الجامعة العربية الامريكية

كلية الدراسات العليا

التنظيم القانوني لمكافحة جريمة التزوير الإلكتروني في التشريع الفلسطيني -دراسة مقارنة-

إعداد

يزيد عثمان محمد ابو حلو

إشراف

الدكتور أمين إسحق الغنيمات

تم تقديم هذه الرسالة استكمالاً لمتطلبات درجة الماجستير في تخصص العلوم الجنائية.

حزيران/ 2024

©الجامعة العربية الأمريكية -2024 . جميع حقوق الطبع محفوظة.

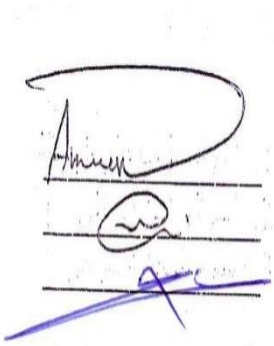
إجازة الرسالة

التنظيم القانوني لمكافحو جريكة التزوير الالكتروني في التشريع الفلسطيني – دراسة مقارنة-

إعداد

يزيد عثمان محمد أبو حلو

نوقشت هذه الرسالة بتاريخ 2024/6/30 وأجيزت.

أعضاء لجنة المناقشة:		التوقيع
1. د. أمين عتمات	مشرفا ورئيساً	
2. د. أحمد الأشقر	ممتحناً داخلياً	
3. د. عصام الأطرش	ممتحناً خارجياً	

الإقرار

أنا الموقع أدناه مقدم الرسالة الموسومة:

" التنظيم القانوني لجريمة التزوير الإلكتروني في التشريع الفلسطيني -دراسة مقارنة- "

أقر بأن ما اشتملت عليه الرسالة إنما هو إنتاج جهدي الخاص باستثناء ما تمت الإشارة إليه حينما ورد، وأن هذه الرسالة ككل .أو أي جزء منها لم يقدم من قبل لنيل أي درجة علمية أو بحث لدى أي مؤسسة تعليمية أو بحثية أخرى.

اسم الطالب الرباعي: يزيد عثمان محمد ابو حلو

الرقم الجامعي: 202020230

التوقيع:..

التاريخ: 2024/11/02

الإهداء

إلى الذي غاب عنا جسداً، وبقي حاضراً بروحه ...

إلى من دعمني وساندني وبقى أثره الجميل في داخلي

عمي الغالي(.....).

إلى صاحب السيرة العطرة، والفكر المستنير...

إلى من كان له الفضل الأول في بلوغي التعليم العالي..

(والدي الغالي)، أطال الله في عمره.

إلى من وضعتني في طريق الحياة، وقدمت كل التضحيات من أجلي

(أمي العزيزة) ....

إلى السند الأكبر في مسيرتي التعليمية .....

إلى من شاركني فرحتي وحزني وما كنت هنا لولاه

(العم الحبيب علي)

إلى جدي العزيز المرحوم سامي الذي اشتاق له ....

لطالما كان قدوتي ومصدر إلهامي الدائم الجد العزيز (سامي)

إلى من أصبحت بعطفهم وحنانهم شمعة تضيئ في كل مكان ...

إليكم أخوتي وأخواتي.

الشكر والتقدير

الحمدلله الذي بنعمته تتم الصالحات، وأفضل الصلاة والتسليم على سيد الخلق والمرسلين سيدنا محمد بن عبد الله صلى الله عليه وسلم .

لا يسعني وقد أنعم الله تعالى عليَ بإتمام هذا الرسالة، إلا أن أتقدم بخالص الشكر وعظيم التقدير إلى إستاذي الفاضل الدكتور إمين إسحق الغنيمات المشرف على هذه الرسالة، حيث لم يبخل علي بعلمه وجهده ووقته، وملحوظاته الدقيقة، وعونه ومساعدته وتوجيهاته الشديدة التي طالت كل جزء من أجزاء الرسالة، وأسهمت في إنجازها بشكل الصحيح.

كما ويسعدني تقديم جزيل الشكر والتقدير إلى الأساتذة أعضاء لجنة المناقشة، لقبولهم مناقشة هذه الرسالة، وعلى ما سيقدمونه لي من توجيهات وملاحظات ستسهم في إثرائها .

ولا يفوتني أن أقدم بجزيل الشكر والتقدير للسادة الأفاضل أعضاء هيئة التدريس في كلية الحقوق، الذين نهلت من علمهم الغزير، فلهم مني كل الاحترام والتقدير.

الباحث

يزيد عثمان محمد ابوحلو

الملخص

تناولت الرسالة الحديث عن التزوير الإلكتروني، كونه أحد أخطر الجرائم التي تتم بواسطة الحاسب الآلي والإنترنت حيث أن هذه الخطورة تزداد يوماً بعد يوم وذلك نتيجة التطور الكبير في تكنولوجيا واستخدامات الحاسواب والإنترنت وسيطرة الجانب المعلوماتي على شتى مجالات الحياة، وتسعى هذه الرسالة لبيان موقف التشريع الفلسطيني من هذه الجريمة وبيان توافقه مع التشريعات، وهل وفق المشرع الفسطيني في وضع عقوبات تتناسب مع خطورة وجسامة هذه الجريمة كون جرائم التزوير لا تقتصر على جانب معين في الدولة بل تهدد النظام الاجتماعي والاقتصادي للدولة، وتهدف هذا الرسالة إيضاً إلى البحث في أنواع جريمة التزوير الإلكتروني وتوضيحها وعلى ماذا تقع ومقارنتها مع التشريعات الأخرى وبيان أوجه القصور التي شابت التشريعات الفلسطينية، كما وبينت هذه الرسالة دور النصوص القانونية الإجرائية والموضوعية وكيفية تطبيقها على جريمة التزوير الإلكتروني، وتم اللجوء إلى استخدام المنهج الوصفي التحليلي والمنهج المقارن لتوصل إلى نتائج متعلقة في موضوع الدراسة، حيث كان من أهم النتائج التي تم التوصل إليها التزوير الإلكتروني يعد من الجرائم المستحدثة التي ظهرت في الآونة الأخيرة، نتيجة التقدم العلمي والتكنولوجي كما أن التزوير الإلكتروني يشكل خطورة لصعوبة اكتشافه من قبل المحققين كونه لا يترك أي أثر مادي.

فهرس المحتويات

إجازة الرسالة ..... أ
الإقرار ..... ب
الإهداء ..... ت
الشكر والتقدير ..... ث
الملخص ..... ج
فهرس المحتويات ..... ح
مقدِمة ..... ه
مشكلة الدِراسة ..... و
أهمية الدِراسة ..... ز
أهداف الدِراسة ..... ط
أدوات الدِراسة ..... ط
منهج الدِراسة ..... ي
محددات الدِراسة ..... ي
الدراسات السابقة ..... ك
خطة الدراسة ..... ل
الفصل الأول: القواعد الموضوعية لجريمة التزوير الإلكتروني 1
المبحث الأول: ماهية جريمة التزوير الإلكتروني 2
المطلب الأول: مفهوم جريمة التزوير الإلكتروني 2
الفرع الأول: التعريف التشريعي لجريمة التزوير الإلكتروني 3
الفرع الثاني: التعريف الفقهي لجريمة التزوير الإلكتروني 4
الفرع الثالث: التعريف الدولي لجريمة التزوير الإلكتروني 5
المطلب الثاني: خصائص جريمة التزوير الإلكتروني 8
الفرع الأول: إمكانية ان تكون جرائم عابرة للحدود 9
الفرع الثاني: جريمة تقنية خاصة 10
الفرع الثالث: جرائم معقدة الكشف والإثبات 10

المبحث الثاني: التكييف القانوني لمحل الجريمة 12
المطلب الأول: تحديد محل جريمة التزوير الإلكتروني 12
الفرع الأول: المستند الإلكتروني 12
الفرع الثاني: التوقيع الإلكتروني 14
المطلب الثاني: أنماط تجريم التزوير الإلكتروني 17
الفرع الأول: أنماط التزوير الإلكتروني وفقاً لمحل الجريمة 17
الفرع الثاني: أنماط التزوير الإلكتروني وفقاً لوقت إرتكاب الجريمة 20
المطلب الثالث: أركان جريمة التزوير الإلكتروني 23
الفرع الأول: الركن المادي 23
الفرع الثاني: الركن المعنوي 24
الفرع الثالث: الضرر 25
الفصل الثاني: القواعد الإجرائية لمكافحة جريمة التزوير الإلكتروني 27
المبحث الأول: الجهات المختصة بالملاحقة في جرائم التزوير الإلكتروني 27
المطلب الأول: دور الضبط القضائي في مكافحة جريمة التزوير الإلكتروني 27
الفرع الأول: إجراءات الضبط القضائي في معاينة جهاز الكمبيوتر 28
الفرع الثاني: إجراءات الضبط القضائي في التفتيش 30
المطلب الثاني: نيابة مكافحة الجرائم الإلكترونية 32
الفرع الأول: نشأة نيابة مكافحة الجرائم الإلكترونية 32
المبحث الثاني: الاختصاص القضائي في جريمة التزوير الإلكتروني 35
المطلب الأول: قواعد الاختصاص القضائي المتعلقة في جريمة التزوير الإلكتروني 35
الفرع الأول: مبدأ الاختصاص الإقليمي 36
الفرع الثاني: مبدأ الاختصاص الشخصي 37
الفرع الثالث: مبدأ العينية 38
الفرع الرابع: مبدأ العالمية 39
المطلب الثاني: سلطة القاضي في قبول الدليل الإلكتروني 40
الفرع الأول : حجية الدليل الإلكتروني أمام القضاء الجنائي 40
الفرع الثاني: العقوبات المقررة لجريمة التزوير الإلكتروني 43
الفرع الثالث: مشروعية الدليل الإلكتروني 47

الخاتمة 49
التوصيات 50
قائمة المصادر والمراجع 51
Abstract 56

مقدِمة

يُشكل التَقدم والتَطور التكنُولوجي الذي يشهدُه العالم ركيزة تؤدي إلى ظهور العديد من الجرائم، ومن بينها جريمة التزوير الإلكتروني وهي تعتبر من الجرائم ذات الطابع الخاص نظراً للطبيعة الخاصة لها، والتي جعلتها تختلف عن جريمة التزوير العادية وجَريمة التزوير في المحررات التقليدية سواء من ناحية اكتشافها وصعوبة إثباتها، واتساع طُرق اِرتكابها التي تتناسب مع ما تشهده التقنيات الحديثة من تطور علمي وتكنولوجي الذي أثر على التطور السريع الهائل للنشاط الإجرامي في هذا النوع المستحدث من الجرائم فأثارها لا تقتصر على فرد معين أو مؤسسة أو على الدولة الواحدة وإنما تتجاوز الحدود الإقليمية لها فهي تتميز بأنها جريمة تقع بيئة إفتراضية غيرَ ملموسة، كما وأنه إذا ما تشابهت الجريمة التقليدية عن نظيرتها الإلكترونية فنجد تشابه كبير بين الجرائم التقليدية والإلكترونية لكن ما يختلف شرط أو اثنان متعلقان بالحاسب الآلي أو البيانات أو شبكة الإنترنت فهنا تثور الخلافات والتساؤلات عن ما هي الأفعال التي تعد مجرمة وما هي شروط مثل هذا الأفعال، ومتى تعد الجريمة مكتملة الأركان، ويجب فرض الجزاء على الفعل إذا ما أضفنا إليه صفة التجريم كما أن هذه الجريمة أصبحت من الجرائم العابرة للحدود نظراً لارتكابها عن طريق الإنترنت الذي جعل العالم وكأنه قرية صغيرة فلا بد من الوقوف على حل ومواجهة مثل هذه الجريمة على الصعيد الدولي وليس على الصعيد المحلي والوطني فقط.[1]

وقد حرص المشرع الفلسطيني على مواكبة التطور التشريعي باستحداث القرار بقانون رقم(10) لسنة 2018 بشأن الجرائم الإلكترونية، لأن هذه الجرائم من الجرائم المعقدة التي من الصعب اكتشاف مرتكبينها كونهم قادرين على تدمير المعلومات التي قاموا بتزويرها خلال عدة ثواني، ونَقف على هذه الجريمة في أمكانية تطبيق النصوص القانونية لجريمة التزوير التقليدية على جريمة التزوير الإلكتروني وتبدأ الإهمية من حيث إيجاد وسائل متقدمة وحديثة للكشف بطريقة سريعة عن هذه الجريمة وإثباتها بطرق يسيرة ومتطورة، ولكي تشعر المتعاملين الإلكترونيين بالطمأنينة والأمان لتفادي ارتكاب مثل هذه الجرائم لأن ارتكابها يُزعزع الثقة بين المتعاملين الإلكترونيين، ما يؤدي إلى إفساد العديد من المعاملات الكترونية وغيرها كون التعامل الإلكتروني هو عصب الحياة العملية والعلمية في الوقت الحاضر، وتتمثل مشكلة هذا الموضوع في أن بعض

---

[1] عمار فتيحة، جريمة التزوير الالكتروني، مجلة القانون والمجتمع ، المجلد 7، العدد1، 2019، ص167.

الدول أصدرت تشريعات خاصة بالجرائم الإلكترونية، في حين أن بعضها لم يصدر مثل هذه التشريعات الخاصة لهذه الجرائم فكيف يتم الوقوف ومواجهة هذا النوع المتطور من الجرائم عند ارتكابها كما وتتمثل المشكلة الأخرى هل أن هذه الدول عندما ترتكب هذه الجريمة يتم تطبيق نصوص قانون العقوبات التقليدية عليها، أم أنه يصدر قانون خاص بها وهي تحتاج إلى مهارة فنية مما يجعل أركان هذه الجريمة وأشكالها وطرقها مختلفة عن تلك المعروفة في جريمة التزوير العادية، بالتالي ظهور طرق وأساليب جديدة متطورة جدا لا يمكن حصرها لأن وقوع التزوير يرتبط أساسا بالجانب التقني أين تتعدد تصبح لا حصر لها، وكون الباحث يعمل في جهاز الشرطة في نطاق اختصاصه، فإن أغلب القضايا التي يتم العمل بها هي من الجرائم الالكترونية بمختلف أنواعها كما وأنها تستغرق وقت ليتم اكتشاف مرتكبها وهذا كله يؤثر على العلاقات الاجتماعية وغيرها، وكما وأن جريمة التزوير الإلكتروني كونها من الجرائم المعقدة وكون مرتكبها على إلمام تام في التعامل مع الحاسب الآلي والإنترنت ولديهم مهارات فنية، لذلك بحاجة إلى من هم أوسع معرفة لكشف هذه الجريمة وتدريب وتعيين خبراء ومختصين بالحاسب الآلي لحل واكتشاف هذه الجريمة وإثباتها ورجال الضبط القضائي وكيفية التعامل مع مسرح الجريمة والحفاظ على الأدلة، كما ويجب توفير معمل كامل لبحث الادلة الرقمية وجرائم تكنولوجيا المعلومات.

مشكلة الدِراسة

تتمثل مشكلة البحث في عدة جوانب متشابكة. أولاً، هناك حاجة لمعرفة القوانين المطبقة عند ارتكاب جرائم التزوير الإلكتروني، حيث تختلف القوانين والعقوبات بين الدول، مما يعقد التعامل مع هذه الجرائم. ثانيًا، يجب تحديد البيانات والمعلومات التي تشكل جريمة التزوير الإلكتروني، فهناك غموض حول ما يعتبر تزويرًا إلكترونيًا وما لا يعتبر كذلك. ثالثًا، هناك تساؤل عن مدى فاعلية الآليات الموضوعية والإجرائية التي وضعتها التشريعات الجنائية لمواجهة التزوير الإلكتروني، وما إذا كانت هذه الإجراءات كافية وفعالة في التصدي لمتغيرات هذا النمط الجديد من الجرائم. بشكل عام، تبرز الحاجة إلى دراسة وتحليل الجوانب القانونية والعملية المتعلقة بجرائم التزوير الإلكتروني وسبل مواجهتها بفعالية.

لذلك كان لا بد من معرفة القوانين المطبقة ومعرفة البيانات والمعلومات التي يصح ولا يصح بشأنها قيام جريمة التزوير الالكتروني، لأنه يوجد بعض المعلومات مصرح بها، وجريمة التزوير الإلكتروني هي جريمة حديثة تتسم بصعوبات خاصة صعوبة تحديد الحيز المكاني هذه الجرائم لا تنحصر في حدود جغرافية محددة، بل تمتد لتشمل مناطق جغرافية خارج حدود الدول و اختلاف

القوانين والعقوبات: القوانين والعقوبات المتعلقة بجرائم التزوير الإلكتروني تختلف بين الدول، مما يعقد التعامل مع هذا النوع من الجرائم.

بناءً على ذلك، فإن التصدي لجرائم التزوير الإلكتروني يتطلب تنسيقًا دوليًا وتعاونًا بين مختلف الدول لمواجهة هذه الجرائم التي لا تعترف بالحدود الجغرافية.

ومن هنا تثار مشكلة الدراسة بالتساؤل الرئيس الآتي:

ما هو النظام القانوني الذي خصصه المشرع الفلسطيني لجريمة التزوير الالكتروني، ومدى إمكانية تطبيق نصوص التشريع الفلسطيني على هذه الجريمة مقارنة بالتشريعات المقارنة والاتفاقيات الدولية ؟

هناك عدة تساؤلات فرعية تنبثق من التساؤل الرئيس لهذه الدراسة وتتمثل التساؤلات الفرعية فيما يلي:

1 .هل نظم المشرع الفلسطيني جريمة التزوير الإلكتروني ؟

2 .ما هي أنماط التجريم لجريمة التزوير الإلكتروني ؟

3 .ما هي الطبيعة الخاصة التي تميز التزوير الإلكتروني ؟

4. هل يوجد شروع في جريمة التزوير الإلكتروني ؟

5.هل شدد المشرع الفلسطيني عقوبة التزوير الإلكتروني في جميع المستندات ؟

6. ما هو القصد الجنائي في عقوبة التزوير الإلكتروني ؟

7. ما هي الاتفاقيات الدولية التي جرمت التزوير الإلكتروني ؟

أهمية الدِراسة

يعد موضوع التزوير الالكتروني من المواضيع التي تتطور بشكل كبير في وقتنا الحاضر، وذلك نتيجة التطور الكبير الذي في التكنولوجيا واستخدامات الحاسوب والإنترنت وسيطرة الجانب المعلوماتي في شتى مجالات الحياة، وتكمن أهمية هذه الدراسة في كونها تسلط الضور على الجرائم المرتبطة بهذا الجانب على اعتبارها من الجرائم المستحدثة التي لم تتناولها الدراسات بشكل كبير، حيث ان مسألة التزوير الإلكتروني من المسائلة التي تزداد صعوبتها يوما بعد يوم وهي تعتبر من أخطر الجرائم المتعلقة المساس بأنظمة المعالج الآلية التي تستهدف الاشخاص الطبيعيين والمعنويين وتشكل خطر كبير على المجتمع ككل.

