وكبير على جميع دول العالم فهي مرتبطة بالسياسة الجنائية للمجتمعات والتي بدورها لها تأثير على السياسة العامة للدولة والتي من أبرز أهدافها توفير الأمن والاستقرار لشعوبها، وكذلك فإن جرائم الإحتيال الإلكتروني من الجرائم الواقعة على الأموال والتي تمس المجتمع في مشاريعه التنموية والمالية وتصبح الدولة في محل شك في مدى مصداقية وجدية الإستراتيجية الإقتصادية والتنموية للحكومة فهو يهدد الأوضاع الإقتصادية خاصة في حالة قيام المُحتالين بتهريب الأموال المتأتية من جرائم الإحتيال الإلكتروني إلى الخارج.

أهداف الموضوع

من بين الأهداف التي نسعى للوصول إليها من وراء التطرق لهذا الموضوع:

- معرفة الإطار المفاهيمي لجريمة الإحتيال الإلكتروني.
- معرفة أبرز جرائم الإحتيال الإلكتروني التي يرتكبها المُحتال المعلوماتي.
- الوصول إلى الأساليب التي يستعملها المُحتال المعلوماتي في سرقة ونهب أموال الضحايا.
- إبراز أوجه التشابه والإختلاف بين جريمة الإحتيال الإلكتروني والجرائم المرتبطة والمشابهة لها.
- المساهمة في تبيان أخطر جرائم الإحتيال الإلكتروني من أجل إيجاد الحلول التي يمكن من خلالها التصدي لجرائم الإحتيال الإلكتروني أو على الأقل التقليل منها.
- كما نأمل أن تساهم دراستنا في دعم الأبحاث والدراسات السابقة أو تكون انطلاقة وبداية لأبحاث ودراسات جديدة للمستقبل.

المنهج المعتمد في الدراسة

إعتمدنا في دراستنا على المنهج الوصفي والتحليلي وذلك من خلال تحليل الإطار المفاهيمي لظاهرة الإحتيال الإلكتروني، وشرح التعريف الإصطلاحي والقانوني للإحتيال الإلكتروني، وتفسير خصائص الإحتيال الإلكتروني، وإبراز الفوارق بين الإحتيال الإلكتروني والجرائم المشابهة له، إضافة إلى ووصف أبرز مظاهر الإحتيال الإلكتروني، وذلك من خلال تحليل أشكال الإحتيال الإلكتروني التي يرتكبها المحتال المعلوماتي، والتطرق للإحتيال الإلكتروني بواسطة بطاقة الإئتمان الممغنطة، ثم إلى الإحتيال في مجال التجارة الإلكترونية، إضافة إلى مظاهر الإحتيال الإلكتروني التي يستعملها المُختال المعلوماتي عبر الأنترنيت من خلال الرسائل النصية القصيرة ومن خلال إنشاء مواقع إحتيالية تقوم بجمع التبرعات الخيرية وسرقتها.

الإشكالية

الإشكالية الرئيسية التي نسعى للإجابة عليها

- **ما هي أبرز مظاهرالإحتيال الإلكتروني التي يمكن للمُحتال المعلوماتي أن يقوم بإستخدامها في الإستيلاء على ممتلكات الضحايا (المجني عليهم)؟**

أما الأسئلة الفرعية التي طرحناها للموضوع فتتمثل فيما يلي:

- ما هي الوسائل التي يستعملها المُحتال المعلوماتي في إرتكاب جرائم الإحتيال الإلكتروني؟
- هل يقوم المُحتال المعلوماتي بإرتكابه جريمته في الفضاء الإلكتروني فقط؟
- ما هي العلاقة بين المُحتال الذي يحتال على ضحاياه في البيئة الإلكترونية والمُحتال الذي ينصب على ضحاياه بواسطة البطاقات الممنغطة؟
- كيف يمكن التمييز بين الإحتيال الإلكتروني والإحتيال التقليدي والكلاسيكي؟
- ما هي حالات الإحتيال التي يرتكبها المُحتال المعلوماتي بواسطة البطاقات الممنغطة؟

تقسيم الدراسة

وللإجابة على هذه الإشكالية الرئيسية والأسئلة الفرعية نقترح خطة دراسة ممنهجة في مبحثين على النحو الآتي:

تطرقنا في المبحث الأول لتحديد مقومات جرائم الإحتيال الإلكتروني، والذي تم تقسيمه إلى ثلاثة مطالب، خصصنا المطلب الأول لتعريف جريمة الإحتيال الإلكتروني، والمطلب الثاني لخصائص جريمة الإحتيال الإلكتروني، والمطلب الثالث لتمييز جرائم الإحتيال الإلكتروني عن الجرائم المشابهة لها.

وتطرقنا في المبحث الثاني لأشكال جرائم الإحتيال الإلكتروني التي يستخدمها المُحتال المعلوماتي، والذي تم تقسيمه إلى ثلاثة مطالب، خصصنا المطلب الأول للإحتيال الإلكتروني بواسطة بطاقة الإئتمان الممنغطة، والمطلب الثاني للإحتيال في مجال التجارة الإلكترونية، والمطلب الثالث لصور الإحتيال عبر الأنترنيت.

المبحث الأول

تحديد مقومات جرائم الإحتيال الإلكتروني

الإحتيال الإلكتروني أو الإحتيال بواسطة جهاز الكمبيوتر أو الهاتف الذكي أو عليهما أصبحت من الظواهر المنتشرة في أغلب الدول وهي من أبرز الجرائم الحديثة والمستجدة التي ترتكب في مجال تكنولوجيا المعلومات ويتحقق هذا النوع من الجرائم كلما كانت هناك رغبة للمُحتال في تحقيق ربح مادي غير مشروع تقابلها خسارة مادية تلحق بالمجني عليه، وقد أصبح لجهاز الحاسب الآلي دور بارز في أنشطة البنوك والمؤسسات المالية بسبب ظهور عمليات التحويل الإلكتروني للأموال وإستخدام بطاقات الإئتمان الممغنطة وأجهزة الصرف الآلي وبالتالي أصبح مجالا خصبا لجريمة الإحتيال الإلكتروني لأن المعلومات المرتبطة بالأمور الإقتصادية والمالية أصبحت مخزنة في أجهزة الحاسب الآلي والوصول إليها سهلا.

وقد عرف الإحتيال الإلكتروني إنتشارا واسعا في دول العالم وزاد حجمها مع التطور العلمي والتكنولوجي السريع وزيادة الإهتمام بهذا النوع الجديد من الاحتيال وعليه سنتطرق إلى الإطار المفاهيمي للإحتيال الإلكتروني من خلال تعريف الإحتيال الإلكتروني، ثم إبراز مميزاته الخاصة، ثم التطرق للجرائم المشابهة لجرائم الإحتيال الإلكتروني أو المرتبطة به.

المطلب الأول

تعريف الإحتيال الإلكتروني

الإحتيال الإلكتروني هو مجموعة من الأفعال الغير قانونية والمتعمدة يرتكبها المُحتال بهدف الخداع أو التحريف أو الغش أو التدليس من أجل الحصول على شيء ذو قيمة مادية، وترتكب بواسطة أجهزة الهاتف الذكية أو عن طريق أجهزة الحاسب الآلي أو عليه، ولمعرفة أبرز التعاريف التي تناولت تحديد معنى الإحتيال الإلكتروني سنتطرق إلى التعريف الإصطلاحي للإحتيال الإلكتروني، ثم إلى التعريف القانوني للإحتيال الإلكتروني.

الفرع الأول

التعريف الإصطلاحي للإحتيال الإلكتروني

ولمحاولة الإحاطة بأبرز تعاريف الإحتيال الإلكتروني نذكر ما يلي:

أولا: هو كل سلوك إحتيالي وخداعي يرتبط بعمليات التحسيب الإلكتروني يهدف إلى كسب فائدة أو مصلحة مادية[1].

ثانيا: هو فعل أو مجموعة من الأفعال غير المشروعة والمتعمدة التي ترتكب بهدف الخداع أو التحريف للحصول على شيء ذو قيمة يكون نظام الحاسب الآلي ضروريا لارتكابها أو إخفائها[1].

---

[1]-محمد أمين الشوابكة، جرائم الحاسوب والأنترنيت، الطبعة الأولى، دار الثقافة، عمان، الأردن 2004. ص 178.

ثالثا: جريمة الاحتيال الإلكتروني تتحقق عندما تتجه نية الجاني إلى تحقيق ربح مادي غير مشروع ويلحق خسارة مادية بالمجني عليه، ويشترط أن يكون الحاسب الآلي هو وسيلة إرتكاب أو تسهيل أو تعجيل تنفيذ جريمة الاحتيال[2].

