الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد بوضياف بالمسيلة

الكلية: الحقوق والعلوم السياسية. التخصص: الإدارة الكترونية والخدمات الرقمية

القسم: الحقوق.

عنوان المذكرة:

التزوير في المستندات الإلكترونية في القانون الجزائري

مذكرة مقدمة لنيل مقتضيات شهادة الماستر الأكاديمي، تخصص: الإدارة الكترونية

إعداد الطالب. إشراف الأستاذ:

- مصطفاوي اسامة - د.مسعودي هشام

الإسم واللقب	الرتبة العلمية	المؤسسة الجامعية	الصفة
د.جمال الدين ميموني	أستاذ محاضر-أ-	جامعة المسيلة	رئيسا
د.مسعودي هشام	أستاذ محاضر-أ-	جامعة المسيلة	مشرفا ومقررا
د.العمري منير	أستاذ محاضر-ب-	جامعة المسيلة	مناقشا

السنة الجامعية: 2025/2024

استمارة معلومات

الصورة

المعلومات الشخصية:

الاسم: آسيا — اللقب: معطاوي
اسم الأب ولقبه الأم: رزقي فطيمة
تاريخ الازدياد: 1995/01/06 — مكان الازدياد: بـ مقرة
رقم الهاتف: 0668999472
البريد الالكتروني:
العنوان الشخصي: لخراريب

الباكالوريا: 2020

معدل: 9.99 — الشعبة/التخصص: آداب وفلسفة — سنة الحصول على شهادة الباكالوريا: 2020

الليسانس:

التخصص: قانون عام — الشعبة/سنة التخرج: 2023

الماستر:

التخصص: إدارة الموارد البشرية وفعالية التنظيم — الشعبة/سنة التخرج: 2025
المعدل الرئيسي للماستر (المعدل الوحيد):

الوضعية المهنية:

الوظيفة: ——— — عاطل عن العمل: ☑

في حالة موظف:

الوصف العمومي: قطاع خاص
المصلحة المستخدمة: اسم المؤسسة / الشركة:
الرتبة في العمل:

الصيغة:

الوظيفة: — الرتبة في الصنف/الرتبة: — نوع العقد:

امضاء الطالب

CN 201322827
Du: 24/04/2016

تم التوقيع والتصديق على إمضاء
15 سبتمبر 2025
البلدي

الجمهورية الجزائرية الديمقراطية الشعبية
رئيس المجلس الشعبي البلدي
وبتفويض منه العون المكلف
إمضاء: بوراس جمسال

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي و البحث العلمي

جامعة محمد بوضياف بالمسيلة

كلية الحقوق والعلوم السياسية

قسم : الحقوق

المرجع: القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 المحدد للقواعد المتعلقة بالوقاية من السرقات العلمية ومكافحتها

تصريح شرفي

خاص بالالتزام بقواعد النزاهة العلمية لانجاز البحث

أنا الممضي أدناه،

السيد(ة) أسامة مرهاري

الصفة: طالب، أستاذ باحث، باحث دائم طالب

الحامل لبطاقة التعريف الوطنية رقم: 200331823

الصادرة بتاريخ 2016/04/24 عن دائرة/ بلدية عقرة

المسجل(ة) بكلية كلية الحقوق والعلوم السياسية قسم : الحقوق

والمكلف بانجاز أعمال بحث (مذكرة ماستر، مذكرة ماجيستير، أطروحة دكتوراه) الموسومة بـ : مذكرة ماستر

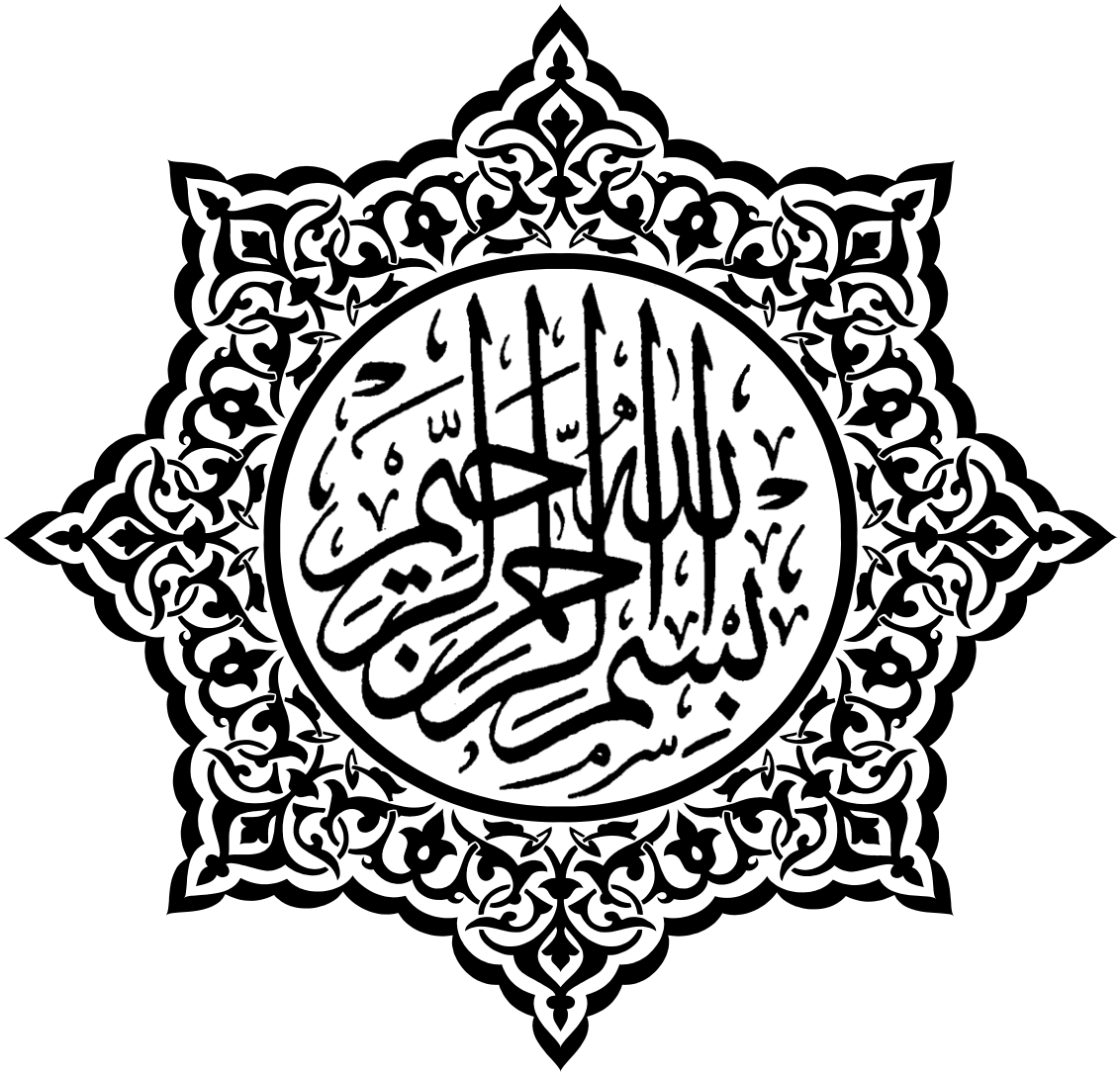
التزوير في المستندات الالكترونية في قانون الجزائي

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ

إمضاء المعني

مصادقة على إمضاء
15 سبتمبر 2025
رئيس المجلس الشعبي البلدي
إمضاء، بوراس جمال


بسم الله الرحمن الرحيم

شكر وعرفان

نشكر الله سبحانه وتعالى على فضله وتوفيقه لنا ، والقائل في محكم تنزيله

﴿وَإِذْ تَأَذَّنَ رَبُّكُمْ لَئِن شَكَرْتُمْ لَأَزِيدَنَّكُمْ . . . .﴾ الآية رقم: (07) سورة إبراهيم

الحمد لله أولا و أخيرا و له الثناء بكرة و أصيلا ، ونحمده على ما يسر لنا من أسباب النهوض بهذا البحث المتواضع .

وبعد حمد الله نتوجه بالشكر و التقدير الى كل من مدا لنا يد العون سواء بالتوجيه أو بالتنبيه الى المصادر و المراجع، و نخص بالشكر والتقدير الأستاذ **د . مسعودي هشام** الذي تفضل بالإشراف على هذا العمل و أبدى من النصح و التوجيه و كان لنا خير معين .

قائمة المختصرات

-المختصرات باللغة العربية:

ص : الصفحة

ج ر: جريدة رسمية

ط: طبعة

ع: عدد

ص. ص: الصفحة إلى الصفحة

غ ج: غرفة جزائية

م ق : مجلة قضائية

ق إ ج : قانون الإجراءات الجزائية

ق ع : قانون العقوبات

-المختصرات باللغة الفرنسية:

P: Page

Op.cit: ouvrage preite

N: Numero.

j.s.p: juris-classeurperiodique(semaine juridique)

مقدمة

مقدمة:

تعدد في عصرنا الحالي العديد من المعاملات الرقيمة في مجال التكنولوجيا، أصبحت المعاملات والاتصالات الإلكترونية جزءًا لا يتجزأ من حياتنا اليومية، برزت تحديات قانونية وأمنية جديدة تستلزم اهتمامًا خاصًا من بين هذه التحديات، تبرز جريمة تزوير المستندات الإلكترونية كشكل مستحدث ومتطور من أشكال التزييف التقليدي، إلا أنها تحمل في طياتها تعقيدات وآثارًا أوسع نطاقًا نظرًا لطبيعة البيئة الرقمية التي ترتكب فيها.

لم تعد ظاهرة التزوير مقتصرًا على تغيير الحقائق المادية في الورق أو المحررات التقليدية. اليوم، امتدت براثن هذه الجريمة لتشمل العالم الافتراضي، مستهدفة البيانات الرقمية المخزنة والمعالجة والمنقولة عبر الوسائل الإلكترونية المختلفة. فالمستند الإلكتروني، بما يحمله من قيمة قانونية واقتصادية واجتماعية متزايدة، أصبح هدفًا جذابًا للمحتالين والمجرمين الذين يسعون لتحقيق مكاسب غير مشروعة أو إلحاق الضرر بالآخرين.

إن طبيعة المستند الإلكتروني غير المادية، وقابليته للتعديل والنسخ بسهولة، وسرعة انتشاره عبر الشبكات الرقمية، كلها عوامل تضفي على جريمة تزويره أبعادًا جديدة وتجعل اكتشافها ومكافحتها أكثر صعوبة وتعقيدًا. فبينما كان التزوير التقليدي يترك آثارًا مادية ملموسة قد يستدل بها المحققون، فإن التزوير الإلكتروني غالبًا ما يتم بأساليب تقنية متطورة لا تترك أثرًا واضحًا، أو قد تخفي آثارها ببراعة فائقة.

إضافة الى ذلك، فإن نطاق تأثير جريمة تزوير المستندات الإلكترونية يتجاوز الحدود الجغرافية بسهولة، مما يجعل التعاون الدولي ضروريًا لمواجهتها بفعالية. فقد يتم إنشاء مستند مزور في بلد ما واستخدامه في بلد آخر، مما يعقد إجراءات التحقيق والملاحقة القضائية.

إن محاولة فهم جريمة تزوير المستند الإلكتروني يتطلب الإلمام بالجوانب القانونية والفنية على حد سواء، يجب تحديد مفهوم المستند الإلكتروني وأنواعه، وتبيان الأفعال التي تشكل جريمة تزويره، وتحديد المسؤولية الجنائية عنها، واستعراض الأدلة الرقمية التي يمكن الاعتماد عليها في إثباتها، كما يستلزم الأمر التعرف على التقنيات والأساليب التي يستخدمها مرتكبو هذه الجريمة، وكيفية تطوير آليات للكشف عنها ومنعها.

إن جريمة تزوير المستند الإلكتروني في التشريع الجزائري تمثل امتدادًا لمفهوم التزوير التقليدي المنصوص عليه في قانون العقوبات، ولكنها تتكيف مع طبيعة المستندات الرقمية وخصائصها الفريدة. فالمستند الإلكتروني، بما يحمله من قيمة قانونية واقتصادية، أصبح هدفًا للمحتالين الذين يسعون إلى تحقيق مكاسب غير مشروعة أو إلحاق الضرر بالغير عبر التلاعب بمحتواه أو إنشائه بصورة مصطنعة.

تتميز جريمة تزوير المستند الإلكتروني في الجزائر بتعقيداتها الخاصة، بدءًا من تحديد مفهوم "المستند الإلكتروني" في النصوص القانونية، مرورًا بتحديد الأفعال التي تشكل جريمة التزوير في هذا السياق الرقمي، وصولًا إلى التحديات التي تواجه إثبات هذه الجرائم وملاحقة مرتكبيها. فغياب الحدود المادية للمستند الإلكتروني وسهولة نسخه وتعديله ونقله عبر الشبكات، يضفي على هذه الجريمة أبعادًا جديدة تتطلب فهمًا معمقًا للإطار القانوني والتكنولوجي على حد سواء.

- مشكلة الدراسة:

وفي ضوء هذه الأهمية المتزايدة لجريمة تزوير المستندات الإلكترونية وتأثيراتها الخطيرة على الأفراد والمؤسسات والمجتمع ككل، يصبح من الضروري إلقاء الضوء على مختلف جوانب هذه الجريمة، بدءًا من تعريفها وأنواعها، مرورًا بأركانها وعقوباتها، وصولًا إلى التحديات التي تواجه مكافحتها وسبل تعزيز الجهود القانونية والتقنية لمواجهتها بفاعلية. وعليه سنحاول طرح الإشكالية التالية:

كيف تعامل المشرع الجزائري مع جريمة التزوير في المستندات الإلكترونية؟ وما السبل والإجراءات التي اتخذها المشرع الجزائري للقضاء على هاته الجريمة؟

- الأسئلة الفرعية:

- ماهي جريمة التزوير؟ وما طرقها وخصائصها؟
- ما هو المستند الالكتروني؟ وكيف يتم تحريره واثباته؟
- ماهي الإجراءات والقوانين التي سنها المشرع الجزائري للقضاء على هذه الجريمة؟

- ما مدى حجية جريمة تزوير المستند الإلكتروني المستمد من الجرائم الماسة بالمعاملات الإلكترونية في الإثبات الجنائي؟

- أسباب اختيار الموضوع:

يرجع سبب اختيارنا لموضوع الدراسة لأسباب ذاتية وأخرى موضوعية، نوردها فيما يلي:

1- الأسباب الذاتية:

ترجع هذه الأسباب للرغبة الشخصية للباحث في دراسة موضوع جريمة التزوير في المستند الإلكتروني والتعمق فيها، ومراد ذلك أن هاته الجريمة أصبحت ظاهرة عالمية وليست في الجزائر فقط، ومن أحدث وأبرز سمات هذا العصر، كما أن موضوع بحثنا يندرج ضمن تخصصي وما دفعني للبحث فيه ودراسة جوانبه، وكيف تعامل المشرع الجزائري مع هذا النوع من أنواع الجريمة.

2- الأسباب الموضوعية:

يكتسب اختيار موضوع جريمة تزوير المستند الإلكتروني في التشريع الجزائري أهمية بالغة لعدة أسباب جوهرية تلامس الواقع القانوني والاجتماعي والاقتصادي الراهن في الجزائر:

-الأهمية التي يكتسبها المستند الإلكتروني في ظل التطور الاقتصادي والمالي الحاصل على المستوى الدولي وخطورة التعامل بالمستندات الإلكترونية في المجالات المالية وفي مختلف القطاعات والتعاملات الإلكترونية، مما نتج عنها عدة جرائم إلكترونية لدى الأفراد و الوصول إلى ما هو واقع في مجال التعاملات الإلكترونية وتقريب الحقائق إلى ذهن القارئ.

- تسليط الضوء على متانة قطاع المعلوماتية في مواجهة الجرائم المحيط به وتفعيل دور الآليات لحماية المستند الإلكتروني وذكر الحماية الجنائية المقرر لعملية الحماية.

-التحديات القانونية المستجدة: طبيعة المستند الإلكتروني غير المادية وسهولة تعديله ونسخه ونقله تطرح تحديات قانونية جديدة لم تكن موجودة في سياق التزوير التقليدي للمستندات الورقية. تحتاج التشريعات إلى التكيف مع هذه الخصائص الفريدة لتحديد الأفعال

المجرمة بدقة وتوفير آليات فعالة للإثبات والملاحقة. دراسة هذا الموضوع تساهم في فهم مدى كفاية النصوص القانونية الحالية في مواجهة هذه التحديات والحاجة إلى تطويرها أو إصدار تشريعات جديدة.

-الأهمية الاقتصادية والتجارية: يعتمد الاقتصاد الحديث بشكل كبير على المعاملات الإلكترونية، تزوير المستندات الإلكترونية يمكن أن يؤدي إلى خسائر مالية كبيرة للأفراد والمؤسسات والاقتصاد الوطني ككل. دراسة هذا الموضوع تساهم في تحديد الآثار الاقتصادية لهذه الجريمة وتقديم توصيات لتعزيز الأمن القانوني للمعاملات الإلكترونية وحماية الاستثمارات.

- الفراغ القانوني المحتمل أو الحاجة إلى التوضيح: قد يكون هناك غموض أو نقص في النصوص القانونية الحالية المتعلقة بتزوير المستندات الإلكترونية، أو قد تحتاج بعض المفاهيم إلى توضيح وتفسير في ضوء التطورات التكنولوجية، دراسة هذا الموضوع يمكن أن تساهم في تحديد الثغرات القانونية وتقديم اقتراحات لتفسير النصوص القائمة أو سن تشريعات جديدة تعالج هذه الثغرات بشكل شامل.

- التأثير على الإجراءات القضائية: يمكن أن يؤثر تزوير المستندات الإلكترونية على سير الإجراءات القضائية ونتائجها، خاصة مع تزايد الاعتماد على الأدلة الرقمية في المحاكم. فهم كيفية تزوير هذه المستندات وكيفية التحقق من صحتها أمر بالغ الأهمية لضمان عدالة الأحكام القضائية.

- أهمية الدراسة:

تكتسي أهمية الموضوع باعتباره مفهوم جديد وحديث، بحيث أصبح موضوع الساعة ومحل انشغال مجموعة من الباحثين وكذلك لردود الفعل المنصبة عليه، وكذلك الدور الذي يلعبه المستند الإلكتروني في الحياة اليومية وفي جميع المجالات الحيوية لما له من أهمية على المستوى الأكاديمي والتطبيقي، وتتجلى أهمية البحث أيضا في تسليط الضوء على أحد التوجيهات الحديثة في مجال المعاملات، حيث تثبت مجموعة من معارك الاقتصاد الوطني العمل بهذا النوع من مستندات لملائمة التطورات الرقمية.

– تعزيز الأمن القانوني للاقتصاد الرقمي: تسعى الجزائر إلى تطوير اقتصاد رقمي قوي. تحقيق هذا الهدف يتطلب توفير بيئة قانونية آمنة وموثوقة للمعاملات الإلكترونية. تجريم تزوير المستندات الإلكترونية بشكل فعال يساهم في تحقيق هذا الأمن القانوني وجذب الاستثمارات في هذا المجال.

– حماية الأفراد والمؤسسات من الاحتيال: يمكن أن يؤدي تزوير المستندات الإلكترونية إلى عمليات احتيال واسعة النطاق تلحق أضرارًا مالية ومعنوية كبيرة بالأفراد والمؤسسات. دراسة هذا الموضوع تساهم في تطوير آليات قانونية وقضائية لحماية الضحايا وملاحقة الجناة.

– تحديد المسؤولية الجنائية بوضوح: نظرًا للطبيعة التقنية لجرائم تزوير المستندات الإلكترونية، قد يكون تحديد المسؤولية الجنائية أمرًا معقدًا. دراسة هذا الموضوع تساعد في وضع أسس واضحة لتحديد أركان الجريمة وتحديد مسؤولية الأفراد والكيانات المتورطة فيها.

– تطوير آليات الإثبات الرقمي: تتطلب مكافحة جرائم تزوير المستندات الإلكترونية تطوير آليات فعالة لجمع الأدلة الرقمية وتقديمها في المحاكم. دراسة هذا الموضوع تساهم في فهم التحديات المتعلقة بالإثبات الرقمي واقتراح حلول قانونية وتقنية لتجاوزها.

-أهداف الدراسة:

يهدف تناولنا لموضوع جريمة تزوير المستند الإلكتروني في التشريع الجزائري إلى تحقيق مجموعة من الأهداف الرئيسية من بينها:

– تحديد الإطار القانوني الحالي: يهدف البحث إلى استعراض وتحليل النصوص القانونية الجزائرية ذات الصلة بجريمة التزوير، وتحديد مدى شموليتها وتكيفها مع طبيعة المستندات الإلكترونية وخصائصها الفريدة.

– توضيح مفهوم المستند الإلكتروني في القانون الجزائري: يسعى الموضوع إلى تقديم فهم واضح ومحدد لمفهوم المستند الإلكتروني في سياق التشريع الجزائري، خاصة في ظل غياب تعريف صريح له في قانون العقوبات، وذلك بالاستعانة بالقوانين الأخرى ذات الصلة.

– بيان الأفعال التي تشكل جريمة تزوير إلكتروني: يهدف البحث إلى تحديد وتصنيف مختلف الأفعال التي يمكن أن تقع ضمن نطاق جريمة تزوير المستند الإلكتروني في القانون

الجزائري، مع الأخذ في الاعتبار الوسائل والتقنيات الحديثة المستخدمة في ارتكاب هذه الجرائم.

– تحليل أركان جريمة تزوير المستند الإلكتروني: يسعى الموضوع إلى تفصيل الأركان القانونية لجريمة التزوير في سياق المستندات الإلكترونية (الركن المادي والمعنوي والقانوني)، وتوضيح كيفية تطبيق هذه الأركان على الوقائع الرقمية.

– منهج الدراسة:

في دراستنا لموضوع جريمة تزوير المستند الإلكتروني في التشريع الجزائري، يمكن اعتماد المنهج الوصفي التحليلي كمنهج رئيسي، باعتبار المنهج الذي يتلائم مع دراستنا:

1. المنهج الوصفي:

وصف الإطار القانوني: سيتم وصف وتحليل النصوص القانونية الجزائرية ذات الصلة بجريمة التزوير بشكل عام، وتلك التي يمكن تطبيقها على المستندات الإلكترونية بشكل خاص. يشمل ذلك استعراض مواد قانون العقوبات المتعلقة بالتزوير، والقوانين المتعلقة بالمعاملات الإلكترونية والتوقيع الإلكتروني، وأي نصوص قانونية أخرى ذات صلة.

2. المنهج التحليلي:

تحليل النصوص القانونية: سيتم تحليل النصوص القانونية ذات الصلة بشكل معمق لفهم مقاصد المشرع، وتحديد مدى كفايتها في معالجة جرائم تزوير المستندات الإلكترونية، وتحديد الثغرات أو أوجه القصور المحتملة.

تحليل المفاهيم القانونية: سيتم تحليل المفاهيم الأساسية المتعلقة بالموضوع (مثل المستند الإلكتروني، التزوير الإلكتروني، الركن المادي والمعنوي) في سياق البيئة الرقمية وتحديد مدى انطباق المفاهيم التقليدية عليها أو الحاجة إلى تكييفها.

– الدراسات السابقة.

توجد بعض الدراسات السابقة، التي تناولت مواضيع مختلفة حول جريمة التزوير المستند الالكتروني والتي تتوافق في بعض النقاط ببحثنا إلا أنها تختلف عنه في بعض الزوايا. سنتطرق إلى البعض من هذه الدراسات فيما يلي:

الدراسة الأولى:

أطروحة دكتوراه، بعنوان: الحماية الجنائية للمحررات الإلكترونية من التزوير، من إعداد الطالبة: إلهام بن خليفة، مقدمة لكلية الحقوق والعلوم السياسية، جامعة باتنة، تقترب هذه الدراسة من بحثنا كون الطالبة تطرقت للحماية الموضوعية والإجرائية معا للمحررات الإلكترونية وذلك في ظل التشريعات المقارنة والاتفاقيات الدولية وهي تقريبا نفس موضوعنا في البعض من الجوانب. كما تحدثت دراسة الطالبة عن قواعد الاختصاص المتعلقة بجريمة التزوير في المحررات الإلكترونية، وهي نفس المعايير، إلا أن دراستنا تختلف مع دراسة الطالبة في كون دراستنا ترتكز على جريمة التزوير في المستند الالكتروني في التشريع الجزائري.

الدراسة الثانية:

مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية بعنوان: الحماية الجنائية للمستند الالكتروني(دراسة مقارنة)، للطالبة: بوكريف سعدية، مقدمة عن كلية الحقوق والعلوم السياسية جامعة أكلي محند اولحاج – البويرة – قسم القانون العام، حيث تتطابق دراستنا وتتشابه معها من الناحية القانونية، بحيث تطرقت الطالبة الى معظم التشريعات مثل المصري والفرنسي والألماني والتي تهدف الى حماية المستند الالكتروني وعدم تعرضه للتزوير، كما عملت الطالبة على مطابقة لتشريعات المذكورة مع التشريع الجزائري إلا أن دراستنا تختلف مع دراسة الطالبة في كون دراستنا ترتكز على جريمة التزوير في المستند الالكتروني في التشريع الجزائري.

-خطة الدراسة:

من أجل الإحاطة بالجوانب المتعلقة بهذا الموضوع، تم تقسيم المذكرة إلى فصلين في كل فصل تناولنا مجموعة من المباحث، حيث تناولنا بالدراسة في الفصل الاول الإطار المفاهيمي للتزوير في المستند الإلكتروني والذي تطرقنا فيه الى مبحثين، المبحث الاول: ماهية التزوير الإلكتروني، وام فيها الاعتماد على مطلبين: المطلب الأول: مفهوم التزوير.

المطلب الثاني: مفهوم التزوير الالكتروني، اما المبحث الثاني: تضمن مطلبين: المطلب الأول: مفهوم المستند الإلكتروني، المطلب الثاني: مفهوم جريمة المستند الالكتروني.