كما وتبين هذه الدراسة موقف المشرع الفلسطيني من هذه الجريمة وتوافقه مع غيره التشريعات وهل كانت العقوبة متناسبة مع الجريمة المرتكبة، هل منح كل جهات الاختصاص أن تنظر هذا

الجانب من الموضوع . ومعرفة ما هي البيانات التي يقع بشانها جريمة التزوير، حيث أن جرائم التزوير الإلكتروني لم تقتصر على جانب معين في الدولة بل تهدد النظام القانوني والاقتصادي والاجتماعي للدولة، تكمن أهمية الموضوع بربط الحداثة بالتقليد وذلك بالمقارنة بين جرائم التزوير الحديثة والتقليدية.

كما وتبرز أهمية هذه الدراسة في بيان الأضرار الناجمة عن هذه الجرائم الخطيرة قانونيا واقتصاديا وسياسيا واجتماعيا ، فمن الناحية القانونية تؤثر على المنظومة القانونية بإيجاد الثغرات والتناقضات المختلفة بين النصوص القانونية، ومن الناحية الاقتصادية تؤثر سلبا على الاقتصاد وتنخر في ثباته واستقراره، ومن الناحية السياسية فأثرها مدمر حيث يتسلل أصحاب النيات القذرة الى التزوير مع ما يتناسب مع مصالحهم فينجم الفساد، ومن الناحية الاجتماعية تؤثر جرائم التزوير سلبا على الطبقات الاجتماعية فتتزايد الهوة بينها ويزداد العداء بين أبناء المجتمع الواحد.

وكان لا بد من تكثيف الدراسات والأبحاث لفهم هذه الجريمة فهما علميا شاملا ومتكاملا على اعتبار أن ذلك الفهم هو المدخل الطبيعي للتوصل إلى مواجهة هذه الجرائم والتصدي لها بالفاعلية المطلوبة، وتحديد الإطار العام لها وكشف الإشكاليات التي تعترض إجراءات التحقيق فيها، تنسيق الجهود الدولية لمواجهتها من خلال ما يمكن أن تسفر عنه هذه الدراسة من نتائج وما تنتهي اليه من توصيات وما تتضمنه من حقائق ومعلومات مما يؤدي في النهاية إلى إمكانية وضع هذه الجرائم تحت السيطرة والتمكن من مواجهتها. .

تظهر أهمية الدراسة في التعرف على الإطار القانوني لجريمة التزوير الإلكترونية وتكتسي هذه الدراسة أهمية نظرية وعملية في كونها دراسة جديدة لم يتطرق لها أي باحث من قبل ومن الناحية النظرية يبرز دور هذه الدراسة في كونها تأخذ منحنى جديد من ناحية تطبيق القانون كون هذا النوع من الجرائم بدأ الاهتمام الجدي والواضح به منذ بضع سنوات من خلال النص على قرار بقانون بشأن الجرائم الإلكترونية والتي منها التزوير والنص على إنشاء نيابة متخصصة في الجرائم الإلكترونية ويكون الكتابة عن هذا القانون بمثابة التجدد والتغيير الفكري حيث يجب أن يكون هناك دراسات واضحة عن مثل هذا النوع من القوانين وهذه الجزئية بالذات تشكل نقطة تحول واختلاف للقضاة وحتى يستطيع الأشخاص المعنين من تطبيق قواعده على الفهم الصحيح لنصوص القانون.

أهداف الدِراسة

كون أن جرمية التزوير الالكتروني من أخطر الظواهر الإجرامية المستحدثة نتيجة سهولة ارتكابها وتنفيذها وسهولة محو أثارها وإتلاف أدلتها الأمر الذي يثير مشكلات كبيرة في جمع الأدلة وإثبات هذه الجرائم مما دفعنا في البحث في هذه الموضوع وذلك من أجل توضيح معالم هذه الجريمة والوقوف على الجهود المبذولة للحد من هذه الجريمة في فلسطين ويهدف الباحث في هذه الدراسة على توضيح ما يلي:

1 .توضيح ماهية جريمة التزوير الإلكترونية من وجهة نظر القانون الفلسطيني ومقارنتها مع التشريعات العربية الأخرى وذلك بالتطرق إلى تعريف هذه الجريمة وتبيان صورها وشروط إعمال نص القانون عليها وما هي الأفعال التي تعد جريمة تزوير الإلكترونية والقصد المتطلب لقيام أركان هذه الجريمة.

2 .البحث في جريمة تزوير التوقيع الإلكتروني كنوع من أنواع التزوير الواقع على المحررات الإلكترونية كونها من المواضيع المستحدثة والتي تضيف الجديد إلى الدراسات القانونية.

3. تبيان دور النصوص القانونية الموضوعية والإجرائية وكيفية تطبيقها على جريمة التزوير الإلكترونية والتعمق في دور مأموري الضبط القضائي والنيابة العامة والمحاكم في تتبع المجرم في هذا النوع من الجرائم والتعرف على فاعلية الأساليب التي يتم اتباعها في إثبات جرائم التزوير الإلكتروني.

أدوات الدِراسة

1.المصادر: القوانين الفلسطينية والقوانين المقارن .

2 .المراجع: الكتب والدراسات والمقالات والمجلات التي تناولت موضوع التزوير الإلكتروني، والأحكام القضائية الصادرة عن المحاكم الفلسطينية.

3. المقابلة (مصادر شخصية): طبيعة البحث توجب على الباحث إجراء المقابلات الشخصية مع المتعاملين بالجرائم الالكترونية خاصة بالتزوير الإلكتروني، سواء في إدارات الشرطة المتمثلة في إدارة المباحث او وحدة الجرائم الإلكترونية ومديري هذه الإدارات .

منهج الدِراسة

المنهج الوصفي : وذلك من خلال دراسة المفاهيم العامة حيث أخذ القواعد القانونية وتجسيدها بجرائم التزوير الإلكترونية وربطها بها حتى يتم تبسيط الدراسة لإيصال الأفكار المناسبة للتبسيط على من يقرأ الدراسة في فهم المطلوب منها وتوضيح تعريفات قانونية وفقهية للتزوير الإلكتروني وبيان خصائصها وأركانها، وأهم صور الجرم.

المنهج التحليلي : بشقيه (الاستقرائي والاستنباطي) في دراسة وتحليل وذلك بتوضيح وتحليل القواعد القانونية وربط الجرائم بها حتى يتم استخلاص الأسس التي تبنى عليها الدراسة من خلال تحليل آليات وإجراءات النصوص القانونية المنظمة لجريمة التزوير الالكتروني وتحليلها بشكل من التفصيل ثم بيان الاستنتاجات بشأنها ومن ثم تقديم الحلول المناسبة مما توصل إليه الفقه والتشريع والقضاء المقارن .

المنهج المقارن : من خلال بيان موقف التشريعات المقارنة من جريمة التزوير الإلكتروني وتوضيح الإجراءات التي اعتمدتها مختلف التشريعات والأنظمة في مواجهة هذه الجريمة ومحاولة سد الثغرات في النصوص القانونية والوصول إلى اقتراحات وحلول مناسبة لها في محاولة التعرف على التباين التشريعي والاجتهاد القضائي بين كل من التشريع الفلسطيني من جهة، وبعض التشريعات الجنائية المقارنَة ذات الصلة وذلك عن طريق تقسيم الدراسة إلى فصول ومباحث ومطالب تبعها ذلك خاتمة مشتملة على النتائج والتوصيات وقائمة المصادر والمراجع حسب مقتضيات الدراسة التي تستند على مصادر رئيسة تستند عليها هذه الدراسة تبعه ذلك كتابتها بصورة سليمة مستندة في ذلك إلى الأسلوب العلمي الذي يستند على تلخيص الدراسات من المراجع والمصادر وتوثيقها بصورة دقيقة عن طريق ذكر اسم الكاتب ومرجعه ودار النشر والصفحة.

محددات الدِراسة

تتمثل الصعوبات في حداثة موضوع البحث وقلة الباحثين في هذا المجال وقلة مراجعهم المتخصصة في الجانب الإجرائي لجريمة التزوير الالكتروني بالرغم من وجود مراجع بشكل كبير فيما يتعلق بالجريمة الإلكترونية غير أنه لا تتوفر مراجع كافية متعلقة بجريمة التزوير الإلكتروني وقلة وجود أحكام قضائية تتعلق بذات الموضوع.

كما أنه لا يمكن دراسة هذا الموضوع من الناحية القانونية دون التقنية مما يشكل ذلك صعوبة في البحث لعدم التخصص في المعلوماتية.

الدراسات السابقة:

1. دراسة اسامة طلحي، ومحمد الشريف بولعراس، (2022)، **بعنوان "جريمة التزوير المعلوماتية"** وقد تناولت هذه الدراسة الجوانب القانونية لجريمة التوزير المعلوماتية، وذلك من خلال بيان ماهية جريمة التزوير وأركانها والاثار الناتجة عنها، كما وبينت مدى إمكانية انطباق النصوص الجزائية لجريمة التزوير التقليدية على جريمة التزوير الإلكتروني، وبينت بعض صور جريمة التزوير الإلتكروني.
2. دراسة وفاء صدراتي، (2021)، **بعنوان" آليات مكافحة جريمة التوزير الالكتروني"** وقد ركزت هذه الدراسة على جريمة التزوير الإلكتروني ببيان مفهومها والقواعد الموضوعية لمكافحة جريمة التزوير الإلتكروني سواء على مستوى التجريم او على مستوى العقاب، كما وتناولت هذه الدراسة الآليات الإجرائية لمكافحة جريمة التزوير الإلتكروني على المستوى الداخلي والخارجي.
3. دراسة لبنى ملوك، (2020) **بعنوان" جريمة التزوير الإلكتروني"** وقد تناولت هذه الدراسة القواعد الموضوعية لجريمة التزوير الإللكتروني وذلك ببيان ماهية التزوير الإلكتروني ونصوص التجريم العامة والخاصة للتزوير الإلكتروني، كما وبينت القواعد والأحكام الأجرائية في هذه الجريمة من خلال إجراءات جمع الأدلة والاختصاص القضائي في جرائم التزوير الألكتروني.
4. دراسة رائدة باسيس، (2018)، **بعنوان " جريمة التزوير في المحررات الإلكترونية"**، وبينت هذه الدراسة المفصود بالمحررات الإلتكرونية والأسباب التي أدت الى ظهورها، كما وتناولت أركان جريمة التزوير في المحررات الإلكترونية وطرق التزوير فيها.
5. دراسة سمير بن حليمة، (2018) بعنوان **" القصد الجرمي في تزوير التوقيع الإلكتروني"** وقد تناولت هذه الدراسة القصد الجنائي كركن في جريمة التزوير الإلكتروني، وبينت كيف عالجت التشريعات العربية والغربية هذه الجريمة من خلال النصوص المختلفة، وركزت على الإطار المفاهيمي للتوقيع الإلكتروني ومسألة القصد الجنائي.
6. دراسة ياسمين بوعروة، (2014) بعنوان **" جريمة التزوير المعلوماتية"** وقد ركزت هذه الدراسة على مكافحة التزوير المعاوماتي من خلال النصوص التشريعية وتناولت مدى

صلاحية النصوص التي المنظمة لتزوير المحررات في مكافحة التزوير الإلتكروني، وقد بينت مدى مكافحة التزوير المعلوماتي من خلال النصوص المنظمة والمستحدثة في الإتفاقيات الدولية والتشريع المقارن.

7. دراسة عبد الله بن سعود محمد السراني، (2011)، بعنوان **"فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الالكتروني"**، وقد تناولت هذه الدراسة خصائص جريمة التزوير الإلكتروني والأساليب المستخدمة في إثبات جرائم التزوير الإلكتروني، وبينت صور جريمة التزوير الإلكتروني في الدوائر الحكومية، وعلى فاعلية الأساليب التي يتبعها المحقق الجنائي في إثبات جرائم التزوير الإلكتروني.

خطة الدراسة

قسم الباحث هذه الدراسة الى فصلين على النحو الاتي:

الفصل الاول: القواعد الموضوعية لمكافحة جريمة التزوير الإلكتروني.

المبحث الاول: تحديد المقصود بجريمة التزوير الإلكتروني.

المبحث الثاني: التكييف القانوني لمحل الجريمة .

الفصل الثاني: القواعد الإجرائية لمكافحة جريمة التزوير الإلكتروني .

المبحث الاول: تحديد الجهات المختصة بالملاحقة .

المبحث الثاني: بيان الاختصاص القضائي في جريمة التزوير الإلكتروني .

الفصل الأول

القواعد الموضوعية لجريمة التزوير الإلكتروني

إنَ جريمة التزوير منَ الجَرائم التي تُخل بالأمانة العامة، فقانون العقوبات جاء لحماية المصالح القانونية التي يتم الاعتداء عليها أو التي من المحتمل أن تتعرض للاعتداء، وهي حِماية ثقة الأفراد في المحررات التي منحها المشرع أهمية قانونية، وتعد في نفس الوقت أدوات لا يمكن الاستغناءِ عنها لتسيير الحياة اليومية لأفراد المجتمع، أفرد المشرع الفلسطيني قسماً كاملاً وهو القسم السابع من قانون العقوبات للحديث عن التزوير وكان بِعنوان التزوير وسك النقود وما شابه ذلك من الجرائم وهذا الفصل احتوى على ستة أفرع تناول المشرع الحديث بالتفصيل عن جريمة التزوير، وأفرد المشرع فصل للتزوير، وفصل لعقوبة التزوير.[2]

وعرفت التشريعات الفلسطينية التزوير على أنه "تنظيم مستند كاذب بنية الاحتيال أو الخداع "، وفي مشروع قانون العقوبات تم تعريفه على أنه "كل تغيير للحقيقة في محرر رسمي أو عرفي بقصد الغش بأحد الطرق التالية...."، والتشريعات المصرية لو تورد تعريف للتزوير أنما اقتصرت على بيان طرائق التزوير وتنوع المحررات، وفي التشريعات الأردنية عرف التزوير على أنه"تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط يحتج بهما نجم أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي".[3]

قسم الباحث هذا الفصل إلى مبحثين تناول في المبحث الأول ماهية جريمة التزوير الإلكتروني وفي المبحث الثاني سيتم عرض التكييف القانوني لمحل الجريمة .

---

[2] خليل ، أحمد حسن سعيد ، جريمة التزوير في التشريع الفلسطيني ، رسالة ماجستير، الجامعة الإسلامية، غزة، 2015، ص21.

[3] خليل ، أحمد حسن سعيد، **مرجع سابق**، ص19.

المبحث الأول: ماهية جريمة التزوير الإلكتروني

تعد جريمة التزوير الإلكتروني من الجرائم المستحدثة، حيث أن الوسائل التقنية كالحاسب الآلي هي الأداة المستعملة في هذه الجريمة، وهذا النوع من الجرائم ظهر نتيجة التطور التكنولوجي في مختلف المجالات حيث أنَ العالم أصبح قريةً صغيرة، ونتج عن هذا تسهيلات عديدة خاصة منها في مجال تقديم الخدمات وكل أمور الحياة إلا أنَ هذا التقدم والتطور رافقه سلبيات تتمثل في ظهور الجرائم المستحدثة التي أصبحت لا تعترف بالحدود الجغرافية، وأًحد أًهم هذه الجرائم جرائم التزوير الإلكتروني .[4]

وجرائم التزوير تتسم بمفهوم محدد يميزها عن غيرها من الجرائم الإلكترونية التي من المحتمل أن ترتكب بالطرق الإلكترونية عن طريق الحاسبات الآلية، أو شبكات الإتصالات والأنترنت أو عن طريق الوسائل والأساليب التقليدية، وهذا الموضوع بحاجة إلى تسليط الضوء على جريمة التزوير الإلكتروني من خلال تقسيم هذا المبحث إلى مطلبين نتناول في المطلب الأول الحديث عن مفهوم جريمة التزوير الإلكتروني، وفي المطلب الثاني التركيز على موقف المشرع الفلسطيني والتشريعات ذات الصلة .

المطلب الأول: مفهوم جريمة التزوير الإلكتروني

يعد التزوير الإلكتروني من الجرائم الخطيرة التي لا تقل أهميةً عن التزوير التقليدي، ويعود ذلك إلى أن التزوير الإلكتروني يمكن ارتكابه في إي وقت، ومن الصعب على المحققين الكشف عنه كونه لا يترك أي دليل مادي يدل على ارتكابه .[5]

لبحث المفهوم المرتبط بجريمة التزوير الإلكتروني يجدر بي أن أقسم هذا المطلب إلى ثلاثة فروع حيث أتناول في الفرع الأول التعريف التشريعي، واخصص الفرع الثاني لبيان رأي الفقه في جريمة التزوير الإلكتروني، وأتحدث في التعريف الدولي نظرا لمكانة الجريمة في الصعيد الدولي متطرق له في الفرع الثالث.

---

[4] الجبوري، عمر عبد السلام حسين، جريمة التزوير الالكتروني في التشريع الأردني، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، 2017، ص14.

[5] خليفة فتحية، ومهداوي محمد صالح، مجلة الدراسات القانونية ، المجلد 8، العدد2، 2022، ص257.