رابعا: جريمة الاحتيال الإلكتروني يشترط لقيامها عنصران، الأول حصول ربح غير مشروع والثاني إلحاق خسارة مادية بالمجني عليه ويشترط أن تتم هذه العملية من خلال الحاسب الآلي[3].

خامسا: الاحتيال في مجال التجارة الإلكترونية هو كل سلوك خداعي مرتبط بالكمبيوتر يهدف بواسطته الشخص إلى الحصول على فائدة أو مصلحة مادية، ومن أشكاله المنتشرة له استغلال مواقع الانترنيت للاحتيال على الغير عبر مشاريع وهمية أو من خلال الوصول إلى أرقام بطاقات ائتمان العملاء واستغلالها في عمليات شراء أو دفع غير مشروعة وأنشطة التلاعب بالأسهم المالية وإدارة المحافظ الإلكترونية ومزادات البضائع على الانترنيت وغيرها[4] .

سادسا: الاحتيال المعلوماتي هو التلاعب العمدي بمعلومات وبيانات تمثل قيمة مادية يختزنها نظام الحاسب الآلي، أو إدخال غير مصرح به لمعلومات وبيانات صحيحة أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة أو أية وسيلة أخرى من شأنها التأثير على الحاسب الآلي حتى يقوم بعملياته بناءا على هذه البيانات أو الإحتيال المعلوماتي[5] .

نلاحظ من خلال هذه التعاريف المتنوعة والمختلفة أن الإحتيال الإلكتروني هو ذلك السلوك والتصرف والفعل الذي يهدف من خلاله المُحتال المعلوماتي إلى الحصول على كسب مالي أو مادي، أو الإستفادة من خدمة أو منفعة أو فائدة مهما كانت قيمتها، وإلحاق ضرر وخسارة بالضحية (المجني عليه)، ويتمثل هذا السلوك أو التصرف أو الفعل في إستعمال أساليب إحتيالية منحرفة عن الإعتقاد السائد الذي كان يظنه المجني عليه، وتكون الوسائل المستعملة في هذه الأساليب الإحتيالية إما الحاسب الآلي أو الهاتف الذكي أو البطاقات الممغنطة.

وعليه يمكننا القول بأن الحاسب الآلي والهاتف الذكي والبطاقات الممغنطة من أخطر الوسائل التي يستعملها المُحتال المعلوماتي في النصب وسرقة ممتلكات الغير، وذلك نظرا لسهولة إرتكابها من طرف المُحتال وصعوبة إكتشافها من طرف الضحايا (المجني عليهم)، وإستغلال المُحتال للأشخاص الذين يرغبون في الربح السريع والثراء الفاحش وكسب المال الكثير مهما كان مصدره، وإيهامهم بمشاريع خيالية ووهمية تمكنهم من تحقيق الأرباح دون وجود الخسارة في هذه المشاريع الوهمية.

---

[1] محمد محمد شتا، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، مصر، الإسكندرية (2001). ص 7 .

[2]- عمر محمد أبو بكر يونس، الجرائم الناشئة عن إستخدام الأنترنيت، أطروحة دكتوراه مقدمة إلى كلية الحقوق، جامعة عين الشمس، دار النهضة العربية، القاهرة، 2004، ص 995

[3]. تيسير أحمد حسين الزعبي، جريمة الإحتيال الإلكتروني، دراسة مقدمة إستكمالات لمتطلبات الحصول على درجة الماجستير في القانون العام، كلية الدراسات القانونية، قسم القانون، جامعة جدارا، السنة الجامعية، 2010/2009. ص 94.

[4]. حطاب كمال، الحماية الجزائية للتجارة الإلكترونية، أطروحة دكتوراه في العلوم، تخصص علوم قانونية، فرع علوم جنائية، كلية الحقوق والعلوم]السياسية، جامعة الجيلالي إلياس، سيدي بلعباس، الجزائر ، 2016/2015، ص 143

[5] معتوق عبد اللطيف، الإطار القانوني لمكافحة الجرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة لنيل شهادة الماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر ، السنة الجامعية، 2012/2011. ص 42

الفرع الثاني

التعريف القانوني للإحتيال الإلكتروني

نص المشرع الجزائري على أنه يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 10.000.000 دج كل من بقوم عمدا وعن طريق الغش بما يأتي:

أولا: تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

ثانيا: حيازة أو إفشاء أو نشر أو إستعمال لأي عرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم[1].

يظهر أن المشرع الجزائري عرف الإحتيال الإلكتروني بأنه ذلك السلوك الإجرامي الذي يرتكبه المُحتال المعلوماتي متعمدا مستخدما طرقا وأساليب إحتيالية عن طريق الغش، ويتمثل الإحتيال الإلكتروني حسب قانون العقوبات الجزائري في حالتين:

* الحالة الأولى، عندما يقوم المُحتال المعلوماتي بستة (6) تصرفات وأفعال وتتمثل هذه الأفعال في (التصميم، البحث، التجميع، التوفير، النشر، الإتجار)، وترتكب جميع هذه الأفعال بواسطة الكمبيوتر أو الهاتف الذكي أو البطاقات الممنغطة من خلال سرقة بياناتها ومعلوماتها أو تزويرها، وقد إشترط المشرع الجزائري أن تكون هذه الأفعال من الجرائم المنصوص عليها في هذا القسم، ويقصد المشرع بمعنى هذا القسم جميع الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات.

* أما الحالة الثانية، فتتمثل في قيام المُحتال المعلوماتي بأربعة (4) سلوكيات وأفعال وتتمثل هذه الأفعال في (الحيازة، الإفشاء، النشر، الإستعمال)، وترتكب هذه الأفعال بواسطة الكمبيوتر أو الهاتف الذكي أو البطاقات الممنغطة، أي بمعنى أن يقوم المُحتال المعلوماتي بالحصول على المعلومات لغرض الإمتلاك والإكتساب أو لغرض التهديد والإبتزاز من أجل الحصول على الأموال أو لغرض التشهير وفضح الأشخاص أو إستعمالها لأية أغراض أخرى، وقد إشترط المشرع الجزائري أن تتعلق هذه الأفعال بالجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات.

[1] المادة 394 مكرر 02 من القانون رقم 06/24 المؤرخ في 19 شوال عام 1445 هـ، الموافق 28 أفريل سنة 2024 م، يعدل ويتمم الأمر رقم 156/66 المؤرخ في 08 يونيو سنة 1966 م، المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 30، الصادر بتاريخ: 21 شوال عام 1445 هـ، الموافق 30 أفريل سنة 2024 م.

المطلب الثاني

خصائص جريمة الإحتيال الإلكتروني

يتميز الإحتيال الإلكتروني بمجموعة من الصفات التي تختلف إختلافا جذريا عن الإحتيال العادي والكلاسيكي من بينها أنها جريمة ترتكب في بيئة إفتراضية عن طريق نبضات إلكترونية غير مرئية في بيئة الحاسب الآلي، إضافة إلى أنها من الجرائم العابرة للحدود الإقليمية فيمكن أن يكون المُحتال الإلكتروني في بلد والمجني عليه(الضحية) في بلد آخر، كذلك فالإحتيال الإلكتروني يتميز بطابع ذهني على خلاف الجرائم التي تعتمد على الجهد العضلي فهي جريمة تعتمد على ذكاء المُحتال. وتتمثل أهم هذه الخصائص فيما يلي؛

الفرع الأول

جريمة الإحتيال الإلكتروني تقع في البيئة الإلكترونية

جريمة الإحتيال الإلكتروني تقع في بيئة إلكترونية أي بمعنى أنها تتم في بيئة الحاسوب والأنترنيت عن طريق نبضات إلكترونية غير مرئية تنتقل بين أجهزة الحواسيب عبر النظم المعلوماتية ويعتمد على جوانب الإخفاق والقصور في الشبكات ونظم التحكم بتكنولوجيا المعلومات[1].

أي بمعنى أن المحل والمكان الذي ترتكب فيه جرائم الإحتيال الإلكتروني هو محل ومكان إفتراضي يختلف إختلافا جذريا عن الإحتيال الذي يقع في البيئة التقليدية والكلاسيكية، فمثلا المُحتال في البيئة التقليدية قد يستعمل أسماء أو صفات كاذبة أو يستعين بشخص آخر متواطئ معه يدعم أقواله ويؤيد إدعاءاته الكاذبة، وكذلك من خلال إستعماله لوثائق وأوراق مزورة مثل (العقود، الشهادات، التصاريح، البطاقات...) وغيرها من الأوراق والوثائق المزورة، وعلى خلاف المُحتال المعلوماتي الذي يرتكب جريمته في بيئة إفتراضية يكون مصدرها الحاسب الآلي أو الهاتف الذكي أو البطاقات الممنغطة (بطاقة هوية، رخصة سياقة، بطاقة دفع...)

