ISSN: 2706-6495

التزويـــــــرالإلكتروني بين التشريع التقليدي وآليات المواجهة الحديثة

Electronic Counterfeiting Between Traditional Legislation and Modern Coping Mechanisms

إعداد الباحث/ أحمد محمد محروس عبدالعال

مستشار قانوني أول مكتب وائل بن سحيم محامون ومستشارون قانونيون، حاصل على ليسانس الحقوق جامعة طنطا، محامي إستئناف مقيد بنقابة المحامين المصرية، منتسب مهني بالهيئة السعودية للمحامين

E-mail: ahmedmahrous589@gmail.com

الملخص:

أدت تقنية المعلومات وظهور الحاسوب والإنترنت إلى تحقيق إنجازات بارزة في العلم الحديث، وتُعتبر وأكثرها فائدة للإنسان في مختلف المجالات، وقد رافق هذه الإنجازات ظهور خبراء جدد لم تعهدهم البشرية من قبل، يمتلكون المهارات والخبرة في استغلال هذه التقنية لأغراض إجرامية. وقد تحولت الجريمة من طبيعتها التقليدية وأبعادها المحدودة إلى أبعاد جديدة تعتمد هذه التقنية على تنفيذ الأعمال الإجرامية، مستخدمة أساليب مبتكرة وطرق لم تكن معروفة سابقًا. من هذا المنطلق يأتي البحث الحالي إلى توضيح مفهوم التزوير الإلكتروني وأركانه والنتائج المترتبة عليه، وتوضيح إمكانية تطبيق النصوص القانونية المتعلقة بجريمة التزوير التقليدي على جريمة التزوير الإلكتروني، وتوضيح الآليات والإجراءات المتبعة لمكافحة جريمة التزوير الإلكتروني، لتحقيق أهداف البحث اعتمد الباحث على المنهج الوصفي التحليلي القانوني، حيث قمنا بوصف البيانات والعناصر والخصائص المتعلقة وتتناول جرائم التزوير الإلكتروني.

وتوصل البحث إلى مجموعة من النتائج من أبرزها: شهد النظام السعودي تطوراً ملحوظاً في مواجهة الجرائم الإلكترونية، وجرائم التزوير الإلكتروني؛ تُعتبر جريمة التزوير الإلكتروني تهديداً كبيراً على الأصعدة الاقتصادية والسياسية والاجتماعية، وذلك بسبب انتشار التعاملات الإلكترونية وزيادة الاعتماد على التكنولوجيا في المستقبل: تتراوح عقوبة التزوير الإلكتروني في النظام السعودي بين الغرامة والسجن لمدة لا تتجاوز خمس سنوات، أو تطبيق العقوبتين معاً، بالإضافة إلى عقوبة تكميلية تتمثل في مصادرة الأجهزة والبرامج والنظم المستخدمة في ارتكاب الجريمة. وفي ضوء ما توصل له البحث قدم الباحث مجموعة من التوصيات المفيدة والمهمة.

الكلمات المفتاحية: مكافحة، جرائم، التكنولوجيا، التزوير الإلكتروني.

ISSN: 2706-6495

Electronic Counterfeiting Between Traditional Legislation and Modern Coping Mechanisms

Abstract:

Information technology and the emergence of computers and the Internet have led to remarkable achievements in modern science, and are considered the most beneficial to humans in various fields. These achievements have been accompanied by the emergence of new experts that humanity has not known before, who possess the skills and experience in exploiting this technology for criminal purposes. The crime has transformed from its traditional nature and limited dimensions to new dimensions that depend on this technology to carry out criminal acts, using innovative methods and methods that were not previously known. From this standpoint, the current research comes to clarify the concept of electronic forgery, its pillars and the consequences thereof, and to clarify the possibility of applying legal texts related to the crime of traditional forgery to the crime of electronic forgery, and to clarify the mechanisms and procedures followed to combat the crime of electronic forgery. To achieve the objectives of the research, the researcher relied on the descriptive analytical legal approach, where we described the data, elements and characteristics related to and dealing with electronic forgery crimes. The research reached a set of results, the most prominent of which are: The Saudi system has witnessed a remarkable development in confronting electronic crimes and electronic forgery crimes; The crime of electronic forgery is considered a major threat at the economic, political and social levels, due to the spread of electronic transactions and the increased reliance on technology in the future: The penalty for electronic forgery in the Saudi system ranges between a fine and imprisonment for a period not exceeding five years, or the application of both penalties together, in addition to a complementary penalty of confiscating the devices, programs and systems used in committing the crime. In light of the findings of the research, the researcher presented a set of useful and important recommendations.

Keywords: combat, crimes, technology, electronic counterfeiting.

1. المقدمة:

يشهد عالم اليوم تطورات وتطورات تكنولوجية وهندسية في العديد من المجالات، بالإضافة إلى انتشار استخدام الإنترنت على نطاق واسع. فقد دخلت التكنولوجيا في العديد من المجالات التجارية والمدنية، وأصبحت المعاملات والعقود التجارية تتم من خلال هذه الأساليب الحديثة، باستخدام العديد من التقنيات الجديدة مثل الحوسبة السحابية Cloud Computing وأنظمة الذكاء الاصطناعي Artificial intelligence systems، والمنصات الرقمية Digital Platforms.

وتعتبر جرائم التزوير من أكثر المواضيع حساسية في النظام الجزائي الحديث. وذلك لوجود ارتباط بين جرائم التزييف وتبعاتها الدينية والاجتماعية والاقتصادية، ولأنها تساهم في انتشار الفساد بكل أنواعه. ولهذا فإن الأديان السماوية المقدسة منذ أن خلق الله الإنسان على الأرض قد أدانت التزوير ورفضته، وخصت الشريعة الإسلامية هذه الجرائم باعتبارها منكرات يجب أن يعاقب عليها بالقوانين حماية للفرد والمجتمع.

لقد أدركت عديداً من التشريعات الجديدة المرتبطة بجرائم التزوير التي أفرزتها تقنيات نظم المعلومات. وتمكنت هذه التشريعات من تجاوز المفهوم التقليدي للتزوير من حيث الوعاء والمحل، وهو أمر إيجابي بالنظر إلى حجم الجرائم الإلكترونية وأهميتها، بالإضافة إلى اتساع نطاق استخدامها.

ويُعد التزوير جريمة خطيرة يعاقب عليها القانون في المملكة العربية السعودية، حيث يُعتبر آفة اجتماعية تهدد أمن واستقرار المجتمع وتؤدي إلى العديد من الأضرار على مختلف الأصعدة. لذلك، قامت المملكة بوضع قوانين وعقوبات صارمة لمكافحة قضايا التزوير، بهدف حماية المجتمع والأفراد من آثارها السلبية الكبيرة.

وفي ظل الثورة المعلوماتية التي يشهدها العالم، أصبحنا نعيش حياة مليئة بالاتصالات السريعة ونقل المعلومات عبر المسافات، بالإضافة إلى تبادل البيانات دولياً ومحلياً. كما أن هذه الثورة ساهمت في تعامل مختلف الأنظمة المتقدمة، وقد تداخلت أرجاء العالم مع بعضها البعض، حيث يشاهد الناس ويتبادلون الحوار، مما أتاح للإنسان التحرر من قيود المكان. وبذلك، أصبح وكأنه يتواجد في أكثر من مكان في الوقت نفسه.

وقد أدى هذا الانفتاح إلى ظهور جرائم ثورة المعلومات. والواقع أن هذه الظاهرة حديثة النشأة، حيث ترتبط بتكنولوجيا حديثة، وهي تكنولوجيا الحاسوب، خاصة في بدايات القرن الماضي.

ونتيجة للاعتماد المتزايد على الحواسيب في جميع جوانب حياتنا، زادت جرائم التكنولوجيا بشكل كبير، وتنوعت أساليبها وازدادت مخاطرها وخسائرها. أصبحت هذه الجرائم من أخطر التهديدات التي تواجه المصالح والحقوق القانونية، خاصة المعتمدة على تأكيد المعلومات والبيانات، مثل جرائم التزوير الإلكتروني. فهذه الجرائم تتضمن بيانات حساسة قد تكون عرضة للاعتداءات، حيث يتم تغيير حقيقتها بهدف الغش، مما يؤدي إلى أضراراً مادية أو معنوية أو اجتماعية، وغيرها من الأضرار التي تلحق بالآخرين. لذا، يُعتبر التزوير من أخطر أساليب الغش في مجال معالجة البيانات الآلية (حسبو، 2000، ص 38 – 39).

وتُعتبر جريمة التزوير الإلكتروني من أنواع الغش المعلوماتي، الذي نتج عن الثورة المعلوماتية التي أدت إلى ظهور وسائل معلوماتية قادرة على تخزين البيانات بكميات هائلة. وقد حلت هذه الوسائل محل الوثائق التقليدية مثل الأوراق والدفاتر. وقد أثبتت التجارب العملية أن الوثائق التقليدية لا يمكن أن تضاهي الوسائل المعلوماتية من حيث سعة التخزين، وسرعة استرجاع المعلومات، وتنظيمها بشكل فعال. وهذا يبرز مدى كفاءة النصوص المتعلقة بالتزوير التقليدي في التعامل مع هذه الظاهرة (حجازي، 2004، ص 135).

وأدت تقنية المعلومات وظهور الحاسوب والإنترنت إلى تحقيق إنجازات بارزة في العلم الحديث، تُعتبر أكثرها فائدة للإنسان في مختلف المجالات الحياتية، وذلك في الاقتصاد والطب والتعليم والعديد من المجالات الأخرى. وقد رافق هذه الإنجازات ظهور خبراء جدد لم تعهدهم البشرية من قبل، يمتلكون المهارات والخبرة في استغلال هذه التقنية لأغراض إجرامية. وأدى ذلك لظهور الجرائم المعاصرة، حيث تحولت الجريمة من طبيعتها التقليدية وأبعادها المحدودة إلى أبعاد جديدة اعتماداً على التقنية لتنفيذ الأفعال الإجرامية، مستخدمة أساليب مبتكرة وطرق لم تكن معروفة سابقًا.