الفرع الأول: التعريف التشريعي لجريمة التزوير الإلكتروني

لم يتطرق قانون العقوبات لسنة 1960 لتعريف جريمة التزوير الإلكتروني؛ كون أن هذا النوع من الجرائم حديث الظهور فقد عرف جريمة التزوير بصورته التقليدية على أنه" تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط يحتج بهما نجم أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي"[6]، وقد ورد في قانون البينات الفلسطيني رقم (4) لسنة 2001 نص متعلق بتزوير وهو "1.يكون الإدعاء بتزوير السند في أية حالة يكون عليها الدعوى بطلب يقدم إلى محكمة الموضوع ويبين فيه كل مواضع التزوير المدعى بها.2.يجب على مدعي التزوير أن يعلن خصمه بمذكرة يبين فيها مواضع التزوير وإجراءات التحقيق التي يطلب إثبات التزوير فيها خلال المدة التي يحددها القاضي، وإلا جاز للقاضي الحكم بسقوط إدعائه".[7]

والتزوير التقليدي يقع على المستندات ومنها المستند الرسمي والمحررات الذي عرفته محكمة التمييز الأردنية على أنه" المحرر الذي يحرره موظف عمومي مختص بتحريره بمقتضى وظيفته أو ينسب زوراً إلى موظف مختص ويعطي شكل المحررات الرسمية الصادرة"[8] ويشترط في هذه المستندات أن تصدر من موظف عام أو مكلف بخدمة عامة وهذا الموظف يجب أن يكون مختصا وقد قام بتحرير السند ضمن اختصاصه وحدود سلطته مراعياً بذلك أحكام القانون[9]، والمحررات هي عبارة عن كل ما يدونه الأفراد بلغة مفهومة وتتضمن كلمات وحروف يقصد بها الوصول إلى معنى معين ومنها المحررات العرفية كالعقود [10].

واختلف مشروع قانون العقوبات مع القرار بقانون حيث إن القرار بقانون رقم 10 لسنة 2018 الذي يعنى بشأن الجرائم الإلكترونية لم يقم بتعريف جريمة التزوير الإلكتروني بشكل واضح وصريح، إلا أنه نص في المادة 11 منه على "1.كل من زور مستنداً إلكترونياُ رسمياً من مستندات الدولة أو الهيئات أو المؤسسات العامة معترفاً قانوناً في نظام معلوماتي، يعاقب بالسجن لمدة لا تقل عن خمس سنوات،

ويرى الباحث أن القرار بقانون بشأن الجرائم الالكترونية رقم (10) لسنة (2018) لم يشتمل على تعريفات كافية وواضحة بما يخص بعض الجرائم والمسائل كما أنه يستخدم مصطلحات فضفاضة، حيث أنه لم يضع تعريف واضح لجريمة التزوير الإلكتروني فكان من الأولى على المشرع أن يضع تعريفاً واضحاً لجريمة التزوير الإلكتروني .

---

[6] المادة 260 من قانون العقوبات رقم 16 لسنة 1960 النافذ في الأراضي الفلسطينية.
[7] انظر المادة رقم (59) من قانون البينات الفلسطيني رقم (4) لسنة 2001.
[8] نجم، محمد صبحي ، **قانون العقوبات القسم الخاص** ، الأردن ، مكتبة الثقافة للنشر والتوزيع ، 1995 ص 76.
[9] ياسر زبيدات ، شرح قانون البينات الفلسطيني (فلسطين – 2010) ص91
[10] فتيحة، عمارة (جريمةالتزوير الإلكترونية) مجلة القانون والمجتمع ، المجلد 7، العدد1، 2019 ، ص 168.

الفرع الثاني: التعريف الفقهي لجريمة التزوير الإلكتروني

تتعدد التعريفات الفقهية للتزوير فقد عرف على أنه "تغيير الحقيقة في محرر بقصد الغش بإحدى الطرق التي حددها القانون تغييراً من شأنه أن يسبب ضرراً"، وعُرف كذلك على أنه "تغيير الحقيقة بقصد الغش في محرر واقعاً على شيئ مما أعد هذا المحرر لإثباته ومن شأنه أن يسبب ضرراً "، وَعرفه الفقيه الكارسون على أنه (تغيير الحقيقة بقصد جنائي في محرر بأحدى الطرق التي بينها القانون تغييراً من شأنه أن يسبب ضرراً)، كما وعرفه الفقه المصري على أنه (تغيير الحقيقة بقصد الغش بأحدى الطرق المقررة في القانون في محرر يحميه القانون).[11]

ونَتيجة التطورات العلمية والتكنولوجية ظهر نموذج جديد من التزوير، وهو التزوير الإلكتروني حيث أن هذا النوع من التزوير تم تعريفه من قبل الفقهاء على أنه "أي تغيير في الحقيقة يرد على مخرجات الحاسب الآلي سواء تمثلت في مخرجات ورقية مطبوعة أو مرسومة أو محررات وهي ذات أثر في الإثبات حق أو واجب، وعُرفت أيضاً على أنها أي إستخدام لبرامج معالجة آلياً وبرمجيات اختراق بهدف تغيير بيانات أو معلومات بهدف الحصول على البيانات الأصلية أو العبث بها بنية استخدامها[12].

ويراد بالاستخدام هنا تغيير المعلومات الواردة على المعاملات الإلكترونية أو المستندات الإلكترونية أو وسائل الدفع الإلكترونية المستحدثة والمأخوذة من الوسائل التقليدية للدفع والتي منها الشيك الإلكتروني وهي من وسائل الدفع الأكثر انتشاراً على المستوى الدولي والعالمي فيمكن للجاني أن يقوم بتزوير أي معلومة في هذا الشيك باستخدام وسائل إلكترونية لجلب مصلحة مالية لنفسه أو لغيره وهناك نظام أخر للدفع وهو نظام تحويل الأموال بين طرفين بواسطة وسيط ثالث ونظام البطاقات الإلكترونية والعملات الرقيمة وغيرها من وسائل الدفع التي يمكن أن تكون محلاً لجريمة التزوير الإلكتروني[13].

وبهذا فإن جريمة تزوير المستندات الإلكترونية تقع على معلومات مدخلة بواسطة وسائل إلكترونية بواسطة نظام معلوماتي معين[14]، كإضافة بيانات أو تغيير توقيع أو تغيير فحوى مستند

---

[11] العارضي، فرقد عبود ، **جريمة التزوير الالكتروني**، مجلة الكوفة للعلوم السياسية والقانونية، جامعة الكوفة، العدد13، 2012، ص147.

[12] حفضي عباس ، **جرائم التزوير الإلكترونية** ، رسالة مقدمة لنيل درجة الدكتوراة في القانون ، جامعة وهران ، الجزائر ، 2015 ، ص2

[13] رضوان، رضا عبد الحكيم إسماعيل، (جرائم تزوير بطاقات الدفع الإلكترونية) مجلة البحوث الأمنية، كلية الملك فهد الأمنية ، مجلد 17 ، العدد 39 ص 200-201.

[14] عمارة، فتيحة، **مرجع سابق**، ص 172.

بشطب شرط أو عبارة مهمة بقصد العبث في أصل السند أو إخفاء معلومة من المستحيل إدراكها بالعين المجردة[15].

وعرف علي عبد القادر القهوجي التزوير الإلكتروني على أنه "تغيير للحقيقة يرد على مخرجات الحاسب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي عن طريق الطابعة أو كانت مرسومة عن طريق الراسم، ويستوي في المحرر الإلكتروني أن يكون مدوناً باللغة العربية أو أية لغة أخرى لها دلالة، وقد تتم في مخرجات ورقية شرط أو محفوظة على دعامة، وشرط أن يكون المحرر الإلكتروني ذا أثر في إثبات حق أو أثر قانوني".[16]

كما وعرف الفقه الفرنسي التزوير في المحررات على أنه :"تغيير في الحقيقة وقائع اعد المحرر لإثباتها متى كان من شأنه أن يسبب ضرراً ارتكب بقصد الغش وقصد بذلك الإضرار ".وهذا التعريف هو للأستاذ جرسون الذي درج غالبية الفقه الفرنسي والمصري على اعتماده .[17]

الفرع الثالث: التعريف الدولي لجريمة التزوير الإلكتروني

تطرقت العديد من الإتفاقيات الدولية لجريمة التزوير الإلكتروني، وكونها من الجرائم التي تعد عابرة للقارات فهي تحتاج لتعاون دولي للسيطرة عليها فهي جريمة يمكن ارتكابها على بعد آلاف الأميال ويستدعي هذا الاستعانة بالتقنيات الدولية للتعرف على الأجهزة التي تمت منها عملية التزوير واسترجاع المعلومات المحذوفة أو المستخدمة كدليل مادي لإثبات هذا التعدي[18]، حيث أن الجريمة الإلكترونية تنشأ وتبدأ في دولة ويمكن أن تنتهي أثارها في دولة أخرى بسبب ترابط شبكة المعلومات التي يمكن أن تنشأ مشكلة في موضوع الاختصاص للقواعد القانونية الموضوعية والإجرائية[19]، وهذا ما أوجب علي كباحث أن أقوم بمناقشة التعريفات الخاصة بهذه الجريمة في القوانين الدولية.

---

[15] بنيوسف، إدريس، (أساليب التزوير وكشفها عن طريق عملية الاستكتاب)، مجلة الملف، دار السلام للطباعة والنشر، العدد7 ، ص 139.

[16] الطاهر، برهوم ، **جرائم التزوير الإلكتروني**، رسالة مقدمة لنيل درجة الماجستير في القانون الجنائي، جامعة العربي التبسي، تبسة، قسم الحقوق، تبسة، 2019، ص9.

[17] علي، بلعيشة، **الحماية الجنائية للمستند الإلكتروني** ، رسالة مقدمة لنيل درجة الماجستير في القانون، العام، جامعة عبد الحميد بن باديس مستغانم ، قسم القانون العام، الجزائر ، 2019، ص46.

[18] السيراني، عبدالله بن سعود ، فاعلية الاساليب المستخدمة في اثبات جريمة التزوير، (جامعة نايف العربية للعلوم الامنية) الرياض 2011، ص 128

[19] حفصي عباس، **مرجع سابق**، ص52.

يعتبر المشرع الدولي أنَ المعلومات الورقية هي ليست فقط التي تقبل التزوير وإنما المعلومات الإلكترونية أيضاً تخضع للتزوير واستخدامها بشكل غير مشروع[20]، وهذا ما صرح به القانون الدولي في مواقع معينة حيث تطرق المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات البرازيلي لعام 1994 المتعلق بالجرائم الإلكترونية لجريمة التزوير الإلكتروني بأنه استخدام الأجهزة الإلكترونية بغير الطرق الصحيحة لمعالجة البيانات المنصوص عليها في القانون البرازيلي الوطني[21].

أما بخصوص اتفاقية عام 2001 التي تعنى بمكافحة الإجرام السيبيري أو الإجرام الافتراضي أو الكوني والمعروفة أيضاً باتفاقية (بودابيست)، فقد تضمنت في المادة رقم (7) منها على تعريف لجرائم التزوير الإلكتروني بالقول بأنه "إدخال أو إفساد أو تعطيل أو محو أو شطب عن قصد وبدون وجه حق" وبهذا فإن التزوير الإلكتروني هو استخدام أي من الطرق المذكورة في التعريف السابق عن قصد يستهدف المعلومات الإلكترونية بهدف إحداث ضرر وحددت أيضاً الطرق المستخدمة لإحداث هذا الضرر والتي بينتها على وجه الخصوص بالإدخال أو الإتلاف أو المرور ضمن نشاطات الحاسب الآلي وأي اعتداء على الحاسب الآلي بنية الغش للحصول على منفعة اقتصادية[22].

ومن الإتفاقيات التي كافحت الجرائم الإلكترونية إيضاً الإتفاقية العربية لمكافحة جرائم تقنية المعلومات عام 2010، وذلك يأتي ضمن الجهود الحثيثة التي تبذلها جامعة الدول العربية لتدعيم التدابير الأمنية لمكافحة الجرائم المتعلقة بتقنية المعلومات في ضوء الأسس النظامية والبيئة القانونية[23]، ونصت هذا الإتفاقية على التزوير في المادة العاشرة فنصت على "استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييراً من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة ".[24]ومما تجدر الإشارة إليه أن فلسطين قامت بالانضمام إلى هذه الإتفاقية، فصادقت على الإتفاقية بتاريخ 2010\12\21، وتمت المصادقة على هذه الإتفاقية بتاريخ 2013\5\21.

---

[20] العفيفي، يوسف خليل، ، **الجرائم الالكترونية في التشريع الفلسطيني** ، رسالة مقدمة لنيل درجة الماجستير في القانون العام، الجامعة الاسلامية ، قسم القانون العام، غزة ، 2013 ص82.

[21] حفصي عباس، **مرجع سابق**، ص18.

[22] عمر عبدالسلام الجبوري، **مرجع سابق**، ص94.

[23] المطيري، خالد ظاهر عبد الله جابر السهيل، (مواجهة الجرائم المعلوماتية في ضوء التشريعات الجنائية المعاصرة والاتفاقيات الدولية)، بحث منشور.

[24] انظر المادة(10) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

ومن الدول التي اعتنت بجريمة التزوير الإلكتروني هي فرنسا فقد عرفت في المادة 1/441 من قانون العقوبات الفرنسي جريمة التزوير الإلكتروني على أن" التزوير هو تغيير تدليسي للحقيقة بأي وسيلة أو وثيقة أو أي وعاء أخر للتعبير عن الفكر يكون الغرض منه أو كنتيجة له شأن في إثبات حق أو واقعة لها آثار قانونية ويكون من طبيعة هذا الفعل إحداث ضرر" وإن هذا التعريف الوارد قد شمل كافة أنواع التزوير سواءً التزوير التقليدي أو التزوير الإلكتروني[25].

أما الدول العربية كدولة مصر مثلاً فقد نصت في قانون التوقيع الإلكتروني في المادة 23 منه على أنه يعاقب بعقوبات جزائية متمثلة في الحبس والغرامة كل من " 1. أتلف أو عيب توقيعاً أو وسيطاً أو محرراً إلكترونياَ، أو زور شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق أخر2. استعمل توقيعاً أو وسيطاً أو محرراً إلكترونياً معيباً أو مزوراً مع علمه بذلك" وقد تم النص على هذا التعريف ونص على التجريم على هذه الجريمة كون أن المشرع المصري قد منح الثقة للمستندات والتعاملات الإلكترونية[26].

وقد أفرد المشرع الجزائري فصلاً كاملاً في قانون العقوبات وهو الفصل السابع لتحديد جرائم التزوير وتبيان عقوباتها وهي من المادة 197 وحتى المادة 253 منه وقد أعطى لجرائم التزوير الإلكتروني حقها من الأحكام[27]، وبين كيف يتم التزوير الإلكتروني وذلك بإزالة كلمة أو رقم أو رمز أو إضافتها لتغيير مضمون مستند واعتبرها من أهم الطرق المستخدمة في التزوير المادة والتي نص على عقوبات عليها[28].

وقد عرف قانون التزوير والتزييف في المملكة المتحدة والخاص بالمحررات لعام 1981 السند والمحرر القابل للتزوير وذلك بأنه" كل أسطوانة أو شريط ممغنطة أو شريط صوتي أو أي جهاز أخر سجل فيه أو عليه معلومات أو حفظت بوسائل ميكانيكية أو إلكترونية أو بوسائل أخرى" [29].

أما المشرع الأردني فقد نص في قانون الجرائم الإلكترونية رقم 27 لسنة 2015 على جريمة التزوير في المادة رقم (4) منه بالقول " كل من أدخل أو نشر أو استخدم قصدا برنامجا عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات إلغاء أو حذف أو اضافة أو تدمير أو إفشاء

---

25 عبد العال، أسامة حسين محيي الدين (جريمة تزوير المستند الإلكتروني) ، مجلة العلوم القانونية والإقتصادية، موقع دار المنظومة ، المجلد 64 العدد 1. ص50

26 عمر عبدالسلام الجبوري، مرجع سابق، ص33.

27 حفصي عباس، **مرجع سابق**، 2014، ص أ.

28 راندة باديس، **جريمة التزوير في المحررات الإلكترونية**، رسالة مقدمة لنيل درجة الماجستير في القانون العام، جامعة العربي بن مهيدي ، قسم القانون العام ، الجزائر 2017 ص 47.

29 العارضي، فرقد عبود عواد (جريمة التزوير الإلكتروني دراسة مقارنة) ، مجلة الكوفة للعلوم القانونية والسياسية ، موقع دار المنظومة، المجلد 5 العدد ، 13ص169.

أو إتلاف أو حجب أو تعديل أو تغيير أونقل أو نسخ أوالتقاط او تمكين الأخرين من الاطلاع على بيانات او معلومات او اعاقة او تشويش او ايقاف او تعطيل عمل نظام معلومات او الوصول إليه او تغيير موقع الكتروني او الغائه او إتلافه أو تعديل محتوياته أو أشغاله أو انتحال صفة أو انتحال شخصية مالكه دون تصريح" وتبعاً لهذا التعريف فقد كان للمشرع الأردني نظرة أوسع في تعريف جريمة التزوير الإلكتروني[30].

يرى الباحث أنه يجب على المشرع الفلسطيني في قانون العقوبات تعديل نصوصه لتشمل على التزوير الإلكتروني وتوضيح أحكامه، كما هو الحال في بعض الدول الغربية كفرنسا التي نصت عليه في المادة 441\1 من قانون العقوبات الفرنسي.

المطلب الثاني: خصائص جريمة التزوير الإلكتروني

نتيجة التطورات العلمية والتكنولوجية التي حصلت في الآونة الأخيرة التي أدت إلى ظهور العديد من الجرائم المستحدثة وخاصة الجرائم الإلكترونية، وأحدى هذه الجرائم التزوير الإلكتروني الذي أصبح جريمة شائعة في الوقت الحاضر، [31]يعد التزوير الإلكتروني من الجرائم الخطيرة التي تمس الحياة الشخصية للأفراد، وهذه الجريمة تتميز بعدد من الخصائص، ومن هذه الخصائص ما يلي .

---

[30] عمر عبدالسلام الجبوري، مرجع سابق، ص37.

[31] عزيزة، رابحي ، الأسرار المعلوماتية وحمايتها الجزائية، رسالة مقدمة لنيل درجة الدكتوراة في القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، 2018، ص93.