الفرع الثاني

جريمة الإحتيال الإلكتروني من الجرائم العابرة للحدود الوطنية

ويقصد بها أنها تشكل صورة من صور الجرائم العابرة للحدود الإقليمية بين دول العالم مع وجود الحاسوب فهي مرتبطة بالشبكة العنكبوتية دون الخضوع لحدود الزمان والمكان، ولذلك كان من السهولة إرتكاب الإحتيال مع القدرة على كشفه وهذه الصفة أنشأت فيها الكثير من المشاكل حول تحديد الدولة التي تكون صاحبة الإختصاص القضائي في حالة ما إذا كان المُحتال من دولة والضحية من دولة أخرى، إضافة إلى إشكالية القانون الواجب التطبيق وأساليب

[1]. وائل محمد نصيرات، غادة عبد الرحمن الطريف، جريمة الإحتيال عبر شبكة المعلومات الدولية، دراسة مقارنة النظام السعودي والقانون الأردني، مجلة دفاتر السياسة والقانون، عدد جوان، المجلد 10، العدد 19، 2018، جامعة قاصدي مرباح، ورقلة، الجزائر.

وإجراءات الملاحقة القضائية ولهذا لا بد من وجود تعاون دولي قضائي بين الدول أثناء عمليات البحث والتحري والتحقيق وإبرام العديد من المعاهدات والإتفاقيات الدولية في مجال المساعدة القانونية المتبادلة[1].

أي بمعنى أن جرائم الإحتيال الإلكتروني من الجرائم التي ترتكب في نطاق جغرافي شاسع جدا لا حدود له فمثلا المُحتال المعلوماتي قد يرتكبه جريمته وهو مقيم في قارة معينة بينما الضحية (المجني عليه) مقيم في قارة أخرى، فالإحتيال الإلكتروني غير خاضع لزمن معين أو لمكان محدد ولا يعترف بالحدود، وبالتالي فإن الإحتيال الإلكتروني من أخطر الجرائم بعد جرائم الفساد، والذي تتطلب مكافحته جهود دولية معتبرة في مجال التعاون القضائي الدولي والمساعدة القانونية المتبادلة للسيطرة على جرائم الإحتيال الإلكتروني، ولا سيما من خلال التعاون مع منظمة الشرطة الدولية (الإنتيربول)، أو من خلال إبرام الإتفاقيات الدولية الثنائية والإقليمية والجماعية في مجال تسليم المجرمين أو الإنابة القضائية أو تبادل المعلومات، وذلك لتسهيل جميع إجراءات البحث والتحري والتحقيق المتعلقة بجرائم الإحتيال الإلكتروني.

الفرع الثالث

جريمة الإحتيال الإلكتروني جريمة ذات طابع ذهني وتقني

الإحتيال الإلكتروني له طابع عقلي وتفكيري وذهني على عكس الجرائم التي تعتمد على الجهد العضلي أو الجسدي فهي جريمة تعتمد على ذكاء المُحتال ودهائه، إضافة إلى أنها من الجرائم التي تتطلب في غالب الأحيان التخصص والدراية من طرف المُحتال بمجال نشاطه حيث يعتاد المُحتالون على إستخدام أساليب معينة في الاحتيال فيتخصص به لأنه يكون على دراية بضحاياه وكيفية خداعهم والنصب عليهم، ويعتمد إرتكاب الإحتيال الإلكتروني على أسلوب لا يحتاج فيه المُحتال إلى مجهود عضلي مثل جرائم الضرب والجرح والقتل فهي تنفذ بأقل جهد و لا تتطلب نوعا من الإيذاء أو التخريب أو التدمير بل تعتمد فقط على مدى الرصيد الثقافي والمعرفي الذي يتمتع به المُحتال في مجال تقنية المعلومات وشبكة الانترنيت والإحاطة ببعض البرامج التشغيلية وتسمى "الجرائم الناعمة"[2].

أي بمعنى أن جرائم الإحتيال الإلكتروني من الجرائم التي يكون فيها المُحتال المعلوماتي يتمتع بقدرات ذات جودة عالية ورصيد معرفي وثقافي كبير بكل ما يتعلق بالإعلام الآلي والرقمنة وبالمجال المعلوماتي بصفة عامة، إضافة إلى إكتساب المُحتال المعلوماتي مهارات ذهنية وفكرية متطورة تتميز بسرعة الإستيعاب والفهم وإتخاذ القرارات الصحيحة والصائبة وقلة الأخطاء والغلطات، والقدرة على معرفة الأدلة والبراهين والإطلاع عليها والتصرف بها (سرقتها، محوها، نسخها، تغييرها...)، وبالتالي فإن جرائم الإحتيال الإلكتروني ليست من الجرائم التي تتطلب بذل جهد عضلي كبير من أجل إرتكابها بل يكفي لإرتكبها تفكير ذهني من المُحتال المعلوماتي.

---

[1] بولحية شهيرة، سويح دنيا زاد، الإحتيال الإلكتروني، مجلة الدراسات القانونية والإقتصادية، العدد 04،ديسمبر، المركز الجامعي، سي الحواس، بريكة، باتنة، الجزائر، 2019، ص 41.

[2]. بولحية شهيرة، سويح دنيا زاد، المرجع نفسه. ص .41.

الفرع الرابع

جريمة الإحتيال الإلكتروني تقوم على تغيير الحقيقة وعلى حرية الإرادة

الإحتيال الإلكتروني يقوم على تغيير الواقع والحقيقة وذلك كون الفاعل يستخدم وسائل التدليس والخداع والكذب والتضليل لكي يصل إلى هدف محدد وهو إكمال عملية الإحتيال، إضافة إلى أن الإحتيال الإلكتروني يصيب إرادة المجني عليه بعيب الرضا لأنه بدلا من أن يتصرف الضحية (المجني عليه) بإرادته الحرة ويكون على علم وبينة من أمره ووعي بتصرفاته فيغرر به ويضله المُحتال[1].

أي بمعنى أن جرائم الإحتيال الإلكتروني من الجرائم التي يهدف من خلالها المُحتال المعلوماتي إلى تغيير واقعة حقيقية إلى واقعة خيالية ومزيفة غير موجودة على أرض الواقع وهي من تأليف المُحتال، إضافة إلى محاولة المُحتال المعلوماتي طمس وإخفاء الواقعة الأصلية وإستبدالها بواقعة مؤلفة من خياله غير حقيقية، ويستعمل من خلالها المُحتال المعلوماتي أساليب وطرق إحتيالية (التدليس، الكذب، التضليل...)، وتدفع هذه الأساليب الإحتيالية الضحية (المجني عليه) على تصديق الواقعة المزيفة، وعليه فإن الإحتيال الإلكتروني يمس بإرادة الضحية بعيب الرضا، وذلك لأن تصرفه لم يكن وفقا لإرادته الحرة بل تدخلت فيها إرادة المُحتال المعلوماتي وقامت بتوجيهها وفقا لإرادتها.

الفرع الخامس

جريمة الإحتيال الإلكتروني جريمة يصعب إكتشاف أدلتها

الإحتيال الإلكتروني يقع في بيئة إفتراضية لا تخلف أية آثار على مرتكبيها لأن الضحية لا يلاحظها رغم أنها تقع أثناء وجوده على الشبكة وهذا بفضل القدرات الفنية والتقنية التي يتمتع بها المُحتال والتي تمكنه من الجريمة بدقة[2].

المُحتال يلجأ إلى استعمال وسائل عديدة لعرقلة الوصول إلى أدلة الإدانة ومن بين هذه الوسائل تقنيات التشفير والترميز[3]، ويستخدم المُحتالون كذلك مسألة التدابير الامنية لمنع مشكلة التفتيش والإطلاع على الأدلة أو ضبطها عن طريق إخفاء هوياتهم وإستخدام كلمة السر، وخاصة عند استخدامهم لشبكة الانترنيت وذلك بالاستعانة بالبرامج والتطبيقات التي تعمل على طمس هويتهم عبر شبكة الأنترنيت، فالمُحتال الذي يستخدم الوسائل الإلكترونية في احتياله يتميز بالذكاء والإتقان الفني للعمل الذي يقوم به والذي يتميز بالطبيعة الفنية، ولذلك فإنه يتمكن من إخفاء الأفعال

---

[1] أسامة حمدان الرقب، جرائم النصب والإحتيال، الطبعة الأولى، دار يافا العلمية للنشر والتوزيع، عمان، الأردن 2012. ص ص، 24،26.