ومن النتائج الناتجة عن انتشار هذه الأساليب الحديثة في العمل، ظهور الوثائق الإلكترونية التي تُنتجها مؤسسات عامة وخاصة بنشاطها، إذ يتم العمل إلكترونياً بالكامل، مما يجعل تأمين الوثائق الإلكترونية أمرًا بالغ الأهمية. فمن المؤكد أن النسخة الإلكترونية من الوثيقة الورقية، ويمكن تعرضها للتدمير غير المتعمد نتيجة للتقادم في الأنظمة والأجهزة، مما يستدعي من الفنيين نقلها لأنظمة حديثة، أو عند حدوث خطأ في النظام يتطلب إعادة تحميله، أو عندما يتعرض النظام الحاسوبي لهجمات من فيروسية غير معروفة (تمام، 2000، ص 167).

وفي تصنيفات جرائم نظم المعلومات الحديثة، تُعتبر جرائم التزوير الإلكتروني من أخطر الجرائم في عصرنا الحالي، حيث تحتل مرتبة متقدمة. يعود ذلك إلى تأثيراتها السلبية الكبيرة على المحررات والوثائق والمستندات المزورة، والتي غالبًا ما تترتب عليها تبعات مالية وأضرار تلحق بالصالحين العام والخاص. وقد تصل هذه الأضرار أحيانًا إلى فترات زمنية طويلة نتيجة استمرار وجود تلك المحررات المزورة.

ومن البديهي نؤكد على أن الظلال التي خلفتها برمجيات تكنولوجيا المعلومات والحواسيب قد أضفت مستوى احترافيًا في معالجة الصور للمستندات والمحرمات. هذه البرمجيات زادت من تعقيد عملية الكشف عن التزوير من خلال التحريف أو التغيير، إلى درجة يصعب معها على الحواس البشرية إدراكها. لقد استُخدمت هذه التقنيات، أو أولئك الذين يسعون لاستعراض مهاراتهم في هذه البرمجيات، لنصب الكمائن لمن يحتاجون إلى مصالح مالية، معتقدين ببساطة أن هذه الأفعال لا تمثل جريمة. ولا شك أن هؤلاء القلة قد ابتعدوا عن خالقهم، وظنوا لجهلهم أنهم خالدون في هذه الحياة، وأنهم لن يعودوا إلى ربهم. لذا، فقد التصقوا بالأرض ومادتها، وركنوا إليها، وأصبحوا ماديين يعبدون المادة ويؤلهونها، مما أدى إلى موت أرواحهم وازدياد شهواتهم. وقد انغمسوا في تغذيتها بأكل الحرام بكل صوره وألوانه، حتى أصبح العالم يعج بالفساد الناتج عن تزوير الحقائق والوقائع للحصول على ما ليس لهم حق فيه.

1.1. مشكلة البحث:

تبدأ دراسة هذا الموضوع بتسليط الضوء على جريمة التزوير الإلكتروني، التي تثير العديد من التحديات على الصعيدين المحلي والدولي. يتجلى ذلك في مدى كفاية النصوص القانونية التقليدية لمواجهة الجريمة الإلكترونية، بالإضافة إلى وضع تشريعات جديدة تتماشى مع تطور هذه الأنماط الإجرامية.

2.1. تساؤلات البحث:

يتفرع عن مشكلة البحث التساؤلات التالية:

1- ما هو التزوير الإلكتروني؟

2- هل يمكن تطبيق نصوص جريمة التزوير التقليدية على التزوير الإلكتروني؟

3- هل يتطلب تجريم التزوير الإلكتروني بشكل عام ووجود نص قانوني خاص؟

ISSN: 2706-6495

4- هل تعتبر الآليات والإجراءات المتبعة لمكافحة جريمة التزوير الإلكتروني كافية لردع هذه الجريمة؟

3.1. أهمية البحث:

تتجلى الأهمية في تناول الظاهرة الحديثة للجرائم الإلكترونية، وخاصة جريمة التزوير الإلكتروني. فرغم الفوائد العديدة للتطور التكنولوجي، إلا أنه يحمل في طياته كثيراً من السلبيات التي تهدد الأمن والاستقرار، ومن أبرزها جريمة التزوير الإلكتروني التي تؤثر بالسلب على الثقة العامة. ومع تزايد وتطور هذه الجرائم، وخاصة التزوير الإلكتروني، وتبرز تلك الأهمية في التالي:

1- التصدي لمثل هذه الجرائم الخطيرة التي تؤدي إلى زعزعة الثقة العامة.

2- مواجهة هذه الجرائم نظرًا لاستمرارها وتجدد أنشطتها.

3- تسليط الضوء على هذا النوع من الجرائم التي تحمل آثارًا سلبية عديدة تهدد أمن وسلامة المجتمع.

4.1. أهداف البحث:

يأتي البحث الحالي لتحقيق الأهداف التالية:

1- توضيح مفهوم التزوير الإلكتروني وأركانه والنتائج المترتبة عليه.

2- توضيح إمكانية تطبيق النصوص القانونية المتعلقة بجريمة التزوير التقليدي على جريمة التزوير الإلكتروني.

3- توضيح الآليات والإجراءات المتبعة لمكافحة جريمة التزوير الإلكتروني.

5.1. منهج البحث:

تم الاعتماد بشكل أساسي على المنهج الوصفي التحليلي القانوني، حيث قمنا بوصف البيانات والعناصر والخصائص المتعلقة وتتناول جرائم التزوير الإلكتروني.

6.1. خطة البحث:

مقدمـــة.

المبحث الأول: مفهوم جريمة التزوير الإلكتروني:

المطلب الأول: تعريف جريمة التزوير الإلكتروني.

المطلب الثاني: خصائص جريمة التزوير الإلكتروني.

المبحث الثاني: صور جريمة التزوير في المعاملات الإلكترونية والعقوبات المقررة لها:

المطلب الأول: صور جريمة التزوير في المحررات الإلكترونية.

المطلب الثاني: العقوبات المقررة لجريمة التزوير الإلكتروني.

الخاتمة والنتائج والتوصيات.

المراجـــــع.

المبحث الأول: مفهوم جريمة التزوير الإلكتروني

يُعتبر التزوير من الجرائم التي تحتاج إلى دقة في معالجتها وعناية خاصة وذلك لتعقيدها وتنوع طرق التزوير وتطورها المستمر. فلم يعد التزوير مقتصرًا على مفهومه التقليدي، بل تطور ليشمل ما يُعرف بالتزوير الإلكتروني. وقد أدى هذا التطور إلى اهتمام الدول المتقدمة بتناول جريمة التزوير في صيغتها الحديثة ضمن قوانينها العقابية، بهدف توفير حماية جزائية للمعلومات والبيانات المتاحة على الشبكة الإلكترونية، والتي تتعلق بإثبات حقوق أو مراكز قانونية معينة (عبيد، 2016، ص 121).

وتُعتبر جريمة التزوير الإلكتروني من الجرائم الحديثة، حيث تُستخدم الوسائل التقنية مثل الحاسوب كأداة رئيسية في ارتكابها. وقد نشأت هذه النوعية من الجرائم نتيجة للتطور التكنولوجي الذي شهدته مختلف المجالات، مما جعل العالم يبدو كقرية صغيرة. وقد أتاح هذا التطور الكثير من التسهيلات، خاصة في تقديم الخدمات ومختلف جوانب الحياة. ومع ذلك، رافق هذا التقدم بعض السلبيات، أبرزها ظهور جرائم جديدة لا تعترف بالحدود الجغرافية، ومن أهم هذه الجرائم جريمة التزوير الإلكتروني (الجبوري، 2017، ص 14).

وجريمة التزوير الإلكتروني واحدة من أنواع الجرائم التي تندرج تحت فئة الجرائم الإلكترونية[1]، وتُعد من أخطر أساليب الغش في مجال المعلوماتية، حيث تستخدم أجهزة الكمبيوتر والإنترنت بديلاً عن الأوراق في معظم الأحيان. ولم يقتصر هذا الأمر على مجال محدد، بل شمل جميع المعاملات مثل عمليات الدفع، وطلبات البضائع، وتحويل الأموال بين البنوك.

تتميز جريمة التزوير الإلكتروني بمفهوم خاص عن الجرائم الإلكترونية الأخرى التي يمكن ارتكابها إما بالطرق التقليدية أو من خلال الوسائل الإلكترونية مثل الحاسب الآلي وشبكات الاتصالات والإنترنت (العبادي، 2015، ص 177).

لذا، من الضروري فهم مفهوم جريمة التزوير الإلكتروني من خلال تعريف التزوير من الناحية اللغوية والفقهية والقانونية. هذا سيمكننا من التوصل إلى مفهوم التزوير وفهم جميع الجوانب المتعلقة به بدقة، بالإضافة إلى توضيح خصائصه وطبيعته.

المطلب الأول: تعريف جريمة التزوير الإلكتروني:

يعتبر التزوير الإلكتروني جريمة خطيرة تضاهي في أهميتها التزوير التقليدي. ويرجع ذلك إلى إمكانية ارتكابه في أي وقت، فضلاً عن صعوبة اكتشافه من قبل المحققين، حيث إنه لا يترك أي دليل مادي يشير إلى حدوثه (خليفة وصالح، 2022، ص 257).

وتُعد جريمة التزوير الإلكتروني واحدة من الجرائم الأكثر تعقيداً، حيث ترتبط بشكل وثيق بالثقة العامة. لذا، سنقوم بتعريف التزوير من الناحيتين اللغوية والقانونية، بالإضافة إلى الفقهية، كما يلي (زين الدين، 2008، ص 334):

أولاً: تعريف التزوير في اللغة:

هو الزور والباطل والكذب والتقليد والمحاكاة والبعد عن الحق، وهو أيضاً لفظ مشتق من كلمة مزور هو الكذب والتلفيق وإدخال الباطل، وله معنى واسع يشمل كل أنواع الخداع والاحتيال (زين الدين، 2008، ص 334).