الفرع الأول: إمكانية ان تكون جرائم عابرة للحدود

تتمتع جرائم التزوير الإلكتروني بخصائص دولية، نتيجة ارتكابها بواسطة شبكة الإنترنت الذي يتيح لدول العالم التواصل بشكل دائم ومستمر، ولا تعترف هذه الجرائم بالحدود الدولية وهي شكل جديد من أشكال الجرائم العابرة للحدود بين الدول ، حيث يمكن ارتكاب العديد من الجرائم ومن بينها التزوير الإلكتروني بواسطة أنظمة المعلومات .[32]

يمكن للمجرمين ارتكاب جرائمهم في دولة وهم موجودون في دولة أخرى وذلك نتيجة الروابط الإلكترونية غير المرتبطة بالحدود، فجرائم التزوير الإلكتروني جرائم عابرة للحدود الجغرافية للدول [33]حيث يعمل الإنترنت على تقليص المسافات، وهذا النوع من الجرائم غير مقتصر على الحدود المحلية أو الإقليمية أنما يمتد للعالمية وترتكب جرائم التزوير الإلكتروني من قبل أصحابها وهم متواجدون في دولة أخرى ذلك يعني عدم التواجد المادي للجرم المعلوماتي في مكان الجريمة، وجرائم التزوير الإلكتروني من الممكن أن يتعدى ارتكابها أكثر من دولة وذلك يثير إشكالية في أي قانون واجب التطبيق عليها.[34]

ومن القضايا التي أكدت على هذه الخاصية، قضية معروفة باسم نقص المناعة المكتسبة إيدز، وتتخلص وقائعها عام 1989، حيث قام أحد الأشخاص ويدعى جوزيف بيب بنسخ أحد البرامج بهدف أعطاء بعض النصائح الخاصة بمرض الإيدز، لكن في الحقيقة هذا البرنامج يحتوي على فايروس يؤدي إلى تعطيل جهاز الحاسب الآلي عن العمل فيقوم الجاني أو الفاعل بطلب مبلغ مالي للحصول على عنوان إلكتروني مضاد للفيروس، وفي الثالث من فبراير تم إلقاء القبض على الجاني في أوهايو في أمريكا وطلبت المملكة المتحدة تسليم الجاني لإرسال البرامج على أراضيها، وبالفعل تمت محاكمته أمام القضاء الانكليزي، إلا أن إجراءات محاكمته لم تستمر بسبب حالته العقلية.[35]

ويرى الباحث أن هذه الخاصية من خصائص جريمة التزوير الإلكترونية هي من أبرز السمات التي تجعل الجريمة عالمية وهذا يشكل صعوبة في الاختصاص القضائي كونها عابرة للحدود، لذلك لا بد من إيجاد حل لهذه الإشكالية .

---

[32] فريحة ، حسين، (الجرائم الالكترونية والانترنت)، مجلة المعلوماتية، موقع دار المنظومة، العددالسادس والثلاثون، المجلد36، 2011، ص3.

[33]أسامة الطلحي مرجع سابق، ص16.

[34] فريحة، حسين، مرجع سابق، ص2.

[35] رحيمة، نمديلي، ، 25\مارس\2017، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة ، مركز جيل البحث العلمي.

الفرع الثاني: جريمة تقنية خاصة

تتميز جرائم التزوير الإلكتروني بأنها جرائم تقنية أي أنها ترتكب من خلال شبكة الأنترنت وأجهزة الحاسب الآلي، تعد هذه الجريمة من الجرائم المستجدة التي لها أبعاد خطيرة في ظل العولمة، فهي من الجرائم المستحدثة التي يتم ارتكابها عن طريق الحاسب الآلي، حيث أن التطور في الفترة الماضية جعل التكنولوجيا شيء أساسي في مختلف مناحي الحياة وجعل من العالم قرية صغيرة، ولهذا التقدم أبعاده السيئة على أمن الدولة، حيث أن التقدم التكنولوجي تجاوز أجهزة الدولة الرقابية وبالتالي أصبح يشكل خطراً وتهديداً على أمن الدولة ويشكل عائقاً في تطبيق قوانين الدولة[36].

يدخل في مجال المعالجة الإلكترونية للبيانات أيضاً ارتكاب جرائم التزوير الإلكتروني من قبل الأفراد، سواء من حيث جمع البيانات أو، تجهيزها، أو تهيئتها لإدخالها على جهاز الحاسب الآلي بهدف الحصول على المعلومات التي يرغب في تزويرها أو تعديلها، ويدخل مرتكب الجريمة في مجال المعالجة الإلكترونية للكلمات والنصوص بواسطة استخدام طرق اوتاميتكية تمكن مستخدم الحاسب الآلي من كتابة الوثائق المطلوبة أو تغيير المحتوى بدقة عالية، وذلك بواسطة استخدام الأدوات التي تحت يده، وبفضل الحاسب الآلي وأمكانياته في التعديل والتصحيح والتخزين والطباعة والاسترجاع، وجميع الأفعال المادية التي لها صلة بإرتكاب جرائم التزوير الالكتروني.[37]

الفرع الثالث: جرائم معقدة الكشف والإثبات

تتميز الجرائم الإلكترونية بشكل عام وجرائم التزوير الإلكتروني بذات بعد وجود أثر مادي لها كما هو الحال بالنسبة لجرائم التزوير التقليدي حيث تظهر آثاره بالقشط أو الإضافة أو تغيير الخط أو إستخدام أدوات كيمائية على سبيل المثال، على العكس من التزوير الإلكتروني حيث أن المجرم يتعامل مع أنظمة إلكترونية ومعلومات ولا تظهر آثار لها في هذه الحالة، فجرائم التزوير الالكتروني عي عبارة عن جرائم فنية ملموسة.[38]

وتتسم هذه الجرائم بأنها خفية، وحتى أثناء وجود المجني عليه على شبكة لا يستطيع كشف أن هناك جريمة تزوير قد تمت إلا بعد مدة من إرتكابها ويمكن أن يكتشفها عن طريق الصدفة، وهي

---

[36] ابراهيم ، خالد ممدوح ، فن التحقيق في الجرائم الالكترونية، دار الفكر الجامعي، 2009، ص. 86

[37] عباس، حفصي، مرجع سابق، ص54.

[38] أسامة الطلحي، مرجع سابق، ص17.

تعد خفية لأن المجرم يتعامل مع نبضات الكترونية غير مرئية، وعلم الجاني ومعرفته الفنية في مجال المعلوماتية يضعف من قدرة المجني عليه على إرتكاب الجريمة لأنه يلجأ إلى استخدام طرق وأساليب لا ينتبه إليها المستخدم العادي .[39]

وصعوبة الإثبات في الجرائم الالكترونية يعود إلى عدة عوامل نوضحها:

1.صعوبة الاحتفاظ بدليل الجريمة الإلكترونية، حيث أن المجرمين يستطعيوا تغيير المعلومات المتواجدة على أجهزة الحاسب الآلي وتحريفها، كما يمحو أثر هذه الجريمة في أقل من ثانية.

2.تعتمد الجرائم الإلكترونية على الذكاء والخداع في التعرف على مرتكبيها، وذلك يؤدي إلى صعوبة التعرف على مرتكبي الجريمة كون الشركات والمؤسسات والبنوك لا تفصح وتبلغ السلطات المختصة عن وقوع جريمة لديها من هذا النوع حتى لا تخسر ثقة العملاء وتهتز سمعتها، وهذا النوع من الجرائم يعتمد على خبرات عالية ومعرفة بنظم المعلومات فهي جريمة فردية، وجرائم التزوير الإلكتروني تقع أثناء معالجة المعطيات والبيانات وإذا انتفى هذا الشرط لا تقع الجريمة، ومجلس الشيوخ في فرنسا حاول وضع تعريف محدد لعملية المعالجة الآلية للمعطيات والبيانات، لكنه إنحاز عنه كون أن هذه الجريمة عملية فنية تخضع لتطور السريع .

3.تقع هذه الجرائم في أوساط إلكترونية، بالتي لا يترتب عليها أي آثار مادية، فهذه الجريمة إلكترونية لا توجد بها مستندات ورقية ولا شهود يمكن استجوابهم والتحقيق معهم .

4.الجرائم التي تقع على الانترنت تحتاج لخبرة فنية كما ذكرنا سابقاً، فهي تحتاج إلى كم واسع من المعلومات لارتكابها أو التحقيق فيها، وهناك صعوبة في التعامل مع الدليل الإلكتروني فبدون قصد يتسبب المحقق في إتلاف الدليل الإلكتروني أو تدميره في حالة محو البيانات المتواجدة على الإسطوانة الصلبة، فمن المهم في وقتنا الحاضر لرجال الضابطة القضائية تلقي دورات تدريبية لمكافحة الجرائم الإلكترونية والتغلب عليها .[40]

ويرى الباحث أن خصائص جريمة التزوير الإلكتروني جعل منها جريمة موضوع النظر في الوقت الحالي خاصة أنها جريمة ذات طابع دولي وتتصف بالعالمية فهذه الخاصية هي بمثابة ظرف مكاني متعلق بالجريمة وهي من أشد خصائص التزوير الإلكتروني خطورة كونها تؤدي إلى عدم معرفة القانون الواجب التطبيق عليها نتيجة ارتكابها من خلال العديد من الدول.

---

[39] عزيزة ، الرابحي، مرجع سابق، ص95.

[40] فريجة، حسين، مرجع سابق، ص3.

المبحث الثاني: التكييف القانوني لمحل الجريمة

ظهرت أنواع جديدة من الجرائم في الآونة الأخيرة نتيجة التطور التكنولوجي الحاصل، حيث أصبحت ترتكت الجرائم من خلال وسائل إلكترونية متطورة في بيئات إلكترونية، من الصعب الوقوف على طبيعتها، والدليل على إرتكابها يكمن في الطابع الإلكتروني، وغير ذلك من سرعة إرتكاب الجرائم، [41] ضمن هذه الجرائم تزوير التوقيع الإلكتروني، وتزوير المستندات أو المحررات الإلكترونية، فكان من المهم الحديث عن هذه الجرائم وتوضيح محلها في المطلب الأول، وتحديد أركانها في المطلب الثاني.

المطلب الأول: تحديد محل جريمة التزوير الإلكتروني

أن محل الجريمة في جرائم التزوير الإلكتروني من الممكن أن يقع على التوقيع الإلكتروني، أو المستندات الإلكترونية، وسنتعرف في هذا المطلب على هذه الجرائم في الفرع الأول نتناول (تزوير المستندات الإلكترونية)، وفي الفرع الثاني نتناول (تزوير التوقيع الإلكتروني).

الفرع الأول: المستند الإلكتروني

المستندات الإلكترونية حلت محل المستندات الورقية في أغلب المعاملات التجارية، والمساس بمحتوى هذه المستندات يؤدي إلى وقوع المتعاقدين في عيب من عيوب الإرادة، وجريمة التزوير الإلكتروني على المحررات والمستندات، حيث أن وجود المحررات هو شرط لقيام جريمة التزوير ويعرف المحرر على أنه "كل وثيقة تتضمن بيانات مكتوبة أو مطبوعة أو مصورة "، كما اتجه رأي إلى أنه "كل مكتوب، أو كل دعامة أخرى للفكر ولكنه يجب أن يكون ذا قيمة"، وذهب آخرون إلى أنه كل مكتوب بخط اليد"، بينما المستند الإلكتروني هو كل مسطور يتضمن علامات ينتقل بها الفكر من شخص إلى آخر لدى النظر إليها، وهذه قد تكون مركبة من حروف أو علامات اصطلاحية متفق عليها وأن لم تكن من نوع الحروف المعروفة "، كما أتجه جانب من الفقه إلى أن المستند الإلكتروني هو عبارة عن معلومات تم إنشاؤها أو إرسالها أو تخزينها أو استلامها بوسيلة إلكترونية أو ضوئية أو رقمية أو صوتية ما دامت تتضمن إثبات واقعة أو تصرف قانوني محدد وتتضمن توقيع إلكتروني ينسب هذه الواقعة أو التصرف لشخص محدد.[42]

---

[41] ، عباس، حفصي، مرجع سابق، ص86.
[42] المغربي، طه عثمان، مرجع سابق، ص442.

وعرفت المادة (1) من القرار بقانون رقم(10) بشأن الجرائم الإلكترونية لسنة (2018) المستندات الإلكترونية على أنها"السجل الإلكتروني الذي يصدر باستخدام أحدى وسائل تكنولوجيا المعلومات، يتم أنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة تكنولوجيا المعلومات على وسط مادي أو على وسيط إلكتروني آخر، ويكون قابل للاسترجاع بشكل يمكن فهمه".[43]

وعرفته إيضاً المادة(2) من قانون الأنسترال النموذجي بشأن التجارة الإلكترونية "هي معلومات يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة.والمستندات الإلكترونية تتمتع بأهمية نتيجة التطورات التكنولوجية التي حصلت فأصبح اللجوء إلى المستندات الورقية كوسيلة مادية لتجسيد المعلومة وإرسالها أصبح يقل في السنوات الأخيرة حيث تم استبدالها بمستندات جديدة وحديثة تتناسب مع التطورات التي حصلت، وتتميز بطبيعتها اللامادية وبخذف الطابع المادي للوثيقة وتمكين الأطراف المتخاطبة من تبادل المعلومات عن بعد دون تجسيمها في كتابة خطية، والكتابة التي يحرر بها المستندات الإلكترونية تكون على شكل معادلات خوارزمية تنفذ عن طريق عمليات إدخال البيانات وإخراجها عن طريق شاشة الحاسوب، ونظراً لأهمية المستندات الإلكترونية التي تتبين من خلال تماثله مع المستند الورقي توقيعا وكتابة فالمستندات الالكترونية تلعب دور في التجارة الدولية وتسهل تحقيقها لإهدافها .[44]

ونص القرار بقانون على تزوير المستندات الإلكترونية في المادة (11) من القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الإلكترونية حيث نصت على "كل من زور مستنداً إلكترونياً رسمياً من مستندات الدولة أو الهيئة أو المؤسسات معترفاً به قانوناً....."[45].

والتزوير في المستندات الإلكترونية لا يقل خطورة عن التزوير في المستند الورقي، ويتبين ذلك من خلال عدة جوانب، نوضحها:1.المستندات الإلكترونية حلت محل المستند الورقي في أغلب المعاملات، والمساس بضمون المستندات هذه يؤدي إلى وقوع المتعاقد في عيوب الإرادة كالغلط والتدليس، وذلك يقود حتماً إلى الكثير من المشاكل، وهذا يشكل تهديدا لاستقرار المعاملات التجارية الإلكترونية.2.أن التعامل بالمستندات الإلكترونية والاعتماد على الطبع الورقي لأصل المستندات الإلكترونية بقود إلى نتيجة مهمة، مضمونها أن المساس بمضمون المستندات

---

[43] أنظر المادة(1) من القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية.

[44] بنعومر، زينب، جريمة تزوير المستندات الإلكترونية ، بحث منشور، المعهد العالي للقضاء، المملكة المغربية، 2009-2011، ص22.

[45] أنظر المادة(11) من القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الإلكترونية .

الإلكترونية يترتب عليه المساس بالصورة الورقية طبق الإصل.3.رغبة المنظمين في حماية الثقة المفترضة في المحرر كوسيلة لتمثيل البيانات والمعلومات التي يحتوي عليها، وخصوصاً إذا كانت قد صدرت عن جهات رسمية، وثقة الجمهور في مجال التجارة الإلكترونية هي تلك التي يضعها المجتمع في المظاهر الضرورية لاستقرار التعاملات.[46]

الفرع الثاني: التوقيع الإلكتروني

نتيجة التطورات التي حصلت على عناصر العقد وطريقة إبرامه بطريقة إلكترونية عبر الانترنت، أصبح التوقيع التقليدي هو ليس الطريقة الوحيدة المتبعة في توثيق المحررات، بل تم استحداث طريقة أخرى تتمثل في التوقيع الإلكتروني، ونتيجة الاهتمامات الدولية بالتوقيع الإلكتروني اتجهت العديد من الدول إلى تعريفه، فعرفته المادة 2\أ من قانون الأمم المتحدة النموذجي بشأن التوقيعات الإلكترونية لسنة 2001 على أنه "بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقياً، ويجوز أن تستخدم لتعيين هوية الموقع بالنسبة لرسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات ".وتم تعريفها في المادة 2\1 من التوجيه الأوروبي بشأن التوقيعات الإلكترونية رقم 93 لسنة 1999 الصادر في 13 ديسمبر عام 1999 على أنه "بيان على شكل إلكتروني يرتبط أو يتصل منطقياً ببيانات إلكترونية أخرى ويستخدم كوسيلة لتمييز الشخص وتحديد هويته ".[47]

كما وعرفه القانون العراقي في المادة رقم 1من قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم 78 لسنة 2012 على أنه"علامة شخصية تتخذ شكل حروف أو أصوات أو رموز أو إشارات أو أرقام أو غيرها وله طابع متفرد يدل على نسبته إلى الواقع ويكون معتمدا من جهة التصديق".[48]

وتم تعريفه في المادة (1) من القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الإلكترونية الفلسطيني على أنه "بيانات إلكترونية مضافة أو ملحقة أو مرتبطة بمعاملة إلكترونية، ولها طابع يسمح بتحديد هوية الشخص الذي وقعها، ويميزه عن غيره بغرض الموافقة على مضمون المعاملة".[49]

---

[46] المغربي، طه عثمان، مرجع سابق، ص435.
[47] الفقى، عبد الحليم فؤاد، جريمة التزوير الإلكتروني، جلة كلية الشريعة والقانون، بتفهنا الأشراف، 2017، ص3726.
[48] انظر المادة((1) من قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي رقم (78) لسنة 2012.
[49] انظر المادة(1) من القرار بقانون رقم(10) لسنة 2018 بشأن الجرائم الإلكترونية .

وعرفه قرار بقانون رقم(15) لسنة (2017)بشأن المعاملات الإلكترونية في المادة (1) على أنه "مجموعة بيانات إلكترونية، سواء كانت حروف أو أرقام أو رموز أو أي شكل آخر مشابه، مرتبطة بمعاملة إلكترونية بشكل يسمح بتحديد هوية الشخص الذي وقعها وتميزه عن غيره بغرض الموافقة على مضمون المعاملة الإلكترونية".[50]

وعرفه جانب من الفقهاء على أنه "مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته"، أو هو كل توقيع يتم بطريقة غير تقليدية ويتم بطريقة إلكترونية، وعبارة عن مجموعة من الأرقام التي تنجم من عملية حسابية مفتوحة باستخدام الكود السري الخاص".[51]

وذهب التشريعات المصرية إلى تعريفه على أنه"ما يوضع على محرر إلكتروني ويتخذ شكل حروف وأرقام أو إشارات أو رموز أو غيرها ويكون له طابع منفرد يسمح بتحديد هوية الموقع ويميزه عن غيره".[52]

ويرى الباحث بعد التطرق إلى تعريف التوقيع الإلكتروني في التشريعات المقارنة أن هذه التشريعات أعطت حجيه للتوقيع الإلكتروني نتيجة الإهمية التي يتمتع بها في مجال الإثبات حيث يلعب دورا هام في عملية الإثبات، ولم تميز هذه التشريعات بين التوقيعات التقليدية والتوقيعات الإلكترونية .