[2] . عبد المومن بن الصغير، الطبيعة الخاصة للجريمة المرتكبة عبر الأنترنيت في التشريع الجزائري والتشريع المقارن، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، 2015، ص 350 .

[3] حجازي عبد الفتاح، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنيت، دار الكتب القانونية، القاهرة، مصر ، 2007. ص 89.

غير المشروعة التي يقوم بها أثناء تشغيله لهذه الوسائل الإلكترونية ويستخدم في ذلك التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي تتم عن طريقها تسجيل البيانات[1].

أي بمعنى أن أدلة جرائم الإحتيال الإلكتروني تختلف إختلافا جذريا عن أدلة الإحتيال التقليدي والكلاسيكي، فأدلة جرائم الإحتيال الإلكتروني بصفة خاصة وأدلة الجرائم السبيرانية بصفة عامة يصعب إكتشافها وإستخلاصها والحصول عليها، وذلك لأنها تقع في بيئة إفتراضية لا يمكن السيطرة عليها أو محاصرتها أو تطويقها لأنها أدلة معلوماتية تتكون من برامج وتطبيقات وملفات ووثائق ومستندات تقع داخل الحاسب الآلي أو الهاتف الذكي أو البطاقات الممنغطة، وذلك على عكس أدلة الإحتيال التقليدي والكلاسيكي التي يسهل إستخلاصها والحصول عليها ومعرفتها لأنها عبارة عن أدلة مادية ملموسة مثل بطاقات الهوية المزورة أو شهادات الأشخاص أو من خلال إعتراف الأشخاص المشاركين في جرائم الإحتيال التقليدية والكلاسيكية، أو عبارة عن أسلحة أو دماء أو أية آثار مادية أخرى مثل الأسنان أو الشعر وغيرها من الأدلة التقليدية الملموسة..

المطلب الثالث

تمييز جريمة الإحتيال الإلكتروني عن الجرائم المشابهة لها

من بين الجرائم المشابهة لجريمة الإحتيال الإلكتروني جريمة السرقة وجريمة خيانة الأمانة وجريمة التزوير الإلكتروني، ويمكننا إبراز أوجه التشابه والاختلاف بين مختلف هذه الجرائم في النقاط التالية:

الفرع الأول

تمييز جريمة الإحتيال الإلكتروني عن جريمة السرقة

جريمة السرقة تهدف إلى الاستيلاء على ملكية الغير للأشياء المنقولة وحرمان أصحابها وملاكها الشرعيين والأصليين من حق التملك بها، وجريمة السرقة تطال الحيازة دون أن تؤدي إلى إخراج موضوعها من حيازة صاحبها، وعلى خلاف الإحتيال الإلكتروني فهو يتمثل في القيم المادية المتعلقة بالأموال النقدية والسلع والبضائع وذلك عن طريق التلاعب في المعلومات المتعلقة بمثل هذه الأشياء التقليدية قليلة بالمقارنة القيم المادية[2].

يتضح أن جريمة الإحتيال الإلكتروني تتشابه مع جريمة السرقة في أن كلاهما يتمثل في الإعتداء على ملكية الغير والإستلاء عليها وإنتقال ملكيتها من أصحابها الحقيقيين والشرعيين إلى المُحتالين والسُراق، إضافة إلى أن كلاهما من الجنايات والجنح التي ترتكب ضد الأموال، وكلاهما يتمثل في الإختلاس بنقل الشيء ونزعه من حيازة الضحية (المجني عليه) إلى حيازة المُحتال أو السارق، وكلاهما يتم دون الإرادة الحرة للمجني عليه.

---

[1]. عماد بلغيث، جغلولي يوسف: ، صعوبات التحقيق في الجرائم الإلكترونية، مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد 06، العدد 03 سبتمبر، 2021.ص 79.

[2] نايلة عادل محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان ، 2005. ص 421

وتختلف جريمة الإحتيال الإلكتروني عن جريمة السرقة في كون الإحتيال الإلكتروني يقع في بيئة إفتراضية أما السرقة في البيئة التقليدية والكلاسيكية، إضافة إلى أن جريمة الإحتيال الإلكتروني يكون بإستعمال أساليب وطرق إحتيالية (التدليس، الكذب، الخداع...)، أما جريمة السرقة فتقع عن طريق العنف والتهديد والإكراه والضغط، إضافة إلى أن جريمة الإحتيال الإلكتروني تكون ببذل جهد ذهني وفكري أما جريمة السرقة فتكون ببذل جهد عضلي.

الفرع الثاني

تمييز جريمة الإحتيال الإلكتروني عن جريمة خيانة الأمانة

تتشابه جريمة الإحتيال الإلكتروني مع جريمة خيانة الأمانة في تسليم الجاني للمال برضى المجني عليه، أما فيما يتعلق بأوجه الاختلاف فيمكن إبرازها في النقاط التالية:

1–التسليم في الإحتيال الإلكتروني يقوم على إرادة المجني عليه (الضحية) المشوب بعيب الغلط، أما التسليم في خيانة الأمانة يقوم على نقل الحيازة الناقصة للشيء إلى الجاني (المُحتال).

2–التسليم في الإحتيال الإلكتروني يمثل عنصر الاستيلاء على المال على عكس خيانة الأمانة فإن التسليم يكون سابقا على الإستيلاء ولا يتحقق إلا بفعل لاحق للتسليم.

3–في خيانة الأمانة يتم التسليم بناءا على عقد من عقود الأمانة التي يجعل (المُحتال) يظهر الشيء بمظهر المالك وتجعل الحيازة تامة ثم يقوم بتبديد الشيء أو اختلاسه[1].

نلاحظ أن جريمة الإحتيال الإلكتروني تتشابه مع جريمة خيانة الأمانة في كون أن كلاهما يتمثل في إختلاس الشيء ونقله ونزعه من حيازة الضحية (المجني عليه) إلى حيازة المُحتال أو خائن الأمانة، وكلاهما يتم دون إرادة المجني عليه وبالتأثير عليها، إضافة إلى أن كلاهما من الجنايات والجنح التي ترتكب ضد الأموال.

وتختلف جريمة الإحتيال الإلكتروني عن جريمة خيانة الأمانة في كون الأولى تتم في بيئة إفتراضية أما الثانية فتتم في بيئة تقليدية وكلاسيكية، إضافة إلى أن جريمة الإحتيال الإلكتروني لا يشترط فيها نوع أو مصدر الشيء المختلس، أما جريمة خيانة الأمانة فقد إشترط المشرع الجزائري في قانون العقوبات أن تتعلق بنوع معين من العقود ذكرها على سبيل الحصر، وتتمثل هذه العقود في (عقد الإيجار، وعقد الوديعة، وعقد الوكالة، الرهن الحيازي، وعقد عارية الإستعمال، وعقد العمل بأجر أو بدون أجر).

[1] الشحات إبراهيم محمد منصور الجرائم الإلكترونية في الشريعة والقوانين الوضعية، بحث فقهي مقارن، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2011. ص 61.

الفرع الثالث

تمييز جريمة الإحتيال الإلكتروني عن جريمة التزوير الإلكتروني

يقصد بالاحتيال الإلكتروني إساءة استخدام الحاسب الآلي والتلاعب بأنظمة المعالجة الإلكترونية للمعلومات والبيانات للحصول بغير حق على أموال أو خدمات.

أما التزوير الإلكتروني فهو كل تغيير للحقيقة يقترن بقصد الغش يقع في محرر بإحدى الطرق التي تصف عليها القانون ويكون من شأنه أن يسبب ضررا للغير[1].

الإحتيال الإلكتروني و التزوير الإلكتروني هي أمور غير حقيقية ووهمية في صورة أمور حقيقية وصادقة، أي بمعنى أن كلاهما يقوم على الكذب.

ولا يكفي الكذب وحده لقيام الإحتيال الإلكتروني أما التزوير الإلكتروني يكفي الكذب وحده لقيامه ولذلك فإن التزوير الإلكتروني يجب أن يقع على محرر، أما الإحتيال الإلكتروني فهو غير محدد ويشمل عدة طرق وأساليب، وكذلك يعتبر التزوير الإلكتروني من جرائم الغش المعلوماتي وهذا المفهوم للتزوير عام يشمل جميع أنواع الغش بما في ذلك الاحتيال[2].