(1) تعرف الجريمة الإلكترونية على أنها: "فعل غير مشروع يرتكب متضمناً استخدام أي جهاز إلكتروني أو شبكة معلوماتية خاصة أو عامة كالإنترنت"، للمزيد انظر: غازي، محمود إبراهيم (2014): الحماية الجنائية للخصوصية والتجارة الإلكترونية، ط1، مكتبة الوفاء القانونية، الإسكندرية، مصر، ص 118 وما بعدها.

والتزوير هو: الزور بالضم: الكذب (الجوهري، 672/2؛ ابن فارس، 444/1)، ومنه قوله تعالى: (وَٱجۡتَنِبُواْ قَوۡلَ ٱلزُّورِ 30) (سورة الحج: الآية 30)، والزور: يدل على الميل والعدول، لأنه مائل عن طريق الحق (الرازي، 1399هـ، 63/3؛ الزبيدي، 1422هـ، 461/11)، والتزوير: من زور، قلد: تقليد الشيء مع ادعاء هذا المزور هو الأصل مع أنه ليس كذلك (قلعجي وقنيبي، 1408هـ، ص 129)، أي أن الزور هو الكذب الذي قد حسن وسوى في الظاهر ليحسب أنه صدق (العسكري، 1997، ص 47).

ثانياً: تعريف التزوير في الاصطلاح:

عرف التزوير بأنه: " تغيير الحقيقة أو استبدال أمر غير صحيح بالواقع الصحيح يعد من الأمور" (هلال، 1996، ص 3؛ القاضي، 2013، ص 143).

وهو: "تغيير الحقيقة سواء بالشهادة أو القول أو الكتابة أو العمل، وتحريفاً للواقع، وهذا يؤدي إلى منح الحق لمن لا يستحقه أو حرمان المستحق من حقه، أو حتى الاستيلاء على حقوق الآخرين، أو الحصول على ما لا يستحقه بطرق غير مشروعة، مما قد يسبب الأذى للآخرين" (مراد، 2011، ص 34).

وورد تعريف آخر للتزوير بأنه: " إظهار الكذب في محرر على أنه حقيقة يعد خداعاً لعقيدة الآخرين" (حمودة، 2003، ص 249). والتزوير هو: " تقليد شيء ما مع التظاهر بأن هذا التقليد هو النسخة الأصلية، رغم أنه ليس كذلك" (العبيدي صدام؛ والعبيدي عواد، 2020، ص 25).

وقام المنظم السعودي بتعريف التزوير في نظامه الجزائي لجرائم التزوير، الذي أصدر بموجبه المرسوم الملكي رقم (م/11) بتاريخ 1435/2/18هـ. وقد تم تعريفه في (1) على أنه : "كل تغيير للحقيقة بإحدى الطرق المنصوص عليها في هذا النظام - حدث بسوء نية – قصداً للاستعمال فيما يحميه النظام من محرر أو خاتم أو علامة أو طابع، وكان من شأن هذا التغيير أن يتسبب في ضرر مادي أو معنوي أو اجتماعي لأي شخص ذي صفة طبيعية أو اعتبارية".

ثالثاً: تعريف التزوير فقهاً:

التزوير هو فعل مادي يُعتبر نوعًا من الكذب، يقوم به فرد بهدف تغيير الحقيقة في مستند أو وثيقة رسمية أو عامة، وذلك باستخدام وسائل محددة ينص عليها القانون. ويترتب على هذا الفعل إلحاق الضرر بحقوق أو مراكز قانونية لأحد أو بعض الأطراف المعنية بالمستند أو الوثيقة المتنازع عليها (سعد، 2005، ص 14). وهو أي وسيلة يستخدمها فرد لخداع شخص آخر (عقاد، 1993، ص 392).

وتتنوع التعريفات الفقهية للتزوير، حيث يُعرف بأنه: "تغيير الحقيقة في مستند بهدف الغش، باستخدام إحدى الطرق التي حددها القانون، يُعتبر تغييراً قد يؤدي إلى حدوث ضرر. كما يُعرف أيضاً بأنه: "تغيير الحقيقة بقصد الغش في مستند يتعلق بشيء تم إعداد هذا المستند لإثباته، مما قد يسبب ضرراً"، وعرفه الفقيه الكارسون على أنه: " تغيير الحقيقة بشكل متعمد في مستند باستخدام إحدى الوسائل التي حددها القانون، كما عرفه الفقه المصري على أنه: "تعديل الحقيقة بغرض الاحتيال باستخدام إحدى الوسائل المنصوص عليها في القانون في وثيقة يحميها القانون" (العارضي، 2012، ص 147).

وعرفه الفقه الجنائي بأنه "تغيير للحقيقة بهدف الغش في سندات أو وثائق أو أي محررات أخرى، باستخدام إحدى الطرق المحددة قانوناً". ويكون هذا التغيير من شأنه إلحاق الضرر بمصلحة عامة أو بمصلحة فرد معين، ويكون مصحوبًا بنية استخدام المحرر المزور للغرض الذي أُعد من أجله (سرور، 1991، ص 402).

وبتحديد المعنى بشكل أدق، يعرف البعض التزوير الإلكتروني بأنه أي تعديل أو تغيير في الحقيقة يتعلق بالتوقيع أو الوثيقة الإلكترونية (غنام، 2000، ص 33).

ورأى البعض الآخر أن ذلك يعد تغييرًا للحقائق في الوثائق المعلوماتية بهدف استخدامها (القهوجي، 2000، ص 63).

وعرف أيضاً بأنه: " التسلل إلى قواعد البيانات في النظم المعلوماتية بطرق قانونية أو غير قانونية، وتعديل المعلومات من خلال حذف بيانات قائمة أو إضافة بيانات لم تكن موجودة من قبل" (السيراني، 2011، ص 54)، وهو أيضاً: " التعديل المتعمد للمعلومات الموجودة في الوثيقة المعلوماتية بهدف إحداث تضليل" (الجبوري، 2017، ص 17).

ويعرف التزوير الإلكتروني أيضاً بأنه: "تغيير الحقيقة بأي وسيلة سواء في وثيقة أو على سند، متى كان لهذا السند تأثير في تحقيق الحقيقة أو لعب دوراً في تحقيق نتيجة معينة" (تمام، 2000، ص 407).

هذا وإن التزوير الإلكتروني هو تعديل الحقيقة الذي يؤثر على مخرجات الحاسوب، سواء كانت هذه المخرجات على شكل مستندات ورقية مطبوعة أو رسومات مرسومة (حجازي، 2002، ص 170).

ونتيجة للتطورات العلمية والتكنولوجية، ظهر هذا النوع من التزوير الذي يُعرف بالتزوير الإلكتروني. وهو: "أي تغيير للحقيقة يطرأ على مخرجات الحاسوب، سواء كانت هذه المخرجات ورقية مطبوعة أو مرسومة أو مستندات لها تأثير في إثبات حق أو واجب". كما تم تعريفه أيضاً بأنه "أي استخدام لبرامج معالجة آلية أو برمجيات اختراق بهدف تعديل البيانات أو المعلومات بغرض الحصول على البيانات الأصلية أو التلاعب بها بنية استخدامها" (حفظي، 2015، ص 2).

والمقصود بالاستخدام هنا هو تعديل المعلومات الموجودة في المعاملات الإلكترونية أو المستندات الإلكترونية أو وسائل الدفع الإلكترونية الحديثة المستمدة من الوسائل التقليدية. ومن بين هذه الوسائل، يُعتبر الشيك الإلكتروني من أكثر وسائل الدفع شيوعًا على الصعيدين الدولي والعالمي. يمكن للجاني التزوير باستخدام تقنيات إلكترونية لتحقيق منفعة مالية لنفسه أو للآخرين. بالإضافة إلى ذلك، هناك نظام آخر للدفع يتمثل في تحويل الأموال بين طرفين عبر وسيط ثالث، بالإضافة إلى نظام البطاقات الإلكترونية والعملات الرقمية، وغيرها من وسائل الدفع التي قد تكون عرضة لجريمة التزوير الإلكتروني (رضوان، 2008، ص 200–201).

وبذلك، تُعتبر جريمة تزوير المستندات الإلكترونية ناتجة عن معلومات تم إدخالها باستخدام وسائل إلكترونية من خلال نظام معلومات محدد (فتيحة، 2019، ص 172).

ومن الاستعراض السابق للتعريفات الفقهية، يمكن أن نستنتج أنه لكي نعتبر الفعل جريمة تزوير إلكتروني، يجب أن يتم التزوير على مستند إلكتروني، وأن يتعارض هذا التزوير مع الحقيقة الموجودة في المستند. ويكون الهدف من ذلك هو إثبات حق غير موجود في الأساس، وإحداث أثر قانوني معين، مما يؤدي إلى إلحاق الضرر بالآخرين.

رابعاً: موقف المنظمات والهيئات الدولية والإقليمية للتزوير الإلكتروني:

تباينت التشريعات في تعريف التزوير الإلكتروني، حيث عرفت "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات" هذا النوع من الجرائم[1] في المادة (10) على أنه: "استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييراً من شأنه إحداث ضرر وبنية استعمالها كبيانات صحيحة".

(2) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

وقد عُرفت باسم الاتفاقية الأوروبية لمكافحة الجرائم الإلكترونية "اتفاقية بودابست"[1] التزوير الإلكتروني وهذا في المادة (7) التي تنص على: "أن التزوير المرتبط بالحاسب الآلى وهو يتكون من خلق أو تعديل غير مصرح به للبيانات المسجلة بطريقة من شأنها أن تجوز هذه البيانات المسجلة له قوة دامغة مختلفة عن سياق المعاملات القانونية، والتي تكون مؤسسة على صحة البيانات المستخرجة، وبالتالي تكون موضوعاً لخداع المصالح القانونية المحمية".