اما فيما يخص الفصل الثاني والذي جاء بعنوان: الآليات القانونية لتجريم تزوير المستند الالكتروني، تم الاعتماد أيضا على مبحثين: المبحث الأول: الحجية القانونية لتزوير المستندات الالكترونية وتم فيه التعرض الى: المطلب الأول: المواثيق والأعراف الدولية .

المطلب الثاني: النظام القانوني للمستند الالكتروني، وكما تم في المبحث الثاني: والذي جاء بعنوان افعال المساس بالمستند الالكتروني في التشريع الجزائري وفيه أيضا:المطلب الاول: الفعل الماس بالمستند الالكتروني،المطلب الثاني: اجراء المشرع الجزائري من جريمة تزوير المستند الالكتروني.

وفي الختام هذه الدراسة تم التطرق الى خاتمة تضمنت مجموعة من النتائج والتوصيات.

الفصل الأول

الإطار المفاهيمي للتزوير في المستند الإلكتروني.

المبحث الاول: ماهية التزوير الإلكتروني.

المطلب الأول: مفهوم التزوير.

الفرع الأول: تعريف التزوير.

الفرع الثاني: خصائص جريمة التزوير.

المطلب الثاني: مفهوم التزوير الالكتروني.

الفرع الأول: تعريف التزوير الالكتروني.

الفرع الثاني: خصائص وصور التزوير الإلكتروني.

المبحث الثاني: التزوير في المستند الإلكتروني.

المطلب الأول: مفهوم المستند الإلكتروني.

الفرع الأول: تعريف المستند الالكتروني.

الفرع الثاني: خصائص المستند الإلكتروني.

الفرع الثالث: المستند الالكتروني وما يميزه عن المستند التقليدي.

المطلب الثاني: مفهوم جريمة المستند الالكتروني.

الفرع الأول": تعريف جريمة تزوير المستند الإلكتروني.

الفرع الثاني: اركان جريمة تزوير المستند الإلكتروني.

خلاصة الفصل.

تمهيد:

مع التطور التكنولوجي السريع والتحول نحو الرقمنة في مختلف جوانب الحياة، أصبحت المستندات الإلكترونية جزءًا أساسيًا من المعاملات الإدارية، التجارية، والقانونية. فلم تعد الوثائق الورقية هي الوسيلة الوحيدة لتوثيق البيانات والمعلومات، بل حلت مكانها المستندات الإلكترونية التي يتم إنشاؤها وتبادلها وحفظها عبر الوسائط الرقمية.

في هذا السياق، برزت جريمة تزوير المستند الإلكتروني كأحد أخطر الجرائم الإلكترونية التي تهدد أمن المعلومات وموثوقية التعاملات الرقمية. يتمثل هذا النوع من الجرائم في تغيير أو تعديل محتوى المستند الإلكتروني بشكل غير مشروع، سواء كان ذلك بإضافة معلومات كاذبة، أو حذف بيانات أساسية، أو التلاعب بالتوقيعات الرقمية، بهدف الخداع أو تحقيق منفعة غير قانونية.

وتكمن خطورة هذه الجريمة في سهولة تنفيذها وصعوبة اكتشافها، نظرًا للطبيعة الرقمية للمستندات التي يمكن نسخها، توزيعها، والتلاعب بها بسرعة كبيرة دون ترك أثر مادي مباشر. كما أن هذا النوع من التزوير لا يعرف حدودًا جغرافية، إذ يمكن أن يتم في بلد ويؤثر في بلد آخر، مما يجعل مكافحته تتطلب تعاوُناً دوليًا وإجراءات قانونية صارمة.

وعليه سنحاول في هذا الفصل التطرق الى المباحث التالية: **المبحث الاول: ماهية التزوير الإلكتروني، المبحث الثاني: التزوير في المستند الإلكتروني**

المبحث الاول: ماهية التزوير الإلكتروني.

يشهد العالم تحولًا متسارعًا نحو الرقمنة في مختلف جوانب الحياة، مما أوجد بيئة خصبة لظهور أشكال جديدة من الجرائم، من بينها التزوير الإلكتروني. يُعد التزوير الإلكتروني بمثابة الوجه الرقمي لجريمة التزوير التقليدية، حيث يتم استخدام الوسائل التقنية والتكنولوجية لارتكاب فعل التغيير أو التحريف في البيانات أو المستندات الإلكترونية بهدف تحقيق منفعة غير مشروعة أو إلحاق ضرر بالآخرين. وعليه اعتمدنا في هذا المبحث على مايلي: المطلب الأول: مفهوم التزوير، المطلب الثاني: التزوير الإلكتروني.

المطلب الأول: مفهوم التزوير.

يُعد التزوير من أقدم الجرائم التي عرفتها البشرية، وهو فعل ينطوي على تغيير الحقيقة أو تحريفها بهدف خداع الآخرين وتحقيق منفعة غير مشروعة أو إلحاق ضرر بهم. يتجاوز مفهوم التزوير مجرد الكذب أو الإدلاء بمعلومات خاطئة، ليشمل صنع أو تغيير أو تقليد شيء ما ليبدو حقيقيًا أو أصليًا بهدف التضليل.

كما عملنا في هذا المطلب التطرق الى الفرعين الموالين: الفرع الاول: تعريف التزوير، الفرع الثاني: خصائص التزوير.

الفرع الأول: تعريف التزوير.

التزوير هو عملية تغيير متعمد للحقيقة بقصد الخداع، ويُعدّ من الأفعال غير القانونية التي تمسّ الثقة والمصداقية في المعاملات والوثائق. قد يكون التزوير في الوثائق الرسمية، أو التوقيعات، أو حتى في البيانات والمستندات الإلكترونية، ويهدف عادة لتحقيق منفعة شخصية أو إلحاق ضرر بالغير[1] يُعتبر التزوير جريمة يعاقب عليها القانون لما لها من آثار خطيرة على الأفراد والمؤسسات والمجتمع ككل.

أولا: التزوير لغة.

مصدر: زور، وهو من الزور.

[1] العبيدي صدام حسين، والعبيدي عواد حسين ياسين، أحكام جرائم التزوير التقليدي والإلكتروني في الفقه الاسلامية القانون الوضعي، ط1، المركز العربي للنشر والتوزيع، 2020، ص 25.

والزور: الممل والكذب؛ قال ابن فارس: الزاي والواو والراء أصل واحد يدل على الحمل والعدول، ومن ذلك الزور الكذب، لأنه مائل عن طريق الحق ويقال زور فلان الشيء تزويرا، حتى يقولون زور الشيء في نفسه: هيأه، لأنه يعدل به عن طريقة تكون أقرب إلى قبول السامع".[1]

وأن الزور لغة: الكذب، والتزوير: تزيين الكذب.

فالتزوير يكون فيه القول والفعل، والكذب لا يكون إلا في العقول.

فالتزوير هو محاولة تزيين الكذب وطمس الحقيقة والباس الباطل ثوب الحق.

والتزوير هو: الزور بالضم: الكذب[2] ، ومنه قوله تعالى: (وَاجْتَنِبُواْ قَوْلَ الزُورِ 30)[3] ، والزور: يدل على الميل والعدول، لأنه مائل عن طريق الحق[4].

ثانياً: التزوير اصطلاحاً.

والتزوير اصطلاحاً له عدة تعريفات:

عرف التزوير بأنه: " تغيير الحقيقة أو استبدال أمر غير صحيح بالواقع الصحيح يعد من الأمور " [5]

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[6] وورد تعريف آخر للتزوير بأنه: " إظهار الكذب في محرر على أنه حقيقة يعد

---

[1] دردوس مكي، القانون الجنائي الخاص في التشريع الجزائري، ج 2،ط1، ديوان المطبوعات الجامعية، الجزائر، ب.ت.ن، ص65.

[2] الجوهري، 2/672، ابن فارس، 1/444،دار القلم ، بيروت ، لبنان، ص2252.

[3] سورة الحج، الآية 30.

[4] الرازي، احمد بن فارس القزويني، معجم المقاييس اللغة 3/63، دار الفكر، 1399هـ، ص223.

[5] العكسري أبو هلال الحسن ابن عبد العبد الله، الفروق اللغوية، تحقيق: محمد إبراهيم سليم، دار العلم والثقافة للنشر والتوزيع، القاهرة، 1996، ص3.

[6] مراد عبد الفتاح، شرح جرائم التزييف والتزوير، ط1،دار الاحمدي للنشر والتوزيع،الإسكندرية، 2011، ص 34.

خداعاً لعقيدة "الآخرين"[1] والتزوير هو: " تقليد شيء ما مع التظاهر بأن هذا التقليد هو النسخة الأصلية، رغم أنه ليس كذلك".[2]

عرفه جارسون (GARSON) فقال: هو تغيير الحقيقية بقصد الغش فيه محور بإحدى الطرق المبينة قانوناً تغييراً من شأنه أن يسبب ضرراً.

وعرفه جارو (Garelu) فقال: التزوير يتكون . الحقيقية في محور يقصدالخيش تغييراً من شأنه أن يسبب ضرراً.

وعرفه قوان (Guan) فقال: التزوير بصفته جريمة هو تزييف في الحقيقة من شأنه الإضرار ويقع في محور واحدى الوسائل المبينة في القانون.[3]

وعليه : فالتزوير فعل يتمثل فيه تحريف يحدثه الجانب عمداً ويقصد الغش في محور بإحدى الطرق المبينة في القانون ويكون من شأنه أن يسبب للغير ضرراً حقيقياً أو احتمالاً وهو تعريف يتفق في جوهره مع ما جاه به جارسون و جارو و قوان، ويمتاز عنه بشرط القران العبد بنية الغش وكذلك بإدخال الضرر المحتمل في التحريم.

ثالثاً: التزوير شرعاً.

يعرف عند الفقهاء كالتالي بأنه: " تحسين الشيء ووصفه بخلاف صفته، حتى تحول إلى من سمعه أو رأه بخلاف ما هو عليه في الحقيقة، فهو تمويه الباطل بما يوهم أنه حق".

وقيل هو كل قول أو عمل يراد به تريدين الباطل حتى يظن انه حق، سواء أكان ذلك في القول كشهادة الزور، أم الفعل كمحاكاة الخطوط أو النقود يقصد إثبات الباطل.

وهذا التعريف اعتماده الكثير من علماء الشريعة كونه شاملاً كاملا.[4]

---

[1] حمودة علي حمودة علي، شرح قانون العقوبات ،2003، ص 249.

[2] العبيدي صدام حسين، والعبيدي عواد حسين ياسين، المرجع السابق، ص 25.

[3] دردوس مكي، المرجع السابق، ص66.

[4] جلال ثروت، نظم القسم الخاص، الجزء الثالث، دار المطبوعات الجامعية، 1995، ص220.

رابعا: تعريف التزوير فقها.

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[1]، وهو أي وسيلة يستخدمها فرد لخداع شخص آخر[2]

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[3]

رابعاً: التزوير قانوناً

هو تغيير الحقيقة بقصد الغش، وبإحدى الطرق التي عينها القانون تغييراً من شأنه أن ضرراً، سواء أكان الضرر حالاً أو محتمل الوقوع.

الفرع الثاني: خصائص جريمة التزوير.

لجريمة التزوير عدة الخصائص تميزهما عن باقي الجرائم الاخرى، وذلك نظراً لإخلالها بالثقة العامة وتأثيرها على الأفراد ومعاملاتهم القانونية والإدارية من جهة أخرى، وتكمن هذه الخصائص فيما يلي:

أولاً: حريمة ذات طابع دولي: أهم ما يميز جريمة التزوير من فورها من الجرائم هو طابعها الدولي، وذلك بسبب الاتصالات السريعة يرون أقطار العالم والمبادلات الاقتصادية والاجتماعية والثقافية بين الدول، ومع انتشار للمعلومة العلمية بشكل سريع على مستوى العالم الحديث، إذ أصبح من الضروري قيام السلطات المعنية في كل دولة بالاهتمام بها

[1] سعد عبد العزيز، جرائم التزوير وخيانة الأمانة واستعمال المزور، ط1، دار هومة، الجزائر، 2005، ص14.

[2] عقاد محمد، جريمة التزوير في محررات الحاسب، دراسة مقارنة، بحث مقدم في المؤتمر السادس المنعقد خلال فترة 25-1993/10/28، الجمعية المصرية للقانون الجنائي، دار النهضة العربية، ص 392.

[3] سرور أحمد فتحي، الوسيط في قانون العقوبات، القسم الخاص، ط4، دار النهضة العربية، 1991، ص 402.

ومكافحتها والعقاب عليها وملاحقة مرتكبيها، بغية تحقيق الأمن والاستقرار في البلاد.[1]

ثانياً: جريمة ذات طابع اقتصادي: تمس حريمة التزوير بالاقتصاد الوطني بدرجة كبيرة، ويظهر ذلك من خلال أزمة اقتصادية وفقدان الدولة الثقة في معاملاتها سواء بين الأفراد داخلياً أو بين الدول خارجيا، وبالتالي إهدار الموارد المالية والدخل الوطني كما أنها تعتبر كجريمة مساهمة، ذلك أنها ترتكب المعرفة ومساعدة عصابات منظمة وتحتاج إلى استخدام عدد كبير من الأفراد ذوي الخبرة الفنية والعلمية".[2]

ثالثا: جريمة ذات طابع تقني علمي: تعتمد حركة التزوير على المعلومات والمعارف الفنية والتكنولوجية التي فرضها التقدم الحضاري للمدينة الحديثة، ويتطلب ارتكابها تعتمد مختلف العلوم التقنية والفنية والصناعية فهي تستلزم تخصص ذوي المهارات الغنية المتخصصة، كما أنها تحتاج لعمليات ذهنية، ولعل السبب الرئيسي في التزايد الرهيب والمثور لهذا النوع من الإحرام هو الاستغلال السلبي للثورة التكنولوجية خاصة بالنسبة لوسائل الطباعة الحديثة وأجهزة الكمبيوتر.[3]

المطلب الثاني: مفهوم التزوير الالكتروني.

يعرف التزوير الإلكتروني بأنه كل تغيير أو تحريف أو إنشاء غير مصرح به للبيانات أو المستندات الرقمية، أو استخدام هذه البيانات أو المستندات المزورة، بهدف تحقيق منفعة غير مشروعة أو إلحاق ضرر بالآخرين، حيث سنتطرق من خلاله الفروع الآتية: الفرع الأول: تعريف التزوير الالكتروني، الفرع الثاني: خصائص وصور التزوير الإلكتروني.

الفرع الأول: تعريف التزوير الالكتروني.

[1] يوسف الأبيض، لحوص التزييف والتزوير ، دار المطبوعات الجامعية ، مصر، 2006، ص89.

[2] سليمان عبد المنعم، قانون العقوبات الخاصة، القوائم الماسة بالمصلحة العامة، الجامعة الجديدة للنشر، الاسكندراية،1993، ص290.

[3] أحمد أبو الروس، قانون جرائم التزييف والتزوير، المكتب الجامعي الحديث، الاسكندرية 1997، ص 482.

في العصر الرقمي الحديث، أصبحت التكنولوجيا جزءًا لا يتجزأ من حياتنا اليومية، مما أدى إلى تسهيل العديد من المعاملات وتبسيط الوصول إلى المعلومات. ومع ذلك، هذا التطور السريع صاحبه نوع جديد من الجرائم الإلكترونية، من بينها التزوير الإلكتروني.

التزوير الإلكتروني يشير إلى عمليات التلاعب والتزييف في البيانات أو الوثائق الرقمية باستخدام تقنيات حديثة، بهدف الخداع أو الاحتيال لتحقيق مكاسب غير مشروعة. يمكن أن يشمل ذلك تزوير التوقيعات الرقمية، والتلاعب في المستندات الإلكترونية، وحتى تغيير البيانات في قواعد المعلومات.[1]

كما يعرف في أيضا 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"[2] ،وهو أيضاً: " التعديل المتعمد للمعلومات الموجودة في الوثيقة المعلوماتية بهدف إحداث "تضليل"، 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" [3]

هذا وإن التزوير الإلكتروني هو تعديل الحقيقة الذي يؤثر على مخرجات الحاسوب، سواء كانت هذه المخرجات على شكل مستندات ورقية مطبوعة أو رسومات مرسومة[4]

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

[1] السيراني عبد الله بن سعود محمد، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، ط1، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية. 2011، ص 54.

[2] الجبوري عمر عبد السلام حسين، جريمة التزوير الإلكتروني في التشريع الأردني، رسالة ماجستير، جامعة الشرق الأوسط الأردن،2017، ص17.

[3] تمام أحمد حسام طه، الجرائم الناشئة عن استخدام الآلي، دراسة مقارنة، ط1، دار النهضة العربية، مصر،2000، ص 407.

[4] حجازي عبد الفتاح بيومى، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، القاهرة،2002، ص 170.

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"[1]

التعريف التشريعي للتزوير الإلكتروني.

إختلفت التشريعات في تعريف التزوير الإلكتروني وفيما يلي نورد أهم القوانين التي تطرقت إلى تعريفه، حيث عرفته الإتفاقية العربية لمكافحة جرائم تقنية المعلومات[2] في المادة 10 على أنه إستخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه إحداث ضرر وبنية إستعمالها كبيانات صحيحة.

كما عرفه المشرع الفرنسي في المادة 441/1 من قانون العقوبات بأنه كل تغيير في الحقيقة عن طريق الغش يمكن أن يسبب ضررا، يتم إرتكابه بأي وسيلة كانت على محرر مكتوب أو أي دعامة أخرى تحتوي تعبير عن فكرة يكون الهدف منه إثبات حق أو واقعة لها آثار قانونية.

Constitue un faux toute altération frauduleuse de la vérité, de nature àcauser un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un .fait ayant des conséquences juridiques[3]

وعرفه المشرع المصري في المادة 23 فقرة من قانون التوقيع الإلكتروني بنصها" يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تزيد على مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من قام بإتلاف أو تشويه توقيع أو وسيط أو محرر أو سند إلكتروني، أو عمد إلى تزوير أي منها عن طريق الاصطناع أو التعديل أو التحوير أو بأي

[1] حفظي عباس ، جرائم التزوير الإلكتروني، رسالة دكتوراه جامعة وهران، كلية الحقوق والعلوم السياسية ، قسم الحقوق، ، الجزائر، 2015، ص 2.

[2] الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على الرابط : https://ar.m.wikisource.org أطلع عليه بتاريخ 19/12/2024

[3] Code pénal français dernier modification, Édition 02/12/2024.

وسيلة أخرى"، أما بالنسبة للمشرع الجزائري فلم يحذو حذو التشريعات السابقة حيث أنه لم يدرج تعريفا للتزوير الالكتروني بشكل خاص ضمن قانون العقوبات رغم تناوله لجريمة التزوير من المادة 214 إلى المادة 229. [1]

ثالثا: التعريف الفقهي للتزوير الالكتروني.

تعددت التعريفات الفقهية للتزوير الالكتروني وهذا ما جعل التشريعات تختلف في صيغ تجريمه فهناك من يعرفه بأنه تغيير الحقيقة في البيانات أو المعلومات المعالجة عن طريق الحاسب الآلي والي أصبح لها كان مادي ملموس يقابل أصل المحرر المكتوب.[2]

وعرفه الأستاذ عبد القادر القهوجي " يقصد به تغيير الحقيقة في مخرجات الحاسب الآلي، سواء تمثلت في مخرجات ورقية مكتوبة عبر الطابعة، أو رسومات صادرة عن الراسم، ويستوي في ذلك أن يكون المستند الإلكتروني محرراً باللغة العربية أو بأي لغة أخرى تحمل دلالة مفهومة. كما قد يكون المستند في شكل مخرجات ورقية محفوظة على دعامة، كبرنامج منسوخ على أسطوانة، شريطة أن يكون لهذا المستند الإلكتروني أثر في إثبات حق أو ترتيب أثر قانوني".[3]

كما تم تعريفه أيضا بأنه" الدخول بطريقة مشروعة أو غير مشروعة على قاعدة البيانات الموجودة في نظم المعلومات، وتعديل البيانات سواء بإلغاء بيانات موجودة بالفعل

[1] قانون التوقيع الإلكتروني المصري رقم 15 لعام 2004 على الرابط http://borai.com ، أطلع عليه بتاريخ 2025/02/21

[2] براهيمي حنان، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2014-2015، ص189.

[3] حفصي عباس، جرائم التزوير الإلكترونية أطروحة مقدمة لنيل شهادة دكتوراه، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة وهران ،1 2014 - 2015 ص18.

أو بإضافة بيانات لم تكن موجودة من قبل[1]، وهو أيضا التغيير المتعمد للمعلومات الواردة في المستند المعلوماتي بغرض التضليل[2].

وعليه سارت جميع التعريفات في اتجاه واحد بأن لتزوير الالكتروني " هو التلاعب أو التغيير المتعمد في البيانات أو المعلومات الرقمية المخزنة[3] أو المنقولة عبر الوسائط الإلكترونية، بهدف خداع الأطراف المعنية لتحقيق مكاسب غير قانونية أو إخفاء حقائق معينة".

الفرع الثاني: خصائص وصور التزوير الإلكتروني.

1/ خصاص التزوير الإلكتروني.

الخصائص نوردها فيما يلي:

أولا: خاصية إرتكاب التزوير الكتروني خلال مرحلتي الإدخال والمعالجة.

يتم التزوير الالكتروني خلال مرحلة الإدخال، بإدخال معلومات غير صحيحة للإعتداد بها على أنها معلومات صحيحة أو عدم إدخال معلومات أساسية وذلك بغية تزييف الحقيقة[4]، غالبًا ما يقوم بهذه الأفعال الموظفون المكلفون بتسيير الأنظمة المعلوماتية داخل الإدارات أو الشركات.

ففي مرحلة المعالجة يمكن إدخال تعديلات على برامج الحاسب الآلي لتحقيق الغرض الإجرامي من خلال التلاعب في نظم المعلومات، كما قد يتم التزوير المعلوماتي أيضًا عبر تغيير النتائج خلال مرحلة الإخراج[5]، فبعد الإنتهاء من عملية إدخال المعلومات ومعالجتها

---

[1] عبد الله بن سعود محمد السراني، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2011، ص 54.

[2] Protéger contre la falsification de document, publié le 23/12/2019 sur: https://nec-itplatform.com

[3] الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، المرجع السابق.

[4] عبد السلام حسين الجبوري، جريمة التزوير الإلكتروني في التشريع الأردني (دراسة مقارنة) رسالة مقدمة إستكمالا لمتطلبات الحصول على درجة الماجستير، كلية الحقوق جامعة الشرق الأوسط، 2017، ص 17.

[5] عبد الله بلقاسم، الطبيعة الخاصة لجريمة التزوير في المحررات الإلكترونية، مجلة الدراسات القانونية المقارنة، المجلد6، العدد الثاني،ط1، جامعة حسيبة بن بوعلي الشلف الجزائر، الصادر في 27/12/2020، ص 982.

بشكل صحيح يتم الدخول إلى نظام المعالجة الآلية بهدف تحريف الحقيقة، مثل قيام موظف بالدخول إلى قاعدة المعطيات الخاصة بالجنسية ويستبدل معلومات جنسيات صحيحة ويدرج فيها معلومات تخص أشخاص أجانب من أجل نسخها وتسليمها لهم.

ثانيا: خاصية الأثر اللامادي للتزوير الإلكتروني.

التزوير في المستندات الورقية تظهر فيه آثار التغيير بالإضافة أو الحذف باستخدام أدوات أو مواد كيمائية[1]، وهذا عكس التزوير الإلكتروني حيث أنه لا يترك أي آثر يدل على إرتكابه، لذلك يمكن وصفه بأنه تزوير ناعم وغير ملموس يتسم بالخفاء باعتباره يتم من خلال الوصول إلى المعلومات المطلوبة وتغييرها حسب الهدف الذي يصبو إليه الجاني، وما تجب الإشارة إليه في هذه النقطة أن خاصية الأثر اللامادي للتزوير الإلكتروني يزيد من صعوبة إكتشافه إذ يكتشف في معظم الأحيان عن طرق الصدفة.

ثالثا: خاصية المعرفة التقنية.

يُرتكب التزوير الإلكتروني باستخدام وسائل تقنية متطورة، الأمر الذي يستلزم من مرتكبه قدراً عالياً من الذكاء والمعرفة بوسائل التكنولوجيا الحديثة، معتمداً في ذلك على قدراته الذهنية لا الجسدية، إذ إن مسرح الجريمة هنا بيئة رقمية بحتة.

ويجدر التنويه إلى أن المزور الإلكتروني قد يُقدم على فعله بدوافع متعددة، منها شعوره بالكبرياء أو رغبته في الانتقام نتيجة فصله من العمل أو الاستغناء عن خدماته، وقد يكون الدافع إثبات الذات وتحقيق انتصار شخصي عبر إبراز مهاراته في تحدي أنظمة أمن المعلومات، أو حتى بدافع التسلية. غير أن الدافع الأكثر شيوعاً يتمثل في السعي وراء منفعة مالية أو تحقيق أرباح لصالحه أو لصالح الغير.

وعليه، فإن جريمة التزوير لا تقع بمحض الصدفة، بل غالباً ما تُخطط لها بعناية من قبل أشخاص ذوي خبرة ومهارات تقنية عالية ومع ذلك، قد يحدث التزوير أحياناً بصورة غير مقصودة، كما في حالة إغفال أحد الموظفين إدراج بيانات أساسية دون قصد أو نية إجرامية.

[1] عبد السلام حسين الجبوري، المرجع السابق، ص17.

رابعا: خاصية إنتمائه للإجرام العابر للحدود.

يتميز التزوير الإلكتروني بأنه يتعدى الحدود الجغرافية للدول، فهو ذو أبعاد دولية فيمكن أن يرتكب الجاني التزوير في بلد معين وتظهر نتائجه في بلد آخر أو عدة دول أخرى، كما يمكن أن يرتكبه شخص واحد ولكن يلحق أضرار بعدة أشخاص وهذا لكون تنفيذه يتم عبر الشبكة المعلوماتية، وخاصية إنتمائه للإجرام العابر للحدود تثير صعوبة مواجهته والتصدي له كجريمة معلوماتية خطيرة.[1]

2/ صور التزوير الإلكتروني.