يظهر أن جريمة الإحتيال الإلكتروني تتشابه مع جريمة التزوير الإلكتروني في كون أن كلاهما يتم في بيئة إفتراضية، وكلاهما يعتمد على إستعمال طرق وأساليب إحتيالية مبنية على التزييف والتزوير وعلى التضليل والغش والخداع، وكلاهما يتم فيهما التفتيش والمعاينة وجميع إجراءات البحث والتحري والتحقيق على الحاسب الآلي أو الهاتف الذكي، إضافة إلى أن كلاهما أدلتهم يصعب إستخلاصها وإكتشافها، وتتمثل هذه الأدلة في برامج ومعطيات ومعلومات يتم إستخلاصها من الكمبيوتر أو الهاتف الذكي، وكلاهما يؤثر على إرادة الضحية (المجني عليه) بتوجيهها.

وتختلف جريمة الإحتيال الإلكتروني عن جريمة التزوير الإلكتروني في كون جرائم الإحتيال الإلكتروني أوسع من جرائم التزوير الإلكتروني، وجرائم الإحتيال الإلكتروني تستعمل فيها إضافة إلى الطرق والأساليب الإحتيالية أساليب أخرى مثل التهديد أو التشهير أو الإبتزاز وغيرها من صور ومظاهر وأشكال الجرائم الإلكترونية، أما جرائم التزوير الإلكتروني فيقتصر إرتكابها فقط على الوثائق والأوراق والمحررات وتغيير وإستبدال المعلومات والبيانات، إضافة إلى أن جرائم التزوير الإلكتروني هي جزء من جرائم الإحتيال الإلكتروني.

---

[1] . محمد عبد الله أبو بكر ، موسوعة جرائم المعلوماتية، جرائم الكمبيوتر والأنترنيت، د ط المكتب العربي الحديث، الإسكندرية، 2011. ص 170.

[2] أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية ، 2006. ص 323.

المبحث الثاني

أشكال جرائم الإحتيال الإلكتروني التي يستخدمها المُحتال المعلوماتي

إنتشرت صور وأشكال عديدة ومتنوعة للنصب والإحتيال الإلكتروني في الفترة الأخيرة ومن أبرز هذه الصور والمظاهر الإحتيالية ،الإحتيال الإلكتروني الذي يقع بواسطة بطاقة الإئتمان الممغنطة والإحتيال الذي يقع في مجال التجارة الإلكترونية وهذان الصورتان من أكثر المظاهر إنتشارا وشيوعا، إضافة إلى أشكال الإحتيال الإلكتروني التي يستعملها المُختال المعلوماتي عبر الأنترنيت، وذلك من خلال الرسائل النصية القصيرة، ومن خلال الإحتيال الذي يكون عن طريق إنشاء مواقع إحتيالية تقوم بالإستيلاء وسرقة التبرعات الخيرية.

المطلب الأول

الإحتيال الإلكتروني بواسطة بطاقة الإئتمان الممغنطة

للحاسب الآلي دور كبير في أنشطة البنوك والمؤسسات المالية وبروز بطاقة الإئتمان الممغنطة كبديل عن النقود في التعاملات التجارية، وأصبحت هذه البطاقات مألوفة لدى الناس غير أن إستخدامها أثار الكثير من المشاكل من الناحية القانونية في نطاق القانون الجزائي فزاد حجم التعامل بها مما أدى إلى زيادة حجم الجرائم المتعلقة بها، ويتمثل هذا النوع من الإحتيال في الاستخدام غير المشروع لبطاقات الإئتمان الممغنطة سواء كانت مسروقة أو مفقودة أو مزورة بالإستيلاء على أموال أصحاب الحساب الشرعية لها وإستخدامها لأنفسهم أو الحصول على أرقامها السرية عند إستعمالها عبر الانترنيت، ويتمثل الإستخدام غير المشروع لبطاقات الإئتمان الممغنطة في صورتين:

الفرع الأول

إستخدام بطاقات الإئتمان الممغنطة من قبل حاملها الشرعي

لكل بطاقة خدمة خاصة تقدمها لحاملها الشرعي فعليه أن يحسن إستخدامها ومن بين الحالات التي يسيء الحامل الشرعي إستخدام بطاقة الإئتمان الممغنطة نذكر ما يلي:

أولا: في حالة قيام حامل البطاقة بسحب النقود بواسطتها من جهاز توزيع النقود وهو يعلم بعدم كفاية رصيده لدى البنك المانح، وخاصة عندما يتم سحب النقود من أجهزة لا ترتبط مباشرة بحساب العميل في البنك[1]، وهذا يعتبر إخلالا بالالتزامات التعاقدية إتجاه الجهة المانحة للبطاقة تعرضه للمساءلة المدنية[2].

[1] عمر السالم، الحماية الجنائية لبطاقة الوفاء، دراسة مقارنة، جمهورية مصر العربية، القاهرة ، 1994. ص 45.

[2] جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الإئتمان الممغنطة، دراسة تطبيقية في القضاء الفرنسي والمصري، جمهورية مصر العربية، القاهرة، 1999. ص 40.

ثانيا: في حالة قيام حامل البطاقة كأداء وفاء متجاوزا الحد المسموح له في شبكة البطاقات البنكية من أجل الوفاء بقيمة مشترياته، فبعض البطاقات تُخول لحاملها الحصول على السلع والخدمات من الجهات المقبولة من البنك المانح لها دون دفع ثمنها نقدا أو بشيك وإنما بمجرد تقديمها، وهذه البطاقات تمنح حاملها إتخاذ الإجراءات اللازمة لخصم المبلغ الذي يحدده لمصلحة شخص آخر من حسابه لدى البنك المانح للبطاقة[1].

ثالثا: في حالة قيام حامل البطاقة بإستخدامها كأداة ضمانة لشيكاته متجاوزا بذلك الحد المصرح له به من طرف البنك فبعض بطاقات الإئتمان تسمح لحاملها شراء السلع أو الحصول على خدمات بموجب شيكات تضمنها هذه البطاقات بحد أقصى يحدده البنك المانح لها، وهذا النوع وسيلة لضمان حصول التاجر أو مقدم الخدمة على المقابل الذي تمت تسويته عن طريق الشيك، ويقوم التاجر أو مقدم الخدمة بتدوين البيانات الرئيسية على ظهر الشيك بعد التأكد من تاريخ صلاحيتها، وأن الشيك والبطاقة يحملان نفس التوقيع ونفس الحساب ونفس إسم البنك[2].

رابعا: في حالة الإستخدام المقنع لبطاقة الإئتمان وذلك بقيام حاملها الشرعي بإبلاغ البنك المانح لها عن فقدانها أو سرقتها في حين أن البطاقة لا تزال عمليا في حيازته ويقوم باستعمالها، وفي هذه الحالة يفترض أن يكون حاملها قد فقد صفته الشرعية لها وللبنك الحق بإعتبار كل تصرف يتم بواسطتها بعد ذلك يعد تصرفا غير شرعي[3].

نلاحظ أن هناك حالات كثيرة ومتعددة لعمليات الإحتيال الإلكتروني التي ترتكب بواسطة بطاقات الإئتمان، والتي يكون المُحتال المعلوماتي فيها هو صاحبها وحاملها الشرعي، حيث يقوم المُختال المعلوماتي بسحب نقود من صراف آلي أو جهاز توزيع النقود وهو يعلم بعدم وجود أي رصيد في حسابه البنكي، أو أن رصيده الموجود في البنك أقل من الرصيد الذي أراد المُحتال سحبه من البنك.

إضافة إلى قيام المُحتال المعلوماتي (صاحب البطاقة) بإستعمال البطاقة وتقديمها للحصول على سلع وخدمات ومشتريات تفوق قيمتها القيمة المسموح بها من طرف البنك المانح.

وكذلك من بين أساليب الإحتيال قيام المُحتال المعلوماتي بإستخدام بطاقة الإئتمان كوسيلة ضمان لشيكاته في شراء السلع والمشتريات والحصول على الخدمات غير أنه يتجاوز بذلك الحد المصرح به من طرف البنك.

إضافة إلى ذلك من بين الأساليب الإحتيالية التي ترتكب بواسطة بطاقة الإئتمان قيام المُحتال المعلوماتي بالكذب على البنك والتصريح بضياع البطاقة أو سرقتها بينما البطاقة لا زالت بحوزة المُحتال ولا زال يستعملها.

---

[1] حجازي عبد الفتاح بيومي: :مكافحة جرائم الكمبيوتر والانترنيت في القانون العربي النموذجي، جمهورية مصر العربية، القاهرة، 2007،ص. 560 ،..