وهناك عدة صور للتوقيع الإلكتروني، والفقه أجمع على ثلاث طرق وهي التوقيع البسيط، والتوقيع الرقمي، والتوقيع المؤمن نوضحها فيما يلي:

-التوقيع البسيط: وله صور متعددة، إلا أنها تتفق جميعاً في أن التكنولوجيا المستخدمة في إنشائها أي وسيلة من شأنها تأمين ذلك التوقيع المنشأ، وحمايته من التلاعب فيه وهذا يثير نوعاً من عدم الثقة يؤدي إلى الشك في نسبة ذلك التوقيع إلى صاحبه، والتوقيع الإلكتروني تأمينه يتحدد بموجب عدة عوامل منها قوة الاتصال بين منظومة إنشاء التوقيع، والوثيقة التي سيتم توقيعها، والمقدرة على حماية الوثيقة من التلاعب .[53]

---

[50] أنظر المادة(1) من القرار بقانون رقم(15) لسنة (2017) بشأن المعاملات الإلكترونية.

[51] الفقي عبد الحليم، مرجع سابق، ص3728.

[52] الغالبي، رامي أحمد كاظم، جريمة تزوير التوقيع الالكتروني، بحث منشور.

[53] مشري، راضية، جريمة تزوير التوقيع الإلكتروني، حوليات جامعة قالمة للعلوم الإجتماعية والإنسانية، العدد20، جوان، 2017، ص126.

-التوقيع الإلكتروني المؤمن :ويختلف التوقيع هذا عن التوقيع البسيط في أن الأول يستخدم تكنولوجيا مصممة ليحقق ترابط أكبر بين هوية الموقع وتوقيعه الثاني، ويضيف على التوقيع نوعاً من الثقة والتصديق بالتالي يعطيه قدرة أكبر على الإثبات .

-التوقيع الرقمي :وهذا النوع يعتمد على التشفير الذي يؤكد صحة البيانات، ويهدف التشفير إلى تحويل الرسائل إلى أشكال غير مفهومة والتوقيع الرقمي يستخدم في ما يعرف باسم التشفير والترميز بالمفتاح العمومي الذي يستعمل في إنشاء مفتاحين مختلفين لكن مترابطان رياضياً .[54]

وأقرت العديد من التشريعات القانونية الحماية الجزائية للتوقيع الإلكتروني من التزوير، فالمشرع المصري نص في قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 للحماية القانونية، حيث نصت المادة 23\ب"كل من أتلف أو عيب توقيعاً أو وسيطاً أو محرراً إلكترونياً أو زور شيئاً بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر".جمع المشرع المصري عدة أنماط للسلوك الإجرامي التي تمس التوقيع الإلكتروني بالإضافة لتزوير في نص واحد، مثل الأتلاف والتغيير والتعديل والتحوير.[55]

بينما التشريع الإماراتي أقر الحماية الجنائية للمستندات الإلكترونية في قانون المعاملات والتجارة الإلكترونية رقم (1) لسنة 2006، وخصص الفصل التاسع منه للحديث عن العقوبات التي تقع على جريمة تزوير التوقيع الإلكتروني [56]، بينما المشرع الفلسطيني نص على تجريم التزوير الإلكتروني في القرار بقانون الخاص بالجرائم الإلكترونية رقم (10) لسنة 2018 حيث نصت المادة 11\4"كل من زور أو تلاعب بتوقيع أو أداة أو أنظمة توقيع إلكترونية رسمية، سواء تم ذلك باصطناعه أو إتلافه أو تعييبه أو تعديله أو تحويره، أو بأي طريقة أخرى تؤدي إلى تغيير الحقيقة في بياناته أو معلوماته ".فنصت المادة على عدة طرق للسلوك الأجرامي منها التحوير والتعييب والتعديل .[57]

ويرى الباحث أن التشريعات العربية تشابهت في إقرار الحماية الجزائية للتوقيعات الإلكترونية حيث نصت في أغلب نصوص موادها على تجريم المساس بالتوقيعات الإلكترونية وقامت بتحديد طرق السلوك الإجرامي التي تتمثل في التعديل وتحوير والتعييب والإتلاف.

---

[54] مشتري، راضية، مرجع سابق، ص127.
[55] طلحي، أسامة، مرجع سابق، ص67.
[56] طلحي، أسامة مرجع سابق، ص68.
[57] أنظر المادة(11) من القرار بقانون رقم (10) لسنة (2018) بشأن الجرائم الإلكترونية .

المطلب الثاني: أنماط تجريم التزوير الإلكتروني

منذ منتصف القرن العشرين شهد العالم ثورة تكنولوجية ومعلوماتية كبيرة تعتمد على الحاسبات الآلية، واستخدمت التكنولوجيا في مناح هامة وخطيرة، فنطاقها إتسع ليعم مختلف المناحي وهذا التطور يلمس الإدارة العامة لتتحول ملامحها من بيئة ورقية إلى بيئة إلكترونية وذلك لتوفير الوقت والجهد والكلفة، والتقليل من التضخم الورقي، وتطوير أداء الخدمة، لكنه في ذات الوقت يحمل معه خطورة الاعتداء على هذا النوع من المحركات التي باتت تشكل جسماً كبيراً يهدد الثورة على مستوى دولي وعدم الاقتصار على المستوى المحلي فقط ولا سيما في ظل التطور المتزايد للمعلوماتية، وصاحب هذا التطور الغش المعلوماتي، ومن أبرز صوره التزوير في المحررات الإلكترونية، وجريمة التزوير في الإلكتروني تختلف وفقاً لمحل الجريمة، وقت ارتكابها نوضح ذلك في الفروع التالية.

الفرع الأول: أنماط التزوير الإلكتروني وفقاً لمحل الجريمة

أن أنماط جريمة التزوير ترد على ثلاثة أنواع، تتمثل في المحررات الرسمية، والمحررات العرفية، ويرد إيضاً على الوثائق الإدارية نوضح هذه الأنواع فيما يأتي :

-المحررات الرسمية:وتعرف المحررات الرسمية على أنها كل محرر يصدر أو من شأنه أن يصدر من موظف ومن يشبهه مختص بمقتضى وظيفته بتحريره وإعطائه الصفة الرسمية أو يتدخل في تحريره أو التأشير عليه، وفق ما تقتضيه القوانين واللوائح التنظيمية التي تصدر إليه من جهته الرئيسة.[58]

وعرف الفقه المحررات الرسمية على أنها هي تلك المحررات التي يقيد فيها الضابط العمومي كالموثقين والمحضرين والقضائيين ومحافظي البيع بالمزاد العلني وكل التصرفات أو العقود ويجري فيها لتختلف الإثباتات، على سبيل المثال التبليغ الذي يعد من المحضر القضائي.[59]

وعرف قانون البينات السندات الرسمية في المادة (9) على أنها"هي السندات التي ينظمها الموظفون العموميون ومن في حكمهم اللذين من اختصاصهم تنظيمها طبقاً للأوضاع القانونية، أما

[58] صدراتي، وفاء، مرجع سابق، ص96.
[59] صدراتي، وفاء، مرجع سابق، ص98.

السندات التي ينظمها أصحابها ويصدقها الموظفون العموميون ومن في حكمهم اللذين من اختصاصهم تصديقها طبقاً للقانون فتعتبر رسمية من حيث التاريخ والتوقيع فقط".[60]

نص المشرع المصري في قانون العقوبات المصري في المادة (211) على أن "كل صاحب وظيفة عمومية ارتكب اثناء تأدية وظيفته تزويراً في أحكام صادرة أو تقارير أو محاضر أو وثائق أو سجلات أو دفاتر أو غيرها من السندات والأوراق الأميرية سواء كان ذلك بوضع الإمضاءات أو بزيادة كلمات أو بوضع كلمات أو صور أشخاص آخرين مزورة يعاقب بالأشغال الشاقة المؤقتة أو بالسجن "، وكذلك نصت المادة 213 على أن "يعاقب بالأشغال الشاقة المؤقتة أو السجن كل موظف في مصلحة عمومية أو محكمة غير بقصد التزوير موضوع السندات وأحوالها في حال تحريرها المختص بوظيفته سواء كان ذلك تغيير إقرار أولي الشأن الذي كان الغرض من تحرير تلك المستندات إدراجه بها أو بجعله واقعة مزورة في صورة واقعة صحيحة مع علمه بتزويرها أو بجعله واقعة غير معترف بها في صورة واقعة معترف بها".[61]

ونص القرار بقانون بشأن الجرائم الإلكترونية على هذا النوع من التزوير في المادة(11) حيث نصت على "كل من زور سنداً رسمياً إلكترونياً من مستندات الدولة أو الهيئات أو المؤسسات العامة معترفاً به قانوناً في نظام معلوماتي، يعاقب بالسجن مدة لا تقل على خمس سنوات، وبغرامة لا تقل على ثلاث ألاف دينار أردني .....".[62]

ونص القرار بقانون بشأن الجرائم الإلكترونية على هذا النوع من التزوير في المادة(11) حيث نصت على "كل من زور سنداً رسمياً إلكترونياً من مستندات الدولة أو الهيئات أو المؤسسات العامة معترفاً به قانوناً في نظام معلوماتي، يعاقب بالسجن مدة لا تقل على خمس سنوات، وبغرامة لا تقل على ثلاث ألاف دينار أردني .....".[63]

يرى الباحث أن التشريعات الفلسطينية أقرت الحماية الجزائية للمستندات ومنحتها حجية في الإثبات، وذلك من خلال تناولها في نصوص موادها وتجريم أي إعتداء يقع عليها .

والمحررات الرسمية يجب أن تتوافر فيها عدة شروط، وهما الصفة والاختصاص والشكل، وبالإضافة إلى ذلك يجب أن يصدر المحرر عن الدولة أو أحد الأشخاص المعنوية، وأن يتم تدوينه طبقاً للأوضاع والإجراءات القانونية، الدولة تستعين بمجموعة من الأشخاص ليؤدوا بعض المهام

---

[60] انظر المادة(9) من قانون البينات في المواد المدنية والتجارية رقم(4) لسنة(2001).
[61] عثمان المغربي، مرجع سابق، ص432.
[62] أنظر المادة(11) من القرار بقانون رقم(10) لسنة(2018) بشأن الجرائم الإلكترونية.
[63] أنظر المادة(11) من القرار بقانون رقم(10) لسنة(2018) بشأن الجرائم الإلكترونية.

الموكلة بها، وهؤلاء الأشخاص هم الموظفون العموميون، والمحررات الصادرة عنهم تحوز صفة الرسمية، ذلك من الواجب أن تصدر المحررات الرسمية من قبل الموظف العام، والمحررات التي لا تصدر عن الموظفين العموميين لا تحوز صفة الرسمية، مثل المحررات التي تصدر عن الشركات، بينما العنصر الثاني فهو التدوين طبقاً للأوضاع القانونية، وبموجب ذلك يعد المحرر رسمياً إذا كان الموظف العام مكلف بتدوينه، ودور الموظف العام يقتصر على إثبات ما يملئ عليه والموظف العام دوره في تحرير السندات الرسمية لا يقتصر على القوانين واللوائح المنظمة لها، بل وأنه يستمد إختصاصه من مديره أو رؤسائه، حيث يوكلونه بحدود القانون، وقد تستمد المحررات رسميتها من ظروف أنشائها أو الجهة التي أصدرتها أو بالنظر إلى البيانات التي يتضمنها وتحتم على الموظف في التدخل.[64]

-ثانيا:التزوير في المحررات العرفية :تعرف المحررات العرفية على أنها الأوراق التي يحررها أصحاب الشأن من تلقاء أنفسهم دون تدخل الموظف العام في تحريرها، بعكس المحررات الرسمية التي يتولى تحريرها الموظف العام، وبعبارة أكثر وضوحاً المحرر العرفي هو كل محرر لا تنعقد له صفات المحرر الرسمي، فالمحررات العرفية هو كل محرر ليس له صفة الرسمية ويعد المحرر عرفياً حتى لو وصفه صاحبة كذباً بأنه محرر رسمي واسند ظهوره إلى موظف عام، ولكن كان في الظاهر عباراته توحي أنها لم تصدر من موظف عام .[65]

وتم تعريف المحررات العرفية في المادة (15) من قانون البينات في المواد المدنية والتجارية على أنه "هو السند الذي يشتمل على توقيع من صدر منه أو على خاتمه أو بصمته ....".[66]

والمحررات العرفية تعتبر حجة على تعتبر حجة على من وقعها ما لم ينكر ما هو منسوب إليه من خط أو أمضاء أو ختم عند الإطلاع عليه، وفق ما نصت عليه المادة(16) من قانون البينات الفلسطيني.[67]

المحررات العرفية هو كل محرر لا يعد رسميا أو عموميا أو مصرفيا أو تجاريا، أو وثيقة تثبت حقاً شخصياً أو تمنح الإذن، والمحررات العرفية من الممكن أن تكون على شكل محررات عرفية إلكترونية تستخدم من أجل إثبات العقود المدنية التي تعقد بواسطة طريق إلكتروني، وكذلك عقود التجارة الإلكترونية سواء كان موقع عليها إلكترونياً، أو تم التصديق عليها عن طريق شهادات

---

[64] صدراتي، وفاء، مرجع سابق، ص100.
[65] صدراتي ، وفاء، مرجع سابق، ص115.
[66] انظر المادة (15) من قانون البينات في المواد المدنية والتجارية رقم(4) لسنة(2001).
[67] انظر المادة(16)من قانون البينات في المواد المدنية والتجارية رقم(4) لسنة (2001).

إلكترونية تكون محملة على شريط ممغنط أو ميكروفيلم أو أقراص صلبة، ونصت المادة 11 الفقرة 2 [68]من القرار بقانون رقم(10) لسنة 2018 على "اذا وقع التزوير فيما عدا ذلك من المستندات، وكان من شأن ذلك إحداث الضرر، يعاقب بالحبس أو بغرامة....."فهذه المادة نصت على غير المستندات الرسمية ومن المحتمل أن تكون هذه السندات عرفية أو وثائق إدارية أو غير ذلك من ما شابه .

كما أن التزوير في المستندات الرسمية تكون عقوبته أشد من التزوير في المحررات العادية، كون التزوير في المحررات الرسمية يمس مصلحة الدولة ونزاهة الوظيفة وكرامتها، بينما التزوير في المحررات العادية يمس مصلحة الأفراد فالمشرع كفلها بالحماية لكن فرض عليها عقوبات أخف من المستندات الرسمية، حيث نص المشرع في المادة 11 من القرار بقانون بشأن الجرائم الإلكترونية على "1.كل من زور مستندا إلكترونيا من مستندات الدولة أو الهيئات أو المؤسسات العامة معترفا به في نظام معلوماتي، يعاقب بالسجن مدة لا تقل على خمس سنوات، وبغرامة لا تقل على ثلاثة الاف دينار أردني، ولا تزيد على خمسة ألاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونا".[69]

كما ونصت الفقرة الثانية من ذات المادة على عقوبة التزوير في المستندات غير الرسمية حيث تم المعاقبة عليها بالحبس أو بغرامة لا تقل على ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونا.

ويرى الباحث أن التشريعات الفلسطينية أقرت الحماية الجزائية للمستندات الإلكترونية حيث أقرت عقوبات لكل من يقوم بتزوير هذه المستندات وقامت بتشديد العقوبة على تزوير المستندات الإلكترونية الرسمية.

الفرع الثاني: أنماط التزوير الإلكتروني وفقاً لوقت إرتكاب الجريمة

تتعدد أنماط وأشكال التزوير الإلكتروني وفقاً لوقت أرتكاب الجريمة ومن هذا الأنماط بطاقات الإئتمان الإلكترونية حيث أن الانتشار السريع لبطاقات الإئتمان الإلكترونية، دفع بالمتعاملين إلى اللجوء إلى استخدامها والاعتماد عليها، كونها تغني عن حمل الأموال التي من الممكن أن تتعرض للضياع أو السرقة، وتوفر عليهم الوقت والجهد في إنجاز معاملاتهم، حيث توفر على المتعامل بها

---

[68] أنظر المادة(11) من القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية.
[69] انظر المادة(11) من القرار بقانون رقم(10) لسنة 2018 بشأن الجرام الإلكترونية.