أولاً: نشر أو استخدام شهادة تصديق إلكتروني مزورة.

– **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.[2]

– **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:

[1] لامية طالة، كهينة سلام الجريمة الإلكترونية بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي، مجلة الرواق للدراسات الاجتماعية والإنسانية، المجلد 6، العدد الثاني، المركز الجامعي أحمد زيانة غليزان الجزائر الصادر في 30/12/2020 ، ص 75.

[2] حجازي عبد الفتاح بيومى، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، المركز القومي للإصدارات القانونية، القاهرة.2011، ص 465.

يتم تزوير التوقيع الإلكتروني بطرق مختلفة تماما، حيث يكون التوقيع المزور مطابق تماما 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 صادرا عن مالك نظام التوقيع الإلكتروني، بل هو صادر عن شخص آخر تمكن من اختراق النظام وسرقة بيانات التوقيع[1].

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[2]

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[3].

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

[1] عبد الله بن سعود محمد السراني، المرجع السابق، ص40.

[2] Maintaining – Christensen, S., Duncan, W.: The Statute of Frauds in the Digital Age the Integrity of Signatures, E LAW, Murdoch University Electronic Journal of law., 2003, p8.

[3] Bhatla, T. P., Prabhu, V. & Dua, A. Understanding Credit Card Frauds, © Tata Consultancy Services.Linköping University.2002., p1.

الائتمان أو بطاقات الخصم[1]. وانتحال الهوية والتزوير المالي من أبرز أشكال الاحتيال الإلكتروني. ويقوم الجناة بتزوير بطاقات الائتمان، حيث تعتبر من أكثر وسائل الدفع شيوعاً في الوقت الحالي، ويستخدمونها في عمليات الدفع. ويمكن تلخيص أبرز أساليب الاحتيال التي تتم من خلال البطاقات الائتمانية[2] فيما يلي:

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.

---

[1] Bergman, Bengt, E – Fraud: State of the art and Countermeasures, Student Thesis,2005.p20.

[2] بصلة رياض فتح الله، جرائم الاحتيال بالبطاقات الانتمائية،وأساليب مكافحتها، اعمال ندور تزوير البطاقات الانتمائية ، اكاديمية نايف للعلوم الأمنية ، الرياض،2002، ص100.

المبحث الثاني: التزوير في المستند الإلكتروني.

تتسم البيئة الرقمية بخصائص تجعل المستندات الإلكترونية عرضة للتزوير بطرق قد تكون أكثر سهولة وإخفاءً مقارنة بالمستندات الورقية. فباستخدام برامج تعديل النصوص والصور والبيانات، يمكن للمزورين إجراء تغييرات دقيقة قد يصعب اكتشافها بالعين المجردة. كما أن طبيعة المستندات الإلكترونية غير المادية تجعل عملية التحقق من أصالتها أكثر تعقيدًا وتعتمد على آليات تقنية متخصصة، بحيث سنحاول في هذ المبحث التعرف على مايلي من خلال المطالب التالية: المطلب الأول: مفهوم المستند الإلكتروني، المطلب الثاني: مفهوم جريمة المستند الالكتروني.

المطلب الأول: مفهوم المستند الإلكتروني.

في خضم الثورة الرقمية التي يشهدها عالمنا المعاصر، برز المستند الإلكتروني كبديل عصري وفعال للمستندات الورقية التقليدية. لم يعد مفهوم المستند مقتصرًا على الأوراق المحفوظة في الخزائن والأرشيفات، بل اتسع ليشمل أي معلومة أو بيانات يتم إنشاؤها أو تخزينها أو تبادلها بوسائل إلكترونية على وسيط رقمي، اعتمدنا في هذا المطلب على الفروع التالية: الفرع الأول: تعريف المستند الالكتروني، الفرع الثاني: خصائص المستند الالكتروني، الفرع الثالث: المستند الالكتروني وما يميزه عن المستند التقليدي.

الفرع الأول: تعريف المستند الالكتروني.

المستند الإلكتروني هو مجموعة من البيانات أو المعلومات التي تُنشأ أو تُرسل أو تُستقبل أو تُخزَّن عبر وسائط إلكترونية، بحيث يمكن استرجاعها والاطلاع عليها عند الحاجة. بحيث سنحاول تفصيل ذلك من التعاريف اللغوية الاصطلاحية. [1]

أولا: لغة

فبالنسبة لكلمة "المستند" فمن الناحية اللغوية فهي مأخوذ من السند، وهو كل ما ارتفع

[1] بصلة رياض فتح الله، المرجع السابق، ص101.

من الأرض من قبل الجبل أو الوادي ويجمع على إسناد، ويقال ساندته إلى الشيء فهو يتساند إليه، أي استندته إليه وتساندت إليه أي استندت[1]، ويقال سند الشيء أي دعمه ورتقه، وساند الرجل أي عاضده، وسند إلى الشيء أي جعله له متكأ، ومن ثم فالسند هو كل ما يستند إليه ويعتمد عليه من حائط أو غيره، ومنه أطلق على صك الدين وغيره، سند، وهو في الاقتصاد ورقة مالية مثبتة لغرض حاصل ذو فائدة ثابتة.[2]

والمسند من الحديث، ما اتصل إسناده حتى يسند إلى "**النبي صلى الله عليه وسلم**"، وبناء على ذلك فإن المستند هو كل ما يمكن الاستناد إليه والاعتماد عليه أو الاحتماء به لدرء خطر، أو إثبات حق والمطالبة به ومنه أسندت إليه أمري، وهو سندي ومستندي.

السند: في اللغة العربية هو أداة الإثبات لها لفظان السند والورقة، ولما كان لفظ الورقة أعم المعني من لفظ السند إذن يمكن تعريفه بأنه الورقة المعدة للإثبات أي الدليل المهئ.[3]

فلفظ الورقة يستعمل في الأدلة الكتابية جميعا، سواء أعدت للإثبات أو لم تكن معدة ونقول الورقة الرسمية والورقة المصرفية قاصدين بذلك الدليل الكتابي الذي يثبت به التصرف ولو لم يكن معدا للإثبات، كالرسائل والبرقيات والدفاتر التجارية.[4]

أما كلمة إلكتروني فيتجه العلماء إلى تعريفها بأنها: " كل ما يختص بدراسة حركة وسلوك الإلكترونيات المسببة للتيار، سواء كان ذلك باستخدام الصمامات المفرغة، أو المحتوية على غازات، أو الصمامات الضوئية أو أشياء المواصلات وهكذا، أو هو فرع

[1] د. أحمد مختار عمر، معجم اللغة العربية المعاصرة، عالم الكتب، القاهرة، 2008، ص52.

[2] العسكري أبو هلال بن عبد الله، الفروق اللغوية، تحقيق: محمد إبراهيم سليم، دار العلوم الثقافية للنشر والتوزيع، القاهرة، 1997، ص188.

[3] كواحلة يمينة، محاضرات على الخط في مقياس إدارة المستند الرقمي، مقدمة لطلبة السنة الأولي ماستر: علوم اقتصادية، تخصص اقتصاد رقمي، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة لونيسي علي، البليدة 02، 2022/2021، ص ص5-6.

[4] كواحلة يمينة، المرجع السابق، ص6.

الكهرباء الذي يهتم بتصرفات واستعمال الأنابيب وشبه المواصلات وسائر الدوائر التي تستعمل فيها".[1]

يتضح أن مصطلح (إلكتروني) يشمل كل ما يرتبط بالتكنولوجيا الحديثة، ويمتلك خصائص كهربائية أو رقمية أو مغناطيسية أو لاسلكية أو بصرية أو كهرومغناطيسية أو مؤتمتة أو ضوئية وما شابه ذلك. وتظهر المعلومات ذات الطبيعة الإلكترونية في أشكال متعددة كالنصوص، والرموز، والأصوات، والصور، وبرامج الحاسب الآلي، وقواعد البيانات. كما يمكن أن تكون هذه المعلومات ضمن نظام يُستخدم لإنشاء أو استخراج أو إرسال أو استلام أو تخزين أو عرض أو معالجة البيانات أو الرسائل بوسائل إلكترونية.[2]

ثانيا: اصطلاحا.

ومن ذلك أن المستند الإلكتروني هو عبارة عن معلومات تم إنشاؤها أو إرسالها أو تخزينها أو استلامها بوسيلة الكترونية أو ضوئية أو رقمية مادامت تتضمن إثبات واقعة أو تصرف قانوني محدد وتتضمن توقيع الكتروني ينسب هذه الواقعة أو التصرف لشخص معين.

يعرفه **العلامة العبودي:** أقراص الكترونية تسجل فيها المعلومات من خلال كتابة غير تقليدية للمعلومات مستخرجة من وسائط خزن لتقنيات علمية تعمل على تحويل الحروف المكتوبة والسندات المرسلة عن طريقها إلى نبضات كهربائية، فيتحول الضغط على الحروف إلى إشارة كهربائية تؤدي إلى طبع هذه الحرف أو استنساخها عن بعد بسرعة قياسية لا تزيد عن دقيقة واحدة مهما طالت المسافة.[3]

---

[1] علي محمد أحمد أبو العزء، التجارة الإلكترونية وأحكامها في الفقه الإسلامي، ط1، دار النفائس، الأردن، 2008ء ص38.

[2] رضا متولي وهدان، النظام القانوني للعقد الإلكتروني، مجلة البحوث القانونية والإقتصادية، مجلة فصلية محكمة يصدرها أساتذة كلية الحقوق جامعة المنصورة، العدد الثاني والأربعون، أكتوبر 2007، ص28.

[3] كواحلة يمينة، المرجع السابق، ص6.

ثالثا: التعريف الفقهي.

جاء اهتمام الفقهاء بالبحث عن تعريف متكامل حول المستند الالكتروني حيث جاءت معظم الاجتهادات في قالب واحد، بحيث اعتبره جانب منهم الكتابة الواردة على دعامة إلكترونية، والتي تثبت تصرفا قانونيا ويترتب عليها أثر قانوني، وقد استند جانب آخر إلى التعريف السابق، مع استلزام شرط تحرير المستند من طرف موظف عام مختص، وذلك حتى تثبت الصفة الرسمية لذلك المستند.[1]

هذا ولقد اتجه جانب من الفقه إلى تعريف المستند الإلكتروني على أنه: "كل دعامة مادية أو غير مادية، تصلح لأن تدون عليها المعلومات أو الآراء"، أو هو: "الشيء المادي الذي يمكن أن يدون عليه شيء معنوي"، و يرى جانب آخر أن المقصود بالمستند في مجال المعلوماتية: " كل شيء مادي متميز قرص أو شريط ممغنط أو خلافه) يصلح لأن يكون دعامة أو محلا لتسجيل المعلومات المعالجة بواسطة نظام المعالجة الآلية".[2]

وقد ذهب بعض الفقه إلى إطلاق مصطلح (المستند المعالج آلياً) على المستند الإلكتروني، مُعرفاً إياه بأنه: كل دعامة مادية مُعدة لاستقبال المعلومات وتخزين المعطيات عليها، من خلال تطبيق إجراءات المعالجة الآلية للمعلومات[3]." وبعبارة أخرى فهو يقصد بالمستند المعالج آليا: " الدعامة المادية التي تم تحويل المعطيات المسجلة عليها إلى لغة الآلة".[4]

---

[1] حمدي أحمد سعد أحمد، المر جع السابق، ص.14.

[2] عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، تقديم فتوح الشاذلي، دار الثقافة للطباعة والنشر، عمان، الأردن، 1999، ص 150.

[3] محمد عقاد، جريمة التزوير في محررات الحاسب الآلي، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون، دار النهضة العربية، القاهرة، 1995، ص36.

[4] لقد أطلق المشرع الجزائري على نظام المعالجة الآلية للمعلومات مصطلح نظام المعالجة الآلية للمعلومات والمعطيات للإشارة فلقد عرفت الاتفاقية الدولية للإجرام المعلوماتي أي اتفاقية بودابست الموقعة في 8 نوفمبر 2001" النظام المعلوماتي في مادتها الثانية بحيث جاء في نصها ما يلي: " نظام معلوماتي (système informatique) يعني كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة، والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى تنفيذاً لبرنامج معين، بأداء معالجة آلية للبيانات". يراجع:هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، ط1، دار النهضة العربية، القاهرة، 2007، ص111.

رابعا: التعريف التشريعي.

جاء تعريف المستند الإلكتروني في القانون النموذجي للأونسيترال19، في المادة الثانية الفقرة (أ)، تحت مسمى (رسالة بيانات)، حيث اعتبرها بأنها: المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك – على سبيل المثال لا الحصر – تبادل البيانات إلكترونياً، أو البريد الإلكتروني، أو البرق، أو التلكس، أو النسخ البرقي. ومن خلال التمعن في نص هذه المادة، يتضح أن المشرع استعمل مصطلح (رسالة بيانات) بدلاً من (المستند الإلكتروني)، وذلك بالنظر إلى تعدد الوسائل التي يتم بواسطتها التعامل مع هذا المستند، والتي ورد ذكرها على سبيل المثال لا الحصر..[1]

عرّف **المشرّع الأمريكي** المستند الإلكتروني في القانون الموحد للتجارة الإلكترونية، بموجب المادة الثانية الفقرة السابعة، بأنه السجل الذي يتم إنشاؤه أو تكوينه أو إرساله أو استلامه أو تخزينه بوسائل إلكترونية، ومن خلال هذا التعريف يتضح أن المشرّع الأمريكي اعتمد مصطلح (السجل) بدلاً من مصطلحي (رسالة البيانات) أو (المعلومات)، رغم أن هذين الأخيرين يعدّان أكثر دقة من الناحية المفاهيمية [2].

أما **التشريع الفرنسي**، ووفقاً للقانون الصادر سنة 1988 بشأن بعض الجرائم المعلوماتية، فقد عرّف المستندات المعالجة آلياً بأنها تلك التي تخضع للمعالجة بواسطة الحاسب الآلي، والتي تُصاغ ابتداءً بإحدى لغات البرمجة. وبذلك يكون استعمال مصطلح (المحررات المعلوماتية) بمثابة خطوة أولى تسبق عملية المعالجة الآلية، ليقع التزوير لاحقاً على هذه المستندات المعالجة آلياً تحديداً، وهو ما قصده المشرّع الفرنسي. وتكمن أهمية ذلك

[1] قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية السنة الرابط : https://uncitral.un.org أطلع عليه بتاريخ 2025/04/03

[2] صالح شنين، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، رسالة دكتوراه في القانون الخاص، جامعة تلمسان، 01، ص 45.

في كونه يعكس حداثة المصطلح ويُحسب للمشرع الفرنسي انفتاحه على استخدام مفاهيم تقنية جديدة.[1]

إلى جانب التعاريف الصادرة عن المنظمات الدولية والهيئات المهنية، فقد أولت التشريعات الوطنية كذلك اهتماماً بتعريف المستند الإلكتروني، ومن بين هذه التشريعات ما جاء في دول الخليج والمشرق العربي، حيث نص القانون الاتحادي رقم1 لسنة 2006 بشأن المعاملات والتجارة الإلكترونية على استعمال مصطلح (السجل) أو (المستند الإلكتروني)، وقد عرّفته المادة 1/9 بأنه: كل سجل أو مستند يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية، سواء على وسيط ملموس أو على أي وسيط إلكتروني آخر، شريطة أن يكون قابلاً للاسترجاع بصيغة يمكن فهمها."[2]

وهو نفس التعريف الذي نصت عليه المادة 2/7 من القانون الإماراتي المتعلق بالمعاملات والتجارة الإلكترونية.[3]

أما قانون المعاملات الإلكترونية الأردني فقد استعمل مصطلح (السجل الإلكتروني) للتعبير عن المستند الإلكتروني، حيث عرّفته المادة (2/7) بأنه: القيد أو العقد أو رسالة المعلومات التي يتم إنشاؤها أو إرسالها أو تسلّمها أو تخزينها بوسائل إلكترونية. كما نصت الفقرة (6) من المادة ذاتها على تعريف (رسالة المعلومات)، واعتبرتها بأنها: المعلومات التي يتم إنشاؤها أو إرسالها أو تسلّمها أو تخزينها بوسائل إلكترونية أو بوسائل مشابهة، بما في ذلك تبادل البيانات[4].

أما المشرّع المصري، فقد استعمل في قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية وصناعة تكنولوجيا المعلومات مصطلح (المحرر الإلكتروني) للدلالة على المستند

[1] هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، ص 120.

[2] قانون اتحادي رقم (1) لسنة 2006 في شأن المعاملات والتجارة الإلكترونية، ج. ر، ع442 ، س. السادسة والثلاثون بتاريخ 31/1/2006.

[3] قانون رقم (2) لسنة 2002 بشأن المعاملات والتجارة الإلكترونية في الإمارات العربية الصادر بتاريخ 30 ذي القعدة 1422 الموافق 12 فبراير 2002.

[4] التنظيم القانوني رقم 85 لسنة 2001 المؤرخ في 31 ديسمبر 2001 المتعلق بالمعاملات الإلكترونية الأردني، ع.4524، والذي أصبح ساري المفعول بتاريخ 31 مارس 2002.

الإلكتروني. وقد عرّفته المادة (1/ب) من هذا القانون بأنه: رسالة تتضمن معلومات يتم إنشاؤها أو دمجها أو تخزينها أو إرسالها أو استلامها كلياً أو جزئياً بوسيلة إلكترونية أو ضوئية أو بأي وسيلة أخرى مشابهة، بما في ذلك البريد الإلكتروني أو البرق أو التلكس أو النسخ البرقي[1]."

أما المشرع **الجزائري** فلم يتطرق إلى تعريف المستند الإلكتروني، بل ترك مهمة تعريفه إلى الفقهاء، مكتفيا بتعريف الكتابة الإلكترونية[2]، التي تعرض لها بموجب المادة 323 مكرر من القانون المدني التي تنص: " ينتج الإثبات بالكتابة من تسلسل حروف أوصاف أو أية رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها".[3]

الفرع الثاني: خصائص المستند الإلكتروني.

في ظل التحول الرقمي المتسارع، أصبحت المستندات الإلكترونية جزءًا أساسيًا من الحياة اليومية للأفراد والمؤسسات. تُستخدم هذه المستندات في المعاملات الرسمية، التعاقدات، والمراسلات، مما يجعل فهم خصائصها أمرًا ضروريًا لضمان الأمان والكفاءة في التعامل معها، فيما يلي:

أولا: القيمة القانونية.

يُعد المستند الإلكتروني الأداة الأساسية لتجسيد مفهوم الحكومة الإلكترونية، التي تقوم على توظيف نظم المعلومات الرقمية في إنجاز المعاملات الإدارية الإلكترونية، وتقديم الخدمات العامة، وتعزيز قنوات التواصل مع المواطنين بما يحقق مزيداً من الشفافية والإفصاح. ويُشكل هذا المستند تحولاً جوهرياً في طبيعة التعبير عن المعاني والأفكار

[1] القانون رقم 15 لسنة 2004 بشأن تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

[2] يرى الأستاذ الزهر بن سعيد أن اعتراف المشرع الجزائري بالكتابة الإلكترونية من شأنه أن ! حداً للغموض والجدل الذي كان يكتنف هذا النوع من الكتابة، كما يرى أنه باعترافه هذا يكون قد واكب التطور التقني الهائل في مجال التجارة الإلكترونية... الخ. مأخودة من لزهر بن سعيد، المرجع السابق، ص. 144.

[3] قانون رقم 05-10 المؤرخ في 13 جمادى الأولى عام 1426هـ الموافق 20 يونيو 2005 المعدل والمتمم للأمر رقم 58-75 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر س 1975 المتضمن القانون المدني الجزائري، ج.ر، ع.44، س. 2005.

الإنسانية المترابطة، إذ يصبح وسيلة للتفاهم وتبادل الأفكار بين الأفراد، إضافة إلى تمتعه بقيمة قانونية تجعله محل ثقة واعتماد في المعاملات بين الأفراد والمؤسسات والجهات الحكومية. وبناءً على ذلك، فإن أي مساس بمضمونه أو تغيير في الحقائق التي يتضمنها يُعرضه للمساءلة القانونية.[1]

ثانيا: السرية.

تتسم المستندات الإلكترونية بالسرية، إذ لا يحق الاطلاع عليها إلا للمرسل أو المرسل إليه، لما تنفرد به من خصوصية مدعومة بتقنيات متطورة توفر لها الحماية والأمن. وقد عززت تشريعات المعاملات الإلكترونية هذه الحماية بهدف ترسيخ الثقة فيها، وذلك من خلال النص على اعتماد وسائل تقنية تضمن سلامتها، مثل أنظمة التشفير، إضافة إلى شهادات التصديق الصادرة عن جهات رسمية موثوقة تثبت أن الحقوق المقررة في المحررات تعود فعلاً إلى صاحب التوقيع المثبت عليها.[2]

ثالثا: الصفة الإلكترونية.

يكتسب المستند أو المحرر الصفة الإلكترونية من خلال خضوعه لعمليات تقنية مثل الكتابة أو الضغط أو التخزين أو الاسترجاع أو النقل أو النسخ، وجميعها تتم عبر وسائط تكنولوجية إلكترونية، بحيث لا يمكن استخدامه خارج هذا الوسط. ويتميز المحرر الإلكتروني كذلك بإمكانية تحميله ونقله من جهاز إلى آخر بواسطة دعامات إلكترونية.

وعلى خلاف المستند التقليدي المرتبط بدعامة ورقية لا تنفصل عنها المعلومات المدونة عليها، فإن المستند الإلكتروني يُسجل على دعامات تقنية مثل الأقراص الصلبة أو المرنة أو الضوئية وغيرها وبالتالي، في حين يظل المضمون في السند التقليدي مرتبطاً

[1] إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة للنشر، الإسكندرية، 2002، ص 17.

[2] إلهام بن خليفة، الحماية الجنائية لمحررات الإلكترونية من التزوير، أطروحة دكتوراه في العلوم القانونية والإدارية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2016، ص 23.

ارتباطاً وثيقاً بالورق كوسيط وحيد للتخزين، فإن المستند الإلكتروني ينفرد بمرونة أكبر من خلال إمكانية تخزين محتواه على وسائط إلكترونية متعددة.[1]

الفرع الثالث: المستند الالكتروني وما يميزه عن المستند التقليدي.

مع تطور التكنولوجيا وزيادة الاعتماد على الحلول الرقمية، يُتوقع أن يستمر التحول نحو المستندات الإلكترونية، مما يتطلب من الأفراد والمؤسسات التكيف مع هذه التغييرات لضمان الكفاءة والأمان في التعاملات اليومية، وعليه سنحاول معرفة الفرق بين المستند الإلكتروني والمستند التقليدي.

هناك عدة جوانب تجعل المستند الإلكتروني يختلف عن المستند التقليدي ومن خلال هذه النقطة نبرز نقاط التشابه والإختلاف بينهما.

أولا: نقاط الاتفاق.

بالنسبة للنقاط التي يلتقي فيها كل من المستند الإلكتروني والمستند التقليدي نجد بأن كلاهما ناتج عن كتابة حروف، رموز أو علامات تعبر عن فكرة معينة وهما محل حماية جزائية[2]، حيث أن الإعتداء عليهما وتغيير مضمونهما يعتبر جريمة تزوير يعاقب عليها إذ يتمتعان بنفس الحماية الجزائية.

كذلك نجد بأن للمستندات الإلكترونية ذات الحجية المقررة للمستندات التقليدية في عملية الإثبات" هذا ما ذهب إليه المشرع الجزائري من خلال المادة 323 مكرر 1 من القانون 05-10 إذ جعل الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق مع تأكيد هوية الشخص الذي أصدرها". [3]

هذا ما ذهب إليه المشرع الفرنسي أيضا في القانون المدني في المادة 1366[4].

---

[1] كحلول سماح، حجية الوسائل التكنولوجية في إثبات العقود التجارية، مذكرة ماستر في القانون العام للأعمال، كلية الحقوق السياسية، جامعة قاصدي مرباح، ورقلة 2015، ص 05.

[2] عادل مستاري، رواحنة زوليخة، جريمة التزوير الإلكتروني، مجلة العلوم الإنسانية، المجلد 17، العدد 46، جامعة محمد خيضر، بسكرة، الجزائر، الصادر في مارس 2017، ص 300.

[3] صالح شنين، المرجع السابق، ص45.

[4] Code civil français, dernière modification 08/12/2021.

"L'écrit électronique possède la même valeur probante que l'écrit sur support papier, à condition que l'auteur puisse être dûment identifié et que le document soit établi et conservé dans des conditions garantissant son intégrité".

ثانيا: نقاط الإختلاف.

فيمكن التفرقة بينهما على أساس الوعاء أو المظهر الذي يتم إدراج المعلومات فيه، وعلى ذلك تكون المحررات المعلوماتية هي تلك الموجودة داخل النظام المعلوماتي[1]، عكس المستندات التقليدية التي تكون موجودة على دعامة ورقية نقاط الإختلاف بينهما أيضا سهولة كشف التزوير في المستند التقليدي الذي يمكن تمييز أصله عن النسخ عكس المستند الإلكتروني[2]،كما أن المستندات التقليدية يمكن الإطلاع على محتواها بمجرد النظر إليها بينما المستند الإلكتروني لا يمكن الإطلاع عليه بمجرد الرؤية بل يلزم وضعه في وسيط إلكتروني قابل لقراءته [3]هذا ما يجعله أكثر سرية. ويرى الدكتور أشرف توفيق شمس الدين بأنه إذا كانت طرق التزوير في المستندات التقليدية محددة على سبيل الحصر– فإن هذه الطرق يجب النص عليها بصفة مرنة في المستندات الإلكترونية، ذلك أن طرق التزوير فيها تخضع دائما للتغيير والتطور طالما أن التكنولوجيا الحديثة في تطور مستمر ومتزايد[4].

المطلب الثاني: مفهوم جريمة المستند الالكتروني.