[2] مفلح القضاة، مسؤولية البنوك الناتجة عن إستخدام الكمبيوتر كوسيلة وفاء، بحث مقدم إلى مؤتمر القانون والكمبيوتر المنعقد في كلية الشريعة]والقانون، جامعة الإمارات العربية، 2002. ص 05.

[3] تيسير أحمد حسين الزعبي، المرجع السابق، ص 122.

الفرع الثاني

الإستخدام غير المشروع لبطاقات الإئتمان الممغنطة من قبل الغير

ويتم الإستخدام غير المشروع لبطاقات الإئتمان الممغنطة من قبل الغير في حالتين، في حالة قيام الحائز غير الشرعي بإستخدام بطاقات مسروقة أو مفقودة، وفي حالة قيام الحائز غير الشرعي بإستخدام بطاقة مزورة، وتتمثل تفاصيل هاتين الحالتين فيما يلي:

أولا: في حال قيام الحائز غير الشرعي بإستخدام بطاقات إئتمان مسروقة أو مفقودة

في حالة إستخدامها في سحب النقود قد تستخدم البطاقة المسروقة أو المفقودة في سحب النقود من أجهزة الحاسب الآلي أو في الوفاء بقيمة المشتريات أو الخدمات التي حصل عليها مستخدمها غير الشرعي من التجار، وهذا يتطلب من حاملها غير الشرعي معرفته للرقم السري الخاص بالبطاقة وعندها يمكن القول بأن إستخدام البطاقة بمثل هذه الحالة يشكل جريمة إحتيال لأن تسليم النقود بواسطة هذه الأجهزة يكون إراديا لأن التسليم يتم بعد إدخال البطاقة في الجهاز وتدوين الرقم السري على لوحة المفاتيح[1].

أما في حالة إستخدام البطاقة كأداة وفاء لثمن السلع التي حصل عليها من التاجر فإنه يتم إستخدام البطاقة كأداة وفاء لدى التجار الذين يستخدمون الآلة اليدوية دون الحاجة للرقم السري الخاص بالبطاقة حيث أنه يكتفي بتوقيع حاملها على فاتورة البيع لإنجاز المعاملة، كما يصعب من الناحية العملية على التاجر التحقق من مطابقة التوقيع المدون على فاتورة البيع مع التوقيع الموجود على البطاقة لعدم خبرة التاجر من جهة ولإتقان المُحتال تقليد التوقيع. من جهة أخرى، وبمجرد تقديم البطاقة للتاجر من أجل الوفاء بواسطتها بثمن السلع أو الخدمات التي حصل عليها مستخدمها الغير شرعي فهذا كاف لقيام جريمة الإحتيال، وذلك بإيهام التاجر بأنه الحامل الشرعي للبطاقة وأنه مالك للرصيد في البنك الذي تمثله البطاقة وإنتحاله إسما كاذبا وهو إسم الحامل الشرعي للبطاقة[2]

ثانيا: في حالة قيام الحائز غير الشرعي بإستخدام بطاقة مزورة

في هذه الحالة فإن تزوير بطاقات الإئتمان عبر شبكة الانترنيت يتم عن طريق إنشاء أرقام بطاقات إئتمان خاصة ببعض العملاء لإستخدامها في الحصول على السلع والخدمات، ويعتبر من الأساليب الإحتيالية التي تقوم عليها جريمة الإحتيال أي أن جريمة الإحتيال في هذه الحالة تقوم باستعمال بطاقة مزورة[3].

يظهر أنه من الأساليب الإحتيالية في هذه الحالة هي التي يكون فيها المُحتال المعلوماتي ممثلا في الغير وليس صاحب بطاقة الإئتمان ومالكها الشرعي، ويستخدم المُحتال المعلوماتي في الحالة أسلوبين من الإحتيال وهما:

---

[1]. جميل عبد الباقي الصغير، المرجع السابق، ص 92..

[2] نائلة عادل محمد فريد قورة، المرجع السابق، ض 541.

[3] محمد الشناوي، جرائم النصب المستحدثة ،دار الكتب القانونية، جمهورية مصر العربية، القاهرة، 2008. ص 130.

ويتمثل الأسلوب الإحتيالي الأول في قيام المُحتال المعلوماتي (الغير) بإستخدام بطاقة الإئتمان المسروقة أو المفقودة، حيث يقوم المُحتال بإستخدام البطاقة المسروقة أو المفقودة إما لسحب النقود من الأجهزة، أو إستخدامها للوفاء بقيمة المشتريات والسلع والخدمات التي تحصل عليها.

ففي الحالة الأولى (سحب النقود) يفترض أن المُحتال المعلوماتي قد تمكن من الحصول على الرقم السري الخاص بالبطاقة، وفي الحالة الثانية (الوفاء بقيمة المشتريات لدى التاجر) لا يشترط حصول المُحتال المعلوماتي على الرقم السري الخاص بالبطاقة، ويكفي توقيع المُحتال على فاتورة البيع لأنه من الصعب على التاجر أن يتحقق من مدى تطابق التوقيعات مع بعضها البعض، ويزداد الأمر صعوبة وتعقيدا إذا كان المُحتال من الذين يجيدون تقليد التوقيعات بمهارة.

ويتمثل الأسلوب الإحتيالي الثاني في قيام المُحتال المعلوماتي بإستعمال بطاقة مزورة، وذلك من خلال قيامه بإنشاء وتكوين ونسخ بطاقة إئتمان تتكون أرقامها ومعلوماتها وبياناتها من نفس الأرقام والمعلومات والبيانات لبعض العملاء، وإستخدامها في الحصول على سلع ومشتريات والحصول على خدمات عبر شبكة الأنترنيت.

المطلب الثاني

الإحتيال في مجال التجارة الإلكترونية

ويتمثل الإحتيال في مجال التجارة الإلكترونية في كل سلوك خداعي مرتبط بالكمبيوتر يهدف الشخص بواسطته إلى الحصول على فائدة أو مصلحة مادية، ومن المظاهر المنتشرة له إستغلال مواقع الأنترنيت للإحتيال على الغير عبر مشاريع وهمية، أو من خلال أنشطة التلاعب بالأسهم المالية وإدارة المحافظ الإلكترونية ومزادات البضائع على الأنترنيت وهذه الأنشطة غير الشرعية تهدد جميع المتعاملين عبر الوسائط الإلكترونية[1].

الفرع الأول

الإيهام بوجود مشروع كاذب

ومن صور الإحتيال في مجال التجارة الإلكترونية الإيهام بوجود مشروع كاذب فنشر المعلومات الكاذبة في الصحف وغيرها من وسائل الإعلام يعتبر من الوسائل الإحتيالية فإذا أُوهم المجني عليه(الضحية) بمشروع كاذب أو بُعث فيه الأمل في تحقيق ربح وهمي، والمشروع الكاذب والوهمي هو الذي ليس له في الحقيقة وجود بل مجرد غطاء للاستيلاء على أموال الغير[2].

يتضح أنه من بين الأساليب الإحتيالية التي يستعملها المُحتال المعلوماتي في مجال التجارة الإلكترونية، قيام المُحتال بإيهام الضحايا (المجني عليه) بوجود مشاريع كاذبة، وذلك من خلال إستعمال صور وفيديوهات أو الإستعانة بأشخاص

---

[1] حطاب كمال، المرجع السابق،. ص 144.

[2]. أبو الوفاء محمد أبو الوفاء، جريمة الغش في تداول الأسهم في القانون المقارن والفقه الإسلامي، بحث مقدم إلى مؤتمر أسواق الأوراق المالية والبورصات، كلية الشريعة والقانون، الإمارات العربية المتحدة، 2006. ص 50.

أو مواقع أخرى لإعطاء أكثر مصداقية للمشاريع الوهمية للمُحتال، ودفع الضحايا إلى تصديق المشاريع من أجل إستدراجهم للإستيلاء على أموالهم وممتلكاتهم وأصولهم وأسهمهم، وتقديم وعود للضحايا الذين يرغبون في الربح السريع بأرباح مضمونة وكبيرة ومضاعفة و بنسب عالية بأقل المجهودات بمجرد المشاركة في المشروع، وإنعدام فرص حدوث أية خسارة في هذه المشاريع مع ضمان الربح والفائدة والكسب.