الوقت لتنقل من منطقة إلى أخرى ليدفع ثمن مشترياته ويسدد فواتيره، إلا أن هناك مشكلة تواجه هذه النوع من الدفع وهي التزوير، حيث أنها تؤدي إلى نزع الثقة في التعاملات التجارية والمالية، وهي جريمة ذات طبيعة خاصة، تشتمل على نوع جديد حديث من الجرائم غير مألوف، وهذه الجريمة تحتاج إلى آليات حديثة ومتطورة للكشف عنها وتتبعها ومعرفة مرتكبيها .[70]

وبطاقات الإئتمان تشتمل على جميع البطاقات التي تصدرها البنوك، أو المؤسسات المصرفية على إختلاف أنواعها، وبطاقات الإئتمان واحدة منها، وتقسم هذه البطاقات بحسب أسلوبها إلى بطاقات يدوية، وبطاقات معالجة آلياً، والعمل في الأولى لا يرتبط بنظام المعلومات، بينما الثانية يتطلب عملها الاتصال بنظام المعلومات، وثانية تقسم إلى بطاقة سحب ممغنطة، وبطاقة ذات الذاكرة، فالبطاقة الأولى تسمح لحاملها سحب النقود من أجهزة السحب الآلي، فضلاً عن أنها أداة وفاء.[71]

وتزوير بطاقات الإئتمان يتضمن تغيير الحقيقة التي تحتويها كغيره من المستندات الرسمية أو العرفية، حيث يتم التلاعب بالمعلومات والبيانات، سواء كانت مدمجة أو ظاهرة ويهدف الفاعلون من وراء هذا التزوير إلى الحصول على الأموال واستخدامها في عملية الوفاء عن بعد من خلال التسوق من المواقع الإلكترونية عن طريق الأنترنت، وهذا النوع من التزوير قد يكون جزئيا من خلال تغيير بيانات البطاقة الموجودة الصادرة عن بنك من البنوك ويطلق عليه التزوير الجزئي، والتزوير الكلي حيث يتمثل في اصطناع بطاقة جديدة تحمل بيانات بطاقة صحيحة، وهذا النوع من التزوير تتعدد طرقه وأساليبه حيث من الممكن أن تكون على شكل، تزوير الإشعارات وهذا يكون عند اتفاق صاحب البطاقة مع البنك على إخراج بطاقة صحيحة تحمل بيانات غير صحيحة مع علمه بأنها غير صحيحة، أو أن يتفق التاجر مع الموظف بتجاوز حد السحب في صرف قيمة إشعارات البيع من البطاقات المزورة، أو أن يقوم موظف البنك بالتلاعب بنفسه عن طريق اختلاس مبلغ من البنك، عند تقديم البطاقة للموظف البنك للسحب والإيداع فيزور قيمة المبلغ ويدخر الفرق لنفسه، ومن المحتمل إيضاً أن يتم الإتفاق ما بين التاجر وحامل البطاقة وذلك عن طريق قيام حامل البطاقة بعمليات شراء وهمية مقابل حصوله على نسبة من قيمة الفاتورة،

---

[70] نقطي ، عبد العزيز ، جريمة التزوير في بطاقات الأئتمان ، مجلة العلوم القانونية والسياسية، جامعة الوادي، المجلد13، العدد1، 2022، ص752.

[71] الحنيص، عبد الجبار، الحماية الجزائية لبطاقات الإئتمان الممغنطة من التزوير، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد24، العدد الثاني، 2008، ص149.

ويحصل هذا عند استيفاء الرصيد الشهري للبطاقة، ويقوم التاجر بعدها بالحصول على قيمة الفاتورة من الجهة المصدرة لها.[72]

ويتلاعب التجار إيضاً في ماكينة البيع الإلكترونية، وذلك عن طريق استغلال الماكينة اليدوية للحصول على إشعارات أكثر دون علم صاحب البطاقة، حيث يكون مطبوع عليها بيانات البطاقة ويقلد توقيع حامل البطاقة بعد ذلك ليحصل على قيمتها من الجهة المصدرة، أو يقوم بالتلاعب في إشعارات البطاقة من أجل الحصول على قيمتها أكثر من مرة، أو يستخدم بطاقات مسروقة من خلال العبث بماكنة البيع الإلكترونية المسلمة له .[73]

ونص المشرع الفرنسي في قانون العقوبات على تعريف التزوير حيث عرفته المادة(441|1) على أنه"كل تغيير تدليسي للحقيقة يكون من طبيعته أن يسبب ضرراً بأي وسيلة كانت في محرر أو أي سند للتعبير عن الرأي والذي من الممكن أن يكون له أثر في أنشاء دليل على حق أو فعل تكون له نتائج قانونية، وقد اعتبر الفقه الفرنسي البطاقة مستندا معدا أو قادرا على إقامة الدليل على حق أو واقعة تحدث نتائج أو آثارا قانونية.[74]

ولم تنص التشريعات العراقية إيضاً على تزوير بطاقات الإئتمان حيث أن نصوصه لم تشتمل على هذا النوع من التزوير لذلك يرجع إلى نصوص قانون العقوبات التقليدية التي نصت على تعريف التزوير في المادة(289) حيث عرفته على أنه "كل تغيير للحقيقة بقصد الغش في سند أو وثيقة أو محرر آخر بأحد الطرق المادية والمعنوية التي نص عليها القانون، تغيير من شأنه إحداث ضرر بالمصلحة العامة أو مصلحة أحد الأشخاص".[75]

وفي التشريعات الفلسطينية نصت المادة (12) من القرار بقانون رقم(10) لسنة (2018) بشأن الجرائم الإلكترونية على ".....2.كل من زور وسيلة تعامل إلكترونية بإي وسيلة كانت، أو صنع أو حاز بدون ترخيص أجهزة أو مواد تستخدم في إصدار أو تزوير بطاقة التعامل الإلكتروني، يعاقب بالعقوبة ذاتها المنصوص عليها في الفقرة(1) من هذه المادة ".

نصت هذه المادة على تزوير بطاقات التعامل الإلكترونية وعاقبت عليها، حيث قامت بتحديد الطرق التي يتم بها تغيير الحقيقة وهي عن طريق التزوير، أو حيازة أجهزة دون ترخيص لتزوير

---

[72]نفطي، عبد العزيز، مرجع سابق، ص758.
[73] نفطي، عبد العزيز، مرجع سابق، ص758.
[74] الجبوري، عبد السلام، مرجع سابق، ص96.
[75] انظر المادة(286) من قانون العقوبات العراقي ، رقم 111 لسنة 1969.

بطاقة التعامل الإلكتروني ويتضح أن المشرع استخدام ألفاظ واسعة النطاق مثل (بإي وسيلة كانت) أي أنه لم يقم بتحديد طرق التزوير .

وتوصل الباحث من خلال ما تم عرضه أن نصوص التشريعات العربية تحتوي على نقص تشريعي في قانون العقوبات بشأن تجريم جرائم التزوير الإلكتروني، على العكس من التشريعات الأجنبية كالتشريع الفرنسي الذي نص على تجريم التزوير الإلكتروني في قانون العقوبات حيث قام بوضع نص عام يمكن المعاقبة من خلاله على كل ما يقع تحته من مفاهيم .

المطلب الثالث: أركان جريمة التزوير الإلكتروني

جريمة التزوير الإلكتروني كغيرها من الجرائم تتطلب ركنا ماديا وركنا معنويا حتى تقوم، سنتعرف في هذا المطلب على هذه الأركان، والتعرف ما إذا كانت تحتاج إلى ركن خاص لقيامها أم لا .

الفرع الأول: الركن المادي

لا يختلف الركن المادي لتزوير الإلكتروني عنه في التزوير التقليدي، لكنه في ذات الوقت يتميز عنه في محله والطرق التي تتم بها، فالتزوير جوهره وأساسه تغيير الحقيقة.[76]

فتغيير الحقيقة هو استبدال الحقيقة بالذي يخالفها، وهذا السلوك المجرم الذي تنطلق به جريمة التزوير وفي حال كان هذا العنصر غير موجود لا تقوم الجريمة والتزوير الالكتروني يقوم بإي طريقة يقرها القانون، وذلك بإدخال بعض البيانات والمعلومات إلى البرنامج من خلال استغلال الأخطاء والعيوب المنطقية التي يحتويها هذا البرنامج، وفي الواقع هي مجموعة من الممرات الخالية والمتروكة في البرنامج.[77]

وتغيير الحقيقة يقصد به تغيير الحقيقة النسبية وليس الحقيقة المطلقة، كأن يثبت في المحررات المزورة ما يخالف إرادة صاحب الشأن حتى لو صادف ذلك الواقع فعلا، كما أن تغيير الحقيقة ينصرف إلى تغيير الحقيقة التي يقترحها المشرع، أي البيانات التي حددها القانون والتي بإكتمالها يعيد المحرر إلى قوته .[78]

---

[76] الطاهر، برهوم، مرجع سابق، ص19.

[77] المطيري، بندر صياح، جريمة التزوير الالكتروني في الكويت، مجلة رماح للبحوث والدراسات، المجلد 88، 2023، ص123.

[78] الجبوري، عبد السلام، مرجع سابق، ص42.

وتغيير الحقيقة يتم بنشاط إيجابي وبنشاط سلبي الذي يتمثل في الترك، وإذا ترتب على الترك تغيير جوهري سبب ضرر للغير، لأن الترك يعتبر تغيير للحقيقة، والتزوير يعد إلكترونيا خاصة إذا كان الترك متعمد ليس على سبيل الخطأ أو السهو.[79]

ومن المهم عند تغيير الحقيقة وجود المحرر الذي يعتبر محل جريمة التزوير، ولا أهمية لنوع المحررات فقد تكون برقية أو حكم أو سهم أو دفتر تجاري أو محررات إلكترونية، وتغيير الحقيقة في كتابة المحرر أي في عباراته أو فيما عليه من تأشيرات وعلامات مختلفة، وفيما عدا ذلك لا يعتبر تزوير ولذلك حكم بعدم وقوع جريمة التزوير في وضع صورة شخصية على رخصة رسمية.[80]

ونصت المادة 11 على تغيير الحقيقة في التزوير الألكتروني حيث جاء في الفقرة 4 أنه "كل من زور أو تلاعب بتوقيع أو أداة أو أنظمة توقيع إلكترونية رسمية، سواء تم ذلك بإصطناعه أو إتلافه أو تعييبه أو تعديله أو تحويره، أو بإي طريقة أخرى تؤدي إلى تغيير الحقيقة في بياناته أو معلوماته ".

الفرع الثاني: الركن المعنوي

لا تقوم جريمة التزوير الإلكتروني دون وجود الركن المعنوي، ويلزم لقيام الركن المعنوي توافر عنصر العلم والإرادة، العلم بعناصر الجريمة وإتجاه إرادة الجاني إلى تحقيق هذه العناصر أو قبولها .[81]

ويشترط لقيام جريمة التزوير الإلكتروني توافر القصد العام والقصد الخاص ويتمثل القصد العام في إدراك الجاني بأنه يغير الحقيقة بإحدى الطرق في المحررات، وهذا التغيير من شأنه أن يحدث الضرر فعليا أو احتماليا، ويشترط أن يثبت علم المتهم على وجه اليقين بأنه يغير الحقيقة، فعلم المتهم بتغيير الحقيقة إذا لم يكن ثابتاً بالفعل، فأن إهماله في تحريرها مهما كانت درجته لا يتحقق به هذا الشرط، وعلم الجاني يفترض بأن ما حصل من تغيير يعتبر محرر في نظر القانون، وهذا التغير قد وقع بطريقة من الطرق التي نص عليها القانون، وفي مجال التزوير الإلكتروني الجاني

---

79 الجبوري، عبد السلام، مرجع سابق، ص43.
80 الجبوري، عبد السلام، مرجع سابق، ص43.
81 المغربي، طه عثمان، مرجع سابق، ص462.

يجب أن يكون عالماً بأنه يقوم بعملية تزوير المعلومات كما يجب أن إرادته تتجه إلى القيام بتزوير.[82]

وفي التشريع الفرنسي قام المشرع الفرنسي باستخدام لفظ يدل على التبصر بكون المحرر مزورا، ليدل على أن الجاني على علم تام بكون المحررات مشوبة بتزوير، ويقوم باستخدامه متعمدا على الرغم من علمه بتزويره، وهذا المفهوم يتطابق مع القصد الجنائي العام .[83]

بينما القصد الجنائي الخاص، لم يشر النص إلى البحث في إراد الجاني إلى إحداث الضرر، وهذا الأمر يدل على أنه لا يتطلب سوى القصد الجنائي العام، والرأي الراج في الفقه الفرنسي على أن لفظ التبصر الذي ورد في النص يتطلب توافر القصدين القصد العام والقصد الخاص الذي يتجسد في نية إحداث الضرر، بغض النظر كان الضرر فعلي أو احتمالي.[84]

١

الفرع الثالث: الضرر

حتى تقوم جريمة التزوير الإلكتروني يجب أن ينتج عن فعل التزوير ضررا، حيث أنه لا يعاقب على التزوير إذا لم يكن هناك ضرر، ولا يشترط وقوع ضرر معين والضرر يقع في جرائم التزوير الإلكتروني بتمام التحريف المفتعل للحقيقة، ثم استخدام الصورة الجديدة للحقيقة من قبل الغير أو من قبل الفاعل حيث أنه يستند في قراره إلى الحقيقة المفتعلة بفعل الفاعل والتي لا يعلم بتزويرها، والضرر قد يكون حالاً أو محتمل الوقوع، ماديا أو أدبيا، أجتماعيا أو فرديا .[85]

ويقصد بالضرر كل مساس بحق أو مصلحة يحميها القانون، ولا يشترط فيه درجة معينة من الجسامة، فجريمة التزوير تقوم حتى لو كان الضرر يسيرا، ولا عبرة بالشخص الذي لحق به الضرر حيث أنه إذا ارتبكت جريمة التزوير وتم إلحاق الضرر بالغير حتى لو كان من غير الأشخاص المستهدفين تقوم جريمة التزوير.[86]

---

[82] فتيحة، عمارة، مرجع سابق، ص186.
[83] فتيحة، عمارة، مرجع سابق، ص186.
[84] فتيحة ، عمارة، مرجع سابق، ص187.
[85] الجبوري، عمر عبد السلام، مرجع سابق، ص60.
[86] المغربي، طه عثمان، مرجع سابق، ص461.

والضرر لا يقوم إيضاً إذا انعدمت المصلحة التي يحميها القانون، كالمدين الذي يصطنع لنفسه سند مخالصة تثبت الوفاء بالدين كاملاً، فذلك يعتبر من باب التزوير حيث أنه غير جائز أن يصطنع الشخص بنفسه دليلاً لنفسه.[87]

وفي قرار لمحكمة النقض الفلسطينية رقم (401) لسنة 2021 قررت المحكمة رداً على الإستئناف المقدم بما يلي"من هذه النصوص يتبين أن أركان جريمة التزوير التي يتوقف على توافرها توقيع العقوبة هي ثلاثة (1.تغيير الحقيقة بإحدى الطرق المنصوص عليها في القانون.2توفر القصد الجرمي .3.حصول الضرر أو احتمال حصوله).[88]

ويرى الباحث في تعليقه على القرار القضائي أن جريمة التزوير الإلكتروني ينطبق عليها هذا النص حيث أنه يجب حتى تقوم جريمة التزوير الإلكتروني توافر الركن المادي والركن المعنوي وعنصر الضرر .

[87] المغربي، طه عثمان، مرجع سابق، ص462.
[88] محكمة النقض ، قرار رقم 401، بتاريخ 5، يناير، 2021.

الفصل الثاني

القواعد الإجرائية لمكافحة جريمة التزوير الإلكتروني

أن جرائم التزوير الإلكترونية تعد من الجرائم المستحدثة التي يتم ارتكابهاعن طريق الوسائل الإلكترونية، فهذا النوع من الجرائم يقع في عالم افتراضي لا وجود مادي له، فهذه الجرائم من أخطر الجرائم التي تعرض الأفراد للضرر والدول إيضا، فالمجرمين أصبحوا أكثر خطورة وحركة من السابق، ونتيجة وجود تقنيات حديثة لإرتكاب الجرائم ذلك أدى إلى سهولة إرتكاب الجرائم .

فكان لا بد من وجود حماية جزائية خاصة بالتزوير الإلكتروني، سنتطرق للحديث عنها في هذا الفصل حيث تم تقسيمه إلى مبحثين رئيسيين، المبحث الأول يتناول الحديث عن (تحديد الجهات القضائية المختصة بالملاحقة)، والمبحث الثاني يتناول الحديث عن (بيان الاختصاص القضائي في جريمة التزوير الإلكتروني).

المبحث الأول: الجهات المختصة بالملاحقة في جرائم التزوير الإلكتروني

كون جريمة التزوير الالكتروني من الجرائم الهامة التي لها خاصية تميزها عن غيرها، فكان من الواجب أن يكون هناك مواجهة تشريعية لمثل هذه الجرائم بحيث تتناسب مع التطور التقني وما رافقه من ظهور جرائم مستحدثة كالتزوير الإلكتروني[89]، نأتي في المطلب الأول للحديث عن دور الضابطة القضائية في مكافحة التزوير الإلكتروني وفي المطلب الثاني نوضح دور نيابة مكافحة الجرائم لتصدي لجريمة التزوير الإلكتروني.

المطلب الأول: دور الضبط القضائي في مكافحة جريمة التزوير الإلكتروني

نتيجة التطور والتقدم الذي حصل في الآونة الأخيرة خصوصاً في مجال التكنولوجيا، أصبحت البيئة الإلكترونية حقيقة لا شك فيها وأصبحت الضرورة لوضع قواعد جزائية موضوعية جديدة قادرة على استيعاب الكم الهائل من المعلومات، وتحارب الجرائم الناجمة عن استخدام هذه التقنية

[89] عبد العال، أسامة حسين، جريمة تزوير المستند الالكتروني ، مجلة العلوم القانونية والاقتصادية ، المجلد64، العدد1، 2021، ص26.

بشكل سيئ [90]، حيث أنه من الواجب التطرق إلى دور الضابطة العدلية، عن طريق بيان الأساليب الفنية التي تستخدمها الأجهزة في تعاملها في هذه الجرائم لذلك سوف يتطرق الباحث إلى إجراءات الضابطة العدلية في معاينة جهاز الكمبيوتر في الفرع الأول، وإجراءات الضابطة العدلية في التفتيش وضبط أدلة الكمبيوتر.

الفرع الأول: إجراءات الضبط القضائي في معاينة جهاز الكمبيوتر

تعرف المعاينة على أنها "هي الكشف الحسي المباشر لإثبات حالة الشيءأو الشخص من خلال الرؤية أو الفحص المباشر".[91]

كما ويعرفها فقهاء آخرون على أنها "وسيلة إثبات مباشرة تمدنا بالإدلة المادية ونستنج منها القرائن".[92]

والمعاينة تعتبر الإجراء الأول من إجراءات تتبع الجاني والقبض عليه، ويمتاز هذا الإجراء بأنه خطير حيث أنه يؤدي لنتائج خاطئة في حال تم تنفيذه بشكل خاطئ، ويؤدي إلى تعميق المسافة بين العدالة والمجرمين.[93]

وتساهم المعاينة في مجال الكشف عن الجريمة الإلكترونية، إلا أن هذه الأهمية تختلف عنها في الجرائم التقليدية وذلك يعود إلى أن هناك مسرح جريمة في الجرائم التقليدية، من خلاله يتم الكشف عن الأدلة، على العكس من الجرائم الإلكترونية حيث أنه لا يوجد هناك مسرح جريمة على أرض الواقع، أنما هو عبارة عن عالم افتراضي يتثمل في البيئة الإلكترونية .[94]

يتوجب على مأموري الضبط القضائي استخدام تقنيات فنية بهدف الوصول إلى مسرح الجريمة ليتمكن من استخلاص الدليل الإلكتروني من مسرح الجريمة الافتراضي، [95]ويجب عليه إيضاً أن يضع يده على الأدلة المادية التي تفيد في التحقيق، وإيضاً وضع الإختام في الأماكن التي أجريت فيها المعاينة في حالة وجود آثار تفيد في الكشف عن الحقيقة.[96]

---

[90] الجبوري، عبد السلام، مرجع سابق، ص11

[91] عوني، رمزي، المعاينة الجنائية ودورها في الإثبات الجنائي في التشريع الفلسطيني، رسالة مقدمة لنيل درجة الماجستير، جامعة النجاح الوطنية ، نابلس، فلسطين، 2019، ص37.