وتناولت كثيراً من الاتفاقيات التزوير الإلكتروني، حيث تُعتبر من الجرائم العابرة للقارات التي تتطلب تعاونًا دوليًا للحد من انتشارها. فهذه الجريمة يمكن أن تُرتكب من مسافات بعيدة تصل إلى آلاف الأميال، مما يستدعي استخدام تقنيات دولية متطورة لتحديد الأجهزة المستخدمة في عملية التزوير واسترجاع المعلومات المحذوفة أو التي يمكن استخدامها كأدلة مادية لإثبات هذا الانتهاك (السيراني، 2011، ص 128)، وتظهر الجريمة الإلكترونية بدولة ما، لكن آثارها قد تمتد إلى دولة أخرى نتيجة الترابط بين شبكات المعلومات. هذا الأمر يثير إشكاليات تتعلق بالاختصاص بالنسبة للقواعد القانونية الموضوعية والإجرائية (عباس، 2015، ص 2).

ويعتبر المشرع الدولي أن المعلومات الورقية ليست الوحيدة القابلة للتزوير، بل إن المعلومات الإلكترونية أيضاً يمكن أن تتعرض للتزوير وتستخدم بشكل غير قانوني (العفيفي، 2013، ص 82)، وقد أشار القانون الدولي في بعض السياقات إلى هذا الموضوع، حيث تناول المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات البرازيلية في عام 1994، الذي ركز على الجرائم الإلكترونية، جريمة التزوير الإلكتروني. وقد عُرّفت هذه الجريمة بأنها استخدام الأجهزة الإلكترونية بطرق غير مشروعة لمعالجة البيانات طبقاً لما أقره القانون الوطني البرازيلي (عباس، 2015، ص 18).

وفيما يتعلق باتفاقية عام 2001 المعنية بمكافحة الجرائم السيبرانية، والمعروفة أيضًا باتفاقية "بودابيست"، فقد تضمنّت في المادة السابعة تعريفًا لجرائم التزوير الإلكتروني، حيث عُرّفت بأنها: "الإدخال أو الإفساد أو التعطيل أو المحو أو الشطب عن عمد وبدون وجه حق". وبالتالي، يُعتبر التزوير الإلكتروني استخدام أي من الطرق المذكورة في التعريف السابق بشكل متعمد يستهدف المعلومات الإلكترونية بهدف إلحاق الضرر بها. كما حددت الاتفاقية الوسائل المستخدمة لتحقيق هذا الضرر، والتي تشمل بشكل خاص الإدخال أو الإتلاف أو التلاعب ضمن أنشطة الحاسوب، وأي اعتداء على الحاسوب بنية الغش للحصول على منفعة اقتصادية (الجبوري، 2017، ص 94).

ومن بين الاتفاقيات التي تمثل جهوداً لمكافحة الجرائم الإلكترونية، تبرز الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي أبرمت في العام 2010. تأتي في إطار المساعي المستمرة التي تبذلها جامعة الدول العربية لتعزيز التدابير الأمنية لمواجهة الجرائم المرتبطة بتقنية المعلومات، وذلك في سياق الأسس النظامية والبيئة القانونية المعمول بها (المطيري، 2020، ص 1–61)، هذا وإن: " استخدام تكنولوجيا المعلومات لتعديل الحقائق في البيانات بشكل يؤدي إلى إلحاق الضرر، مع نية تقديمها كبيانات صحيحة"[2].

والدول التي أولت اهتمامًا بجريمة التزوير الإلكتروني هي فرنسا، حيث عرفت هذه الجريمة في المادة (1/441) من قانون العقوبات الفرنسي على: " التزوير هو تعديل مضلل للحقيقة باستخدام أي وسيلة أو وثيقة أو أي شكل آخر للتعبير عن الأفكار،

(1) حرص مجلس أوروبا على التصدي للجرائم المعلوماتية من خلال اتفاقية بودابست الموقعة في 2001/11/23 والمتعلقة بالإجرام الكوني وتتضمن 48 مادة.

(2) المادة (10) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

بهدف إثبات حقاً أو واقعة لها آثاراً قانونية. ويتميز هذا الفعل بقدرته على إحداث ضرر"، إن هذا التعريف المذكور يتضمن جميع أشكال التزوير، سواء كان تزويرًا تقليديًا أو تزويرًا إلكترونيً (عبد العال، 2022، ص 50).

وعرف النظام السعودي التزوير في النظام الجزائي الخاص بجرائم التزوير، في الفقرة (1) من المادة (1) بالنص التالي: "التزوير: كل تغيير الحقيقة بإحدى الطرق المقررة في هذا النظام – حدث بسوء نية – قصداً للاستعمال فيما يحميه النظام، ومن شأن هذا التغيير يسبب ضرراً مادياً أو معنوياً أو اجتماعياً لأي شخص ذي صفة طبيعية أو اعتبارية"[1].

ومن العرض السابق لتعريف التزوير الإلكتروني يتضح لنا أن التزوير الإلكتروني هو: " تغيير الحقيقة بأي وسيلة كانت بهدف استبدال الباطل بالحقيقة أو تعديل المحتوى بالحذف أو الإضافة مما يؤدي إلى الإضرار بأي شخص".

المطلب الثاني: خصائص جريمة التزوير الإلكتروني

تُعد جريمة التزوير الإلكتروني من أخطر أنواع الجرائم حيث أنها تتعلق بالثقة العامة وتمس الحياة الشخصية للأفراد، خصوصًا عندما يتعلق الأمر بتزوير مستندات رسمية يقوم بها موظف مُكلف بإعدادها، مثل العقود أو الوثائق الإدارية الخاصة بالجهات الحكومية. وتتميز هذه الجريمة بخصائص معينة تميزها عن باقي الجرائم الإلكترونية.

ولم تصدر المملكة العربية السعودية نظاماً خاصاً لمكافحة جريمة التزوير الإلكتروني، بل أصدرت نظامي التعاملات الإلكترونية وذلك بموجب المرسوم الملكي رقم (م/18) بتاريخ 1428/3/8هـ، ونظام مكافحة الجرائم المعلوماتية بموجب المرسوم الملكي رقم (م/17) بتاريخ 1428/3/8هـ.

وقد قام نظام التعاملات الإلكترونية بتجريم بعض الأفعال في مواده، والتي تُعتبر من قبيل التزوير الإلكتروني أو التي تسهم في ارتكاب تلك الجريمة. كما وضع النظام شروطًا لخدمة التصديق الإلكتروني بهدف حماية التوقيع الإلكتروني وتوفير الضمانات اللازمة لحمايته من التزوير. وقد حدد النظام عقوبات تتناسب مع ارتكاب هذه الأفعال، تشمل السجن والغرامة.

وجريمة التزوير في حد ذاتها تهاجم المصلحة العامة، حيث تهدف إلى الإضرار بالثقة المتوقعة في الوثائق، خصوصًا الرسمية منها. يُنظر إلى المحرر الرسمي على أنه رمز للحقيقة. كما أن جريمة التزوير تُصنف كجريمة وقتية، تنتهي بمجرد حدوث التزوير في الوثيقة المعنية (المغربي، 2014، ص 162 -163).

إن وقوع الجريمة في بيئة رقمية وفضاء افتراضي غير ملموس يضفي عليها بعض خصائصها التي تتميز بها عن الجرائم التقليدية. فارتباط التزوير الإلكتروني بأجهزة الحاسوب والإنترنت يمنحها طابعًا خاصًا يميزها عن باقي الجرائم التقليدية. ولا تقتصر هذه الخصوصية على الجريمة نفسها فحسب، بل تمتد لتشمل أيضًا مرتكب الجريمة والمجني عليه.

1- التزوير الإلكتروني عابرة للحدود:

إن تعبير "الجريمة العابرة للدول أو الجريمة عابرة الحدود أو الجرائم عبر الوطنية" تُعرف بتلك التي تمتد عبر عدة دول، مما يعني أنها لا تتقيد بالحدود الجغرافية للدول. في عصر الحواسيب وانتشار شبكة الإنترنت العالمية، أصبح من الممكن ربط عدد هائل من الحواسيب حول العالم بهذه الشبكة، مما يسهل عملية التنقل والتواصل بينها، شريطة تحديد عنوان المستلم أو معرفة كلمة المرور. ويحدث ذلك سواء بطرق قانونية أو غير قانونية (الزغبي والمناعسة، 2010، ص 91).

(1) المادة (1) من النظام الجزائي السعودي لجرائم التزوير الصادر عام 1435هـ.

وفي ظل هذه الظروف، يمكن تصنيف الجرائم التقنية على أنها جرائم عابرة للحدود، حيث يكون الجاني في دولة ما، والمجني عليه في دولة أخرى، وقد يتسبب الضرر في دولة ثالثة في الوقت ذاته. لذلك، تُعتبر الجرائم الإلكترونية نوعاً جديداً من الجرائم الوطنية أو الإقليمية أو القارية.

وتعتبر الجريمة الإلكترونية عابرة للقارات، لأنها لا حدود لها بين البلدان أو القارات. فهي تمثل شكلاً جديداً والتي تتجاوز الحدود الإقليمية بين جميع دول العالم. من خلال نظم المعلومات، يمكن ارتكاب مجموعة متنوعة من الجرائم ذات قدرة تقنية معلوماتية قادرة على تقليص المسافات والتواصل بين العالم قد أثرت أيضاً على طبيعة الجرائم، حيث يلجأ المجرم إلى استخدام هذه التقنية في انتهاك القانون. وهذا يعني أن نطاق الجريمة الإلكترونية لم يعد محلياً، بل أصبح عالمياً (إبراهيم، 2009، ص 77).

2- جريمة التزوير الإلكتروني تتصف بالخفاء:

تتميز الجرائم الإلكترونية بالسرية، حيث تفتقر إلى أثراً مادياً يمكن تتبعه. وتعتبر خطرة وصعبة في تحديد موقع حدوثها أو مكان التعامل معها، نتيجة لتوسع نطاقها الجغرافي وكثرة البيانات المعنية (إبراهيم، 2009، ص 79).