الفرع الثاني

الغش بإتخاذ إسم كاذب أو صفة غير صحيحة

ومن صور ومظاهر الإحتيال في مجال التجارة الإلكترونية الغش بإتخاذ إسم كاذب أو صفة غير صحيحة إذ يكفي لقيام الإحتيال أن يتخذ المُحتال إسما كاذبا أو صفة غير صحيحة حتى ولو لم يتم إستعمال طرق إحتيالية أخرى، والهدف من ذلك هو الحصول على منافع إقتصادية كحيازة مال أو تحويله أو إستخدامه عن طريق وثائق تخص الغير أو التلاعب في البيانات المخزنة، وينطبق هذا الأمر أيضا على المسؤولين في شركات المساهمة إذا أوردوا أسماء للغير كذبا في نشرات الإكتتاب أو إعلاناتها كونهم أعضاء مؤسسين فيها فالناس تثق في مثل هذه الأسماء خاصة إذا كانت من الشخصيات المشهورة والبارزة في المجتمع[1].

نلاحظ أنه من بين الأساليب الإحتيالية التي يستعملها المُحتال المعلوماتي قيامه بإستخدام أسماء كاذبة أو صفات غير صحيحة، ويتمثل إستخدام الأسماء الكاذبة من خلال قيام المُحتال بإنتحال أسماء لأشخاص معروفين بنزاهتهم وشفافيتهم ومصداقيتهم، وتضليل الضحايا (المجني عليهم) الذين يجهلون معرفة الأشكال الحقيقية لهؤلاء الأشخاص المشهود لهم بإستقامتهم، حيث يقوم المُحتالون بإستغلال هذه الأسماء، والإدعاء لدى المجني عليهم من خلال سرقة هذه الأسماء مع أن أسماءهم الحقيقية غير ذلك، أما إستعمال صفات غير صحيحة فتتمثل في قيام المُحتال بالإدعاء بمراكز وصفات ورتب معينة (وزير، برلماني، محام، مؤسس شركة،...).

المطلب الثالث

مظاهر الإحتيال الإلكتروني عبر الأنترنيت

من بين أشكال الإحتيال الإلكتروني والتي تعتبر أقل شيوعا وإنتشارا وخطورة وتأثيرا في الدول والمجتمعات مقارنة مع المظاهر التي سبق ذكرها، مظاهر الإحتيال الإلكتروني عبر الأنترنيت، وذلك من خلال الإحتيال عبر الرسائل النصية القصيرة، والإحتيال بجمع التبرعات الخيرية.

[1]. أبو الوفاء محمد أبو الوفاء، المرجع نفسه، ص 60.

الفرع الأول

الإحتيال عبر الرسائل النصية القصيرة

حيث يتم إرسال رابط من خلال رسالة نصية توجه الضحية عند الضغط عليها إلى موقع تتم عبره عملية الإحتيال الإلكتروني وبعدها يتمكن المُحتال من سرقة معلوماتك الشخصية، وقد تبدو هذه الرسائل حقيقية من الطريقة التنظيمية التي يتبعونها في كتابة النص الذي تتضمنه الرسالة ويقومون بالتزوير كأنهم البنك أو المؤسسة التي تتعامل معها ويدعون في الرسالة أن شخص معين حاول سرقة حسابك ولكي تقوم بتأمينه إضغط على الرابط وبهذه الطريقة يقع الناس ضحايا لعملية الإحتيال ويتعرضون للسرقة.

يظهر أنه من بين الأساليب الإحتيالية التي يستخدها المُحتال المعلوماتي هو الإحتيال الذي عبر الرسائل النصية القصيرة ، ويعتبر هذا النوع من الإحتيال من أكثر مظاهر الإحتيال شيوعا وإنتشارا، حيث نجد أن هناك العديد من الرسائل التي تصل إلى المشتركين عبر مختلف مواقع التواصل الإجتماعي (فيسبوك facebook، واتساب WhatsApp :، فايبر viber، تويتر twitter ، تليغرام Telegram ، وغيرها من المواقع المشابهة لها).

فبعض الرسائل تتدعي بفوز المشترك بجائزة مالية أو حصوله على سيارة أو تلقيه هدايا وغيرها من المغريات، وتطلب منه هذه الصفحات أن يقوم بالضغط على الرابط المرسل إليه من أجل إستكمال إجراءات حصوله على هذه الجوائز والهدايا، وهنالك بعض الإعلانات تكون محملة بالفيروسات، والتي تستخدم لسرقة معلومات وبيانات الضحايا (المجني عليهم)، وبمجرد النقر على هذه الروابط تظهر برامج ضارة، حيث يقوم الحاسب الآلي أو الهاتف الذكي بتحميلها وعند الضغط على تلك البرامج يتمكن المُحتال المعلوماتي من معرفة بيانات ومعلومات الكمبيوتر الخاص بك أو هاتفك الذكي.

الفرع الثاني

الإحتيال بجمع التبرعات الخيرية

حيث يقوم المُحتال بإنشاء موقع مزيف أو إرسال بريد إلكتروني إليك يشجعك على دفع المال وهذا النوع من الإحتيال يستهدف عواطف الناس ويحاول التأثير عليهم من أجل أن يدفعوا الأموال بحجة التعاطف الإنساني مع الغير، ولذلك قبل إعطاء التبرع يجب التأكد بأن تلك الاموال تذهب إلى جهة خيرية مسجلة أو إلى شخص حالته معروفة.

يتضح أنه من بين الأساليب الإحتيالية التي يستعملها المُحتال المعلوماتي الإحتيال عن طريق إنشاء مواقع لجمع التبرعات الخيرية، ويتمثل هذا النوع من الإحتيال في قيام المُختال بإيهام الناس والمؤسسات بقيامه بنشاطات خيرية إنسانية تهدف إلى فك الغبن عن المحتاجين، وذلك من خلال إستغلال عواطف الناس وإقناعهم بالتبرع لجمعيته الوهمية بالأموال أو المواد الأولية أو المواد الغذائية أو الألبسة أو الأثاث، وغيرها من الإحتياجات الضرورية للحياة المعيشية للإنسان، وإدعاء المُحتال بقيامه بتوزيع هذه الأموال والمواد والحاجات المختلفة إلى مستحقيها وإلى المحتاجين.

الخاتمة:

إن الغاية الأساسية التي نسعى للوصول إليها من خلال معالجة موضوع **"أخطر مظاهر جرائم الإحتيال الإلكتروني التي يستخدمها المُحتال المعلوماتي"** ، هي إبراز الأشكال والصور التي يقوم بها المُحتال المعلوماتي في سرقة أموال وممتلكات وأصول ضحياه والنصب عليهم والإستيلاء على هذه الممتلكات وإختلاسها، إضافة إلى الطرق والأساليب التي يستعملها المُحتال في الإيقاع بالمجني عليهم من خلال إستغلال عواطفهم وإنسانيتهم وحبهم لفعل الخير، وأهم هدف هو التصدي للظاهرة الإجرامية بصفة عامة أو على الأقل التقليل من حدتها وخطورتها، وإيجاد الحلول اللازمة والضرورية في التصدي لجرائم المُحتال المعلوماتي، وفضح جميع الأساليب التي يستعملها للإيقاع بالضحايا (المجني عليهم).

ومن بين النتائج التي تم التوصل إليها نذكر ما يلي:

- ✓ الحاسب الآلي والهاتف الذكي من أخطر الوسائل التي يستعملها المُحتال المعلومات في النصب والإستلاء على ممتلكات الضحايا.
- ✓ المُحتال المعلوماتي يرتكب جريمة الإحتيال الإلكتروني في بيئة إلكترونية مصدرها إما الحاسب الآلي أو الهاتف الذكي أو البطاقات الممنغطة.
- ✓ الإحتيال الإلكتروني معالجته تتطلب جهود دولية في مجال التعاون الدولي القضائي للسيطرة على الجريمة في مجال (تسليم المجرمين-الإنابة القضائية-التعاون مع منظمة الشرطة الدولية (الإنتربول)، وفي مجال المساعدة القانونية المتبادلة، والتوقيع على المعاهدات والإتفاقيات..
- ✓ الإحتيال الإلكتروني يمس بإرادة الضحايا بعيب الرضا حيث تتدخل إرادة المُحتال المعلوماتي في توجيهها وفقا لإرادته.
- ✓ ترتبط جرائم الإحتيال الإلكتروني إرتباطا وثيقا بجرائم التزوير الإلكتروني لأن كلاهما يعتمد على الكذب والخداع والغش والتدليس.
- ✓ الإحتيال الإلكتروني الي يرتكب بواسطة بطاقة الإئتمان قد يكون المُحتال المعلوماتي فيها صاحب البطاقة نفسه أو قد يستعملها غيره في الإحتيال.
- ✓ بيئة جرائم الإحتيال الإلكترونية بيئة واسعة جدا والبحث فيه عن الأدلة الجنائية الإلكترونية أمر صعب، ويحتاج إلى فنيين وخبراء حتى تكون لهم القدرة على تطويق ومحاصرة الأدلة الإلكترونية وكشف الأساليب الإحتيالية التي يقوم بها المُحتال المعلوماتي.
- ✓ من أخطر جرائم الإحتيال الإلكتروني قيام المُحتال المعلوماتي بإنشاء بطاقة مزورة تحتوي على أرقام ومعلومات وبيانات تمت سرقتها من العملاء.
- ✓ وكذلك من أخطر صور الإحتيال الإلكتروني هو الإحتيال الذي يقع بواسطة بطاقات الإئتمان الممغنطة مثل إستخدام بطاقات إئتمان مسروقة أو مفقودة أو مزورة، والإحتيال الذي يقع في مجال التجارة الإلكترونية مثل الإيهام بوجود مشروع كاذب أو الغش بإتخاذ إسم كاذب أو صفة غير صحيحة.