[92] عوني، رمزي، مرجع سابق، ص37.

[93] جبوري، عبد السلام، مرجع سابق، ص117.

[94] عوني، رمزي، مرجع سابق، ص82.

[95] عوني رمزي، مرجع سابق، 85.

[96] الجبوري، عمر عبد السلام، مرجع سابق، ص118.

في التشريعات الفلسطينية مأمورو الضبط القضائي والنيابة العامة، يقومون بالتعاون مع بعضهم البعض لمتابعة المجرمين اللذين يهددون النظام والأمن العام، ويكافحون الجرائم الإلكترونية عن طريق ما يلي:[97]

وكما يجب على مأموري الضبط القضائي في مسرح الجريمة القيام بمجموعة من الإجراءات تتمثل في الآتي:

1.توثيق حالة مسرح الجريمة، أي تسجيل كل التفاصيل المتعلقة بحالة الوسائط الذكية، كتسجيل ما إذا كانت هذه الأجهزة متصلة بالإنترنت أم لا، وتحديد وضع الأجهزة كان مفتوحاً أم لا.[98]

2.تحديد هوية وتوثيق أجهزة الوسائط الذكية والأجهزة الملحقة بها التي يتم العثور عليها في مسرح الجريمة .

3.تحديد هوية وتوثيق أجهزة التخزين التي يتم العثور عليها في مسرح الجريمة.

4.تصوير مسرح الجريمة.[99]

5.حفظ الأدلة والمواد الرقمية.

6.حفظ الوثائق المطبوعة.

7.حفظ الأجهزة.

8.إجراء استرجاع للوثائق العالقة، من قبيل طباعة الأوراق العالقة في ماكنة الطباعة.

9.إجراء استرجاع للوثائق الملغاة أو التي تم مسحها.

10.نقل الأدلة التي يتم ضبطها.[100]

وكان هناك مناشدات إلى ضرورة إنشاء أجهزة متخصصة للتحري عن الجرائم الإلكترونية والتي تعتمد على مستوى متقدم من العلم والعمل والمهارة والتفكير المتعلقة باستخدام الإنترنت وبحيث يتمكن أفراد الضبط القضائي من الاستدلال على الآثار المادية في مسرح الجريمة حتى يستطيعوا الوصول للحقيقة والكشف عنها وإمساك المجرمين وإلحاق العقوبة بهم.[101]

والتشريع الفلسطيني في قانون الجرائم الإلكترونية خصص المادة(35) لتحديد الجهة المختصة بالقيام بالمعاينة والتفتيش والإستعانة بالخبراء في مجال الكشف عن الجريمة الإلكترونية بكل

---

[97] أيمن ، محمد الظاهر، الجرائم الإلكترونية وإجراءاتها الجزائية وطرق إثباتها، الطبعة الأولى، 2024، ص203.

[98] مصطفى، عبد الباقي ، التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين، مجلة علوم الشريعة والقانون، المجلد45، العدد4، 2018، ص286.

[99] مصطفى، عبد الباقي، مرجع سابق، ص286.

[100] مصطفى عبد الباقي، مرجع سابق، ص286.

[101] رمزي، عروني، مرجع سابق، ص83.

الطرق المحددة وفقاً للقانون، ويشمل إيضاً وسائل الإثبات التقليدية، وجعل إجراء المعاينة في الجريمة الإلكترونية من صلاحيات النيابة العامة أو من تنتدبه من مأموري الضبط القضائي.[102] والمعاينة قد تكشف عن الحقيقة في الجريمة الإلكترونية، لذا يجب أن تكون هناك جهة مختصة ومؤهلة للقيام بالمعاينة حتى يتم التحفظ على الأدلة الموجودة وهذا ما نصت عليه المادة (53\5) من قانون الجرائم الإلكترونية التي نصت على "يشترط على مأمور الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية ."[103]

ومعاينة رجال الضبط القضائي لمسرح الجريمة لا يوجد به صعوبة، لكن الصعوبة الحقيقة تكون عندما تكون الجريمة واقعة على برامج الحاسب الآلي والوسائط الذكية وما تحتوي عليها هذه الأجهزة من بيانات ، أي عند قيام المجرم الإلكتروني بأعمال تتعلق بالتعدي على كيان أجهزة الكمبيوتر، أي إتلاف برامج االحاسب الآلي أو تزوير المحررات الإلكترونية وتحول هذه الصعوبات دون الحصول على منفعة المعاينة كون جرائم الحاسب الآلي في أغلب صورها تكون مخفية، والمجني عليه لا يدركها ولا يدري بوقوعها وخاصة في حال كان مرتكب الجريمة يتمتع بخبرة فنية عالية وتقنية، بالإضافة إلى أن المجرم يستخدم التدابير الأمنية وهذا يجعل من التفتيش عن الأدلة أمر صعب، كاستخدام كلمات السر للوصول إليها، أو منع الاطلاع على البيانات عن طريق التشفير مثلاً.[104]

الفرع الثاني: إجراءات الضبط القضائي في التفتيش

يعتبر التفتيش من أخطر الإجراءات التي تمس بحياة الإنسان الخاصة، ويتمتع بخصوصية أكبر في الجرائم الإلكترونية وخاصة جرائم التزوير الإلكتروني، لكون خصوصيات الناس محفوظة بوسائل التكنولوجيا الحديثة[105]، ويعرف التفتيش على أنه إجراء تحقيق يقوم به موظف مختص، للبحث عن أدلة مادية لجناية أو جنحة، وذلك في محل خاص أو لدى شخص وفقاً للأحكام المقررة

---

[102] انطر المادة(35) من القرار بقانون رقم(38) لسنة(2021) المعدل للقرار بقانون رقم(10) لسنة (2018) بشأن الجرائم الإلكترونية.

[103]. انطر المادة(35) من القرار بقانون رقم(38) لسنة(2021) المعدل للقرار بقانون رقم(10) لسنة (2018) بشأن الجرائم الإلكترونية

[104] الجبوري، عمر عبد السلام ، مرجع سابق، ص118.

[105] عموري، أشرف أحمد مصطفى، التفتيش في الجرائم الإلكترونية، رسالة ماجستير مقدمة لجامعة القدس، أبو ديس، فلسطين، 2018، ص18.

قانوناً، وهو الإطلاع على محل منحه القانون حرمة خاصة، باعتباره مستودع سر صاحبه، لضبط ما عسى قد يوجد به مما يفيد الحقيقة عن جريمة معينة.[106]

وكون جريمة التزوير الإلكتروني هي من الجرائم المستحدثة التي وجدت نتيجة التطور والتقدم الحاصل في الأونة الأخيرة، و مسرح الجريمة هنا هو عبارة عن عالم أفتراضي وهو أجهزة الحاسب الآلي ومكوناتها، فما مدى إمكانية خضوعها لتفتيش ؟يرى جانب من الفقه أن الهدف من التفتيش هو ضبط الأدلة المادية التي تسهم في الوصول للحقيقة والكشف عنها، بالتالي يدخل في نطاق التفتيش ما تقوم به الأجهزة المختصة من تفتيش للمكونات المادية للحاسب الآلي ومختلف أوعيته بهدف الحصول على معلومات تفيد في الكشف عن الحقيقة طالما أن التفتيش وقع طبقاً للإجراءات القانونية، مع مراعاة أن الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وإمكانية إتلافها لكن حكم هذه المكونات متعلقة بطبيعة المكان الموجدة فيه، سواء في الأماكن العامة أو الأماكن الخاصة، حيث أن المكان يتمتع بأهمية في مجال التفتيش، ففي حال تواجدها في مسكن المتهم كان لها حكمه.[107]

وتظهر الصعوبة في التفتيش في الجرائم الإلكترونية التي تقع على أجهزة الكمبيوتر في حالة إستخدام وسائل فنية في تغيير وإتلاف ما فيه من بيانات ومعلومات من خلال خرقه بفيروس، والصعوبة في هذه الحالة هي أنه لا يوجد خبرة كافية لدى مأموري الضبط القضائي الذين يقومون بالتفتيش، باعتبارها جهة مختصة بالتفتيش، بينما الصعوبة الأخرى فهي أن عملية الضبط تواجه صعوبة في الحالات التي تكون فيها البيانات مخزنة في نظم معالجة مركزية في الكمبيوتر، في شبكة معلومات كبيرة، فصياغة شرط يمنح للمحقق إمكانية ضبط هذا النظام الشبكي بأكمله، وعزله عن البيئة الإلكترونية المحيطة به لا يعد شرطا حقيقيا لمبدأ التناسب كونه يمس بحقوق الغير في النظام محل الضبط.[108]

ويختص مأمورو الضبط القضائي في التفتيش في الجرائم الإلكترونية حيث أن القانون منحهم سلطات واسعة من بينها تفتيش الأماكن والأشخاص ووسائل تكنولوجيا المعلومات المستخدمة وذات العلاقة بالجريمة وذلك في المادة (52) من قانون الجرائم الإلكترونية المعدل لسنة 2021،

---

[106] عموري، أشرف أحمد مصطفى، مرجع سابق، ص20.
[107] طالب، ليندا، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، العدد16، 2017، ص489.
[108] الجبوري، 'عمر عبد السلام، مرجع سابق، ص121.

وبالنظر إلى الطبيعة الخاصة لهذا النوع من الجرائم يحتاج التفتيش إلى مأمور ضبط قضائي متخصص في البيئة الرقمية، للبحث عن الدليل الإلكتروني .[109]

وقانون الجرائم الإلكترونية أنشأ وحدة متخصصة في جهاز قوى الأمن وجهاز الشرطة من مأموري الضبط القضائي تسمى "وحدة الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات"، وذلك بنص المادة(3\1)، وقانون الإجراءات الجزائية الفلسطيني عدد في المادة (21) مأموري الضبط القضائي، وكذلك قانون الشرطة، والقوانين الخاصة الأخرى.

يرى الباحث أن عملية تفتيش مسرح الجريمة الإلكتروني هو موضوع في غاية الحساسية كونه يتعامل مع مسرح جريمة افتراضي وهو الحاسب الآلي ومكوناته ونتيجة لما يتمتع به هذا المسرح من خصوصية وصعوبة في التعامل يجب أن يكون هناك مأمورو ضبط قضائي متمرنون ولديهم خبرات ومهارات كافية وذلك عن طريق إخضاعهم لدورات تدريبية تفيد في مجال الكشف عن الجرائم الإلكترونية .

المطلب الثاني: نيابة مكافحة الجرائم الإلكترونية

نتيجة لحرص الدول على كشف الحقيقة وتتبع الجناة، يتم إنشاء وحدات خاصة للكشف عن الجرائم التي تقع ومن هذه الوحدات نيابة مكافحة الجرائم الإلكترونية، حيث قامت فلسطين بإنشاء نياة متخصصة لمكافحة الجرائم الإلكترونية، وتعد هذه خطوة مهمة للقضاء على الجريمة الإلكترونية التي هي في تزايد تسارع مستمر نتيجة للتطور الذي يحصل في مختلف مجالات الحياة، ونأتي في هذا المطلب لتوضيح نشأتها وإختصاصاتها وآلية عملها .

الفرع الأول: نشأة نيابة مكافحة الجرائم الإلكترونية

تم إنشاء نيابة مكافحة الجرائم في فلسطين بقرار من نائب العام بتاريخ 2016\3\20، وتتشكل النيابة العامة من 1.رئيس مكافحة الجرائم الإلكترونية :حيث كلف النائب العام بتاريخ2016\3\27 رئيس النيابة بمكافحة الجرائم الإلكترونية، ومكتب النائب العام مقره في مدينة رام الله، وتكون وظيفة رئيس النيابة استقبال طلبات الإحتياجات التي ترفع من أعضاء النيابة المتخصصين في المحافظات ليتم التعرف على الخطوط التي إرتكبت منها الجريمة، وإحالة الطلب إلى وحدة الجرائم الإلكترونية في أجهزة الشرطة، وفي حال التوصل إلى معلومات هامة يرسلها

[109] عموري، أشرف، مرجع سابق، ص33.

رئيس النيابة إلى العضو الذي قام بطلبها، وفي معظم الأوقات ونتيجة لإعتبارات خاصة ترسل النتائج مع إحالة الملف لعضو نيابة آخر.[110]

وفي مقابلة أجريت مع رئيس نيابة الجرائم الإلكترونية تم الحديث عن الإجراءات المتبعة في حال وقوع جريمة إلكترونية حيث تطرق إلى الإجراءات و الأصول المتبعة في جرائم التزوير الإلكتروني حيث أن النيابة العامة تباشر إجراءاتها التحقيقية عند تقديم الشكاوي المتعلقة بهذا النوع من الجرائم أو بمجرد علمها بوقوع مثل هذه الجريمة وركز رئيس النيابة على ضرورة ضبط الأداة أو الجهاز أو البيانات الإلكترونية محل الجريمة كونها من العناصر الأساسية في إثبات وقوع الفعل الجرمي ونسبته إلى فاعله و في سبيل ذلك تعمل النيابة العامة على الحصول على أدلة الإثبات وفقا للإجراءات القانونية الأصولية سواء من حيث آلية ضبط الأداة الألكترونية أو الجهاز الذي يتطلب أن يكون وجود مذكرة تفتيش لمنزل المشتبه فيه وفقا لدلائل قوية على حيازته لها وكذلك تطرق إلى وجوب صدور أمر نفاذ مباشر للجهاز للوصول إلى البيانات الإلكترونية المطلوبة بحيث يتم ذلك من مامور ضبط قضائي مؤهل.

واشار إلى قيام النيابة العامة بالاستعانة بشكل كبير بوحدة الجرائم الإلكترونية وجرائم الاتصالات و تكنولوجيا المعلومات في الشرطة الذين لديهم من الكوادر البشرية المؤهلة والأجهزة الإلكترونية المتطورة التي تمكنهم من الوصول إلى البيانات و الأدلة الإلكترونية المطلوبة و هذا إلى جانب الإجراءات التحقيقية التقليدية التي يتم القيام بها في باقي الجرائم الاخرى مثل سماع الشهود و استجواب المتهمين و مواجهتهم بالأدلة و الشهود وغيرها مبينا أن ما يميز هذا النوع من الجريمة هو الحاجة للاستعانة للخبرة الفنية لبيان مواطن التزوير و التلاعب الالكتروني و بعد انتهاء التحقيق يتم التصرف في القضية وفقا لأحكام قانون الإجراءات الجزائية ففي حال وجود الأدلة وقيام أركان الجريمة بحق مرتكبها يتم احالته بموجب قرار ولائحة اتهام حسب الأصول إلى المحكمة المختصة.[111]

كما أنه يجوز لنيابة مكافحة الجرائم اللجوء إلى استخدام برامج الذكاء الاصطناعي للكشف عن الجرائم الإلكترونية حيث أن الذكاء الاصطناعي هو أحد علوم فروع الكمبيوتر المعنية بكيفية محاكاة الآلات لسلوك البشر، فهو علم إنشاء أجهزة وبرامج كمبيوتر قادرة على التفكير بطريقة نفسها التي يعمل بها الدماغ البشري تتعلم مثلما نتعلم وتقرأ كما نقرأ وتتصرف كما نتصرف،

---

[110] عموري، أشرف أحمد مصطفى، مرجع سابق، ص27.

[111] سفيان موسى حسن ابو زهيرة، 22\3\2024، رئيس نيابة الجرائم الالكترونية، نيابة الجرائم الالكترونية، الساعة الواحدة ظهراً، مكتب رئيس نيابة مكافحة الجرائم.

[112]ومن الدول التي كان لها بصمة في هذا المجال الولايات العربية المتحدة حيث أنها استخدمت الذكاء الاصطناعي في الكشف عن الجريمة الإلكترونية نتيجة العدد الهائل من الجرائم الإلكترونية التي ترتكب لديها نتيجة التقدم والتطور التكنولوجي الذي تتمتع به.

في ظل التسارع المتزايد للتغيرات الاقتصادية وصعوبة التنبؤ بسيرورتها، أصبحت البيئة الأمنية الحالية مليئة بالمخاطر. لذلك، أصبح من الضروري على الأجهزة الأمنية اعتماد وتبني أسلوب إدارة المخاطر كمنهج علمي وفعال لمواجهة المخاطر المختلفة. وفي هذا السياق، برز الذكاء الاصطناعي كتقنية فعالة في مكافحة الجرائم الإلكترونية، حيث أصبح أداة محورية في تحقيق أهداف الذكاء الاصطناعي وأهميته في التحقيق الجنائي للكشف عن هذا النوع من الجرائم.[113]

[112] سعود ، عبد القادر الشاعر، دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الالكترونية، مجلة الأبحاق القانونية والاقتصادية، العدد38، المجلد13، 2020، ص10.

[113] سعود، عبد القادر، مرجع سابق، ص16.س

المبحث الثاني: الاختصاص القضائي في جريمة التزوير الإلكتروني

يعرف الاختصاص القضائي على أنه "السلطة التي يقررها القانون للقضاء في أن ينظر في دعاو، حددها المشرع وفق قواعد وإجراءات معينة".والقضاة ملزمون في البداية في النظر في النزاع في الاختصاص الدولي، أي بمعنى الكشف في حالة كان الاختصاص للقضاء الوطني، ثم البحث في الاختصاص الداخلي، ومن الضروري أن يحدد من هي المحكمة المختصة للنظر في النزاع، كونه يترتب على ذلك معرفة القانون الواجب التطبيق، لذلك من الضروري تحديد معايير تتناسب مع طبيعة جرائم التزوير الإلكتروني.[114]

وفي حال كان الشخص الذي ارتكب جريمة التزوير الإلكتروني من خارج الدولة، يتم عن طريق الانتربول مخاطبة الدول المشاركة عن هذا الشخص أنه مطلوب للمحاكمة ويتم تعميم اسمه في المطارات والمعابر ويتم تقييد أوراقه حتى لا يستطيع تجديد أوراقه في السفارات وإلقاء القبض عليه وتسليمه للعدالة لينال عقابه.