مع التوسع الهائل في استخدام التكنولوجيا الرقمية واعتماد المستندات الإلكترونية في مختلف جوانب الحياة، ظهرت جريمة تزوير المستند الإلكتروني كشكل مستحدث من أشكال التزوير التقليدي. لم تعد الجريمة مقتصرة على العبث بالمستندات الورقية، بل امتدت لتشمل التلاعب بالبيانات والمعلومات الرقمية، ولمعرفة هاته الجريمة سنحاول التعرف على

[1] أيمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية– الطبعة الأولى، مكتبة القانون والإقتصاد، المملكة العربية السعودية، 2014، ص 385.

[2] عادل مستاري، رواحنة زوليخة، المرجع السابق، ص 300

[3] صالح شنين، المرجع السابق، ص 48.

[4] إلهام بن خليفة، المرجع السابق، ص 23.

مايلي: الفرع الأول": تعريف جريمة تزوير المستند الإلكتروني، الفرع الثاني: اركان جريمة تزوير المستند الإلكتروني.

الفرع الأول": تعريف جريمة تزوير المستند الإلكتروني.

تُعرف جريمة تزوير المستند الإلكتروني بأنها: "كل تغيير متعمد للحقيقة في مستند إلكتروني، باستخدام وسائل تقنية، بهدف إحداث ضرر أو تحقيق منفعة غير مشروعة."

يشمل ذلك التلاعب في البيانات أو التوقيعات الرقمية أو إنشاء مستندات إلكترونية مزيفة.

تُعد جريمة تزوير المستند الإلكتروني من الجرائم الماسة بالثقة العامة، إذ تقوم على تغيير الحقيقة، باعتبار أن جوهر التزوير – أياً كانت وسيلته – هو الكذب، وغايته النيل من اعتقاد الغير.

ويُعرّف التزوير بأنه تغيير الحقيقة في بيانات محرر معين بإحدى الوسائل التي حددها القانون، على نحو يترتب عليه ضرر بالغير، مع توافر نية استعمال ذلك المحرر فيما زُوِّر من أجله. كما عُرّف أيضاً بأنه تغيير للحقيقة بقصد الغش في محرر، بإحدى الطرق المقررة قانوناً، تغييراً من شأنه أن يُسبب ضرراً للغير. وباختصار، هو إظهار الكذب في صورة الحقيقة خداعاً لاعتقاد الغير. أما الفقه الفرنسي فقد ذهب إلى تعريفه بأنه: تغيير الحقيقة في وقائع أُعد المحرر لإثباتها، متى كان هذا التغيير من شأنه أن يُحدث ضرراً أو ارتُكب بقصد الغش.[1]

غير أنه بعد ظهور التكنولوجيات الحديثة وتقنية الحاسوب الآلي اكتسب التزوير شكلاً جديداً وأضحى يطلق عليه التزوير المعلوماتي، وقد أطلقت هذه التسمية عليه لأنه أصبح يرد على وثائق ومحررات معلوماتية، أي تلك التي يتم الحصول عليها بواسطة جهاز إلكتروني أو كهرومغناطيسي أو أشرطة ممغنطة، ويعرف التزوير المعلوماتي" بأنه التلاعب

[1] حجازي عبد الفتاح بيومى، التزوير في جرائم الكمبيوتر، المرجع السابق، ص 154.

في المعلومات المخزنة في أجهزة الحاسب الآلي المرتبطة بالشبكة أو اعتراض المعلومات بقصد تخزينها".[1]

أورد المشرع الجزائري جرائم التزوير بصورها المختلفة في المواد من 197 إلى 241 من قانون العقوبات[2]، وقسمها إلى مجموعات وهي:

"تزوير النقود وما يتصل بها، تقليد أختام الدولة والطوابع والعلامات التزوير في المحررات، وشهادة الزور وما شابهها". [3]

"كما يُعرَّف التزوير المعلوماتي بأنه تغيير للحقيقة في المستندات المعالجة آلياً أو المستندات المعلوماتية، يتم بنية استعمالها. ويتحقق ذلك من خلال إنشاء أو تعديل غير مشروع للبيانات المسجلة، على نحو يمنحها قوة وحجية تؤدي إلى خداع أصحاب الحقوق القانونية المرتبطة بأمن وسلامة وإمكانية تشغيل البيانات الإلكترونية. وقد أكدت المذكرة التفسيرية للاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية، المعروفة باتفاقية بودابست، هذا المفهوم عند تناولها لجريمة التزوير المعلوماتي في نص المادة (7)."[4]

وجريمة التزوير الإلكتروني واحدة من أنواع الجرائم التي تندرج تحت فئة الجرائم الإلكترونية، 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.

---

[1] فائزة يونس الباشاء، السياسة الجنائية لجرائم الكمبيوتر في التشريع الليبي (نموذجا ومقارنا)، دار النهضة العربية، القاهرة 2013، ص37.

[2] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج2، جرائم الفساد– جرائم المال والأعمال– جرائم التزوير، منقحة ومتممة في ضوء قانون 20 فبراير 2006 المتعلق بالفساد، 96، دار هومة، الجزائر 2008، ص. 307.

[3] المرجع نفسه، ص 307.

[4] محمد حسين علي محمود، التزوير باستخدام الوسائل الالكترونية، رسالة ماجستير في الحقوق، كلية الحقوق، جامعة القاهرة، 2011، ص36.

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[1].

الفرع الثاني: اركان جريمة تزوير المستند الإلكتروني.

لقيام جريمة تزوير المستند الإلكتروني لا بد من توافر مجموعة من الأركان التي تشكل الأساس القانوني لإثباتها ومعاقبة مرتكبها، ومن بين هاته الأركان الركنان المادي والمعنوي والذي سنحاول التعرف عليهما من خلال التالي:

أولا: الركن المادي.

يمثل الركن المادي الجانب الملموس من الجريمة، ويتمثل في الأفعال المادية التي يقوم بها الجاني، وبتجلى الركن المادي من خلال عنصرين، الأول يتمثل في تغيير الحقيقة، أي تغيير في بنود المستند عما كانت عليه ويقصد بالحقيقة "هي ما اتجهت إليه من ينتسب إليه المستند، ويكفي التغيير أن يكون جزئيا أو كليا". وهناك عدة عناصر أساسية يجب توافرها لقيام هاته الجريمة [2]هي:

أ/-وجود محرر.

ب/-تغيير الحقيقة بإحدى الطرق المنصوص عليها قانونا.

ج/-أن يترتب على ذلك ضرر عام أو خاص في الحاضر أو في المستقبل[3].

وسنبين ذلك في العناصر التالية:

أ/ وجود محرر: اشترط في جريمة التزوير التقليدية أن يقع فعل تغيير الحقيقة على محرر من المحررات العمومية أو الرسمية أو في المحررات العرفية أو التجارية أو المصرفية أو في بعض الوثائق الإدارية والشهادات، كما اشترط في المحرر أن يكون في شكل "كتابة" او عبارات خطية، في حين أنه في جريمة التزوير المعلوماتي، فإن المستند المعلوماتي هو

[1] العبادي محمد حميد الرصفان، الجرائم المستحدثة في ظل العولمة، ط1، دار جليس الزمان، عمان. 2015، ص 177.

[2] محمد أمين الرومي، مرجع سابق، ص 74.

[3] خشير مسعود، الحماية الجنائية البرامج الكمبيوتر، دار الهدى الجزائر ،2010، ص ص 134- 135.

الدعامة المادية التي تم تحويل المعطيات المعالجة عليها، فيكون إما قرص مضغوط أو شريط ممغنط. ومنه المستند المعلوماتي الذي يقع عليه فعل التزوير هو كل جسم منفصل أو يمكن فصله عن نظام المعالجة الآلية للمعطيات التي نظمها المشرع الفرنسي في الباب الثالث من القسم الثاني من الكتاب الثاني من قانون العقوبات الفرنسي في المواد من 323-1 إلى 232-7 وتجريم المشرع الفرنسي لتزوير الوثائق المعلوماتية جاء بسبب ارتباط هذه الوثائق أو المستندات المعلومات بقانون الإثبات، لذلك جاءت المادة 441-1 من قانون العقوبات الفرنسي لتجريم التزوير الذي من شأنه أن يسبب ضرراً والذي يتم بأي وسيلة كانت وفي محرر أو سند للتعبير عن الرأي.[1]

"أما المشرع الجزائري فقد تناول جريمة تزوير المحررات في المواد من 214 إلى 229 من قانون العقوبات، حيث اشترط لقيامها وجود محرر بالمعنى التقليدي، الأمر الذي يجعل من غير الممكن تطبيق هذه النصوص على أفعال التزوير المعلوماتي. وهو ما يقتضي بالفعل تدخلاً تشريعياً، إما من خلال تعديل أحكام التزوير التقليدي على غرار ما قام به المشرع الفرنسي عندما استبدل عبارة (أي سند) بمفهوم (المحرر التقليدي)، أو عن طريق إدراج نص خاص بجريمة التزوير المعلوماتي، يكون مستقلاً عن الجرائم المتعلقة بالمساس بنظم المعالجة الآلية للمعطيات المنصوص عليها في القسم السابع مكرر، ضمن المواد من 394 مكرر إلى 394 مكرر 7، والتي جاءت أساساً لتحقيق الحماية الجنائية للنظم المعلوماتية."

ب /تغيير الحقيقة: يقصد بتغيير الحقيقة استبدالها بما يخالف واقعها، ومن ثم لا يعد مجرد الإضافة إلى المحرر أو الحذف منه تغييراً للحقيقة، طالما لم يتأثر مضمونه الأصلي قبل تلك الإضافة أو الحذف. غير أن الأمر يختلف بالنسبة للمستندات المعلوماتية، إذ يُعتبر حذف البيانات أو إضافتها أو التلاعب بها بأي صورة من صور التغيير، سواء أكانت هذه البيانات مخزنة في ذاكرة الحاسب أو مدمجة في برامج التشغيل أو تطبيقاتها، محلاً للتجريم.

[1] معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة ماجستير في العلوم القانونية، تخصص قانون جنائي، جامعة الحاج لخضر، باتنة، 2012، ص ص 46- 47.

ويظهر تغيير الحقيقة في المعلومات المعالجة آلياً على كيان مادي، قد يكون ورقياً أو دعامة إلكترونية مثل الأشرطة الممغنطة أو الأقراص الإلكترونية أو غيرها من الوسائط المماثلة.[1]

ج/ الضرر: الضرر هو عنصر جوهري في جريمة التزوير، إذ لا يكفي لاكتمال الركن المادي في هذه الجريمة تغيير لحقيقة في محرر، وأن يحدث هذا التغيير بإحدى الطرق التي بينها القانون، ولم ينص المشرع الجزائري عند تعرضه لجريمة تزوير المحررات الرسمية على الضرر باعتباره عنصرا في جريمة التزوير[2] ، لأن موضوع الضرر من المسائل الموضوعية لا القانونية.

يمكن القول إن الضرر في جريمة تزوير المستند الإلكتروني يتحقق عند قيام الجاني باستعماله والاحتجاج به في مواجهة الغير، بما يؤدي إلى تعريض مصالح الآخرين للخطر أو توقع تحقق هذا الخطر مستقبلاً وفقاً للمجرى العادي للأمور، ويُقدَّر الضرر في هذه الجريمة من وقت وقوع تغيير الحقيقة في المستند الإلكتروني، ولا يعفى الجاني من المسؤولية الجنائية حتى وإن انتفى احتمال تحقق الضرر بعد ذلك، كما هو الحال مثلاً عند إتلاف المستند الإلكتروني أو موافقة صاحب التوقيع الإلكتروني – بعد تزويره – على مضمون المستند، وبناءً عليه، فإن التزوير في المستند الإلكتروني يتحقق متى وقع تغيير للحقيقة في مستند إلكتروني يتمتع بصفة الحفظ أو الاستلام أو الإرسال عبر وسيلة إلكترونية، وله قيمة قانونية تجعله صالحاً لإثبات حق أو تصرف قانوني، شريطة أن يترتب على ذلك التغيير ضرر فعلي أو محتمل.

ثانيا: الركن المعنوي.

يتطلب هذا الركن إثبات نية الفاعل في ارتكاب الجريمة بقصد الخداع أو الإضرار بالغير. ويشمل ذلك العلم بأن المستند مزور والإرادة في استخدامه لتحقيق غاية غير مشروعة. فإذا كان الفعل غير مقصود أو ناجم عن خطأ غير عمدي، فلا يمكن اعتبار الجريمة مكتملة الأركان.

---

[1] خشير مسعود، المرجع السابق، ص136.

[2] دردوس مكي، القانون الجنائي الخاص في التشريع الجزائري ، المرجع السابق، ص47.

بحيث الركن المعنوي في جريمة تزوير المستندات إلكترونية في القصد الجنائي، على اعتبار أنها جريمة من الجرائم العمدية، وبالتالي يتخذ القصد الجنائي فيها صورة القصد العام والمتمثل في علم الجاني بفعل تغيير الحقيقة في المستند، مع إرادة إلحاق ضرر بشخص ما. وتتخذ صورة القصد الجنائي الذي يأخذ صورتين، **قصد جنائي عام** يقوم على ضرورة توفر على العلم والإرادة في ارتكاب جريمة ما[1]، أما الصورة الثاني فتتمثل في **القصد الجنائي الخاص** الذي يتمثل باتجاه نية الجاني في استعمال المحرر فيما زوّر من اجله ولو لم يستعمله والتزوير إما ماديا أو معنويا يترك أثر على المستند قد يعرف هذا الأثر بالحواس أو بواسطة الخبرة والتزوير المعنوي هو إثبات غير الحقيقة في المستند الإلكتروني مباشرة، ويكون ذلك بإثباته خاصة في المستند، وللتزوير عدة طرق تطرقت إليها مختلف التشريعات وهذا بمراعاة عدة أمور منها: وضع توقيعات مزورة وتغيير المحرر أو الكتابة أو التوقيع وكتابة إضافية أو مقحمة في السجلات أو المحررات العمومية بعد إتمام تحريرها أو اختتامها وأما المشرع المصري فوضع هو الآخر بعض طرق التزوير مثل وضع الأختام أو بصمات مزورة، إذ تعتبر كل المحررات والأختام أو الإمضاءات أو زيادة الكلمات ووضع أسماء أو صور أشخاص آخرين تزويراً.

خلاصة الفصل:

[1] خيثر مسعود، المرجع السابق، ص 138.

سعينا في هذا الفصل إلى توضيح أن جريمة تزوير المستند الإلكتروني تُعد من أبرز التحديات في العصر الرقمي، وذلك نتيجة التوسع الكبير في التعاملات الإلكترونية واعتماد الأفراد والمؤسسات على الوثائق الرقمية، ويُقصد بالمستند الإلكتروني كل وثيقة يتم إنشاؤها أو تخزينها أو نقلها عبر وسائل إلكترونية، وتشمل النصوص والصور والتوقيعات الرقمية والمعاملات المحوسبة.

إذ تقوم جريمة التزوير الإلكتروني على تغيير أو تعديل متعمد وغير مشروع في محتوى المستند الإلكتروني، بهدف الخداع أو تحقيق مصلحة غير مشروعة، يتخذ هذا التزوير أشكالاً متعددة، مثل تعديل البيانات، تغيير التوقيعات الرقمية، أو إضافة معلومات كاذبة.

تتسم هذه الجريمة بخصائص فريدة، أهمها طبيعتها الرقمية التي تجعلها غير ملموسة، وسرعة انتشارها عبر الشبكات، وصعوبة اكتشافها ما لم تكن هناك تقنيات متقدمة للكشف والتتبع، كما تتطلب هذه الجرائم خبرات تقنية متخصصة لإثبات وقوعها بشكل قانوني.

الفصل الثاني

الآليات القانونية لتجريم تزوير المستند الالكتروني

المبحث الأول: الحجية القانونية لتزوير المستندات الالكترونية.

المطلب الأول: المواثيق والأعراف الدولية.

الفرع الأول: الحجية القانونية وفق الاتفاقيات الدولية.

الفرع الثاني: حجية المستند الإلكتروني في الإثبات.

المطلب الثاني: النظام القانوني للمستند الالكتروني.

الفرع الاول: تنظيم المستند الالكتروني.

الفرع الثاني: شروط صحة المستندات الالكترونية.

المبحث الثاني: افعال المساس بالمستند الالكتروني ف التشريع الجزائري.

المطلب الاول: الفعل الماس بالمستند الالكتروني.

الفرع الأول: جريمة التزوير والحماية الجنائية.

الفرع الثاني: جريمة الاتلاف.

الفرع الثالث: جريمة الإحتيال.

المطلب الثاني: اجراء المشرع الجزائري من جريمة تزوير المستند الالكتروني.

الفرع الأول: الموقف الجزائري من جريمة تزوير المستند الالكتروني.

الفرع الثاني: العقوبات المقررة.

خلاصة الفصل.

تمهيد:

مع تزايد الاعتماد على المستندات إلكترونية، برزت الحاجة إلى حمايتها من عمليات التزوير والتلاعب، مما استدعى تدخل المشرع الجزائري لتنظيم هذه المسألة وتجريم أي اعتداء على مصداقية المستندات الإلكترونية.

انطلاقًا من التوجهات العالمية في مجال الأمن الرقمي، وسعى المشرع الجزائري إلى مواكبة هذه المعايير مع احترام الخصوصية القانونية والاجتماعية للبلاد، حيث عمل على إرساء آليات قانونية رادعة لمكافحة جريمة تزوير المستندات الإلكترونية. وقد تجلى ذلك من خلال تبني تعديلات تشريعية جوهرية، تم بمقتضاها إدراج نصوص صريحة في قانون العقوبات وفي القانون المتعلق بالمبادلات والتوقيع الإلكتروني، شملت تعريف المستند الإلكتروني، وتحديد أوجه التزوير المحظورة، وفرض عقوبات صارمة بحق المخالفين.

وتأتي هذه الآليات في إطار بالغ الأهمية يهدف إلى حماية المعاملات الرقمية وتعزيز موثوقيتها، لا سيما في ظل التنامي المستمر للجرائم الإلكترونية التي تستهدف تزوير البيانات والمستندات لأغراض احتيالية أو إجرامية. وعليه، تبرز الحاجة إلى دراسة معمقة للضوابط القانونية التي أقرها المشرع الجزائري لتجريم هذه الأفعال، وعليه سنحاول في هذا الفصل الاعتماد على ما يلي:

المبحث الأول:الحجية القانونية لتزوير المستندات الالكترونية، المبحث الثاني: افعال المساس بالمستند الالكتروني في التشريع الجزائري.

المبحث الأول: الحجية القانونية لتزوير المستندات الالكترونية.

الحجية القانونية للوثائق والمستندات الإلكترونية يقصد بها القوة الإثباتية التي تُمنح للبيانات والمعلومات المتولدة أو المتداولة عبر وسائل الاتصال الحديثة. ويُطرح هنا إشكال حول مدى إمكانية اعتماد هذه المستندات كأدلة إثبات أمام القضاء، خصوصًا وأن إنشاءها وتوقيعها وإرسالها وحفظها يتم في بيئة رقمية بحتة، دون الاستعانة بالوسائل التقليدية للكتابة، إلا إذا اقتضت الضرورة تحويلها إلى نسخة ورقية.[1]

غير أن هذا التردد لم يستمر طويلاً، إذ أدى التوسع السريع في استخدام التكنولوجيات الحديثة لإبرام المعاملات المدنية والتجارية إلى تغيير جذري في المواقف. ومواكبةً لهذا التحول، بادرت الهيئات التشريعية على الصعيدين الدولي والوطني إلى تعديل الأطر القانونية القائمة لتتلاءم مع المستجدات الرقمية، أو إلى استحداث تشريعات خاصة لتنظيم هذه المعاملات. وجاءت هذه التدابير بهدف توفير الحماية القانونية وضمان الحقوق في فضاء يتسم بطابع افتراضي غير، مما أحدث فراغًا تشريعيًا تطلب تدخلاً قانونيًا عاجلاً، وعليه سنحاول في هذا المبحث الاعتماد على المطالب التالية:

المطلب الأول: المواثيق والأعراف الدولية، المطلب الثاني: النظام القانوني للمستند الالكتروني.

المطلب الأول: المواثيق والأعراف الدولية.

سعت الهيئات الدولية إلى وضع مواثيق وأعراف قانونية تهدف إلى تنظيم الفضاء الرقمي وضمان أمن وسلامة المعاملات الإلكترونية. وقد تجسد ذلك في مجموعة من الاتفاقيات والبروتوكولات الدولية التي كرّست مبادئ التعاون القضائي والتقني بين الدول، وسعت إلى توحيد الجهود لمكافحة جرائم التزوير الإلكتروني، من خلال الاعتراف بحجية المستندات الرقمية، وتنظيم التوقيع الإلكتروني، وتعزيز آليات الإثبات في البيئة الرقمية. ومن

[1] عباس العبودي، الحجية القانونية لوسائل التقدم العلمي في الإثبات المدني، المكتبة القانونية، عمان، 2002 ، ص 144.

خلال هذا المطلب تم التطرق الى الفروع التالية: الفرع الأول: الحجية القانونية وفق الاتفاقيات الدولية، الفرع الثاني: حجية المستند الإلكتروني في الإثبات.

الفرع الأول: الحجية القانونية وفق الاتفاقيات الدولية.

أولا – الحجية القانونية للمستندات الالكترونية طبقا للاتفاقيات الدولية.

جاء في المادة (14/3) من اتفاقية الأمم المتحدة الخاصة بنقل البضائع بحرًا (قواعد هامبورغ) لسنة 1978 ما يفيد بأنه: يجوز أن يتم التوقيع على سند الشحن بخط اليد، أو بصورة مطابقة للأصل، أو عن طريق الفاكس، أو بالتثقيب، أو بالختم، أو باستخدام الرموز، أو بأي وسيلة آلية أو إلكترونية أخرى، شريطة ألا يتعارض ذلك مع القوانين السارية في الدولة التي صدر فيها سند الشحن كما نجد أن اتفاقية الأمم المتحدة المتعلقة بعقود البيع الدولي للبضائع (اتفاقية فيينا) عام1981: نصت في المادة(11) منها على أنه: (لا يشترط أن يتم انعقاد عقد البيع أو أثباته كتابة، ولا يخضع لأي شروط شكلية، ويجوز أثباته بأي وسيلة بما في ذلك الإثبات بالبينة) ، كما ان اتفاقية الأمم المتحدة المتعلقة باستخدام الخطابات الالكترونية في العقود الدولية (اتفاقية نيويورك) لسنة2005 نصت في المادة (8) منها على انه : " لا يجوز إنكار صحة المعلومات أو إمكانية إنفاذها لمجرد كونها بشكل خطاب الكتروني) ، كما حددت هذه الاتفاقية معايير تحقق التكافؤ الوظيفي بين الخطابات الإلكترونية والمستندات الورقية، وكذلك بين طرائق التوثيق الإلكترونية والتوقيعات الخطية وذلك في المادة (9) من هذه الاتفاقية".[1]

كما نصت المادة (1) من مشروع الاتفاقية العربية بشأن تنظيم أحكام التوقيع الإلكتروني في مجال المعاملات الإلكترونية في الدول العربية على أن العقود الإلكترونية تخضع للأحكام المقررة للعقود الكتابية، وجاء في المادة (19) من المشروع أن للتوقيع الإلكتروني، في نطاق المعاملات المدنية والتجارية والإدارية، الحجية ذاتها المقررة للتوقيع التقليدي وفقًا لقانون الإثبات في المواد المدنية والتجارية، أما المادة (21) فقد قررت أن

[1] سامح عبد الواحد التهامي، التعاقد عبر الانترنيت، دراسة مقارنة، دار الكتب القانونية ودار شتات للنشر و البرمجيات ، مصر،2008، ص 513.

النسخ الورقية المستخرجة من الوثائق والمحررات الإلكترونية تُعد حجة على الجميع متى كانت مطابقة لأصولها الإلكترونية، وذلك ما دامت هذه الأصول الرسمية والتوقيعات الإلكترونية محفوظة على الدعامة أو الوسيط الإلكتروني.[1]

ثانيا – الحجية القانونية للمستندات الالكترونية طبقاً للقوانين المقارنة.

منحت المادة (14) من قانون تنظيم التوقيع الإلكتروني المصري رقم 15 لسنة 2004 التوقيع الإلكتروني الحجية ذاتها المعترف بها للتوقيعات التقليدية في الإثبات، وذلك في نطاق المعاملات المدنية والتجارية والإدارية. ولكن هذه المعادلة في الحجية مشروطة بمراعاة الشروط المنصوص عليها في القانون عند إنشاء التوقيع وإتمامه، بالإضافة إلى الامتثال للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية.

وبالمثل، ساوت المادة (15) من القانون ذاته بين المحررات والكتابة الإلكترونية والمحررات الكتابية (الرسمية والعرفية) من حيث القوة الثبوتية ضمن ذات نطاق المعاملات. حيث تكتسب المستندات الإلكترونية هذه الحجية متى استوفت الشروط).[2]

وكذلك نجد قانون المعاملات الالكترونية الأردني رقم (15) لسنة 2015 نص في المادة (17) منه على إن:

أ – يكون للسجل الالكتروني المرتبط بتوقيع الكتروني محمي الحجية ذاتها المقررة للسند العادي ويجوز لأطراف المعاملة الالكترونية الاحتجاج به.

ب– يكون للسجل الالكتروني المرتبط بتوقيع الكتروني موثق الحجية ذاتها المقررة للسند العادي ويجوز لأطراف المعاملة الالكترونية والغير الاحتجاج به.

ج– في غير الحالات المنصوص عليها في الفقرتين (أ) و (ب) من هذه المادة يكون للسجل الالكتروني الذي يحمل توقيعاً الكترونياً الحجية ذاتها المقررة للسند العادي في

[1] عمر خالد زريقات، عقود التجارة الإلكترونية (عقد البيع عبر الإنترنيت دراسة تحليلية)، دار الحامد ط1، عمان، 2007، ص216.

[2] المرجع نفسه، ص216.

مواجهة أطراف المعاملة الالكترونية، وفي حال الإنكار يقع عبء الإثبات على من يحتج بالسجل الالكتروني.