- ✓ من بين أسباب التي تؤدي إلى وقوع الضحايا في شباك المُحتال المعلوماتي بسهولة إضافة إلى الرعونة وعدم الإحتياط الجشع والطمع والرغبة في الثراء الفاحش والكسب السريع، و الرغبة في المشاركة في المشاريع التي تنعدم فيها فرص الخسارة والبحث عن الأرباح المضمونة.

ومن بين التوصيات نوصي بما يلي:

- ➢ نوصي بعدم إدخال المعلومات والبيانات الشخصية على جميع المواقع الإلكترونية قبل التأكد من ملكيتها الرسمية لهذه المواقع.
- ➢ نقترح التحديث المستمر للقوانين المتعلقة بالجرائم السبيرانية ومواكبة تقنيات الإعلام الآلي، وسن تشريعات تتماشى والمهارات الفنية والتقنية التي إكتسبها المُحتال المعلوماتي.
- ➢ ندعو إلى إيجاد حلول للمحافظة على الدليل الجنائي الإلكتروني من التعرض للسرقة والإسترجاع، وإحاطته بالحماية اللازمة والضرورية من كل أشكال التعرض بمختلف أنواعها بإتلافها أو حذفها أو مسحها أو سرقتها أو نسخها أو تعديلها أو غيرها من صور طمس الحقيقة.
- ➢ ندعو إلى ضرورة إيجاد حلول تمكن من السيطرة على بيئة الجرائم الإحتيالية وتضييقها ومحاصرتها لمنع ضياع الادلة الجنائية الإلكترونية، وبالتالي تتمكن أجهزة التحقيق القضائية من السيطرة عليه وبالتالي التحكم في الدليل الجنائي الإلكتروني.
- ➢ نقترح توفير الحماية للمواقع والبيانات الشخصية في التشريعات وتوسيع نطاقها من حيث الجرائم.
- ➢ ندعوا المواطنين إلى الحذر من الهدايا والمسابقات المخادعة حيث يقدم المُحتالون في بعض الأحيان هدايا مجانية أو يوفرون بعض الجوائز مقابل ملء إستبيان.
- ➢ نوصي بالإنتباه إلى المنشورات القادمة من حسابات منتحلي الشخصية وذلك لأن الإحتيال على وسائل التواصل بأبسط أشكاله يظهر بإنتحال الشخصية.
- ➢ ندعوا المشتركين عبر مختلف مواقع التواصل الإجتماعي إلى تجنب النقر على روابط الإعلانات والعناوين المغرية.
- ➢ وأخيرا ندعوا إلى عدم المبالغة في البث المباشر وعروض الأفلام الإحتيالية وتجنب المبالغة بالمشاركات لأنها تمنح المُحتالين المعلومات التي يحتاجونها لمهاجمة حسابك والإحتيال عليك.

قائمة المراجع:

أولا: الكتب

01 -أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية ، 2006.

02 -أسامة حمدان الرقب، جرائم النصب والإحتيال، الطبعة الأولى، دار يافا العلمية للنشر والتوزيع، عمان، الأردن 2012.

03 -حجازي عبد الفتاح، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنيت، دار الكتب القانونية، القاهرة، مصر ، 2007.

04 -حجازي عبد الفتاح بيومي، مكافحة جرائم الكمبيوتر والانترنيت في القانون العربي النموذجي، جمهورية مصر العربية، القاهرة، 2007.

05 -جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الإئتمان الممغنطة، دراسة تطبيقية في القضاء الفرنسي والمصري، جمهورية مصر العربية، القاهرة، 1999

06 -الشحات إبراهيم محمد منصور الجرائم الإلكترونية في الشريعة والقوانين الوضعية، بحث فقهي مقارن، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2011.

07 -محمد أمين الشوابكة، جرائم الحاسوب والأنترنيت، الطبعة الأولى، دار الثقافة، عمان، الأردن ، 2004.

08 - محمد الشناوي، جرائم النصب المستحدثة ،دار الكتب القانونية، جمهورية مصر العربية، القاهرة، 2008.

09 -محمد عبد الله أبو بكر ، موسوعة جرائم المعلوماتية، جرائم الكمبيوتر والأنترنيت، د ط المكتب العربي الحديث، الإسكندرية، 2011.

10 -محمد محمد شتا، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، مصر، الإسكندرية ، 2001.

11 -نايلة عادل محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان ، 2005.

ثانيا: الأطروحات ومذكرات التخرج

01 -تيسير أحمد حسين الزعبي، جريمة الإحتيال الإلكتروني، دراسة مقدمة إستكمالات لمتطلبات الحصول على درجة الماجستير في القانون العام، كلية الدراسات القانونية، قسم القانون، جامعة جدارا، السنة الجامعية 2010/2009.

02 -حطاب كمال، الحماية الجزائية للتجارة الإلكترونية، أطروحة دكتوراه في العلوم، تخصص علوم قانونية، فرع علوم جنائية، كلية الحقوق والعلوم]السياسية، جامعة الجيلالي إلياس، سيدي بلعباس، الجزائر، السنة الجامعية، 2016/2015.

03 -عمر محمد أبو بكر يونس، الجرائم الناشئة عن إستخدام الأنترنيت، أطروحة دكتوراه مقدمة إلى كلية الحقوق، جامعة عين الشمس، دار النهضة العربية، القاهرة، 2004.

04 -معتوق عبد اللطيف، الإطار القانوني لمكافحة الجرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة لنيل شهادة الماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر ، السنة الجامعية، 2012/2011.

ثالثا: المقالات العلمية

01 -بولحية شهيرة، سويح دنيا زاد، الإحتيال الإلكتروني، مجلة الدراسات القانونية والإقتصادية، العدد 04، ديسمبر، المركز الجامعي سي الحواس، بريكة، باتنة، الجزائر، 2019.

02 -عماد بلغيث، جغلولي يوسف: ، صعوبات التحقيق في الجرائم الإلكترونية، مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد 06، العدد 03 سبتمبر، 2021.

03 -وائل محمد نصيرات، غادة عبد الرحمن الطريف، جريمة الإحتيال عبر شبكة المعلومات الدولية، دراسة مقارنة النظام السعودي والقانون الأردني، مجلة دفاتر السياسة والقانون، عدد جوان، المجلد 10، العدد 19، 2018، جامعة قاصدي مرباح، ورقلة، الجزائر.

رابعا: الملتقيات والندوات العلمية

01 -أبو الوفاء محمد أبو الوفاء، جريمة الغش في تداول الأسهم في القانون المقارن والفقه الإسلامي، بحث مقدم إلى مؤتمر أسواق الأوراق المالية والبورصات، كلية الشريعة والقانون، الإمارات العربية المتحدة، 2006.

02 -عبد المومن بن الصغير، الطبيعة الخاصة للجريمة المرتكبة عبر الأنترنيت في التشريع الجزائري والتشريع المقارن، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، 2015.

03 -مفلح القضاة، مسؤولية البنوك الناتجة عن إستخدام الكمبيوتر كوسيلة وفاء، بحث مقدم إلى مؤتمر القانون والكمبيوتر المنعقد في كلية الشريعة]والقانون، جامعة الإمارات العربية، 2002.

خامسا: القوانين

- القانون رقم 06/24 المؤرخ في 19 شوال عام 1445 هـ، الموافق 28 أفريل سنة 2024 م، يعدل ويتمم الأمر رقم 156/66 المؤرخ في 08 يونيو سنة 1966 م، المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 30، الصادر بتاريخ: 21 شوال عام 1445 هـ، الموافق 30 أفريل سنة 2024 م.