وجريمة التزوير الإلكتروني متميزة في أنها لا تترك أي أثر مادي على الوثيقة المزورة، إذ يحدث تعديل محتوى المعلومات حال الوصول إليها، مما يجعلها جريمة فنية وغير ملموسة. وبالتالي، يصعب العثور على دليل مادي يثبت وقوع التزوير، حيث تتم هذه الجريمة في بيئة افتراضية، وإذا تم اكتشافها، فإن ذلك غالبًا ما يحدث بالصدفة (السيراني، 2011، ص 66).

وهذه الجرائم لا تترك أي أثر واضح بعد حدوثها، بالإضافة إلى صعوبة الاحتفاظ بأي آثار فنية قد تظهر، إن وجدت. فهي لا تترك بصمات، بل تتحول إلى أرقام تتغير في السجلات. نتيجة لذلك، يتم اكتشاف معظم الجرائم الإلكترونية بالصدفة وبعد فترة طويلة من وقوعها. تعتبر هذه الجرائم من الأنواع الحديثة التي تفتقر إلى الشهود القابلين للاستجواب أو الأدلة المادية القابلة للفحص، مما يزيد من صعوبة الكشف عنها (إبراهيم، 2009، ص 80).

وتزداد صعوبة الحفاظ على الآثار الفنية للجريمة، مما يعيق عملية الإثبات في هذا النوع من الجرائم، بسبب صعوبة الوصول إلى الأدلة غير المرئية باستخدام وسائل الحماية الفنية. غالبًا ما تكون هذه الأدلة مشفرة أو مرمزة، كما هو الحال عندما يستخدم المجرم المعلوماتي كلمات سر أو يضيف تعليمات خفية أو يقوم بترميز المعلومات (هروال نبيلة، 2014، ص 49).

ويجب الإشارة إلى أن اكتشاف العديد من تلك الجرائم يُكتشف بالصدفة. ومن الأسباب التي تؤدي إلى اختفاء هذه الجرائم هو إحجام الضحايا عن الإبلاغ عنها، فنجد أن أغلب الجهات التي تتعرض أنظمتها المعلوماتية للاختراق تكتفي عادة باتخاذ الإجراءات الإدارية الداخلية، دون إبلاغ الجهات المختصة، حتى لا تضر بسمعتها ومكانتها (هروال، 2014، ص 49)، خصوصاً عندما يكون الضحية مؤسسات مالية مثل البنوك والمؤسسات الادخارية، حيث تخشى مجالس إدارتها عادة من أن تؤدي الدعاية السلبية الناتجة عن كشف هذه الجرائم أو اتخاذ إجراءات قانونية بشأنها إلى تراجع الثقة فيها من قبل المتعاملين، مما قد يدفعهم إلى الابتعاد عنها (رستم، 1994، ص 146).

ويتطلب الكشف عن جرائم التزوير الإلكتروني استخدام استراتيجيات تحقيق وتدريب متخصصة. يتعين أن تتوفر خبرة فنية تتناسب مع طبيعة هذه الجرائم، مما يساعد على فهم الخصوصيات والأساليب المستخدمة في ارتكابها. نتيجة لذلك، وجدت أجهزة العدالة، بما في ذلك الضبطية القضائية، جهات التحقيق، والقضاة، نفسها غير قادرة على التعامل مع هذا النوع الجديد والفريد من الإجرام باستخدام الوسائل الاستدلالية والإجراءات التقليدية، مما أدى إلى عدم القدرة على مواجهتها بفعالية (رستم، 1994، ص 27).

وقد يفتقر البعض إلى المهارة والاحترافية في التعامل مع الأدلة الإلكترونية، مما قد يؤدي، عن غير قصد أو بسبب خطأ، إلى إتلاف أو تدمير هذه الأدلة، كما يحدث عند حذف البيانات المخزنة. كما يتجاهل المحقق الأدلة الإلكترونية تمامًا، معتقدًا أنها غير ذات أهمية، أو قد يفشل في مصادرة الأجهزة المستخدمة في ارتكاب الجريمة أو ملحقاتها (إبراهيم، 2009، ص 81).

هذا ومما يجعل من الصعب التعرف على مرتكبيها. قد يلجأ الجاني إلى استخدام اسم مستعار أو تنفيذ جريمته من خلال إحدى مقاهي الإنترنت. وبالتالي، فإن جرائم التزوير تُرتكب دون تحديد هوية الشخص المسؤول أو ضبط الوثيقة المزورة (هروال نبيلة، 2014، ص 52–53).

3- تفرد الشخصية للمجرم ودوافعه:

تُرتكب جريمة التزوير الإلكتروني باستخدام تقنيات متقدمة، مما يتطلب من مرتكبها امتلاك خبرة وتخصص في المجال الإلكتروني، حيث يتعامل مع أجهزة الكمبيوتر وأنظمة المعالجة الآلية للبيانات. قد يكون هذا المجرم الإلكتروني موظفًا متخصصًا في تقنية المعلومات، ويُعتبر من بين أبرز مجرمي المعلوماتية، أو قد يكون من القراصنة أو المخترقين، وهم أفراد يستغلون الحاسوب بطرق غير قانونية. وتنقسم هذه الفئة إلى نوعين: الهاكرز القراصنة الهواة، والكراكزة الذين يُعتبرون قراصنة محترفين (حسين، 2011، ص 96).

ويُعتبر التزوير الإلكتروني من الجرائم التي يُخطط لها من قبل أشخاص يمتلكون مهارات فنية عالية وخبرة وذكاء. تتميز هذه الجريمة بطابعها الذهني والعلمي، حيث تعتمد على المعلومات والمعرفة التقنية والتكنولوجية التي أفرزها التقدم العلمي والحضاري. وبالتالي، إذا حدثت جريمة التزوير عن طريق الخطأ أو بالصدفة، يمكن تصور وجود عقوبة لها، إلا إذا كانت قد ارتكبت عمدًا، حيث قد يغفل بعض الموظفين عن تسجيل أمر معين دون قصد (الجبوري، 2017، ص 19).

المبحث الثاني: صور جريمة التزوير في المعاملات الإلكترونية والعقوبات المقررة لها

إن تغيير الحقيقة هو الركن الأساسي لجريمة التزوير، فإذا غاب هذا الركن فلا يمكن اعتبار الفعل جريمة تزوير، ولا ترتكب جريمة التزوير حتى ولو اعتقد هذا الشخص أن هذه المعلومات غير صحيحة، أو حتى ولو نتج عن فعله ضرر للغير (عبد الستار، 1988، ص 245).

ويأتي التزوير الإلكتروني في أشكال متعددة، فقد يتضمن مستندات مثل المحررات، العقود، بطاقات الهوية، جوازات السفر، شهادات الميلاد، أو شهادات الوفاة. كما يمكن أن يشمل أيضًا الرسائل، سواء كانت تقليدية أو إلكترونية، ويمكن أن يتخذ شكل بطاقات إلكترونية مثل بطاقات التأمين الصحي، بطاقات التعريف، والبطاقات الائتمانية وغيرها.

ويمكن تصور حدوث التزوير الإلكتروني من خلال تعديل الحقائق على الشرائط أو الوثائق التي تمثل مخرجات الحاسب الآلي. يتطلب هذا التغيير في البيانات الموجودة على الجهاز، شرط أن يترتب عليه ضرر بفقدان الثقة في الوثائق عند حدوث التزوير الإلكتروني في المستندات الرسمية، أو أن يلحق الضرر بأحد الأفراد في حالة التزوير الإلكتروني في المستندات العرفية (حجازي، 2009، ص 202).

وقد نصت الفقرة (6) من المادة (23) من نظام المعاملات الإلكترونية السعودي على: "أنه يعد مخالفة لأحكام هذا النظام القيام بأى عمل من الأعمال الآتية: وذكرت منها: تزوير السجل الإلكتروني، أو التوقيع الإلكتروني، أو شهادة التصديق الرقمي أو استعمال أي من ذلك مع العلم بتزويره، وهكذا لم يتعامل مع جريمة التزوير الإلكتروني كجريمة مستقلة، وإنما أشار إلى

مجموعة من الأفعال التي قد تندرج تحت مفهوم الاحتيال الإلكتروني، ويتضح من النصوص أن النظام فرق بين جريمة التزوير التي تقع في السجل، أو التوقيع أو شهادة التصديق، وبين استعمال الأشياء التي وقع عليها التزوير، وإن كان قد قرر لها نفس العقوبة"[1].

المطلب الأول: صور التزوير في المحررات الإلكترونية

من المهم الإشارة إلى أن نظام مكافحة التزوير في المملكة العربية السعودية لا يحتوي على أي نص يذكر بشكل صريح الأفعال المتعلقة بالمستندات الإلكترونية. على الرغم من أنه يتناول تزوير الأوراق الرسمية والسندات والتوقيعات، إلا أن ذلك يقتصر على الأوراق التقليدية ولا يشمل السندات الإلكترونية (المغربي، 2020، ص 452).

أولاً: نشر أو استخدام شهادة تصديق إلكتروني مزورة (حجازي، 2011، ص 465):

- **الصورة الأولى:** في هذه الحالة، يقوم الجاني بنشر أو استخدام شهادة تصديق إلكتروني مزعوم صدورها من مزود خدمات تصديق معين، حيث يظهر اسمه في الشهادة رغم أنها لم تصدر عنه. ويتحقق فعل النشر من خلال توزيع بيانات ومحتوى الشهادة عبر إرفاقها برسالة إلكترونية، والتواصل مع آخرين من خلال البريد الإلكتروني.
- **الصورة الثانية:** يقوم الجاني باستخدام شهادة تصديق إلكتروني تم إيقافها أو إلغاؤها، ما لم يكن الاستخدام بهدف التحقق من التوقيع الإلكتروني أو الرقمي وتم استخدامه قبل صدور القرار بالإيقاف أو بالإلغاء.
- **الصورة الثالثة:** تتمثل الحالة في استخدام الجاني لشهادة تصديق ملغاة أو موقوفة بشكل مؤقت، ما لم يكن الهدف من استخدامها هو التحقق من التوقيع الإلكتروني أو الرقمي تم استخدامه قبل صدور قرار بالإلغاء أو بالوقف.