د- يكون للسجل الإلكتروني غير المرتبط بتوقيع الكتروني حجية الأوراق غير الموقعة في الإثبات.

هـ - يجوز إصدار أي سند رسمي أو تصديقه بالوسائل الالكترونية شريطة ارتباط السجل الالكتروني الخاص به بتوقيع الكتروني موثق، كما إن قانون إمارة دبي رقم 2 لسنة 2002 الخاص بالمعاملات والتجارة الالكترونية نص في المادة (12/2) منه على إن يكون للمعلومات الإلكترونية ما تستحقه من حجية في الإثبات، وفي تقدير هذه الحجية يعطى الاعتبار لما يلي:

أ - مدى إمكانية التعويل على الطريقة التي تم بها تنفيذ واحدة أو أكثر من عمليات الإدخال أو الإنشاء أو التجهيز أو التخزين أو التقديم أو الإرسال.

ب- مدى إمكانية التعويل على الطريقة التي استخدمت في المحافظة على سلامة المعلومات.[1]

ج- مدى إمكانية التعويل على مصدر المعلومات إذا كان معروفاً.

د- مدى إمكانية التعويل على الطريقة التي تم بها التأكد من هوية المنشئ، إذا كان ذلك ذا صلة بأي عامل آخر يتصل بالموضوع.

الفرع الثاني: حجية المستند الإلكتروني في الإثبات.

أولا: حجية المستند في ظل غياب النص:

سنحاول تحديد حجية المستند الالكتروني في ظل غياب النص:

يرى أنصار هذا الاتجاه أن مصطلح المستند لا ينبغي حصره في الشكل الورقي وحده، بل يمتد ليشمل المستند الإلكتروني أيضًا، باعتبار أن مدلول الكلمة لغويًا لا يقتصر على نوع معين من الوسائط فالكتابة في نظرهم، تتمثل في مجموعة من الحروف أو الأرقام أو الرموز

[1] عمر خالد زريقات، المرجع السابق، ص217.

أو الإشارات التي تعبر عن معنى محدد وتُثبت على دعامة تحفظها. وإذا كان يُنظر تقليديًا إلى هذه الدعامة على أنها ورقية تحتوي بيانات موقعة يدويًا من الأطراف، سواء كُتبت بخط اليد أو أُنجزت بواسطة الآلة، فإن التطور التكنولوجي غيّر هذه النظرة، إذ لم يعد الهدف من اشتراط الكتابة هو الورق ذاته، بل إعطاء العقد شكلًا محددًا يضمن إمكانية قراءته وحفظه والرجوع إليه ونسخه عند الحاجة. ومن ثمّ، فإن التمسك بالمفاهيم التقليدية للكتابة والمستند والتوقيع لم يعد يتماشى مع الواقع الحديث، بل يتعين الأخذ بالكتابة الإلكترونية التي توفر ضمانات تقنية تفوق أحيانًا ما توفره الكتابة اليدوية، بما يؤكد أن الكتابة لا ترتبط بالورق ارتباطًا جوهريًا.[1]

إلا أن هناك رأيا فقهيا بوجود صعوبة في إضفاء طابع الإثبات في المحررات الإلكترونية، خاصة في مجال الاتصال وذلك تحت عدة مبررات تتمحور حول الدعامة الإلكترونية قابلة للتعديل والتبديل دون وجود أي دليل يثبت هذا التعديل كما أن هذا النوع لا يترك أثرا مدونا عكس الأثر الذي تتركه الدعامة الورقية، إلا أن هذا الرأي أصبح متجاوزا وذلك بفضل التطور الذي عرفه هذا المجال، فقد ظهرت مجموعة من التطبيقات التي تدعم صحة المستند الإلكتروني، وتقوي كمسألة الضمان والإثبات وجعله بذلك يضاهي على المستند الورقي ومن بين هذه التطبيقات التي ظهرت نجد نظام الإشعار بالتوصل الذي يسمح بالتثبيت من وضع الرسالة الإلكترونية، وتمكن كذلك المرسل من معرفة تاريخ ووقت توصل المرسل إليه بالرسالة من بين التطورات أيضا التي تؤيد قوة المستند الإلكتروني وتضاعف فرصة التمسك به كأداة للإثبات نجد نظام تشفير المعلومات في المستند الإلكتروني وكان لهذا النظام الفضل في الحفاظ على سرية المعلومات وعدم الاطلاع عليها إلا من طرف الأشخاص المرخص لهم بالاطلاع، لا يمكن الاطلاع على المستند الإلكتروني إلا من قبل الأشخاص المصرح لهم بذلك، وهو ما يمنحه مميزات خاصة تضمن استخدامه بشكل آمن من قبل الأطراف المتعاقدة، بل وتوفر له حماية تفوق في بعض الجوانب تلك

[1] عمار كريم كاظم وناريمان جميل نعمة، القوة القانونية للمستند الإلكتروني، كلية القانون العدد السابع، جامعة الكوفة،2007، ص182.

المقررة للمستند الورقي. غير أن هناك رأيًا آخر يوجّه انتقادًا لهذه الوسائل التقنية، إذ يرى أن مساواة الكتابة الإلكترونية بالكتابة اليدوية أمر غير دقيق، على اعتبار أن الكتابة اليدوية تُقرأ بسهولة وبشكل مباشر، بينما تتطلب الكتابة الإلكترونية – عند خضوعها للتشفير لحماية البيانات – إجراءات معقدة لفك الرموز التشفيرية حتى تصبح مفهومة، مما يجعلها غير مقروءة في صورتها الأولية، بخلاف الكتابة اليدوية التي يمكن الاطلاع عليها مباشرة دون وسائط أو إجراءات إضافية.[1]

والجدير بالذكر أن أساس الإثبات هو الحرية في جميع المعاملات التي تسمح بإثبات تصرفات قانونية بكافة الطرق، وإن تطبيق هذا المبدأ يعطي كل أطراف العقد الحرية في إثبات التصرفات القانونية وإقامة الحجة على التزاماتهم وادعاءاتهم بجميع الطرق المتاحة، ومن مميزات تطبيق هذا المبدأ هو إعطاء القاضي الحق في تقدير قيمة الدليل المستمد من الوسائل الإلكترونية، وهذا يخص العقود المدنية الإلكترونية، وهذا في إبرام العقد عن طريق الإيجاب والقبول يؤدي إلى وجود العقد وإنتاج آثاره.[2]

ثانيا: حجية المستند الإلكتروني في ظل وجود نص:

سنتطرق فيه الى تحديد حجية المستند الالكتروني في ظل وجود النص:

إن الإطار القانوني المنظم لفكرة المستند الإلكتروني يتجلى في لجوء العديد من التشريعات المقارنة إلى سن قوانين خاصة تُعنى بتنظيم مختلف صور هذا المستند، مثل التوقيع الإلكتروني، والسجلات الإلكترونية، والعقود الإلكترونية. وتقوم الحجية القانونية للمستند الإلكتروني في مجال الإثبات على مدى القيمة التي يمنحها له المشرع، فإذا نص القانون صراحة على هذه الحجية، أصبح المستند الإلكتروني مساوياً للمستند الورقي من حيث القوة القانونية. ولهذا اتجهت التشريعات الحديثة إلى الاعتراف الواضح بالمستندات الإلكترونية وإقرار مساواتها بالمحررات الورقية، إدراكاً منها للدور المتزايد الذي تؤديه في المعاملات.

[1] عمار كريم كاظم ناريمان جميل نعمة، المرجع السابق، ص 42.

[2] بلعيشة علي، الحماية الجنائية للمستند الإلكتروني، مذكرة لنيل شهادة الماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم الجزائر 2019، ص40.

وقد جاء ذلك ليضع حداً لكل الخلافات التي كانت ترى بعدم إمكانية إضفاء صفة الثبوتية على المحررات الإلكترونية، حيث اعتُبر المستند الإلكتروني المحرر على دعامة إلكترونية ذا ذات الحجية التي تتمتع بها الوثيقة الورقية، وهو ما كُرّس في عدة قوانين، من أبرزها تشريعات التوقيع الإلكتروني والسجلات الإلكترونية، لولاية نيويورك الأمريكية في نص المادة (105) منه على أن: " السجل الإلكتروني يكون له ذات القوة والأثر المقرر للسجلات المحررة بغير الوسائل الإلكترونية".[1]

تتباين التشريعات العربية في تنظيم الحجية القانونية للمستندات الإلكترونية، وإن كانت تتفق جميعًا على منحها قوة إثباتية. ففي البحرين، أقرت المادة (5/1) من قانون المعاملات الإلكترونية أن للسجلات الإلكترونية الحجية ذاتها المقررة للمحررات العرفية. كما يحظر القانون إنكار الأثر القانوني للمعلومات الواردة في السجل الإلكتروني، سواءً ظهرت كاملةً أو جزئيًا فيه، أو تمت الإشارة إليها داخله، وذلك من حيث صحتها وجواز الاعتماد عليها.

أما مشروع القانون الكويتي (للتجارة الإلكترونية لسنة 2006) فقد اتخذ نطاقًا أوسع وشملةً أشمل في المادة (4) منه، حيث منح الحجية القانونية لأي معلومات تتخذ شكل مستند إلكتروني، مساوياً إياها في الأثر القانوني بالمستند التقليدي،).[2]

وبالعودة إلى المشرع المغربي فرغم أنه أقر بأن يمنح للمستند الإلكتروني نفس قوة الإثبات الممنوحة للمستند الورقي، فقد أخضع هذا المبدأ لعدة شروط تتنافى مع وجودها ميزة الإثبات في المستند الإلكتروني وهذه الشروط كالتالي:

1. **الشرط الأول:** هو إمكانية التعرف بصفة قانونية على الشخص الذي صدرت منه وذلك أن تحل المعلومات الإلكترونية على هوية الشخص الذي أنشأ هذه المعلومات أو تسلمه أو أن تشمل أيضا على تاريخ إرسالها وتاريخ تسلمها، وأن تكون هذه المعلومات واضحة وقابلة

[1] المرجع نفسه، ص134.

[2] عمار كريم كاظم و ناريمان جميل نعمة، المرجع السابق، ص 192.

للقراءة وعدم استعمال أي وسائل غير مشروعة القصد منها عدم التعرف على معلومات المستند.

2. الشرط الثاني: هو أن تكون محفوظة ومعدة ضمن شروط تضمن تماميتها ومقتضى هذا الشرط هو أن يكون المستند الإلكتروني قابل للحفظ والتخزين والأرشفة شأنه في ذلك شأن المستند التقليدي، وذلك بالطرق الفنية المعروفة وكما أن المشرع الفرنسي قد منح المحررات الناتجة عن الفاكس والتلكس والميكروفيلم نفس القوة القانونية للمحررات التقليدية سواء كان أصل المستند أو صورته ، ولقد أكد المشرع الفرنسي على أنه في حالة تعرض سند إلكتروني وسند تقليدي يجب على القاضي أن يفاضل بينهما وأن يعتمد على الوسيلة التي أبرم بها السند وكما بينت المادة السادسة من القانون المتعلق بالتبادل الإلكتروني للمعطيات القانونية، حيث يتم الأخذ سلامة الوثيقة وأخذ كذلك صفة الإثبات بموجب قانوني[1]، وهذا ضمن شروط وهي:

1- أن يكون التوقيع الإلكتروني مرتبطًا بصاحبه، ويتم إنشاؤه بوسائل يملكها الموقع ويحتفظ بها تحت رقابته الخاصة بشكل حصري.

2- أن يرتبط التوقيع بالوثيقة الموقعة بطريقة تكشف أي تعديل لاحق قد يطرأ عليها، مع وجوب إنشائه عبر آلية معتمدة لتوليد التوقيع الإلكتروني، تكون صلاحيتها مثبتة بشهادة مطابقة، وتُعد هذه الشروط ضمانات أساسية لصحة التوثيق، إذ إن موثوقية التوقيع تمنح المستند الموقع به قوة إثباتية ومصداقية أكبر.[2]

المطلب الثاني: النظام القانوني للمستند الالكتروني.

نظرًا لخصوصية المستند الإلكتروني، فإنه يخضع لجملة من الأحكام والضوابط التي تميّزه عن غيره من المستندات التقليدية. وتستند صحة هذا النوع من المستندات إلى عدة

[1] عمار كريم كاظم و ناريمان جميل نعمة، المرجع السابق، ص192.

[2] ظهير شريف، رقم 1.07.129 صادر في 19 من ذي القعدة 1428 (30) نوفمبر (2007) بتنفيذ القانون رقم 05-53 المتعلق بالتبادل الالكتروني للمعطيات القانونية (المادة 08).

اعتبارات تتعلق بمراحل إنشائه وتوثيقه، بهدف ضمان سلامته واعتماده كدليل قانوني يمكن الاحتجاج به عند الحاجة.

ومن هذا المنطلق، فإن توثيق المستند الإلكتروني يعد أمرًا ضروريًا، بحيث يتم بطريقة تتيح لأطرافه الرجوع إليه عند الضرورة، مما يعزز من مصداقيته وحجيته القانونية. وعليه، فإن دراسة النظام القانوني للمستند الإلكتروني تستلزم في المقام الأول التطرق إلى مسألة توثيقه وتنظيمه، وفقًا لما نصت عليه التشريعات القانونية ذات الصلة، تم التعرف على ذلك من خلال الفروع التالية: الفرع الاول: تنظيم المستند الالكتروني، الفرع الثاني: شروط صحة المستند الالكتروني.

الفرع الاول: تنظيم المستند الالكتروني.

إن مختلف التعاملات الإلكترونية وكل العقود الإلكترونية تتميز بعدم حضور كل أطرافها أثناء انعقادها في كل المجالات والمعاملات الإلكترونية بكل اختلافاتها وخصوصياتها، ففي مجال التجارة مثلا: المتعاقدان يكونان غائبين مما يخوّل لأصحاب النية السيئة القيام بمجموعة من التصرفات التي يطبعها الاحتيال والغش والتزوير في الخدمة موضوع التعاقد[1]، مما استلزم معه إنشاء جهات توثيق إلكترونية سواء حكومية أو خاصة تتكلف بها النوع من الخدمات ولقد كان المشرع التونسي أول المهتمين عربيا بمجال التعاملات الإلكترونية، حيث نظم هذا المجال في القانون رقم 83 لسنة 2000، في حين لم تنظم مختلف التشريعات الأخرى التعاملات الإلكترونية إلا فيما بعد بقوانينها الخاصة وخاصة في معرفة مقدمي خدمات المصادقات الإلكترونية في تأمين وحفظ الشهادات الإلكترونية ولقد تطرّق القانون المغاربي من خلال المادة 21 من القانون رقم 53-05 [2]إلى المهام التي تناط بمقدم خدمات المصادقة الإلكترونية، وذلك اثناء عرضه للشروط التي يجب أن تتوفر فيه لاكتساب صفة مقدم خدمات المصادقة، وهذه المهام تتجلى كما الآتي:

[1] عمار كريم كاظم وناريمان جميل نعمة، المرجع السابق، ص193.

[2] المادة 21 من القانون رقم 53-05.

1/- يلتزم مقدم الخدمات بالتحقق من هوية الشخص الذي سلمت له شهادة إلكترونية ومطالبته بالإدلاء بوثيقة هوية رسمية للتأكد من أن الشخص يتوفر على الأهلية القانونية للالتزام من جهة، وبالصفة التي يدعيها من جهة أخرى والمحافظة على مميزاته ومراع الوثائق المدلى بها لإثبات هذه الهوية وهذه الصفة.

2/-من مهامه أيضا التأكد وقت تسليم الشهادة الإلكترونية أن المعلومات التي تحتوي عليها صحيحة، وأن الموقع المشار إلى هويته يمتلك معطيات لإنشاء التوقيع الإلكتروني، تطبق معطيات التحقق من التوقيع الإلكتروني المضمن في الشهادة.[1]

3/-إخبار الشخص الذي يطلب تسليمه شهادة إلكترونية كتابة بكيفيات وشروط استعمال الشهادة وكيفية المنازعة وطرق تسوية الخلافات، وتقديم هذه العناصر إلى الأشخاص الذي يستندون إلى شهادة إلكترونية، بإخبار أصحاب الشهادة المؤمنة يستبين يوما على الاقل قبل تاريخ إنتهاء صلاحية شهادتهم، وذلك لتمكينهم من تجديدها أو إلغائها وإبرام تأمين لتغطية الأضرار الناتجة عن أخطائه المهنية وإخبارهم بإلغاء الشهادة الإلكترونية في حالة كان هناك سبب من أسباب الإلغاء.

الفرع الثاني: شروط صحة المستند الالكتروني.

لضمان صحة المستند الإلكتروني في الجزائر واعتباره ذا حجية قانونية، يجب أن يستوفي مجموعة من الشروط القانونية والتقنية.

أولا: الكتابة الإلكترونية.

الكتابة الإلكترونية من أول طرق الإثبات المختلفة في إثبات صحة المستند الإلكتروني ووضعه في قالب قانوني، ونجد أهمية الكتابة في القوانين الحديثة حيث أضيفت عليها حجية مطلقة، مادام التي لم ينكرها أو يدعي تزويرها وتعتبر الكتابة بدقة عن الواقعة التي أدت لإثباتها، فهي دليل واضح عند حدوث نزاع بين أطراف الاتفاق وتعطي أكبر قدر من الاطمئنان لدى المتعاقدين، ويقصد بالكتابة في شكلها التقليدي بأنها : مجموعة الأحرف

[1] منشور بالجريدة الرسمية رقم 5584 بتاريخ 06/12/2007.

والأشكال والرموز والإشارات أو الأرقام المتسلسلة على أن تكون قابلة للقراءة ومترابطة وتعبر عن فكرة معينة".[1]

أما المقصود بها في الشكل الإلكتروني حسب نص المادة 323 مكرر من التقنين المدني الجزائري: " بأنها تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمنها كذا طرق إرسالها".[2]

وبالتالي تعتبر الكتابة الشرط الأساسي والأهم في المستندات الإلكترونية.[3]

ثانيا: التوقيع الالكتروني.

لا يمكن الاعتداد بالمستند الإلكتروني من الناحية القانونية إلا إذا اشتمل على توقيع من صدر عنه باعتبار أنه شرط جوهري سواء في المستند التقليدي أو الإلكتروني والذي يقصد منه مرافقة الموقع وإقراره لما هو مدون وموجود على المستند الإلكتروني، وبذلك فلا المستند ينتج الإلكتروني آثاره القانونية إذا لم يكن موضوع عليه توقيع الإلكتروني يميز هوية الموقع، ويعبر عن اقراره وموافقته لما تضمنه من بنود وشروط في إطار الضوابط التي تنص عليها التشريعات في هذا المجال و حيث نجد قانون الأونيسترال النموذجي قد نص على ذلك في المادة السابعة منه، أين اعتبر صحة المستند الإلكتروني مرتبطة بوجود توقيع إلكتروني عليه، أما التشريعات الوطنية المقارنة فقد نصت على هذا الشرط سواء في القواعد العامة للإثبات مثل التشريع الفرنسي والجزائري، أو في قوانين خاصة مثل التشريع الإماراتي والعراقي، ومن خلال ما سبق تناوله من تشريعات، مقارنة ما نصت عليه لصحة المستند الالكتروني وتمتعه بالحجية الكاملة في الاثبات فإنه لابد أن يتضمن توقيع من صدر عنه حتى يكون منتج لآثاره القانونية، وبالتالي فإن تخلف هذا الشرط ينفي عن الكتابة الإلكترونية صفة المستند الإلكتروني، وعليه فإن توقيع المستند الإلكتروني أمر بديهي للاحتجاج به

[1] براهيمي حنان، جريمة تزوير الوثيقة الرسمية، الإدارية ذات الطبيعة المعلوماتية، أطروحة دكتوراه تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة 2015، ص 107.

[2] الأمر 75/85 المؤرخ في 26/09/1975 المتضمن التقنين المدني الجزائري المعدل والمتمم بالقانون رقم 05/10 المؤرخ في 20/06/2005، ج ر رقم 44 الصادرة بتاريخ 26/06/2005، ص 24.

[3] إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة للنشر، الإسكندرية، 2002، ص 28.

قانونا ولقد عرف أيضا في نص المادة (2) من القانون النموذجي للأونسيترال على أن التوقيع الإلكتروني هو بيانات ذات شكل إلكتروني، تُدرج في رسالة بيانات أو تُضاف إليها أو تُرتبط بها ارتباطًا منطقيًا، ويجوز استخدام هذه البيانات للتحقق من هوية الموقع على رسالة البيانات، وكذلك لإثبات موافقته على ما تضمنته من معلومات.[1]

التوقيع الإلكتروني هو بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق.[2]

كما عرفته المادة 07 من القانون 15-04 انه التوقيع الإلكتروني الموصوف هو التوقيع الذي تتوفر فيه متطلبات معينة.[3]

وكذلك يعرف التوقيع الإلكتروني بأنه جزء صغير مشفر من بيانات يضاف إلى رسالة إلكترونية، فهو جزء من الرسالة ذاتها يشفر ويرسل مع الرسالة، ليتم التوثيق من صحة الرسالة بفك التشفير وانطباق محتواه على الرسالة.[4]

أورد المشرع الجزائري هذا الشرط في المادة الثانية من القانون 15-04 المتعلق بالقواعد العامة الخاصة بالتوقيع الإلكتروني والتصديق، حيث عرّف التوقيع الإلكتروني بأنه: «بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيًا ببيانات إلكترونية أخرى، تستعمل كوسيلة للتوثيق». كما نصت المادة 327 من القانون المدني على الاعتداد بالتوقيع الإلكتروني، بشرط استيفائه للشروط الواردة في المادة 323 مكرر 01 من القانون المدني الجزائري، التي تنص على ما يلي: "يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات

[1] إيهاب فوزي السقا، المرجع السابق، ص 31.

[2] الجريدة الرسمية للجمهورية الجزائرية، العدد 06، 20 ربيع الثاني عام 1436هـ الموافق ل 10 فبراير سنة 2018، ص07.

[3] قانون رقم 15-04 المؤرخ في 01 فبراير 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر.ج.ج، عدد 06 صادر في 10/02/2015.

[4] خالد عبد الفتاح محمد، التنظيم القانوني للتوقيع الإلكتروني، المركز القومي للإصدارات القانونية، الطبعة الأولى، (د.م.ن)، 2009، ص15.

بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي اصدرها وأن تكون منظومة إنشاء التوقيع الإلكتروني محفوظ في ظروف تضمن سلامته".[1]

وقد عرف أيضا التوقيع الإلكتروني على أنه "وحدة قصيرة من البيانات التي تحمل علاقة رياضية من البيانات الموجودة في محتوى الوثيقة ".[2]

وتعرف أعمال لجنة التجارة الدولية التابعة للأمم المتحدة cnudci في قانون التجارة الإلكترونية الصادر عنها عام 1996، على أن التوقيع الإلكتروني هو عبارة عن مجموعة أرقام تمثل توقيعا على رسالة معينة يتحقق هذا التوقيع من خلال اتباع الإجراءات الحسابية المرتبطة بمفتاح رقمي خاص بالشخص المرسل، ومن ثمة فإنه بالضغط على هذه الارقام الخاصة بالشخص يتكون التوقيع الإلكتروني، ويقصد بالتوقيع الإلكتروني في مشروع قانون التجارة الإلكترونية المصري بانه "حروف أو ارقام أو الرموز أو الإشارات لها طابع منفرد تسمح بتحديد شخصية صاحب التوقيع وتمييزه عن غيره"، مما يستفاد من نص المادة على أنه ينبغي أن يكون للتوقيع طابع متميز يتم من خلاله تحديد هوية الموقع وتميزه عن الغير، وهناك صور للتوقيع الإلكتروني وأهمها التوقيع الرقمي أو الكودي والتوقيع البيومتري والتوقيع بالقلم الإلكتروني.[3]

ثالثا: التوثيق أو التصديق الإلكتروني.

التصديق، في جوهره، هو آلية قانونية يتم بمقتضاها اللجوء إلى طرف ثالث مستقل ومحايد (سواء أكان فردًا أم شركة أم جهة متخصصة)، بهدف توثيق المعاملات الإلكترونية بين الأطراف المتعاقدة. ومن هذا المنطلق، يضطلع الموثق أو المصدق بدور الوسيط

[1] الأمر رقم 75-85 المتضمن القانون المدني الجزائري، في المادة 323 مكرر 01 من القانون المدني الجزائري، التي تنص على ما يلي: "يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي اصدرها وأن تكون منظومة إنشاء التوقيع الإلكتروني محفوظ في ظروف تضمن سلامته".

[2] فيصل سعيد الغريب، التوقيع الإلكتروني وحجيته في الإثبات، منشورات المنظمة العربية للتنمية الإدارية، 2005، ص217.

[3] عبد الفتاح بيومي الحجازي، المرجع السابق، ص 16.

الموثوق الذي يمنح الشرعية والمصداقية للمحررات الإلكترونية، مما يعزز ثقة الأطراف فيها ويجعلها قابلة للاحتجاج بها في الإثبات أمام الجهات المختصة.

ونظرًا لأن وظيفته الأساسية تقوم على ضمان قوة الإثبات للمستندات الرقمية وتلافي إنكار التصرفات القانونية الواردة فيها، فقد أُطلقت عليه تسميات أخرى تعبر عن هذا الدور الجوهري، أبرزها "وكلاء الإثبات"[1].

وتلعب شهادة التوثيق الإلكتروني دوراً مهما في عملية التوقيع الرقمي، حيث تؤكد صحة المفتاحين العام والخاص المستخدمين في ذلك، حسب المعلومة الواردة بهذه الشهادة الخاصة بصاحبها، والمنشئة من جهة محايدة، ذلك أن منح هذه الشهادة من جهة التوثيق الإلكتروني يتطلب تقديم المعلومات الخاصة بطلب التوقيع والتأكد من صحتها، ليتم منح هذا الشخص مفتاح تشفير خاص يتسم بالسرية، حيث يحتفظ به الموقع، ويتم تثبيت نصفه في جهاز الكمبيوتر الخاص به، والنصف الآخر في بطاقة إلكترونية، أما جهة التوثيق فتحتفظ بالمفتاح العام، حيث تقوم بإرساله بالبريد الإلكتروني إلى اشخاص الذين يتعامل معهم الموقع، وذلك لاستخدامه في فك التشفير.[2]

[1] عابد فايد عبد الفتاح، الكتابة الإلكترونية في القانون المدني بين التطور القانوني والأمن التقني، دار الجامعة الجديدة، الإسكندرية، 2014 ، ص ص 70-71.

[2] براهيمي حنان ، المرجع السابق، ص 153.

المبحث الثاني: افعال المساس بالمستند الالكتروني في التشريع الجزائري.

تجرّم التشريعات المقارنة، ومن بينها التشريع الجزائري، مجموعة من الأفعال التي تشكّل انتهاكاً لسرية المستندات الإلكترونية. وتتمثّل أبرز هذه الأفعال في الدخول غير المأذون به إلى السجلات أو الأنظمة الإلكترونية، أو نسخ محتوى المستند أو بياناته، أو طباعته دون الحصول على ترخيص مشروع. وفيما يلي تحليل لموقف المشرع الجزائري من التجريم بالاعتماد على المطالب التالية: المطلب الاول: الفعل الماس بالمستند الالكتروني المطلب الثاني: اجراء المشرع الجزائري من جريمة تزوير المستند الالكتروني.

المطلب الاول: الفعل الماس بالمستند الالكتروني.

يُولي المشرع الجزائري أهمية خاصة لحماية المستندات الإلكترونية، باعتبارها أحد العناصر الأساسية في المعاملات الإدارية، الاقتصادية، والقانونية الحديثة. وفي ظل تزايد الاعتماد على الوسائط الرقمية، استحدث التشريع الوطني أحكامًا تُجرّم الأفعال التي تمس بسلامة أو سرية هذه المستندات، سواء من خلال الدخول غير المشروع إلى الأنظمة المعلوماتية، أو التلاعب بالمحتوى، أو التزوير الإلكتروني وعليه تم التطرق الى الفروع التالية: الفرع الأول: جريمة التزوير المستند الالكتروني والحماية الجنائية، الفرع الثاني: جريمة الاتلاف، الفرع الثالث: جريمة الاحتيال.

الفرع الأول: جريمة التزوير المستند الالكتروني والحماية الجنائية.

تتمثل خطورة جريمة تزوير المستند الإلكتروني في أنها تُرتكب عن بُعد، دون حاجة لوجود مادي للجاني، وبأساليب يصعب كشفها، الأمر الذي يجعل من إثباتها وملاحقة مرتكبيها تحديًا حقيقيًا أمام الجهات القضائية. ويُعد التزوير في المستند الإلكتروني ذا أهمية لا تقل عن التزوير في الوثائق الورقية، وتتجلى هذه الأهمية في عدة جوانب:

أ- **الوجه الأول:** أصبح المستند الإلكتروني بديلاً للمستندات الورقية في الكثير من المعاملات التجارية، وبالتالي فإن أي عبث بمحتواه قد يؤدي إلى إصابة رضا المتعاقدين بعيوب الإرادة، كالغلط أو التدليس، مما يثير منازعات تهدد استقرار المعاملات.

ب- الوجه الثاني: إن اعتماد النسخة الورقية المستخرجة من المستند الإلكتروني وقبولها في التعامل، يعني بالضرورة أن أي مساس بمحتوى المستند الإلكتروني سينعكس على النسخة الورقية المطابقة له.

وقد انقسمت التشريعات المقارنة في معالجة مسألة تجريم تزوير المستند الإلكتروني إلى اتجاهين مختلفين:[1]

الاتجاه الأول: يعتمد على وضع نصوص عامة لتجريم فعل التزوير، بحيث يمتد نطاقها ليشمل التزوير الواقع على مختلف أنواع المستندات، بما فيها المستندات الإلكترونية، كما هو الحال في التشريعين الفرنسي والألماني.

الاتجاه الثاني: يتجه إلى تجريم صور محددة من تزوير المستندات الإلكترونية بشكل صريح، ومن بين هذه التشريعات القانون المصر..[2]

أولا: تجريم المستندات الإلكترونية بنصوص عامة:

1/القانون الفرنسي.

يعود أصل تجريم التزوير في المستندات الإلكترونية لدى المشرع الفرنسي إلى الاقتراح الذي تقدم به النائب البرلماني (Jacques Godfrain) بتاريخ 5 أوت 1986، والذي دعا إلى تعديل أحكام جريمة التزوير الواردة في قانون العقوبات لتشمل أيضًا تغيير الحقيقة في البيانات الإلكترونية. غير أن هذا الاقتراح لم يُعتمد آنذاك، حيث رفضه مجلس الشيوخ فيما يخص المحررات. ومع ذلك، صدر القانون رقم 88-19 بتاريخ 5 جانفي 1988، الذي نص صراحة على تجريم صورتين أساسيتين:

الأولى: تزوير المستندات المعالجة آليًا، مهما كان شكلها، متى كان من شأنها الإضرار بالغير (المادة 42).

---

[1] حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنيت دار النهضة العربية، 2000، ص 63.

[2] أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني -دراسة مقارنة-، بحث منشور على شبكة الانترنيت، من خلال الموقع الإلكتروني الآتي:الدليل الإلكتروني القانون العربي، Https://Www.Arabawifo.Com تمت الزيارة 2025/04/05.

الثانية: استعمال المستندات المزورة المشار إليها أعلاه (المادة 462-6).

وقد تبنى هذه الوجهة أيضا قانونا التجارة الإلكترونية لدوقية لكسمبورج الصادر في يونيو سنة 2000، والذي عدّل نص المادة 196 من قانون العقوبات التي تجرم التزوير، فأضاف الكتابة والتواقيع الإلكترونية إلى محل جريمة التزوير بصورتها التقليدية.[1]

2/القانون الألماني.

أقر المشرع الألماني من خلال أحكام قانون العقوبات المتعلقة بجريمة التزوير عقوبات صارمة، حيث نص على الحبس لمدة تزيد عن خمس سنوات أو الغرامة. وجاء في المادة 268 من القانون ذاته تجريم تزوير السجلات المعالجة تقنيًا، إذ نصت الفقرة الأولى، في بندها الأول، على معاقبة كل من يتوصل عن طريق الخداع إلى إنشاء سجل إلكتروني مصطنع أو يقوم بتغيير الحقيقة فيه. كما نص البند الثاني على معاقبة من يستعمل هذا السجل المزور.

وقد ساوى المشرع الألماني بين إنشاء سجل إلكتروني مزيف وبين التلاعب بالنتائج التي يُنتجها هذا السجل، من خلال تدخل الجاني بما يخلّ بعمله. وبعد وضع الإطار العام للتجريم في المادة 268، خصّ المشرع بعض الصور المحددة للمستند الإلكتروني بالتجريم، ومن أبرزها تزوير البيانات ذات القيمة الإثباتية، وذلك بموجب (المادة 269 من ق. العقوبات).[2]

ثانيا: تجريم بعض صور تزوير المستندات الإلكترونية

لقد اقتصرت بعض التشريعات على تجريم بعض صور تزوير المستندات الإلكترونية، ومنها:

1/القانون المصري:

جرّم المشرع المصري تزوير السجلات الإلكترونية الخاصة بالأحوال المدنية، إذ ساوى في القانون رقم 143 لسنة 1994 بين السجلات الورقية ونظيرتها الإلكترونية في

[1] مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، سنة 2001، ص72.

[2] أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، المرجع السابق، ص 22.

مجال تطبيق الأحكام. فقد اعتبر البيانات المسجلة في الحاسبات الآلية بمراكز الأحوال المدنية ومحطات الإصدار المستخدمة لاستخراج الوثائق وبطاقات الهوية بيانات واردة في محررات رسمية. ونصت المادة 72 من القانون ذاته على أنه: «تُعد البيانات المسجلة بالحاسبات الآلية وملحقاتها بمراكز معلومات الأحوال المدنية ومحطات الإصدار الخاصة بها بيانات واردة في محررات رسمية، ويعاقب على تزويرها أو تزوير غيرها من المحررات الرسمية بالأشغال الشاقة المؤقتة أو بالسجن مدة لا تقل عن خمس سنوات».

كما نصت المادة 74 من القانون نفسه على عقوبة كل من اطلع أو شرع في الاطلاع، أو حصل أو حاول الحصول على البيانات أو المعلومات المخزنة في السجلات أو الحاسبات الآلية أو وسائط التخزين الملحقة بها، أو قام بتغييرها، وذلك بالحبس مدة لا تتجاوز ستة أشهر وبغرامة لا تزيد عن 500 جنيه، أو بإحدى هاتين العقوبتين، وذلك دون الإخلال بأي عقوبة أشد يقررها قانون العقوبات أو غيره من القوانين.[1]

2/القانون الجزائري

لقد نص المشرع الجزائري على تزوير المحررات بصفة عامة، فجعل كل منهما مستقلة عن الأخرى، وفي هذا الإطار رتب المشرع على تزوير المحررات الرسمية الجزاءات التالية:

أ/ – جريمة التزوير في محررات رسمية عمومية وترتب عليها العقوبات التالية[2]:

1/–عقوبة السجن المؤبد للقضاة أو الموظفين العموميين الذين ارتكبوا تزويراً في المحررات الرسمية أو العمومية أثناء تأدية مهامهم، وهذا وفقا للمادتين 2 و 25 ق.ع.ج.

[1] أشرف توفيق شمس الدين ،المرجع السابق، ص 23.

[2] حسونة عبد الغني، جريمة التزوير المعلوماتي بين الاحكام التقليدية والنصوص المستحدثة بحث مقدم لأعمال المتلقى الوطني حول الجريمة للمعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية جامعة محمد خيضر، بسكرة ،مابين 16 و 17 نوفمبر 2015، ص68.

2/- عقوبة السجن المؤقت من 10 سنوات إلى 20 سنة، وبغرامة مالية من مليون إلى 2 مليون دينار كل شخص من غير القضاة والموظفين العموميين يرتكب جريمة التزوير في محررات رسمية أو عمومية، وهذا وفقا للمادة 216.

3/-عقوبة الحبس من سنة واحدة إلى 05 سنوات وبغرامة من 500 دج إلى 1000 دج كل شخص ليس طرفا في العقد أدلى أمام الموظف بتقرير يعلم أنه مخالف للحقيقة وفقا للمادة 217.

ب-جريمة التزوير في محررات عرفية أو تجارية أو مصرفية: فقد رتب لها المشرع الجزائري الجزاءات التالية:

1/-عقوبة الحبس من سنة إلى 5 سنوات وغرامة من 500 دج إلى 20000 دج كل من ارتكب تزويراً هي محررات تجارية أو مصرفية أو شرع في ذلك وفقا للمادة 219.

2-عقوبة الحبس من سنة إلى 5 سنوات وغرامة من 500 دج إلى 2000 دج كل من ارتكب في محررات عرفية أو شرع في ذلك وفقا للمادة 220.

ج-جريمة التزوير في الوثائق الإدارية والشهادات: رتب عليها المشرع عقوبة الحبس من 06 أشهر إلى 03 سنوات وغرامة من 1500 دج إلى 15000 دج كل من قلّد أو زيف رخصا أو شهادات أو كتابات أو بطاقات أو منشورات أو إيصالات أو جوازات سفر أو خدمة أو وثائق أو تصاريح أو أوامر خدمة أو من الوثائق التي تصدرها الادارات العمومية بغرض إثبات حق أو شخصية أو صفة وهو ما نصت عليه المادة 222 ق.ع.[1]

الفرع الثاني: جريمة الاتلاف.

أولا: تعريف جريمة الاتلاف.

جريمة إتلاف المستند الإلكتروني هي فعل عمدي يقوم فيه شخص بتعطيل أو حذف أو تشويه أو تعديل مستند إلكتروني بهدف إلحاق الضرر بالغير أو إخفاء معلومات أو تعطيل سير العدالة أو الإدارة.

[1] حسونة عبد الغني، المرجع السابق، ص68.

ويعرف أيضا كل فعل الغاية من القيام به تدمير المعطيات والتدمير كليا وذلك يجعلها غير صالحة للاستعمال، أو تدمير جزئيا ذلك من قيمة أدائها".[1]

كما يعرف أيضا على أنه: " الإفناء لمادة الشيء، أو القيام بإحداث تغييرات عليها بحيث تصبح غير صالحة للاستعمال في الغرض الذي أنشأ لها، وبالتالي تضيع القيمة المادية لهذا الشيء على المالك.[2]

ويقصد به أيضا التأثير على مادة الشيء مضمونة وذلك بأن يقلل أو يزيل من قيمته، وفعل الإزالة يكون بالإنقاص من كفائتة لأوجه الاستعمال المخصصة لها"[3]، وقد يتحقق الإتلاف أو التخريب بوسائل مختلفة مادية أو معنوية سواء بالاعتداء على المعطيات والدعامة الموجودة عليها، أو محو المعطيات دون إصابة الدعامة، أو تعطيل البرامج أو محوها باستخدام أداة لهذا الغرض.[4]

ويتحقق الإتلاف من خلال وسائل وأساليب متعددة تختلف في درجة خطورتها، ومن أبرزها:

1- الفيروسات: وهي برامج خبيثة تمتاز بقدرتها على التكاثر والانتشار من نظام إلى آخر، وغالبًا ما تكون غير مرئية، مما يصعّب اكتشافها. وقد تتسبب في تدمير البرامج أو تغيير المعلومات دون ترك أي أثر.

2- الاستخدام الثنائي للفيروسات: إذ يمكن استخدام بعضها أيضًا لأغراض "مشروعة" مثل حماية النسخ الأصلية من البرامج من النسخ غير المرخص به، من خلال منع تشغيل النسخ غير الأصلية.

---

[1] ايد رجا الخلايلة، المسؤولية التقصيرية الإلكترونية، المسؤولية الناشئة عن إساءة استخدام أجهزة الحاسوب و الانترنت، دراسة مقارنة، ط 1 دار الثقافة، عمان، 2009، ص 109

[2] عبد الفتاح بيومي حجازي، المرجع السابق، ص 329.

[3] محمد حماد مرهج الهيتي، جرائم الحاسوب، ماهيتها أهم صورها و العقوبات التي تواجهها، ط1، دار المنهج، عمان، 2006 ص 1997.

[4] براهيمي حنان، المرجع السابق، ص 54.

3- البرامج المنطقية والزمنية: وهي برامج تُفعّل في أوقات معينة أو عند حدوث شرط معين، وقد تُستخدم لإحداث تلف أو تغيير في البيانات بمجرد تحقق ذلك الشرط.[1]

وتُستخدم في جريمة إتلاف المستندات الإلكترونية عدة وسائل رقمية، من أبرزها ما يُعرف بـ "**القنبلة المعلوماتية**"، وهو مصطلح يُطلق على أنواع من البرامج المعلوماتية التي تهدف إلى تدمير أو تخريب البيانات أو الأنظمة كوسيلة لارتكاب هذه الجريمة. وتنقسم هذه القنابل الإلكترونية إلى ثلاثة أنواع رئيسية:

- **القنابل المنطقية:** وهي أجزاء من برامج تُزرع داخل النظام وتُفعَّل عند توافر شروط أو أحداث معينة، مثل مرور وقت محدد أو حصول تغيّر في معطيات النظام. وتُبرمج عادةً لتعمل على نحو خفيّ بهدف تسهيل تنفيذ أعمال غير مشروعة، من خلال حذف أو تعديل البيانات أو تعطيل النظام.[2]

- **القنابل الزمنية أو المؤقتة:** وهي برامج تُدخل إلى النظام عبر وسيلة تبدو مشروعة، وتُصمَّم بحيث تُفعّل ذاتيًا في وقت محدد، فتقوم بتدمير ملفات أو برامج أخرى أو تعديلها. تعتمد هذه القنابل على مبدأ "التفجير المؤقت" حيث تُبرمج مسبقًا للعمل في توقيت معين دون تدخل بشري مباشر.

- **برامج الدودة (Worm Programs):** وهي عبارة عن أكواد خبيثة تستغل ثغرات في أنظمة التشغيل لتنتقل من جهاز إلى آخر عبر الشبكات أو وسائل الاتصال المرتبطة بها. تتكاثر أثناء انتقالها، مما يسبب استهلاكًا كبيرًا لموارد الشبكة ويؤدي إلى تعطيلها أو شللها التام. ومن أبرز الأمثلة على ذلك:

-برنامج Inter Warm.

- برنامج Wank، الذي استخدم ضد مستخدمي الذرة.

---

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، الأردن، دار الثقافة، 2008، ص 132.

[2] محمد أمين الرومي، المستند الإلكتروني، دار الكتب القانونية، الاسكندرية مصر، المجلة الكبرى، 2008،ص94.

وقد استُخدمت هذه البرامج كذلك في تنفيذ هجمات إلكترونية شملت اختراق البريد الإلكتروني ونشر الفيروسات لأغراض تخريبية أو إرهابية.[1]

ثانيا: أركان لجريمة إتلاف المستند الإلكتروني.

1- الركن المادي لجريمة إتلاف المستند الإلكتروني:

لقيام أي جريمة، لا بد من توافر ركنين أساسيين: الركن المادي والركن المعنوي. ويكمن الركن المادي في جريمة إتلاف المعلومات في النشاط الإجرامي ذاته، أي الفعل الذي يؤدي إلى الإتلاف، سواء كان ذلك بالحذف أو التعديل أو التعطيل.

أما محل الجريمة، فيتمثل في المال محل الحماية القانونية، سواء كان مالًا منقولًا أو ثابتًا، على أن يكون مملوكًا للغير، إذ لا تقوم الجريمة إذا وقع الإتلاف على مال يملكه الفاعل نفسه.

أ- **النشاط الإجرامي:** يمثل النشاط الإجرامي الذي يقوم به الجاني في تخريب الأموال سواء كانت مادية أو معنوية وجعلها غير صالحة للاستخدام سواء كان الإتلاف تاما أم جزئيا.[2] يُعرَّف هذا الفعل بأنه سلوك إجرامي يتمثل في إتلاف أو إزالة وثيقة أو سند أو عقد أو مال منقول بطريق الغش. وتشترط المادة أن يصدر هذا الفعل عن موظف عام أو قاضٍ أو ضابط عمومي، تكون قد أُودعت لديه تلك الوثائق أو الأموال بحكم وظيفته أو بسبب صفته.

1- صفة الجاني: يتمثل الجاني في القاضي الذي يصدر الأحكام، وقد يقوم بحكم وظيفته بإزالة بعض الوثائق لغرض معين، سواء كان قاضيًا تابعًا للقضاء العادي أو الإداري. كما يشمل ذلك الموظف الذي يزاول مهامه بصفة دائمة أو مؤقتة، إضافةً إلى الضابط العمومي الذي يندرج ضمن هذا الإطار.

2- نوع الوثيقة: يشمل الإتلاف جميع أنواع الوثائق، سواء كانت مستندات أو عقودًا تكون تحت يد الموظف، كما يمتد ليشمل الأموال التي تكون في عهدته. ويُقصد بالمال المنقول ذلك المال الذي يمكن نقله أو تغيير موقعه بفعل مادي مباشر.

---

[1] محمد أمين الرومي، المرجع السابق، ص94.

[2] طباش أمين، المرجع السابق، ص76.

الإتلاف العمدي الذي يقع بطريق الغش يُفهم في نطاق القانون الجنائي بمعناه الواسع مقارنة بالقانون المدني؛ إذ يُعتبر منقولًا – في نظر القانون الجنائي – بعض الأشياء التي يعدّها القانون المدني عقارات بالتخصيص، مثل المواشي، وكذلك المحاصيل الزراعية التي يمكن أن تكون محلًا للجريمة عند التعرض لها بالإتلاف.

ويتحقق الركن المادي لجريمة الإتلاف من خلال النشاط الإجرامي الذي يؤثر في مادة الشيء على نحو يُنقص أو يُعدم قيمته الاقتصادية، وذلك بالمساس بكفاءته المعدة للاستعمال. فعلى سبيل المثال، يمكن إتلاف جهاز تلفاز بإدخال تيار كهربائي عالي الشدة يؤدي إلى احتراق مكوناته الداخلية كالمكثفات، ورغم احتفاظ الجهاز بهيكله وشكله الخارجي، إلا أنه يصبح غير صالح للغرض الذي أُعد له وهو المشاهدة.

وتتخذ جريمة الإتلاف صورًا متعددة، ويُلاحظ أن مدلولها في قانون العقوبات يختلف عنه في حالة إتلاف البرامج أو المعلومات الإلكترونية، ويرجع سبب هذا الاختلاف إلى محل الجريمة، حيث يشترط أن ينصب الإتلاف أو التعييب على مال منقول أو عقار مملوك للغير.

أما النشاط الإجرامي، فيتجسد في كل فعل مادي يؤدي إلى تدمير المال أو إنقاص قيمته أو تعطيل منفعته.[1]

لم يقيد المشرع الجزائري النشاط الإجرامي في جريمة الإتلاف بوسيلة محددة، باعتبارها من الجرائم ذات الطابع الحر، الأمر الذي لا يمنع من امتدادها لتشمل إتلاف برامج الحاسوب. فالمشرع لم يحصر أسلوب ارتكاب الجريمة في طريقة معينة، كما لم يشترط تحقق نتيجة واحدة بعينها لقيامها.[2]

[1] سليمان أحمد فضيل، المواجهة التشريعية والأمنية للجزائر الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، دار النهضة العربية، القاهرة، 2007، ص 93.

[2] فشار عطا الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم الى الملتقى المغاربي حول القانون و المعلوماتية بمقر أكاديمية الدراسات العليا بليبيا في أكتوبر 2009، ص 10.

3-محل الجريمة:

ينصرف محل جريمة الإتلاف إلى كل من المكونات المادية والمعنوية لنظم المعلومات. ففيما يتعلق بالمكونات المادية، فهي تشمل الأجهزة والوسائط المعلوماتية مثل الحواسيب،شاشات العرض،الطابعات،الأسطوانات، الكابلات، المفاتيح، والأقراص الممغنطة، سواء كانت حاوية لبيانات أو برامج أو حتى فارغة، طالما أن فعل الإتلاف أو التخريب أدى إلى إنقاص قيمتها الاقتصادية.

أما المكونات غير المادية، فيُطلق على إتلافها عادةً مصطلح تدمير نظم المعلومات، ويُقصد به محو أو تخريب البيانات أو التعليمات البرمجية المخزنة داخل النظام. ولا يهدف هذا السلوك بالضرورة إلى تحقيق منفعة مباشرة مثل الاستيلاء على أموال أو الاطلاع على معلومات، وإنما ينصرف غرضه الأساسي إلى إلحاق الضرر بالنظام المعلوماتي ذاته وتعطيله أو القضاء عليه.[1]

ويتحقق الركن المادي في جريمة الإتلاف التقني بصورتين هما:

أ/ **الإتلاف المباشر:** يتحقق عندما يتمكن الفاعل، بشكل مباشر أو غير مباشر، من الوصول إلى جهاز الحاسوب نفسه، كالدخول عبر لوحة المفاتيح أو عبر أحد منافذ الدخول وبوابات العبور إلى النظام، حيث يقوم بسلوك تقني وإلكتروني مباشر يؤدي إلى الإتلاف.

ب/ الإتلاف غير المباشر: ويتمثل في ولوج الفاعل إلى الحاسوب أو نظام المعلومات بطريقة غير مباشرة، كاستخدام إحدى النهايات الطرفية المرتبطة بالنظام، واستغلال هذا الاتصال لتحقيق غرضه في الإضرار بالنظام أو محتوياته.[2]

-الركن المعنوي لجريمة إتلاف المستند الإلكتروني.

تُعد جريمة إتلاف المستندات الإلكترونية من الجرائم العمدية التي يتطلب قيامها توافر القصد الجنائي العام، المكوّن من عنصري العلم والإرادة.

[1] فشار عطا الله، المرجع السابق، ص10.

[2] المرجع نفسه، ص11.

ويتحقق الركن المعنوي لهذه الجريمة حين يكون الجاني على علم تام بأن فعله المتمثل في تخريب أو تعديل أو محو البيانات والمعلومات الواردة في المستندات الإلكترونية يُشكّل سلوكًا غير مشروع، ويمثّل اعتداءً على الحقوق القانونية لصاحب تلك المعلومات أو الشخص الذي يملك السيطرة عليها.

كما يجب أن يكون الجاني مدركًا أن فعله سيؤدي إلى تغيير جوهري في حالة البيانات أو إتلافها، بحيث تصبح غير قابلة للاستخدام في الغرض الذي أُنشئت من أجله، أو على الأقل تفقد قيمتها المادية أو المعنوية.[1] 2.

ومما لا شك فيه أن الأضرار الناشئة عن تدمير المستندات الإلكترونية والمعلومات التي تتضمنها تفوق نظيرتها الناتجة عن إتلاف المعدات المادية الخاصة بنظم المعلومات، بل وتفوق إتلاف الأشياء المادية، ولعل ذلك يرجع إلى التكلفة الاقتصادية المرتفعة لإعداد البرامج والمستندات الإلكترونية والإمكانيات الفنية المخصصة لإعدادها.[2]

أما بخصوص القصد الجنائي العام الواجب توافره في هذا النوع من الجرائم فإنه لا يشترط أن يكون مباشراً، أي أن تتجه الإرادة إلى النتيجة المتحققة، وإنما قد يكون هذا القصد غير مباشر أو ما يسمى بالقصد الاحتمالي، بحيث يستوي أن تتجه إرادة الجاني إلى وقوع النتيجة من عدمها.[3]

إضافة إلى ضرورة توافر القصد الجنائي العام في جريمة إتلاف المستندات الإلكترونية، فإن بعض التشريعات تتطلب زيادة على ذلك اتجاه إرادة مرتكب الفعل إلى تحقيق قصد خاص،

---

[1] شمسان ناجي صالح الخليلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الأنترنت دراسة مقارنة، دار النهضة العربية ، القاهرة 2009، ص 240.؛

[2] خالد حربي السعدي، جريمة إتلاف برامج ومعلومات الحاسب الآلي في التشريعين الكويتي والمقارن، ط 1، دار النهضة العربية، القاهرة، مصر، 2012، ص 16.