ثانياً: تزوير التوقيع الإلكتروني:

يتم تزوير التوقيع الإلكتروني بطرق مختلفة تمامًا، حيث يكون التوقيع المزور مطابقًا تمامًا للتوقيع الأصلي. يتم ذلك من خلال سرقة نظام التوقيع الإلكتروني عبر التجسس الإلكتروني والتلصص، مما يتيح للجهة المهاجمة الحصول على التوقيع الإلكتروني واستخدامه في توقيع الوثائق والمحررات. وعلى الرغم من أن التوقيع الإلكتروني يبدو سليمًا عند مقارنته بالتوقيع الأصلي، إلا أنه لا يُعتبر صادرًا عن مالك نظام التوقيع الإلكتروني، بل هو صادر عن شخص آخر تمكن من اختراق النظام وسرقة بيانات التوقيع (السيراني، 2011، ص 40).

ويمكن التغلب على هذه المشكلة من خلال استخدام ما يُعرف بالتوقيع الرقمي، الذي يُساهم بشكل كبير في تقليل تزوير التوقيع الإلكتروني بفضل قدرته على تحديد هوية الشخص الذي قام بالتوقيع (Christensen & Duncan, 2003, p. 8).

ثالثاً: تزوير البطاقة الائتمانية:

على الرغم من أن تزوير البطاقات الائتمانية يُعتبر من أخطر أشكال التزوير الإلكتروني، نظرًا لما يشكله من خطر مباشر على حسابات عملاء البنوك، والتي أصبحت الوسيلة الأكثر شيوعًا في عمليات الدفع، إلا أن المشرع السعودي لم يتناول هذه الجريمة بالتجريم بشكل خاص. وبالتالي، تطبق المحاكم أحكام الأنظمة الجزائية الأخرى، مثل نظام التزوير، والتي قد تكون غير كافية لمكافحة هذه الجريمة بفعالية. لذا، يُعتبر تزوير البطاقات الائتمانية من أكبر التهديدات التي تواجه بيئات العمل في الوقت الراهن (Bhatla, Prabhu, & Dua, 2002, p. 1).

(1) الفقرة (6) من المادة (23) من نظام التعاملات الإلكترونية السعودي، الصادر بالمرسوم الملكي رقم (م/18) وتاريخ 1428/3/8هـ.

ويعتبر تزوير البطاقة الائتمانية أحد أشكال التزوير المالي. وبالتالي، يمكن تعريف التزوير المالي بأنه نوع من الاحتيال الذي يستهدف المؤسسات أو المنظمات التي تدير رؤوس أموال كبيرة. وفي هذه الحالة، يتمثل الاحتيال في سرقة الأموال باستخدام بطاقات الائتمان أو بطاقات الخصم (Bergman, 2005, p. 20). وانتحال الهوية والتزوير المالي من أبرز أشكال الاحتيال الإلكتروني. وقد أظهرت إحدى المؤسسات البحثية في الولايات المتحدة أن حوالي 10 ملايين بالغ في البلاد وقعوا ضحايا لسرقات الهوية في عام 2005، مما أدى إلى خسائر تقدر بنحو 15 مليار دولار. كما أصبح انتحال الهوية واحدًا من أبرز خمس مخاطر تهدد الأمن في البيئات الافتراضية (Butler, 2007, p. 517).

ويقوم الجناة بتزوير بطاقات الائتمان، حيث تُعتبر من أكثر وسائل الدفع شيوعاً في الوقت الحالي، ويستخدمونها في عمليات الدفع. ويمكن تلخيص أبرز أساليب الاحتيال التي تتم من خلال البطاقات الائتمانية فيما يلي (بصلة، 2002، ص 100):

1- تحميل العميل لفواتير مزيفة.

2- استخدام خدمات الصراف الآلي لإيداع الشيكات التي لا يوجد عليها رصيد، بحيث يتم إضافة قيمة الشيك إلى رصيد الحساب الأصلي، ثم سحب المبالغ المضافة عبر الصراف الآلي قبل المقاصة بين البنوك.

3- التحايل على أجهزة التحقق من الهوية.

4- استخدام أوراق هوية مزورة للحصول على بطاقات ائتمانية صالحة.

5- سرقة بطاقات الائتمان السارية، أو الحصول على الأرقام السرية لأصحابها الحقيقيين أثناء إرسالها من البنوك إلى العملاء عبر موظفي البريد.

6- الاحتيال باستخدام أجهزة المودم لاكتشاف كلمة المرور أو المفتاح السري للوصول إلى أرقام بطاقات الائتمان المصرفية.

7- إمكانية اختراق النظام وحساب أرقام الهوية الشخصية بأرقام بطاقات مطابقة لبيانات العملاء، واستخدام بطاقات مزورة.

8- قيام حامل البطاقة، أو شخص آخر حصل عليها بعد انتهاء صلاحيتها، بكشط وتعديل تاريخ صلاحية البطاقة المطبوعة.

وتتم عملية تزوير بطاقات الائتمان عن طريق إنشاء أرقام بطاقات تتبع بنك معين، وذلك من خلال إدخال الرقم الخاص بالبنك المصدر للبطاقة إلى الحاسوب باستخدام برامج تشغيل متخصصة. بعد ذلك، يتم استخدام البطاقة المزورة التي لها مستخدم أصلي لإجراء مختلف العمليات المالية. هذا الأمر قد يؤدي إلى تعرض بعض حاملي البطاقات الأصلية لمشكلات نتيجة استخدام بطاقاتهم أو بطاقات مشابهة في عمليات الشراء. وقد لاحظت بعض البنوك تكرار شكاوي حاملي بطاقات الدفع الإلكتروني بشأن عمليات لم يقوموا بها، وتبين أن هذه العمليات تمت عبر الإنترنت بواسطة قراصنة يمتلكون تقنيات تمكنهم من الحصول على أرقام بطاقات العملاء واستخدامها في عمليات الشراء (السيراني، 2011، ص 42).

وتباينت آراء الفقهاء حول التكييف القانوني لاستخدام بطاقة الائتمان المزورة، ويمكننا التمييز بين وصفين رئيسيين هما (الخن، 2011، ص 97):

1- يعتقد أصحاب الرأي الأول أن استخدام البطاقة المزورة في سحب النقود يعد جريمة سرقة باستخدام مفتاح مصطنع، حيث يتم سحب المال من حساب المصرف المجني عليه دون موافقته. تعتبر البطاقة المزورة والرقم السري بمثابة المفتاح المصطنع. كما أن قانون العقوبات لم يحدد بشكل دقيق مفهوم المفتاح المصطنع. ومع ذلك، يرد فقهاء آخرون على هذا الرأي بأن التسليم الإرادي أثناء عملية السحب ينفي وجود العنصر الأساسي لجريمة السرقة. بالإضافة إلى ذلك، لا يمكن مقارنة بطاقات الائتمان بالمفتاح المصطنع.

2- يرى مؤيدو هذا الرأي أن من يستخدم بطاقة مزورة للسحب أو للدفع لدى أحد التجار يُعتبر مسؤولاً عن جريمة الاحتيال، حيث إن استخدام البطاقة يعد وسيلة خداع تهدف إلى إقناع التاجر بوجود ائتمان وهمي، كما يتضمن ذلك استخدام اسم كاذب وصفة غير صحيحة.

المطلب الثاني: العقوبات المقررة لجريمة التزوير الإلكتروني:

مع تطور الجرائم الإلكترونية، التي أصبحت تهدد أمن وسلامة الأفراد والدول، أصبح المجرم الإلكتروني أكثر خطورة وحركة من السابق. كما أن دخول التقنيات الحديثة إلى عالم الجريمة ساهم في تسهيل العديد من الأنشطة الإجرامية.

وتتكون الشبكات الإلكترونية من أجهزة الكمبيوتر المحلية المتصلة ببعضها عبر الشبكات الإقليمية والعالمية. وقد ساهم هذا الربط، عند استخدامها في الأنشطة الإجرامية الإلكترونية، تنشأ العديد من القضايا القانونية المتعلقة بمواجهة هذه الأنشطة. ومن أبرز التحديات التي تبرز في هذا السياق هي مسائل الاختصاص، والمعاينة، والتفتيش، والضبط، والإثبات (بركات ميساء، 2009، ص 82).

وتُطرح في هذا السياق عدة تساؤلات عن الآليات التي ينبغي اتباعها لصياغة الأحكام القانونية الهادفة إلى ردع مثل هذه الجرائم، والتي تتيح للمحاكم الحق في النظر في القضايا المتعلقة بعمليات التزوير الإلكتروني.