[3] أحمد عاصم عجلية، الحماية الجنائية للمحررات الالكترونية، دراسة مقارنة، دار. النهضة العربية، القاهرة، 2014ص ص 207- 208.

كقصد الإضرار بالغير أو قصد تحقيق ربح مادي غير مشروع للجاني أو للغير ومن بين هذه التشريعات القانون البرتغالي والفنلندي.[1]

للإشارة، فقد انتقد جانب من الفقه تطلب القصد الخاص في جريمة الإتلاف المعلوماتي، وبخاصة قصد تحقيق ربح مادي غير مشروع ذلك أن تكريس هذا المبدأ سيؤدي إلى استبعاد جميع الحالات التي لا تتجه فيها نية الجاني إلى تحقيق ربح مادي غير مشروع، وذلك رغم أهمية المعلومات التي قد يتم إتلافها، كما هو حال إتلاف معلومات علمية أو طبية.

هذا عن القصد الخاص المتمثل في تحقيق ربح مادي غير مشروع، أما فيما يخص القصد الخاص المتمثل في الإضرار بالغير فيجب حسب رأي ذات الفقه– أن يفسر تفسيراً واسعاً حيث لا يقتصر على مجرد الخسائر والأضرار المادية التي قد تصيب المجني عليه.[2] وإذا كانت جريمة إتلاف المستند الإلكتروني عمدية فهذا لا يعني أن الخطأ فيها غير متصور، بل يمكن أن تقع هذه الجريمة بطريق الخطأ غير العمدي أي بدون أن يتوافر قصد الإتلاف، وفي هذا يلاحظ أن قانون العقوبات الفرنسي الجديد عاقب على تعديل البيانات والمعلومات أو محوها إذا ما تم بطريق الخطأ، وقد أشار المشرع الفرنسي إلى ذلك في نص المادة 323/1 من قانون العقوبات الفرنسي على تجريم فعل الدخول أو البقاء غير المصرح به داخل النظام المعلوماتي، مع تشديد العقوبة إذا ترتب على هذا الفعل تعديل البيانات المخزنة في النظام. وبالرجوع إلى هذا النص، يتضح أن الركن المعنوي لجريمة الدخول أو البقاء بدون تصريح يتكون من عنصرين: الأول، أن فعل الدخول أو البقاء يتم بصورة عمدية، والثاني، أن ما قد يترتب عليه من إتلاف أو تعديل للبيانات يكون قائماً على أساس مبنيا على الخطأ.[3]

---

[1] أحمد عاصم عجلية، المرجع السابق، ص208.

[2] المرجع نفسه، ص209.

[3] مدحت محمد عبد العزيز إبراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي، دراسة مقارنة، ط 1، دار النهضة العربية، القاهرة، 2015، ص. 11

بعد بيان الأركان الواجب توافرها لقيام جريمة إتلاف المستندات الإلكترونية، فإنه سيتم تحديد العقوبات المقررة لهذه الجريمة.

ثالثا: العقوبة المقررة لجريمة الإتلاف المستند الإلكتروني في التشريع الجزائري.

على الرغم من الخطورة البالغة لفعل الإتلاف الإلكتروني الذي يستهدف المستندات الإلكترونية وما تتضمنه من بيانات ومعلومات، ورغم جسامة الأضرار والخسائر الناتجة عنه، إلا أن الإتلاف الذي يطال المكونات المعنوية لنظم المعلومات يُعد أكثر فداحة وتأثيرًا من الإتلاف الذي يصيب المكونات المادية كالأجهزة والملحقات، نظرًا لما تُمثله البيانات والبرمجيات من قيمة جوهرية في تشغيل النظام وتحقيق وظائفه الأساسية.

إلا أن المتتبع لترسانة النصوص القانونية الجزائرية يجد أن المشرع الجزائري قد حذا حذو نظيره الفرنسي وعمل على تجريم فعل إتلاف المستندات الإلكترونية بطريقة غير مباشرة، وذلك تبعاً لمعالجة تجريم إتلاف المعلومات أو البيانات الإلكترونية أو أنظمة معالجة البيانات والمعطيات الآلية[1]، ويظهر ذلك جلياً في البداية من خلال القانون رقم 04-15 المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات والذي عبر فيه بطريقة غير مباشرة عن هذه الجريمة تحت مصطلح "التخريب الذي يطال منظومة المعالجة الآلية للمعطيات" جاء في نص المادة 394 مكرر من القانون ذاته ما يلي: يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة وبغرامة تتراوح بين 50.000 دج و200.000 دج كل من يتعمد الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك. وتُشدد العقوبة إذا نتج عن هذا الفعل حذف أو تعديل في معطيات المنظومة، أما إذا أدى السلوك إلى تخريب نظام تشغيلها، فتكون العقوبة الحبس من ستة (6) أشهر إلى سنتين، وبغرامة من 50.000 دج إلى 300.000 دج».[2]

[1] قانون رقم 04-15 المعدل والمتمم لقانون العقوبات الجزائري الصادر بموجب الأمر رقم 66-156 المؤرخ في 08 يونيو 1966.

[2] المادة 394 مكرر من القانون رقم 04-15- المعدل والمتمم بالقانون رقم 06-23 المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

وباستقراء نصوص هذا القانون من المادة 394 مكرر إلى غاية المادة 394 مكرر 7 يتبين أن المشرع الجزائري لم يورد مادة صريحة يعاقب فيها على أفعال الإتلاف التي تطال المستندات الإلكترونية، وما تحويه من بيانات ومعلومات.

ولعل ما يؤخذ على المشرع الجزائري أنه لم يشر شأنه شأن التشريع الفرنسي إلى استخدام الفيروسات والبرامج الخبيثة لإتلاف المكونات المنطقية للحاسبات الآلية من مستندات وبيانات وبرامج بإعتبارها أحد وسائل الركن المادي للجريمة، وفي هذا يرى جانب من الفقه إمكانية تطبيق هذه النصوص على حالة استخدام تلك الفيروسات والبرامج الخبيثة طالما ترتب على إدخالها الإضرار بالمستندات الإلكترونية وما تحويه من معلومات وبيانات.[1]

إذا كان هذا موقف المشرع الجزائري سنة 2004 ، فإنه ينبغي الذكر أنه سنة 2014 نص المشرع الجزائري بموجب المادة 17 من القانون 14-03 المتعلق بوثائق وسندات السفر على جريمة الإتلاف التي تطال البيانات المخزنة في النظام البيومتري، وأشار إلى تطبيق العقوبات المنصوص عليها في المواد 394 مكرر إلى 394 مكرر 7 من قانون العقوبات، أي تلك العقوبات المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات السابق بيانها، والواقع أن هذا الأمر منطقي طالما أن النظام البيومتري للبيانات ما هو إلا نظام من نظم المعالجة الآلية حيث نصت المادة 17 من القانون المذكور أنه: « كل شخص... يتلف عمداً سنداً أو وثيقة سفر أو يستعمل عمداً سندا أو وثيقة سفر ... محرفة يتعرض إلى العقوبات المنصوص عليها في قانون العقوبات، وإذا مست الأفعال المذكورة البيانات المخزنة في النظام البيومتري الإلكتروني، فتطبق العقوبات المنصوص عليها في قانون العقوبات، وإذا مست الأفعال المذكورة أعلاه البيانات المخزنة في النظام البيومتري، فتطبق العقوبات المنصوص عليها في قانون العقوبات، لا سيما تلك المنصوص عليها في المواد 394 مكرر إلى 394 مكرر 7.

[1] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلية الاقتصادية، ط 1، منشورات الحلبي الحقوقية، لبنان، 2005، ص205.

أما بخصوص موقف المشرع الجزائري من هذه الجريمة فيلاحظ أن قانون التوقيع والتصديق الإلكترونيين لم يسد الفراغ التشريعي الذي أثار الكثير من الجدل الفقهي والتردد القضائي، فنصوص هذا القانون جاءت خالية من كل نص ينظم جريمة إتلاف المستندات الإلكترونية.[1]

الفرع الثالث: جريمة الإحتيال.

يُعتبر الاحتيال المعلوماتي من أخطر الجرائم الإلكترونية، إذ يستهدف في الغالب الاستيلاء على أموال المؤسسات أو الشركات، سواء من قِبل موظفين من داخلها أو من قِبل جهات خارجية تتمكن من اختراق أنظمتها عبر أساليب القرصنة. وتُعد عمليات الاحتيال المرتبطة بالتحويلات الإلكترونية للأموال والودائع المصرفية من أبرز صوره، حيث يتم استغلال الأنظمة المعلوماتية والتلاعب بها للحصول على الأموال أو الخدمات بطرق غير مشروعة.

كما أن استخدام المستندات الإلكترونية على نحو غير قانوني يشكل اعتداءً خطيرًا على قوتها الثبوتية في المعاملات المصرفية، ويُضعف من حجيتها أمام الغير، بما ينعكس سلبًا على أمن وسلامة التعاملات الإلكترونية ككل.[2]

ولمواجهة هذه التحديات، بات من الضروري تعزيز آليات الحماية التقنية، وفي مقدمتها اعتماد مفاتيح تشفير طويلة ومعقدة، إذ إن زيادة طول المفتاح وصعوبة تركيبه ترفع من مستوى الحماية، وتُصعّب على المخترقين الوصول إلى البيانات أو التلاعب بها، الأمر الذي يُسهم بفاعلية في تأمين المعاملات ومنع محاولات الاحتيال الإلكتروني.

[1] قانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

[2] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلية الاقتصادية، المرجع السابق، ص205.

أولا: تعريف جريمة الاحتيال للمستند الإلكتروني:

تطورت أساليب الاحتيال بشكل ملحوظ، إذ لم تعد تقتصر على المعاملات التقليدية بين الأفراد أو بينهم وبين المؤسسات، بل امتدت لتشمل أيضًا التعاملات الإلكترونية، التي أصبحت بيئة خصبة لممارسات النصب والاحتيال.

تُبين التشريعات المقارنة أن مجرد الكذب، حتى ولو ورد في صيغة مكتوبة، لا يُعد وسيلة احتيالية كافية لقيام جريمة النصب ما لم يُدعَّم بمظهر خارجي يُضفي عليه طابع الخداع. ومن أبرز هذه المظاهر الاستعانة بشخص آخر لتنفيذ الأساليب الاحتيالية، كأن يقوم الغير بدور إيجابي يعزز الكذب من خلال تقديم وثائق مزورة يمكن استعمالها للإيقاع بالمجني عليه. وتتحقق جريمة الاحتيال بالاستعانة بالغير حتى وإن لم يكن هذا الأخير حاضرًا أثناء تنفيذ الجريمة، إذ يكفي أن يكون قد قدّم المستندات التي استُخدمت في عملية الاحتيال.[1]

أما في ميدان المعاملات الإلكترونية، فإن ما يميز جريمة النصب هو اعتماد الجاني على أجهزة الحاسوب سواء كوسيلة لارتكاب الاحتيال أو كمحل للجريمة نفسها. ولهذا اتجهت العديد من التشريعات الحديثة إلى سن نصوص خاصة تُعاقب على الغش والاحتيال المرتكب باستخدام الحاسوب أو ما يماثله، دون الاكتفاء بإخضاعه للقواعد العامة المعمول بها في جرائم الاحتيال التقليدية، إذا يمكن افتراض حالتين هما:

أ/-الحالة الأولى:

في هذه الصورة من صور الاحتيال، يلجأ الجاني إلى استخدام جهاز الحاسوب كوسيلة رئيسية لتنفيذ النشاط الاحتيالي، وذلك بقصد الإيقاع بشخص معين. وتتمثل هذه الوسيلة في نشر إعلانات أو بيانات كاذبة عبر الوسائط الإلكترونية، بهدف خداع الضحية وتحقيق مكاسب مالية من خلال نشاط تجاري غير مشروع.

[1] نائلة عادل محمد فريد قورة، المرجع السابق، ص205.

ويُعد هذا النوع من الاحتيال مثالًا واضحًا على الاستعانة بالوسائل التقنية والمعلوماتية لتحقيق غايات احتيالية، حيث يلعب جهاز الكمبيوتر دورًا محوريًا في تنفيذ الجريمة، وليس مجرد أداة عرضية.[1]

ب/ الحالة الثانية:

يُثار في الفقه تساؤل حول مدى إمكانية وقوع جريمة النصب بين الآلات ذاتها، كأن يستعين المتهم بجهاز كمبيوتر للاحتيال على جهاز كمبيوتر آخر. والأصل أن جريمة النصب تُرتكب ضد الإنسان باعتباره المجني عليه الطبيعي، غير أن التطور التكنولوجي أفرز وضعًا جديدًا أصبحت فيه الآلة تقوم مقام صاحبها في تنفيذ أو استقبال المعاملات، مما يفتح الباب أمام إشكالية قانونية حول من يُعتبر الضحية الفعلية. ومع ذلك، فإن هذا لا يعفي مالك النظام أو المستفيد من الحماية القانونية، بل يظل متمتعًا بالصفة التي تخوله المطالبة بحقه.

وفي التشريع المصري، نصت المادة 336 من قانون العقوبات على أن الحبس يُعاقَب به كل من توصل إلى الاستيلاء على أموال أو منقولات أو سندات أو مخالصات أو غيرها، وذلك باستعمال طرق احتيالية من شأنها إيهام الناس بوجود مشروع كاذب أو واقعة مزورة أو إحداث أمل كاذب في تحقيق ربح وهمي.

أما في التشريع الجزائري، فقد عرّف المشرع الاحتيال بأنه الاستيلاء عمدًا وبطريق الحيلة والخداع على مال مملوك للغير. وقد نصت المادة 372 من قانون العقوبات على جريمة النصب والاحتيال، مقررة العقاب على كل من توصل إلى استلام أو الحصول على أموال أو منقولات أو سندات أو أوراق مالية أو وعود أو مخالصات أو إبراءات من الالتزامات، سواء بالفعل أو بمحاولة ذلك، متى كان عن طريق أسماء أو صفات كاذبة، أو سلطة وهمية، أو اعتماد مالي غير حقيقي، أو بإحداث أمل كاذب في الفوز أو في وقوع حادث أو واقعة وهمية."[2].

---

[1] طباش أمين، المرجع السابق، ص 103.

[2] الأمر رقم 66-156 المتضمن قانون العقوبات الجزائري.

ثانيا: اركان جريمة الاحتيال للمستند الالكتروني.

1- الركن المادي لجريمة الاحتيال: يتمثل في استيلاء الجاني على الحيازة الكاملة لمال مملوك للغير، وذلك باستخدام إحدى وسائل الاحتيال التي حددها القانون على سبيل الحصر.

2- الركن المعنوي لجريمة الاحتيال: يقوم على توافر القصد الجنائي بشقيه، القصد العام، ويقتضي علم الجاني بالعناصر المكونة للجريمة وإرادته في تحقيقها.

القصد الخاص، ويتمثل في نية تملك المال موضوع الجريمة والاستيلاء عليه لحسابه الخاص.[1]

المطلب الثاني: اجراء المشرع الجزائري من جريمة تزوير المستند الالكتروني.

أدرك المشرع الجزائري مبكرًا خطورة جريمة تزوير المستند الإلكتروني، باعتبارها من الجرائم المستحدثة التي تهدد مصداقية الوثائق الرقمية وسلامة المعاملات الإلكترونية. ويهدف هذا الإجراء إلى حماية البيانات والمحررات الرقمية، وضمان حجّيتها القانونية، وتعزيز الثقة في التعاملات الإدارية والتجارية عبر الوسائط الإلكترونية، وعليه سنتعرف على ذلك من خلال الفرعين المواليين: الفرع الأول: موقف المشرع الجزائري من جريمة تزوير المستند الالكتروني، الفرع الثاني: العقوبات المقررة.

الفرع الأول: موقف المشرع الجزائري من جريمة تزوير المستند الالكتروني.

المشرع الجزائري يرى في جريمة تزوير المستند الإلكتروني تهديدًا خطيرًا لتكامل الوثائق الرسمية والثقة العامة، ولذلك فقد اتخذ خطوات تشريعية هامة خلال السنوات الأخيرة لتعزيز الردع وتطوير أدوات الحماية، أدرج المشرع الجزائري الأحكام المتعلقة بجرائم التزوير بصفة عامة ضمن قانون العقوبات، حيث أفرد لها مجموعة من المواد التي تناولت الجريمة من مختلف جوانبها. كما خصّ جريمة تزوير المحررات بتنظيم خاص ضمن نفس القانون، وذلك من المادة 214 إلى المادة 229.

[1] طباش أمين، المرجع السابق، ص 114.

وقد جاء في المادة 214 من قانون العقوبات ما يلي:

"يُعد مرتكبًا لجريمة التزوير، كل موظف أو شخص يؤدي وظيفة عمومية أو خاصة، يقوم أثناء ممارسة مهامه بتغيير الحقيقة في المحررات الرسمية أو العمومية، وذلك من خلال وضع توقيعات مزوّرة، أو إدخال تعديلات على المحررات أو الخطوط أو التوقيعات، أو بانتحال هوية الغير أو الحلول محلها، أو بالكتابة في السجلات أو المحررات العمومية، أو بإجراء تغييرات فيها بعد الانتهاء من إعدادها وإغلاقها."[1]

كما نص في المادة 216 من ذات القانون على التزوير في المحررات الرسمية أو العمومية المرتكب من طرف الأشخاص العاديين غير الذين عينتهم المادة 214 الأنف ذكرها، أما المادة 219 فنظم فيها المشرع فعل التزوير في المحررات العرفية أو التجارية أو المصرفية.[2]

إن المتتبع لترسانة النصوص العقابية الجزائرية يدرك أن المشرع الجزائري قد جعل من جريمة التزوير تنصب على المحررات العادية فقط، ولم يتخذ أي موقف للتوسيع من مفهوم المحرر ليشمل المحررات والمستندات المعلوماتية ضمن المحررات محل جريمة التزوير، كما أنه لم يورد نصاً في قانون العقوبات يعرف فيه جريمة التزوير.[3]

مما سبق يتبين أن المشرع الجزائري لم يواكب نظيره الفرنسي بحيث لم يورد نصا مستقلا للتزوير المعلوماتي بصفة عامة والتزوير في المستندات الإلكترونية بصفة خاصة، كما وأنه لم ينص عليها كجرائم ضمن القواعد العقابية العامة التي تجرم فعل التزوير ولا كأفعال معاقب عليها ضمن جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات[4]، وذلك

---

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج 2، المرجع السابق، ص307.

[2] تنص المادة 219/1 من ق.ع.ج : المعدل والمتمم: «كل من ارتكب تزويراً بإحدى الطرق المنصوص عليها في المادة 216 في المحررات التجارية أو الصرفية، أو شرع في ذلك يعاقب بالحبس من سنة إلى خمس سنوات وبغرامة من 500 إلى 20.000 دينار.

[3] سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2010 – 2011، ص109.

[4] خليفي مريم، الرهانات القانونية للتجارة الإلكترونية، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2011–2012، ص 169.

رغم محاولاته العديدة لسد الفراغ التشريعي في مجال حماية نظم المعلومات، ومكافحة الجريمة المعلوماتية، التي تجسدت بداية بإصداره القانون رقم 04-15 المعدل والمتمم لقانون العقوبات[1]، والذي بموجبه استحدث قسما سابع مكرر في تقنين العقوبات سماه المساس بأنظمة المعالجة الآلية للمعطيات، حيث نص فيه على حماية جزائية للأنظمة المعلوماتية من خلال تجريم بعض أنواع الاعتداء التي تستهدف أنظمة المعالجة الآلية للمعطيات كالدخول غير مشروع للأنظمة المعلوماتية والتلاعب بالمعطيات الخاصة لأنظمة المعلومات[2]، إلا أنه لم يفرد نصاً خاصاً يتضمن التزوير المعلوماتي وتزوير المستندات والمحررات الإلكترونية، وظل المشرع الجزائري على موقفه إلى غاية سنة 2014 حيث أصدر القانون 14-03 المتعلق بمستندات ووثائق السفر[3] ، والذي فرض فيه ضمن أحكامه الجزائية بعض العقوبات على فعل التزوير الذي يمكن أن يطال البيانات الإلكترونية الخاصة بوثائق السفر المخزنة في النظام البيوميتري الإلكتروني بحيث جاء في المادة 17 منه على أن: « كل شخص يزور... عمداً سنداً أو وثيقة سفر... يتعرض إلى العقوبات المنصوص عليها في قانون العقوبات.

[1] هذا القانون قد تم تعديله سنة 2006 بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون العقوبات الجزائري، وقد مس التعديل ثلاث مواد من القانون رقم 04-15 وهي المادة 304 مكرر إلى غاية المادة 304 مكرر 2.

[2] تنص المادة 394 مكرر من ق.ع. ج المعدل والمتمم: "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج. وبخصوص جريمة التلاعب بمعطيات أنظمة المعلوماتية فنص عليها المشرع الجزائري بالمادة 394 مكرر 1 من قانون العقوبات الجزائري وجاء فيها: « يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها».

[3] قانون رقم 14-03 مؤرخ في 24 ربيع الثاني عام 1435 الموافق 24 فبراير سنة 2014 المتعلق بسندات ووثائق السفر، ج.ر . ع. 16، س. 2014.

وإذا مست الأفعال المذكورة أعلاه البيانات المخزنة في النظام البيوميتري الإلكتروني فتطبق العقوبات المنصوص عليها في قانون العقوبات، لا سيما تلك المنصوص عليها في المواد 394 مكرر إلى 394 مكرر 7".

أمام النقص التشريعي الوارد في أحكام قانون العقوبات ينبغي على المشرع الجزائري أن يحذو حذو نظيره الفرنسي بحيث يوسع من المحل الذي يقع عليه فعل التزوير بحيث يشمل المحرر التقليدي وأي محرر آخر مهما كانت طبيعته كما يتوجب عليه التوسيع من طرق التزوير بحيث لا يحصرها في طرق محددة كما فعل في المادة 214 وما يليها من قانون العقوبات وهذا كله لمسايرة الأحداث المتغيرة باستمرار.

لتحقيق هذا كله يتوجب عليه أن يضيف في قانون العقوبات نصا إلى باب التزوير في المحررات يعرف فيه التزوير على النحو التالي: " كل تغيير في الحقيقة بطريق الغش في مكتوب أو أي دعامة أخرى تحتوي تعبيراً على الفكر"[1]، وبهذا التعديل يكون النص أشمل حيث يمكن أن تدرج فيه كل المستندات المعلوماتية حتى وإن كانت غير معالجة آلياً وهو ما يضمن حماية جزائية فعالة.

ولتفعيل آليات جديدة للقضاء على تزوير المحررات والمستندات الإلكترونية تم استحداث قانون خاص لمكافحة التزوير (القانون 24-02 الصادر في 26 فبراير 2024)

[1] القانون رقم 15-104 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، بموجب أحكام هذا القانون، تعتمد هيكلة النظام الوطني للتصديق والتوقيع الإلكترونيين على ثلاث جهات مكملة وهي:

السلطة الوطنية للتصديق الإلكتروني (ANCE)، التابعة لمصالح الوزير الاول، تلعب دورًا مركزيًا في ترقية استعمال التوقيع والتصديق الإلكترونيين وتطويرهما وضمان موثوقية استعمالهما.

السلطة الحكومية للتصديق الإلكتروني (AGCE)، الخاضعة لإشراف وزير البريد والمواصالات السلكية واللاسلكية، مسؤولة عن متابعة ومراقبة نشاط التصديق الإلكتروني للأطراف الثالثة الموثوقة وكذلك توفير خدمات التصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي.

السلطة الاقتصادية للتصديق الإلكتروني (AECE)، التابعة لسلطة ضبط البريد والاتصالات الالكترونية (ARPCE)، مسؤولة عن متابعة ومراقبة مؤديي خدمات التصديق الإلكتروني الذين يقدمون خدمات التوقيع والتصديق الإلكتروني لصالح الجمهور.

بحيث تبنّي قانون 24-02 المعني "بمكافحة التزوير واستعمال المزور"، الذي يُعَدّ إطارًا تشريعيًا شاملاً، ويعاقِب ليس فقط التزوير المادي بل أيضًا الوقائع الافتراضية المرتبطة بالوسائل الإلكترونية مثل العملات الرقمية والمستند الإلكتروني.[1]

كما يشمل قانون 24-02 عقوبات تُعد من أشد العقوبات، تصل في بعض الحالات إلى السجن المؤبد أو حتى 30 سنة، خاصة إذا ارتكب الجريمة موظف عام أو كان يتعلق الأمر بالنقود الرقمية.

بحيث جاء في نص المادة 01من القانون 24-02مايلي:

المادة01: يهدف هذا القانون إلى مكافحة التزوير واستعمال المزور ويهدف، على الخصوص، إلى ما يأتي:

- المساهمة في أخلقة الحياة العامة وتعزيز الثقة العامة.
- القضاء على كل مظاهر الاحتيال للحصول على الخدمات والمزايا مهما يكن نوعها.
- المعالجة العميقة والردعية لكل الاختلالات المجتمعية الناتجة عن التزوير واستعمال المزور، قصد تجسيد الشفافية و إقرار المنافسة الحقيقية والنزيهة في كل المجالات،
- تكريس المساواة أمام القانون.
- الحفاظ على سلامة المحررات والوثائق واستقرار المعاملات.
- ضمان وصول مساعدات الدولة إلى مستحقيها الحقيقيين.
- تحديد الجرائم المتعلقة بالتزوير واستعمال المزور والعقوبات المطبقة عليها.[2]

[1] قانون رقم 24-02 مؤرخ في 16 شعبان عام 1445 الموافق 26 فبراير سنة 2024، يتعلق بمكافحة التزوير واستعمال المزور.

[2] المادة 01من قانون رقم 24-02 مؤرخ في 16 شعبان عام 1445 الموافق 26 فبراير سنة 2024، يتعلق بمكافحة التزوير واستعمال المزور.