ونصت المادة (23) من نظام التعاملات الإلكترونية السعودي على الأفعال التي تُعتبر مخالفات وفقًا لهذا النظام. وقد شملت مجموعة من الأفعال حسب النظام التي تُصنف كجرائم تزوير، بالإضافة إلى أفعال تسهم في تسهيل أو تيسير تلك الخدمات، وهذه الأفعال هي[1]:

1- مزاولة نشاط تقديم خدمات التصديق دون الحصول على ترخيص من الهيئة.
2- استغلال المعلومات التي جمعها مقدم خدمات التصديق عن طالب الشهادة لأغراض غير إطار أنشطة التصديق دون موافقة كتابية أو إلكترونية من صاحبها.
3- إفشاء المعلومات التي اطلع عليها مقدم خدمات التصديق بحكم عمله ما لم يأذن له صاحب الشهادة -كتابة أو إلكترونياً- بالإفصاح عنها أو في الحالات التي يسمح له النظام بذلك.
4- تقديم بيانات كاذبة أو معلومات مضللة من قبل مقدم خدمات التصديق للهيئة أو أي إساءة استخدام لخدمات التصديق.
5- إنشاء أو نشر أو استخدام شهادة رقمية أو توقيع إلكتروني لغرض احتيالي أو لأي غرض غير قانوني.
6- تزوير سجل إلكتروني أو توقيع إلكتروني أو شهادة تصديق رقمية أو استعمال أي منها مع العلم بتزويرها.
7- تقديم معلومات كاذبة عمداً لمقدم خدمات التصديق أو تقديم معلومات كاذبة عمداً عن التوقيع الإلكتروني لأي من الأطراف التي صدقت على ذلك التوقيع بموجب هذا النظام.
8- الدخول إلى نظام التوقيع الإلكتروني الخاص بشخص آخر دون تصريح أو نسخه أو إعادة بنائه أو الاستيلاء عليه.
9- انتحال شخصية شخص آخر أو الادعاء زوراً بأنه مخول بطلب أو قبول شهادة مصادقة رقمية أو طلب إيقاف أو إلغاء عملها.
10- نشر شهادة مصادقة رقمية مزورة أو غير صحيحة أو ملغاة أو موقوفة أو إتاحتها لشخص آخر مع علمه بحالتها، باستثناء حق مقدم خدمات المصادقة المذكور في الفقرة (4) من المادة (الثامنة عشرة).

(1) المادة (23) من نظام التعاملات الإلكترونية السعودي، الصادر بالمرسوم الملكي رقم (م/18)، وتاريخ 1428/3/8هـ.

وكذلك نصت المادة (24) من نظام التعاملات الإلكترونية على أنه: "مع عدم الإخلال بأى عقوبة أشد ينص عليها في نظام آخر، يعاقب كل من يرتكب أياً من الأعمال المنصوص عليها في المادة الثالثة والعشرين من هذا النظام، بغرامة لا تزيد على خمسة ملايين ريال، أو بالسجن مدة لا تزيد على خمس سنوات أو بهما معاً، ويجوز الحكم بمصادرة الأجهزة، والمنظومات، والبرامج المستخدمة في ارتكاب المخالفة"[1].

ونظرًا لأن مواد التجريم في الأنظمة السعودية يجب أن تتماشى مع أحكام الشريعة الإسلامية، يتبين من خلال نص المادة السابقة أن النظام قد اعتمد العقوبات الأساسية التالية:

1- غرامة لا تزيد على خمسة ملايين ريال:

الغرامة هي إحدى العقوبات المنصوص عليها في الشريعة الإسلامية، فقد روى عن رسول الله ﷺ أنه سئل عن الثمر المعلق؛ فقال: "من أصاب بفيه من ذي حاجة غير متخذ خبنه فلا شيء عليه، ومن خرج بشيء منه، فعليه غرامة مثليه والعقوبة، ومن سرق منه شيئاً بعد أن يؤويه الجرين فبلغ ثمن المجن فعليه القطع" (أبو داود السجستاني: سنن أبي داود، تحقيق: شعيب الأرناؤوط، ومحمد كامل قرة بللي، 2009، 13/3).

2- السجن مدة لا تزيد على خمس سنوات:

إن السجن من العقوبات التعزيرية التي لم يشرعها الشرع، وإنما العقوبة التعزيرية هي ما يراه الحاكم من العقوبات المناسبة للجريمة، يقول الإمام الحصكفي – رحمه الله – إلى أن التعزير يكون بالحبس، والصفع على العنق، وفرك الأذن، وبالكلام العنيف، وبنظر القاضي له بوجه عبوس، وشتم بغير القذف – أي شتم لا يصل إلى حد القذف، لا يجوز التعزير بأخذ مال في المذهب، وقيل يجوز، ومعناه أن يمسكه مدة لزجره ثم يعيده له فإن يأس من توبته صرفه إلى ما يرى، وفي المجتبى أنه كان في ابتداء الإسلام ثم نسخ (الحصكفي الحنفي: الدر المختار شرح تنوير الأبصار وجامع البحار، تحقيق: عبد المنعم خليل إبراهيم، 2002، ص 316).

3- السجن والغرامة:

يمكن أن تصل الجريمة إلى مستوى يستدعي تشديد العقوبة على الجاني بما يتجاوز العقوبة السجنية. لذا، فإن المادة المذكورة تتيح للمحكمة إمكانية الجمع بين عقوبة السجن وعقوبة الغرامة.

4- مصادرة الأجهزة والمنظومات والبرامج المستخدمة في ارتكاب الجريمة:

تنص المادة السابقة على جواز مصادرة الأجهزة والأنظمة والبرامج المستخدمة في ارتكاب الجريمة، وقد اختلفت آراء الفقهاء في مشروعية هذه المصادرة، إلا أن الرأي السائد هو أن المصادرة تعتبر مشروعة في الفقه الإسلامي.

يقول الإمام بن تيمية – رحمه الله – أن مذهب مالك، وأحمد وغيرهما: "أن العقوبات المالية كالبدنية تنقسم إلى ما يوافق الشرع، وإلى ما يخالفه، وليست العقوبة المالية منسوخة عندهما، والمدعين للنسخ ليس معهم حُجة بالنسخ لا من كتاب، ولا من سنة، وهذا شأن كثير ممن يخالف النصوص الصحيحة، والسنة الثابتة بلا حجة إلا مجرد دعوى النسخ، وإذا طولب بالناسخ لم يكن معه حجة لبعض النصوص توهمه ترك العمل، إلا أن مذهب طائفته ترك العمل بها إجماع، والإجماع دليل على النسخ، ولا ريب أنه إذا ثبت الإجماع كان ذلك دليلاً على أنه منسوخ، فإن الأمة لا تجتمع على ضلالة، ولكن لا يعرف إجماع على ترك نص،

(1) المادة (24) من نظام التعاملات الإلكترونية السعودي، الصادر بالمرسوم الملكي رقم (م/18)، وتاريخ 1428/3/8هـ.

إلا وقد عرف النص الناسخ له، ولهذا كان أكثر من يدعي نسخ النصوص بما يدعيه من الإجماع، إذا حقق الأمر عليه لم يكن الإجماع الذي ادعاه صحيحاً، بل غايته أنه لم يعرف فيه نزاعاً (ابن تيمية، د.ت، ص 50).

3. الخاتمـــــة:

تناولت الدراسة الحالية مجموعة من المفاهيم والخصائص المرتبطة بالتزوير الإلكتروني، موضحةً طبيعة هذا النوع من التزوير والعقوبات المقررة له. كما توصلت إلى أبرز النتائج والتوصيات، وذلك على النحو التالي:

أولاً: النتائج:

1- شهد النظام السعودي تطوراً ملحوظاً في مواجهة الجرائم الإلكترونية، وجرائم التزوير الإلكتروني.

2- تُعتبر جريمة التزوير الإلكتروني تهديداً كبيراً على الأصعدة الاقتصادية والسياسية والاجتماعية، وذلك بسبب انتشار التعاملات الإلكترونية وزيادة الاعتماد على التكنولوجيا في المستقبل.

3- تتراوح عقوبة التزوير الإلكتروني في النظام السعودي بين الغرامة والسجن لمدة لا تتجاوز خمس سنوات، أو تطبيق العقوبتين معاً، بالإضافة إلى عقوبة تكميلية تتمثل في مصادرة الأجهزة والبرامج والنظم المستخدمة في ارتكاب الجريمة.

4- لا يوجد في المملكة العربية السعودية قانون أو نظام خاص بمكافحة جريمة التزوير الإلكتروني، مما يفرض الاعتماد بشكل كبير على القوانين الأخرى المتعلقة بالتعاملات الإلكترونية أو جرائم التزوير في الوثائق التقليدية.

ثانياً: التوصيات:

1- من الضروري توضيح الأحكام المتعلقة بمكافحة جريمة التزوير الإلكتروني، وذلك بالاستعانة بالخبراء الفنيين في مجال التكنولوجيا لتحديد الأفعال التي تندرج تحت جرائم التزوير الإلكتروني.

2- يجب الرقابة الصارمة على الجهات المصدرة لشهادات التوثيق لضمان التزامها بالمعايير المطلوبة، بالإضافة إلى ضرورة إصدار قانون خاص لمكافحة جرائم التزوير الإلكتروني، يتضمن العديد من صور التزوير الإلكتروني لتعزيز الثقة في المحررات الإلكترونية وحماية المعاملات التي تتم عبر الوسائل الإلكترونية.

3- ينبغي تعزيز التعاون على المستويين العربي والدولي للحد من جريمة التزوير الإلكتروني.

4- ضرورة العمل على زيادة الوعي المجتمعي بشأن مكافحة جريمة التزوير الإلكتروني، حفاظاً على الأمن والسلم الاجتماعي.

5- من الضروري تطوير البرامج الإلكترونية للتصدي لاختراق المعلومات والبيانات الشخصية، وكذلك لتتبع مرتكبي جرائم التزوير الإلكتروني والقبض عليهم.

4. المراجـــــع

أولاً: القرآن الكريم:

1- سورة الحج: الآية 30.

ثانياً: المعاجم:

1- ابن تيمية، أحمد بن عبد الحليم (د.ت): الحسبة في الإسلام أو وظيفة الحكومة الإسلامية، دار الكتب العلمية، بيروت.

2- أبو داود، سليمان بن الأشعث الأزدي السجستاني (2009): سنن أبي داود، تحقيق: شعيب الأرناؤوط، ومحمد كامل قرة بللي، دار الرسالة العالمية، بيروت، 13/3.

3- الحصكفي، محمد بن على بن محمد بن على بن عبد الرحمن الحنفي (2002): الدر المختار شرح تنوير الأبصار وجامع البحار، تحقيق: عبد المنعم خليل إبراهيم، دار الكتاب العلمية، بيروت.

4- الرازي، أحمد بن فارس القزويني (1399هـ): معجم مقاييس اللغة 63/3، دار الفكر.

5- الزبيدي (1422هـ): تاج العروس 461/11، ط1، الطبعة الكويتية.

6- الصحاح للجوهري 672/2، مجمل اللغة لابن فارس 444/1.

7- العسكري، أبو هلال الحسن بن عبد الله (1997): الفروق اللغوية، تحقيق: محمد إبراهيم سليم، دار العلم والثقافة للنشر والتوزيع، القاهرة.

8- قلعجى، محمد رواس، وقنيبي، حامد صادق (1408هـ): معجم لغة الفقهاء، دار النفائس للطباعة والنشر والتوزيع، ط2.

ثالثاً: الكتب:

1- إبراهيم، خالد ممدوح (2009): الجرائم المعلوماتية، ط1، دار الفكر الجامعي، مصر.

2- تمام، أحمد حسام طه (2000): الجرائم الناشئة عن استخدام الآلي، دراسة مقارنة، ط1، دار النهضة العربية، مصر.

3- تمام، أحمد حسام طه (2000): الجرائم الناشئة عن استخدام الحاسب الآلي، الحماية الجنائية للحاسب الآلي، دراسة مقارنة، دار النهضة العربية، القاهرة.

4- حجازي، عبد الفتاح بيومى (2002): الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت: دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، القاهرة.

5- حجازي، عبد الفتاح بيومى (2009): مكافحة جرائم الكمبيوتر والإنترنت، ط1، دار النهضة العربية، القاهرة.

6- حجازي، عبد الفتاح بيومى (2011): الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، المركز القومي للإصدارات القانونية، القاهرة.

7- حجازي، عبد الفتاح بيومي (2004): الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر.

8- حسبو، عمرو أحمد (2000): حماية الحريات في مواجهة نظم المعلومات، دراسة مقارنة، دار النهضة العربية، مصر.

9- حسين، أسامة سمير (2011): الاحتيال الإلكتروني الوجه القبيح للتكنولوجيا، ط1، الجنادرية للتوزيع، الأردن.

10-حمودة، على محمود على (2003): شرح قانون العقوبات – القسم الخاص.

11-الخن، محمد طارق عبد الرؤوف (2011): جريمة الاحتيال عبر الإنترنت، منشورات الحلبي الحقوقية، بيروت.

12-رستم، هشام فريد (1994): الجوانب الإجرائية للجرائم المعلوماتية – دراسة مقارنة، د.ط، مكتبة الآلات الحديثة، مصر.

13-الزغبي، جلال محمد، والمناعسة، أسامة أحمد (2010): جرائم تقنية المعلومات الإلكترونية، دراسة مقارنة، ط1، دار الثقافة للنشر والتوزيع، الأردن.

14-زين الدين، بلال أمين (2008): جرائم نظم المعالجة الآلية للبيانات، ط1، دار الفكر الجامعي، الإسكندرية.

15-سرور، أحمد فتحي (1991): الوسيط في قانون العقوبات، القسم الخاص، ط4، دار النهضة العربية.

16-سعد، عبد العزيز (2005): جرائم التزوير وخيانة الأمانة واستعمال المزور، ط1، دار هومة، الجزائر.

17-السيرانى، عبد الله بن سعود محمد (2011): فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، ط1، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية.

18-عبابنة، محمود أحمد (2009): جرائم الحاسوب، وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان.

19-العبادى، محمد حميد الرصفان (2015): الجرائم المستحدثة في ظل العولمة، ط1، دار جليس الزمان، عمان.

20-عبد الستار، فوزية (1988): شرح قانون العقوبات – القسم الخاص، دار النهضة العربية، القاهرة.

21-عبيد، رؤوف (2016): جرائم التزييف والتزوير، ط2، مكتبة الوفاء القانونية، الإسكندرية.

22-العبيدي، صدام حسين ياسين، العبيدي، عواد حسين ياسين (2020): أحكام جرائم التزوير التقليدي والإلكتروني في الفقه الإسلامي والقانون الوضعي، ط1، المركز العربي للنشر والتوزيع، مصر.

23-غازي، محمود إبراهيم (2014): الحماية الجنائية للخصوصية والتجارة الإلكترونية، ط1، مكتبة الوفاء القانونية، الإسكندرية، مصر.

24-فتيحة، عمارة (2019): جريمة التزوير الإلكترونية، مجلة القانون والمجتمع، مج1، ع1.

25-القاضي، محمد محمد مصباح (2013): قانون العقوبات – القسم الخاص – في الجرائم المضرة بالمصلحة العامة وجرائم الاعتداء على الأشخاص، ط1، منشورات الحلبي الحقوقية، بيروت.

26-مراد، عبد الفتاح (2011): شرح جرائم التزييف والتزوير، الإسكندرية.

27-المغربي، طه عثمان (2014): النظام الجزائي الخاص في المملكة العربية السعودية، مكتبة الرشد.

28-هلال، محمد رضوان (1996): بحوث وآراء جديدة في مجال كشف التزييف والتزوير، عالم الكتب للنشر، القاهرة.

رابعاً: الرسائل العلمية:

1- الجبوري، عمر عبد السلام حسين (2017): جريمة التزوير الإلكتروني في التشريع الأردني، رسالة ماجستير، جامعة الشرق الأوسط، الأردن.

2- حفظي، عباس (2015): جرائم التزوير الإلكتروني، رسالة دكتوراه، جامعة وهران، الجزائر.

3- الجبوري، عمر عبد السلام حسين (2017): جريمة التزوير الإلكتروني في التشريع الأردني (دراسة مقارنة)، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط.

4- عباس، حفصي (2015): جرائم التزوير الإلكتروني، رسالة دكتوراه في القانون، جامعة وهران، الجزائر.

5- العفيفي، يوسف خليل (2013): الجرائم الإلكترونية في التشريع الفلسطيني، رسالة ماجستير في القانون العام، الجامعة الإسلامية، غزة.

6- الجبوري، عمر عبد السلام (2017): جريمة التزوير الإلكتروني في التشريع الأردني، رسالة ماجستير، جامعة الشرق الأوسط، الأردن.

7- هروال، نبيلة هبة (2014): جرائم الإنترنت – دراسة مقارنة، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، الجزائر.

8- بركات، ميساء مصطفى (2009): جرائم التعدى على المعلوماتية (الإتلاف والتزوير)، رسالة ماجستير، كلية الحقوق، جامعة بيروت العربية، بيروت.

خامساً: المجلات العلمية والندوات والمؤتمرات:

1- خليفة، فتحية، وصالح، مهداوى محمد (2022): التزوير المعلوماتي في البيئة الرقمية، مجلة الدراسات القانونية، مج8، ع2، الجزائر.

2- عقاد، محمد (1993): جريمة التزوير في محررات الحاسب، دراسة مقارنة، بحث مقدم في المؤتمر السادس المنعقد خلال الفترة من 25 – 1993/10/28، الجمعية المصرية للقانون الجنائى، دار النهضة العربية.

3- العارضي، فرقد عبود (2012): جريمة التزوير الإلكتروني، مجلة الكوفة للعلوم السياسية والقانونية، ع13، جامعة الكوفة، العراق.

4- غنام، محمد، غنام (2000): مكافحة جرائم الكمبيوتر، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مؤتمر القانون والكمبيوتر والإنترنت.

5- القهوجي، على (2000): الحماية الجنائية للبيانات المعالجة إلكترونياً، مؤتمر القانون والكمبيوتر والإنترنت المنعقد خلال الفترة من 1 – 2000/5/3، كلية الشريعة والقانون، جامعة الإمارات.

6- رضوان، رضا عبد الحكيم إسماعيل (2008): جرائم تزوير بطاقات الدفع الإلكتروني، مجلة البحوث الأمنية، كلية الملك فهد الأمنية، مج17، ع39.

7- المطيري، خالد ظاهر عبد الله جابر السهيل (2020): مواجهة الجرائم المعلوماتية في ضوء التشريعات الجنائية المعاصرة والاتفاقيات الدولية، بحث منشور، مجلة البحوث القانونية والاقتصادية، مج31، ع2.

8- عبد العال، أسامة حسين محي الدين (2022): جريمة تزوير المستند الإلكتروني – دراسة تحليلية مقارنة، مجلة العلوم القانونية والاقتصادية، مج64، ع1.

9- المغربي، طه عثمان (2020): تزويد المستند الإلكتروني، بحث منشور، مجلة البحوث القانونية والاقتصادية، مج، 10، ع 72، مصر.

10- بصلة، رياض فتح الله (2002): جرائم الاحتيال بالبطاقات الائتمانية وأساليب مكافحتها، أعمال ندوة: تزوير البطاقات الائتمانية، أكاديمية نايف العربية للعلوم الأمنية، الرياض.

سادساً: الاتفاقيات والأنظمة:

1- اتفاقية بودابست الموقعة في 2001/11/23 والمتعلقة بالإجرام الكوني وتتضمن 48 مادة.

2- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

3- النظام الجزائي السعودي لجرائم التزوير الصادر عام 1435هـ.

4- نظام التعاملات الإلكترونية السعودي، الصادر بالمرسوم الملكي رقم (م/18) وبتاريخ 1428/3/8هـ.

ISSN: 2706-6495

سابعاً: المراجع الأجنبية:

1- Maintaining – Christensen, S., Duncan, W. (2003): The Statute of Frauds in the Digital Age the Integrity of Signatures, E LAW, Murdoch University Electronic Journal of law.

2- Bhatla, T. P., Prabhu, V. & Dua, A. (2002): Understanding Credit Card Frauds, © Tata Consultancy Services.

3- Bergman, Bengt, E - Fraud (2005): State of the art and Countermeasures, Student Thesis, Linköping University.

4- Butler Rika (2007): A framework of anti-phishing measures aimed at protecting the online consumer's identity, the Electronic Library, Vol. 25, No. 5.

Doi: doi.org/10.52132/Ajrsp/v6.70.2