الفرع الثاني: العقوبات المقررة.

المشرع الجزائري كغيره من التشريعات العربية والدولية على غرار التشريع الفرنسي اقر بوجود عقوبات لجريمة تزوير المستند الالكتروني والمحررات، بحيث عمل على محاربتها والحد منها من خلال إجراءات ردعية.

كما نصت المادة 02 من قانون رقم 24-02 مؤرخ في 16 شعبان عام 1445 الموافق 26 فبراير سنة 2024[1]، يتعلق بمكافحة التزوير واستعمال المزور، والي ينص علي مايلي:

- تزوير الوثائق والمحررات.
- التزوير للحصول على الإعانات والمساعدات العمومية والإعفاءات.
- تزوير النقود والسندات المالية.
- تقليد أختام الدولة والدمغات والطوابع والعلامات.
- شهادة الزور واليمين الكاذبة.

انتحال الوظائف والألقاب أو الأسماء أو إساءة استعمالها.

اما فيما يخص المادة 216من (القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006) يعاقب بالسجن المؤقت من عشر (10) سنوات إلى عشرين (20) سنة وبغرامة من 1.000.000 دج إلى 2.000.000 دج، كل شخص، عدا من عينتهم المادة 215، ارتكب تزويرا في محررات رسمية أو عمومية[2]، والتي تضمنت أيضا:

1 – إما بتقليد أو بتزييف الكتابة أو التوقيع.

2 – وإما باصطناع اتفاقات أو نصوص أو التزامات أو مخالصات أو بإدراجها في هذه المحررات فيما بعد.

[1] المرجع نفسه.

[2] المادة 216من القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006.

3 – وإما بإضافة أو بإسقاط أو بتزييف الشروط أو الإقرارات أو الوقائع التي أعدت هذه المحررات لتلقيها أو لإثباتها.

جاء في نص المادة 218 على جريمة استعمال المحررات المزورة من قانون العقوبات، على استعمال المحررات العرفية أو التجارية أو المصرفية المزورة في المادة 221 من قانون العقوبات، وعلى استعمال الوثائق الإدارية والشهادات المزورة في المواد 222/1 و 223 و 227/2 و 228/3 من قانون العقوبات، إلا أنه لم يتعرض إلى جريمة إستعمال المستندات الإلكترونية المزورة وهو أمر منطقي طالما لم ينص على جريمة التزوير المعلوماتي في قانون العقوبات عند إستحداثه لنصوص تشريعية حديثة تعالج المعاملات الإلكترونية وتحمي نظم المعلومات المختلفة، كالقانون رقم 04-15 المعدل والمتمم لقانون العقوبات المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات[1]، وكذا القانون 04-15 المتعلق بالتوقيع والتصديق الإلكترونيين الصادر في سنة 2015[2]، فنصوص هذه القوانين جاءت خالية من النص على هذه الجريمة، رغم مصادقة الجزائر على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات سنة 2014، والتي أورد فيها نصا يعالج جريمة إستعمال المحررات الإلكترونية المزورة، بحيث ذكر في المادة 10 منها أن جريمة التزوير هي : "استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه إحداث ضرر، وبنية إستعمالها كبيانات صحيحة".

وعليه فإن القانون قانون رقم 24-02 في المادة31 المتعلق بتزوير المحرارت والمستندات جاءت كمايلي[3] "يعاقب بالحبس من عشر (10) سنوات إلى عشرين (20) سنة وبغرامة من 1.000.000 دج إلى 2.000.000 دج، كل شخص، عدا من حددتهم المادة 32 ، ارتكب تزويرا في محررات عمومية أو رسمية":

[1] القانون رقم 04-15- المعدل والمتمم لقانون العقوبات والمتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

[2] قانون رقم 15-2014 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

[3] المادة 31 من قانون رقم 24-02 مؤرخ في 16 شعبان عام 1445 الموافق 26 فبراير سنة 2024 ، يتعلق بمكافحة التزوير واستعمال المزور.

1- إما بتقليد أو تزييف الكتابة أو التوقيع.

2- وإما باصطناع اتفاقات أو نصوص أو التزامات أو مخالصات أو بإدراجها في هذه المحررات لاحقا.

3- وإما بإضافة أو بإسقاط أو بتزييف شروط أو إقرارات أو وقائع أعدت هذه المحررات لتلقيها أو لإثباتها.

أما المادة 32 نصت على مايلي "يعاقب بالسجن المؤقت من عشرين (20) سنة إلى ثلاثين (30) سنة، كل قاض أو موظف أو ضابط عمومي، ارتكب عن قصد تزويرا في محررات عمومية أو رسمية أثناء تأدية وظيفته": منها إحداث تغيير في محررات أو خطوط أو توقيعات أو الكتابة في السجلات أو غيرها من المحررات العمومية أو بالتغيير بعد إتمامها أو قفلها".[1]

خلاصة الفصل:

[1] المادة 32 من قانون رقم 24-02 مؤرخ في 16 شعبان عام 1445 الموافق 26 فبراير سنة 2024، يتعلق بمكافحة التزوير واستعمال المزور.

ختامًا في هذا الفصل حاولنا التعرف على موقف المشرع الجزائري من جريمة تزوير المستند الإلكتروني وعيًا قانونيًا متقدمًا بالتحديات التي تفرضها البيئة الرقمية الحديثة، فمن خلال تطوير التشريعات وتكييف القوانين العامة والخاصة، كقانون العقوبات وقانون مكافحة الجرائم المعلوماتية، تم إرساء آليات فعالة لتجريم هذا النوع من الأفعال وحماية المستندات الإلكترونية من كل صور التلاعب والتزوير، وتُمثل هذه الآليات خطوة أساسية نحو تعزيز الأمن الرقمي وضمان مصداقية الوثائق الإلكترونية، بما يواكب التحولات التكنولوجية ويصون حقوق الأفراد والمؤسسات في العصر الرقمي.

خاتمة

خاتمة:

ختاما في هذه الدارسة سعينا من خلالها إلى تناول موضوع ذي أهمية بالغة من الناحيتين التشريعية والعملية، فقد خصصنا الفصل الأول للتعريف بالمستند الإلكتروني، من خلال إبراز مفهومه وخصائصه وصوره وشروطه، مع التمييز بينه وبين المستند التقليدي، وبيان مدى حجيته في الإثبات.

أما الفصل الثاني فقد عالجنا فيه حجية المستند الإلكتروني وبالإضافة الى العقوبات المقررة عن جريمته، سواء تلك التي تمس بمحتواه كجريمتي التزوير والإتلاف وما أقره المشرع من حماية جنائية لهما، أو تلك التي تمس بسرية المستند، حيث حاولنا تبيان دور المشرع الجزائري وكيف تعامل مع هاته الجريمة من أساليب وطرق وكيفية الحد منها مستقبلا.

بحيث توصلنا الى مجموعة من النتائج وهي كالتالي:

- المستند الإلكتروني أصبح وسيلة حديثة للإثبات، ويكتسب حجية قانونية متى استوفى شروط المشرع.
- التطور التكنولوجي أدى إلى بروز جرائم جديدة تمس المستند الإلكتروني، مثل: التزوير، الإتلاف، وانتهاك السرية.
- أغلب التشريعات، ومنها الجزائري، أقرت حماية جنائية خاصة للمستند الإلكتروني، مع تباين في نطاق هذه الحماية.
- عناصر جرائم المساس بسرية المستند متشابهة في التشريعات المقارنة (الجاني، الوسائل الاحتيالية، القصد الجنائي، الاتصال غير المشروع).
- ضبط الجرائم المعلوماتية يتطلب إجراءات خاصة، أهمها التفتيش الإلكتروني.

التوصيات:

- سنّ تشريعات جزائرية أوضح وأكثر شمولًا لمواكبة التطورات التكنولوجية والجرائم المعلوماتية المستحدثة.
- تعزيز أطر التعاون الدولي لمكافحة الجرائم المعلوماتية نظرًا لطبيعتها العابرة للحدود.

– تدعيم برامج التكوين والتدريب لفائدة القضاة وأعوان الضبطية القضائية في مجال الإثبات الإلكتروني.

– تطوير وسائل وآليات تقنية لحماية المستندات الإلكترونية من التزوير والاختراق وضمان قوتها القانونية.

–إنشاء مراكز بحث متخصصة في الجريمة المعلوماتية لتقديم حلول تشريعية وتقنية تواكب التحديات الحديثة.

قائمة المصادر

والمراجع

قائمة المصادر والمراجع:

أولا: الأوامر والمراسيم:

1. الأمر 75/85 المؤرخ في 26/09/1975 المتضمن التقنين المدني الجزائري المعدل والمتمم بالقانون رقم 05/10 المؤرخ في 20/06/2005، ج ر رقم 44 الصادرة بتاريخ 26/06/2005.

2. الامر رقم 1.07.129 صادر في 19 من ذي القعدة 1428 (30) نوفمبر (2007) بتنفيذ القانون رقم 05-53 المتعلق بالتبادل الالكتروني للمعطيات القانونية (المادة 08).

3. الأمر رقم 66-156 المتضمن قانون العقوبات الجزائري.

4. الأمر رقم 75-85 المتضمن القانون المدني الجزائري.

5. الجريدة الرسمية للجمهورية الجزائرية، العدد 06، 20 ربيع الثاني عام 1436هـ الموافق ل 10 فبراير سنة 2018.

6. قانون اتحادي رقم (1) لسنة 2006 في شأن المعاملات والتجارة الإلكترونية، ج. ر، ع442، س. السادسة والثلاثون بتاريخ 31/1/2006.

7. قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية السنة الرابط: https://uncitral.un.org أطلع عليه بتاريخ 2025/04/03.

8. قانون التوقيع الإلكتروني المصري رقم 15 لعام 2004 على الرابط http://borai.com ، أطلع عليه بتاريخ 2025/02/21.

9. قانون رقم (2) لسنة 2002 بشأن المعاملات والتجارة الإلكترونية في الإمارات العربية الصادر بتاريخ 30 ذي القعدة 1422 الموافق 12 فبراير 2002.

10. قانون رقم 04-15 المعدل والمتمم لقانون العقوبات الجزائري الصادر بموجب الأمر رقم 66-156 المؤرخ في 08 يونيو 1966.

11. القانون رقم 04-15- المعدل والمتمم لقانون العقوبات والمتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

12. قانون رقم 05-10 المؤرخ في 13 جمادى الأولى عام 1426هـ الموافق 20 يونيو 2005 المعدل والمتمم للأمر رقم 58-75 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر س 1975 المتضمن القانون المدني الجزائري، ج.ر، ع.44، س. 2005.

13. قانون رقم 14-03 مؤرخ في 24 ربيع الثاني عام 1435 الموافق 24 فبراير سنة 2014 المتعلق بسندات ووثائق السفر، ج.ر . ع. 16، س. 2014.

14. القانون رقم 15 لسنة 2004 بشأن تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

15. قانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

16. قانون رقم 15-04 المؤرخ في 01 فبراير 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر.ج.ج، عدد 06 صادر في 10/02/2015.

17. القانون رقم 15-104 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

18. قانون رقم 15-2014 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

19. قانون رقم 24-02 مؤرخ في 16 شعبان عام 1445 الموافق 26 فبراير سنة 2024 ، يتعلق بمكافحة التزوير واستعمال المزور.

ثانيا: المواد.

20. المادة 01من قانون رقم 24-02 مؤرخ في 16 شعبان عام 1445 الموافق 26 فبراير سنة 2024، يتعلق بمكافحة التزوير واستعمال المزور.

21. المادة 02 من قانون رقم 24-02 مؤرخ في 16 شعبان عام 1445 الموافق 26 فبراير سنة 2024 ، يتعلق بمكافحة التزوير واستعمال المزور.

22. المادة 21 من القانون رقم 53-05.

23. المادة 214من القانون رقم 82-04 المؤرخ في 13 فبراير 1982.

24. المادة 216من القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006.

25. المادة 31 من قانون رقم 24-02 مؤرخ في 16 شعبان عام 1445 الموافق 26 فبراير سنة 2024، يتعلق بمكافحة التزوير واستعمال المزور.

26. المادة 32 من قانون رقم 24-02 مؤرخ في 16 شعبان عام 1445 الموافق 26 فبراير سنة 2024، يتعلق بمكافحة التزوير واستعمال المزور.

27. المادة 394 مكرر من القانون رقم 04-15- المعدل والمتمم بالقانون رقم 06-23 المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

ثالثا: الكتب.

28. أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج2، جرائم الفساد- جرائم المال والأعمال- جرائم التزوير، منقحة ومتممة في ضوء قانون 20 فبراير 2006 المتعلق بالفساد، 96، دار هومة، الجزائر 2008.

29. أحمد أبو الروس، قانون جرائم التزييف والتزوير، المكتب الجامعي الحديث، الاسكندرية 1997.

30. أحمد عاصم عجلية، الحماية الجنائية للمحررات الالكترونية، دراسة مقارنة، دار. الن هضة العربية، القاهرة، 2014.

31. ايد رجا الخلايلة، المسؤولية التقصيرية الإلكترونية، المسؤولية الناشئة عن إساءة استخدام أجهزة الحاسوب والانترنت، دراسة مقارنة، ط 1 دار الثقافة، عمان، 2009.

32. أيمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية- الطبعة الأولى، مكتبة القانون والإقتصاد، المملكة العربية السعودية، 2014.

33. إيهاب فوزي السقا، جريمة التزوير في المحرارت الإلكترونية، دار الجامعة للنشر، الإسكندرية، 2002.

34. إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة للنشر، الإسكندرية، 2002.

35. بصلة رياض فتح الله، جرائم الاحتيال بالبطاقات الانتمائية، وأساليب مكافحتها، اعمال ندور تزوير البطاقات الانتمائية، اكاديمية نايف للعلوم الأمنية، الرياض،2002.

36. تمام أحمد حسام طه، الجرائم الناشئة عن استخدام الآلي، دراسة مقارنة، ط1، دار النهضة العربية، مصر،2000.

37. جلال ثروت، نظم القسم الخاص، الجزء الثالث، دار المطبوعات الجامعية، 1995.

38. حجازي عبد الفتاح بيومى، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، المركز القومي للإصدارات القانونية، القاهرة،2011.

39. حجازي عبد الفتاح بيومى، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، القاهرة،2002.

40. حسن عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنيت دار النهضة العربية، 2000.

41. خالد حربي السعدي،جريمة إتلاف برامج ومعلومات الحاسب الآلي في التشريعين الكويتي والمقارن، ط 1، دار النهضة العربية، القاهرة– مصر، 2012.

42. خالد عبد الفتاح محمد، التنظيم القانوني للتوقيع الإلكتروني، المركز القومي للإصدارات القانونية، الطبعة الأولى، (د.م.ن)، 2009.

43. خشير مسعود، الحماية الجنائية البرامج الكمبيوتر، دار الهدى الجزائر ،2010

44. د. أحمد مختار عمر، معجم اللغة العربية المعاصرة، عالم الكتب، القاهرة، 2008.

45. دردوس مكي، القانون الجنائي الخاص في التشريع الجزائري، ج 2، ديوان المطبوعات الجامعية، الجزائر، ب.ت.ن.

46. الرازي، احمد بن فارس القزويني، معجم المقاييس اللغة 3/63، دار الفكر، 1399هـ.

47. سامح عبد الواحد التهامي، التعاقد عبر الانترنيت، دراسة مقارنة، دار الكتب القانونية ودار شتات للنشر والبرمجيات، مصر،2008.

48. سرور أحمد فتحي، الوسيط في قانون العقوبات، القسم الخاص، ط4، دار النهضة العربية، 1991.

49. سعد عبد العزيز، جرائم التزوير وخيانة الأمانة واستعمال المزور، ط1، دار هومة، الجزائر، 2005.

50. سليمان أحمد فضيل، المواجهة التشريعية والأمنية للجزائر الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، دار النهضة العربية، القاهرة، 2007.

51. سليمان عبد المنعم، قانون العقوبات الخاصة، القوائم الماسة بالمصلحة العامة، الجامعة الجديدة للنشر، الاسكندراية،1993.

52. شمسان ناجي صالح الخليلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الأنترنت دراسة مقارنة، دار النهضة العربية، القاهرة، 2009.

53. عابد فايد عبد الفتاح، الكتابة الإلكترونية في القانون المدني بين التطور القانوني والأمن التقني، دار الجامعة الجديدة، الإسكندرية، 2014.

54. العبادي محمد حميد الرصفان، الجرائم المستحدثة في ظل العولمة، ط1، دار جليس الزمان، عمان، 2015.

55. عباس العبودي، الحجية القانونية لوسائل التقدم العلمي في الإثبات المدني، المكتبة القانونية، عمان، 2002.

56. العبيدي صدام حسين، والعبيدي عواد حسين ياسين، أحكام جرائم التزوير التقليدي والإلكتروني في الفقه الاسلامية القانون الوضعي، ط1، المركز العربي للنشر والتوزيع، 2020.

57. العسكري أبو هلال بن عبد الله، الفروق اللغوية، تحقيق: محمد إبراهيم سليم، دار العلوم الثقافية للنشر والتوزيع، القاهرة، 1997.

58. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، تقديم فتوح الشاذلي، دار الثقافة للطباعة والنشر، عمان، الأردن، 1999.

59. عقاد محمد، جريمة التزوير في محررات الحاسب، دراسة مقارنة، بحث مقدم في المؤتمر السادس المنعقد خلال فترة 25-1993/10/28، الجمعية المصرية للقانون الجنائي، دار النهضة العربية.

60. العكسري أبو هلال الحسن ابن عبد العبد الله، الفروق اللغوية، تحقيق: محمد إبراهيم سليم، دار العلم والثقافة للنشر والتوزيع، القاهرة، 1996.

61. علي محمد أحمد أبو العزء، التجارة الإلكترونية وأحكامها في الفقه الإسلامي، ط1، دار النفائس، الأردن، 2008.

62. عمر خالد زريقات، عقود التجارة الإلكترونية (عقد البيع عبر الإنترنيت دراسة تحليلية)، دار الحامد ط1، عمان، 2007.

63. فشار عطا الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم الى الملتقى المغاربي حول القانون والمعلوماتية بمقر أكاديمية الدراسات العليا بليبيا في أكتوبر 2009.

64. فيصل سعيد الغريب، التوقيع الإلكتروني وحجيته في الإثبات، منشورات المنظمة العربية للتنمية الإدارية، 2005.

65. محمد حماد مرهج الهيتي، جرائم الحاسوب، ماهيتها أهم صورها و العقوبات التي تواجهها، ط1، دار المنهج، عمان، 2006.

66. محمد عقاد، جريمة التزوير في محررات الحاسب الآلي، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون، دار النهضة العربية، القاهرة، 1995.

67. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، سنة 2001.

68. مدحت محمد عبد العزيز إبراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي، دراسة مقارنة، ط 1، دار النهضة العربية، القاهرة، 2015.

69. مراد عبد الفتاح، شرح جرائم التزييف والتزوير، الإسكندرية، 2011.

70. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلية الاقتصادية، ط 1، منشورات الحلبي الحقوقية، لبنان، 2005.

71. نهلا عبد القادر المومني، الجرائم المعلوماتية، الأردن، دار الثقافة، 2008.

72. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة.

73. هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها، ط1، دار النهضة العربية، القاهرة، 2007.

74. يوسف الأبيض، لحوص التزييف والتزوير، دار المطبوعات الجامعية، مصر، 2006.

رابعا: الرسائل الجامعية.

75. إلهام بن خليفة، الحماية الجنائية لمحررات الإلكترونية من التزوير، أطروحة دكتوراه في العلوم القانونية والإدارية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2016.

76. براهيمي حنان، جريمة تزوير الوثيقة الرسمية، الإدارية ذات الطبيعة المعلوماتية، أطروحة دكتوراه تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة 2015.

77. بلعيشة علي، الحماية الجنائية للمستند الإلكتروني، مذكرة لنيل شهادة الماستر تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم الجزائر 2019.

78. الجبوري عمر عبد السلام حسين، جريمة التزوير الإلكتروني في التشريع الأردني، رسالة ماجستير، جامعة الشرق الأوسط الأردن،2017.

79. حفصي عباس، جرائم التزوير الإلكترونية أطروحة مقدمة لنيل شهادة دكتوراه، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة وهران 1، 2014 – 2015.

80. حفظي عباس، جرائم التزوير الإلكتروني، رسالة دكتوراه جامعة وهران، الجزائر، 2015 .

81. خليفي مريم، الرهانات القانونية للتجارة الإلكترونية، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2011–2012.

82. سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2010 – 2011.

83. عبد السلام حسين الجبوري، جريمة التزوير الإلكتروني في التشريع الأردني (دراسة مقارنة) رسالة مقدمة إستكمالا لمتطلبات الحصول على درجة الماجستير، كلية الحقوق جامعة الشرق الأوسط، 2017.

84. كحلول سماح، حجية الوسائل التكنولوجية في إثبات العقود التجارية، مذكرة ماستر في القانون العام للأعمال، كلية الحقوق السياسية، جامعة قاصدي مرباح، ورقلة 2015.

85. محمد حسين علي محمود، التزوير باستخدام الوسائل الالكترونية، رسالة ماجستير في الحقوق، كلية الحقوق، جامعة القاهرة، 2011.

86. معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة ماجستير في العلوم القانونية، تخصص قانون جنائي، جامعة الحاج لخضر، باتنة، 2012.

خامسا: المجلات.

87. رضا متولي وهدان، النظام القانوني للعقد الإلكتروني، مجلة البحوث القانونية والإقتصادية، مجلة فصلية محكمة يصدرها أساتذة كلية الحقوق جامعة المنصورة، العدد الثاني والأربعون، أكتوبر 2007.

88. السيراني عبد الله بن سعود محمد، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، ط1، المجلة العلمية، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2011.

89. صالح شنين، الحماية الجنائية للتجارة الإلكترونية (دراسة مقارنة)، رسالة دكتوراه في القانون الخاص، جامعة تلمسان، 2025/2014.

90. عادل مستاري، رواحنة زوليخة، جريمة التزوير الإلكتروني، مجلة العلوم الإنسانية، المجلد 17، العدد 46، جامعة محمد خيضر، بسكرة، الجزائر، الصادر في مارس 2017.

91. عبد الله بلقاسم، الطبيعة الخاصة لجريمة التزوير في المحررات الإلكترونية، مجلة الدراسات القانونية المقارنة، المجلد6، العدد الثاني جامعة حسيبة بن بوعلي الشلف الجزائر، الصادر في 27/12/2020.

92. عمار كريم كاظم وناريمان جميل نعمة، القوة القانونية للمستند الإلكتروني، مجلة كلية القانون العدد السابع، جامعة الكوفة،2007.

93. لامية طالة، كهينة سلام الجريمة الإلكترونية بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي، مجلة الرواق للدراسات الاجتماعية والإنسانية، المجلد 6، العدد الثاني، المركز الجامعي أحمد زبانة، غليزان، الجزائر، الصادر في 30/12/2020.

94. محمد أمين الرومي، المستند الإلكتروني، دار الكتب القانونية، الاسكندرية مصر، المجلة الكبرى، 2008.

سادسا: المحاضرات.

95. كواحلة يمينة، محاضرات على الخط في مقياس إدارة المستند الرقمي، مقدمة لطلبة السنة الأولي ماستر: علوم اقتصادية، تخصص اقتصاد رقمي، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة لونيسي علي، البليدة 02، 2022/2021.

سابعا: المواقع الإلكترونية.

96. أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني –دراسة مقارنة–، بحث منشور على شبكة الانترنيت، من خلال الموقع الإلكتروني الآتي:الدليل الإلكتروني القانون العربي، Https://Www.Arabawifo.Comتمت الزيارة 2025/04/05.

97. الإتفاقية العربية لمكافحة جرائم تقنية المعلومات على الرابط : https://ar.m.wikisource.org

98. Protéger contre la falsification de document, publié le sur: https://nec-itplatform.com

ثامنا: المراجع الأجنبية.

99. Bergman, Bengt, E – Fraud: State of the art and Countermeasures, Student Thesis,2005.

100. Bhatla, T. P., Prabhu, V. & Dua, A. Understanding Credit Card Frauds, © Tata Consultancy Services.Linköping University.2002

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

فهرس

الموضوعات

ملخص:

يُعد التزوير في المستند الإلكتروني من أبرز الجرائم المعلوماتية المستحدثة التي فرضتها التطورات التكنولوجية وانتشار التعاملات الرقمية، حيث أصبح المستند الإلكتروني يحتل مكانة موازية للمستند التقليدي في الإثبات متى استوفى الشروط التي حددها المشرع.

بحيث اعتمدنا من خلالها على فصلين فصل اول إطار مفاهيمي للمستند الإلكتروني اما الفصل الثانية تطرقنا من خلاله الى الآليات القانونية لتجريم تزوير المستند الالكتروني.

وتخلص الدراسة إلى أن المشرع الجزائري، رغم سعيه إلى حماية المستند الإلكتروني، ما يزال بحاجة إلى تطوير نصوص أكثر دقة ووضوحًا لمواكبة السرعة الكبيرة للتقنيات الحديثة، وتوحيد المفاهيم مع التشريعات المقارنة، إلى جانب دعم الجانب التقني والتكويني لمكافحة هذه الجريمة بفعالية.

الكلمات المفتاحية: التزوير، المستند، المستند الالكتروني.

Summary :

Electronic document forgery is one of the most prominent emerging cybercrimes imposed by technological developments and the proliferation of digital transactions. Electronic documents have become equivalent to traditional documents in terms of evidence, provided they meet the conditions set by the legislator.

We relied on two chapters. The first chapter is a conceptual framework for the electronic document, while the second chapter addresses the legal mechanisms for criminalizing the forgery of the electronic document.

The study concludes that, despite the Algerian legislature's efforts to protect electronic documents, it still needs to develop more precise and clear texts to keep pace with the rapid development of modern technologies, unify concepts with comparative legislation, and support technical and training aspects to effectively combat this crime.

Keywords: Forgery, Document, Electronic Document.