لذلك سوف نتطرق في هذا المبحث للحديث عن قواعد الاختصاص القضائي المتعلقة في جريمة التزوير الإلكتروني في المطلب الأول، وفي المطلب الثاني نتحدث عن سلطة القاضي في قبول الدليل الإلكتروني.

المطلب الأول: قواعد الاختصاص القضائي المتعلقة في جريمة التزوير الإلكتروني

إن التقدم والتطور في المجالات التكنولوجيه في الحياة الخاصة والعامة واعتماد الناس عليها يقابله استغلال المجرمين لتلك التقنيات في ارتكاب جرائمهم، والقوانين الجزائية الحالية غير كافية لمواجهة الجرائم الإلكترونية بصورها المستحدثة، وذلك لأن النصوص العقابية غير كافية لتوفير الحماية لها، فهناك تشريعات كثيرة تعاني من قصور في تجريم هذه الجرائم بنصوص مستقلة وخاصة، وفي حالة تخصيص نصوص لها من المحتمل أن تعاني من الضيق وعدم استيعاب كافة أشكال التجريم الخاصة بهذه الجرائم.[115]

---

[114] المصري، نداء فايز نائل، خصوصية الجرائم المعلوماتية، رسالة ماجستير، جامعة النجاح الوطنية، نابلس، فلسطين، 2017، ص87.

[115] الجبوري، عمر عبد السلام، مرجع سابق، ص102.

الفرع الأول: مبدأ الاختصاص الإقليمي

يعد هذا المبدأ من المبادئ المستقرة في جميع دول العالم، كونه مرتبط بسيادة هذه الدول ارتباط وثيق ويعتبر من مظاهر سيادة الدول على إقليمها.[116]

ويقصد به أن الدولة وحدها في المختصة في العقاب على ما يقع من جرائم داخل إقليمها دون تدخل غيرها من الدول، فهو يقضي بتطبيق القانون الجنائي الوطني على كافة من تظلهم سماء الإقليم بغض النظر عن جنسيتهم أو معتقدهم أو مركزهم الاجتماعي، سواء كانوا مقيمين على أقليم الدولة أو وجدوا به عرضاً.[117]

وتأخذ غالبية التشريعات بهذا المبدأ، وتمنح الأولوية في تطبيق قواعد الاختصاص، وأخذ بهذا المبدأ التشريع الفرنسي في المادة (113) الفقرة(2) "يطبق القانون الفرنسي على الجرائم المرتكبة على أقليم الجمهورية، وتعتبر قد أرتكبت على أقليم الجمهورية، إذا كان أحد عناصر الجريمة قد أرتكب فيه أو وقع على هذا الإقليم".[118]

ونصت المادة الثانية من قانون الجرائم الإلكترونية إيضاً على "تطبق أحكام هذا القرار بقانون على أي من الجرائم المنصوص عليها فيه، إذا ارتكبا كليا أو جزئيا داخل فلسطين، سواء كان الفاعل أصليا، أو شريكا، أو متدخلا".[119]

والمشرع السوداني أخذ بهذا المبدأ كمبدأ أساسي لتطبيق القانون الجنائي، حيث نصت المادة (1) من القانون الجنائي لسنة 1991 على ما يلي"تسري أحكام هذا القانون على أي جريمة أرتكبت كلها أو بعضها في السودان".[120]

وفي القضاء الأمريكي في الولايات المتحدة الامريكية قرر في جرائم المراهنات والقمار عبر شبكات الانترنت لعام (1999) الاعتماد على مكان وقوع الجريمة، لا مكان تواجد الخادم أو المضيف، وفي القضاء الإنجليزي في بريطانيا نصت المواد (3-4) من قانون إساءة استخدام الحاسب الآلي نظر الدعوى في حال كان هناك ارتباط بين الواقعة وبريطانيا، وفي القضاء الفرنسي إيضاً سلك الاتجاه ذاته، منذ قضية اتحاد الطلبة اليهود ضد ياهو، وأقر القضاء الفرنسي

---

[116] الجبوري، عمر عبد السلام، مرجع سابق، ص103.

[117] على، حنان محمد حسن، مبدأ إقليمية القانون الجنائي في القانون والشريعة والإسلامية، رسالة ماجستير ، جامعة الخرطوم، السودان، 2008، ص7.

[118] المصري، نداء فايز، مرجع سابق، ص88.

[119] انظر المادة(2) من القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[120] على ، حنان محمد حسن، مرجع سابق، ص10.

اختصاصه في هذه الدعوى على الرغم من أن ياهو الفرنسي فرع لمركز رئيسي في الولايات المتحدة.[121]

أما بنسبة لتطبيق مبدأ الاختصاص الإقليمي على الجرائم الإلكترونية الحديثة، فيرى الباحث أنه من غير الممكن تطبيق مبدأ الاختصاص الإقليمي على جرائم التزوير الإلكتروني نتيجة الصعوبات التي يعاني منها تحديد مكان ارتكاب الجريمة وزمانها، ومع التطور والتقدم العلمي أصبح من الهام الخروج عن مبدأ الإقليمية، واللجوء لمبادئ أخرى تتناسب مع وضع هذا النوع من الجرائم.

الفرع الثاني: مبدأ الاختصاص الشخصي

وهذا المبدأ يقوم على أساس الرابطة الجنسية التي تربط الأفراد بدولتهم أينما تواجدوا، ومبرر ذلك الحفاظ على سمعة الدولة ومصلحتها وذلك بعدم ارتكاب أفرادها جرائم خطيرة في الخارج، حيث أن هذا يمس بسمعة الدولة في الخارج بشكل سيئ .[122]

وتم النص على هذا المبدأ في التشريع القطري في المادة (16) من قانون العقوبات القطري، حيث تشترط أن يكون الفعل معاقبا عليه بمقتضى قوانين البلد الذي أرتكب فيه، إلا أنه لم يتم النص عليها في القانون الأردني، واكتفى بأن الفعل معاقب عليه في القانون الأردني .[123]

ونصت المادة (7) من القانون الجنائي السوادني لسنة (1991) وينطبق مبدأ شخصية القانون الجنائي على الجرائم المنصوص عليها في قانون الجرائم المعلوماتية (2007)، كما ونصت المادة (3) من القانون المصري على "كل مصري ارتكب جريمة خارج القطر فعلا يعتبر جناية أو جنحة في هذا القانون يعاقب بمقتضى أحكامه إذا عاد إلى القطر وكان الفعل معاقبا عليه بمقتضى قانون البلد الذي ارتكب فيه ".اشترطت هذه المادة أن يكون مصري الجنسية وقد هرب من بلده، وأن يكون الفعل معاقبا عليه وفقا لقانون البلد الذي ارتكبت به الجريمة .[124]

أخذت التشريعات بهذا المبدأ، ويبرر هذا المبدأ بأن الدولة من الواجب عليها ضمان حسن سلوك رعاياها في الخارج، وذلك نتيجة عدم تسليم الدولة لرعاياها للدول الأخرى، وبدل من تسليمهم تقوم بمعاقبتهم، وأخذ القضاء الفرنسي بهذا المبدأ والولايات المتحدة الإمريكية إيضا أخذت به،

---

[121] المصري، نداء نائل ، مرجع سابق، ص89.
[122] المساعدة، أنور محمد صدقي، إشكالية الاختصاص في الجرائم الإلكترونية، المجلة الدولية للقانون، جامعة قطر ، المجلد2، العدد الرابع، 2018، ص11.
[123] المساعدة، أنور محمد صدقي، مرجع سابق، ص11.
[124] المصري، نداء فايز، مرجع سابق، ص90.

حيث قضت المحكمة في أحدى القضايا في ولاية نيويورك بتطبيق مبدأ الاختصاص الشخصي في جريمة انتهاك قانون المستهلك والدعاية الكاذبة، حول بيع المجلات عبر البريد الإلكتروني.[125]
مبدأ الشخصية يتعارض مع مبدأ أساسي وهو عدم معاقبة الشخص على الفعل ذاته مرتين، هذا من ناحية، من ناحية أخرى قد يجبر المتضرر على الانتقال إلى الدولة حيث ارتكب الفعل ليرفع الدعوى المدنية، وهذا يشكل إشكالية، فمن الواجب وجود قانون جنائي دولي لحلها.[126]
يعتمد هذا المبدأ بشكل رئيس على الجناة من حيث هويتهم وجنسيتهم، بالإضافة إلى أن محاكمة المجرمين في البلاد الأجنبية يتطلب إجراءات معقدة وطويلة، وتكاليف باهضة، ومعرفة الفاعل وهويته في جرائم التزوير الإلكتروني يكون صعباً، كونه يستخدم والإلغاز المعقدة والتشفير والأسماء المستعارة.

الفرع الثالث: مبدأ العينية

يقصد بهذا المبدأ سريان النصوص الجنائية الوطنية على جرائم معينة لو ارتكبت خارج البلاد، وذلك نظرا للخطورة التي تتمتع بها بعض الجرائم، بصرف النظر عن جنسية وصفة مرتكبها لارتباطها بمصالح الدولة العليا .[127]
اقر المشرع العراقي مبدأ العينية في نصوص مواده حيث نصت المادة 9 من القانون العراقي رقم 111 لسنة 1969 على أن (يسري هذا القانون على كل من يرتكب جريمة ماسة خارج العراق بأمن الدولة الداخلي والخارجي أو ضد الجمهورية...)، فهذه المادة لم تشترط الجنسية فيمن يرتكب جريمة واقعة على سلامة الدولة أو استقلالها السياسي في الخارج .[128]
واعتمد المشرع الاردني أيضا مبدأ العينية في المادة (9) حيث تنص على " تسري أحكام هذا القانون على كل أردني أو أجنبي _فاعلا أو شريكا أو محرضا _ارتكب خارج المملكة جناية أو جنحة مخلة بأمن الدولة أو قلد ختم الدولة أو قلد نقودا أو زور اوراق النقد أو السندات المصرفية الاردنية أو الاجنبية المتداولة قانونا أو تعاملا في المملكة".
ونص المشرع الفرنسي على مبدأ العينية في نص المادة 10\113 من قانون العقوبات الفرنسي الجديد، على أنه :"يطبق القانون الفرنسي، على كل الجنايات والجنح التي ترتكب في الخارج،

---

[125] المصري، نداء فايز، مرجع سابق، ص91.
[126] المصري، نداء فايز، مرجع سابق، ص91.
[127] أحمد، جمال زين العابدين، الاختصاص القضائي وإجراءات التحقيق في الجرائم الإلكترونية ، مجلة مستقبل العلوم الإجتماعية، العدد الرابع ، 2021، ص
[128] الجبوري، عمر عبد السلام حسين، مرجع سابق، ص107.

والتي تشكل اعتداء على المصالح الإساسية للأمة، وكذلك جرائم تقليد أختام الدولة وتزويرها، وتزييف العملة المعدنية أو الورقية أو السندات العامة، وعلى إية جناية أو جنحة ترتكب ضد أعضاء البعثات الدبلوماسية أو أماكنهم، أو القنصلية الفرنسية في الخارج ".[129]

ومن الممكن أن يتناسب مبدأ عينية النص مع الجرائم الإلكترونية، وخاصة في حالة كانت الجريمة التي تم ارتكابها تمس سيادة الدولة وكيانها، والتزوير الإلكتروني إذا كان يقع على مستندات رسمية تتعلق بأمن الدولة فهنا يطبق مبدأ العينية على جرائم التزوير الإلكتروني، كونه يتلاءم مع طبيعة هذه الجرائم على اعتبار أنها جرائم عابرة للحدود، إلا أن هناك من التشريعات كالتشريع الأردني حددت الجرائم التي ينطبق عليها مبدأ العينية.

الفرع الرابع: مبدأ العالمية

يسري القانون الجنائي كقاعدة عامة على إقليم الدولة، وهذه الضوابط لا تجدي نفعاً في حال ارتكاب الجريمة العالمية، وكون ملاحقة المجرمين في حال فرارهم إلى الدول الأخرى يشكل مساس بسيادة الدولة وانتهاك لمصالح المجتمع الدولي، وعدم مقدرة الدولة على ملاحقة الجناة أو عدم رغبتها في الملاحقة يتطلب الأمر هذا مد مجال الولاية القضائية وفقا لضوابط أخرى تسمح بمعاقبة الجاني، فامتداد الاختصاص القضائي يعتبر معالجة قانونية، كون المبادئ التقليدية غير كافية لمواجهة الجرائم العالمية.[130]

ونص على هذا المبدأ القانون الأردني في المادة (10) في الفقرة الرابعة منه على "تسري أحكام هذا القانون :

1.على كل أجنبي مقيم في المملكة الأردنية الهاشمية، فاعلاً أو شريكاً أو محرضاً أو متدخلاً ارتكب خارج المملكة الأردنية الهاشمية جناية أو جنحة يعاقب عليها الأردني إذا لم يكن استرداده قد طلب أو قبل .[131]

وأخذ المشرع العراقي بهذا المبدأ تحت عنوان الاختصاص الشامل حيث نصت المادة (13) على أنه "في غير الأحوال المنصوص عليها في المواد 9و10و11 تسري أحكام هذا القانون على كل

---

[129] المصري، نداء فايز نائل، مرجع سابق، ص92.

[130] حميدي، أميمة خديجة، إمكانية تفعيل مبدأ العالمية على الجريمة الإلكترونية، مجلة الحقوق والحريات، المجلد10، العدد01، 2022، ص1933.

[131] انظر المادة(10) من قانون العقوبات الأردني رقم (16) لسنة 1960.

من وجد في العراق بعد أن ارتكب في الخارج بوصفه فاعلا أو شريكا جريمة من الجرائم التالية:تخريب أو تعطيل وسائل المخابرات أو المواصلات الدولية...الخ".[132]

وهذا المبدأ يتناسب مع طبيعة الجريمة الإلكترونية، حيث أنه وفقاً لهذا للمبدأ هذا القانون الجنائي يطبق على كل جريمة يتم القبض على مرتكبها في اقليم الدولة أياً كانت جنسية الجناة أو مكان ارتكاب الجريمة، [133]ويعطي هذا المبدأ لقانون العقوبات مجالاً واسعاً يشمل العالم بإكمله، فلا يقيده جنسية مرتكب الجريمة ولا مكان ارتكابها ولا مساسها بالسيادة أو المصالح الوطنية، بل أنه يتطلب الأمر إلقاء القبض على الجناة في إقليم الدولة ليمنح القانون الجنائي الوطني الاختصاص .

ونتيجة طبيعة الجريمة الإلكترونية وخاصة جرائم التزوير الإلكتروني حيث أنها جرائم عابرة للحدود من ناحية، ومن ناحية أخرى هي جرائم خطيرة، هذا جعل مبدأ الإختصاص العالمي يتناسب مع هذا النوع من الجرائم .

المطلب الثاني: سلطة القاضي في قبول الدليل الإلكتروني

القاضي له الحق في تقدير البينات، وإصدار الإحكام القضائية فهو يلعب دوراً هاماً في مرحلة المحاكمة فهو مكلف بفحص الأدلة وبالخضوع لمبدأ حرية الإثبات، القاضي غير ملزم بالأخذ بما يقدم له من النيابة العامة من أدلة، ويتوجب على القاضي أن يتخذ جميع الإجراءات بهدف الكشف عن الحقيقة، [134] ولا بد أن يتمتع الدليل الإلكتروني بحجية أمام القضاء، ونأتي في هذا المطلب لبيان هذه الحجية .

الفرع الأول : حجية الدليل الإلكتروني أمام القضاء الجنائي

ويعد مبدأ حرية الإثبات من المبادئ الثابتة التي يقوم عليها الإثبات الجنائي، ويقصد بهذا أن الأطراف لهم الحق في اللجوء لكافة طرق الإثبات، لتدليل على صحة إدعاءاتهم وهذا ما جاء في نص المادة (237) من قانون الإجراءات الجزائية الفلسطيني حيث نصت على "تحكم المحكمة بالدعوى حسب قناعتها التي تكونت لديها بكامل حريتها....".[135]

يتوجب على القضاة أن يبذلوا كل ما بوسعهم من أجل الوصول إلى الحقيقة والكشف عن الجناة، وإتخاذ كافة الإجراءات لتأكد من مصداقية أي وسيلة إثبات تثار بغرض الكشف عن الحقيقة

---

[132] انظر المادة(13) من قانون العقوبات العراقي رقم 111 لسنة (1969).
[133] حميدي، أميمة خديجة، مرجع سابق، ص1935.
[134] زايد، محمود صبحي محمد محمود، حجية الدليل الإلكتروني في الإثبات الجنائي وسلطة القاضي في تقديره، مجلة بنها للعلوم الإنسانية، العدد1، الجزء2، 2022، ص39.
[135] انظر المادة(237) من قانون الإجراءات الجزائية الفلسطيني .

وتكوين عقيدة القاضي، ونتيجة طبيعة الدليل الإلكتروني المعقدة يجب التأكد من هذا الدليل قبل الأخذ به حتى ولو كان هذا الدليل مرئياً، لذلك يتوجب على القاضي من أجل الكشف عن الحقيقة الأخذ برأي أهل الخبرة في هذا المجال .[136]

حيث أن الأدلة الإلكترونية يمكن أن يشكك بها من ناحيتين هما :1.امكانية العبث بها لتصبح على هيئة مخالفة للحقيقة.2.وجود خطأ فني في الحصول على هذا النوع من الأدلة، مثل الخطأ في استعمال الأدوات المناسبة للحصول على الدليل، ويعود ذلك إلى الخلل في الشيفرة الوراثية، أو الخطأ في معالجة البيانات بشكل مخالف للطريقة الأصلية ويترتب عليه الخطأ في الحصول على الدليل .[137]

وعلى الرغم من القوة الإقناعية للأدلة الإلكترونية بسبب قيمته العلمية والفنية، إلا أنه يجب أن يخضع لإقتناع القاضي، [138]والدليل الإلكتروني في مختلف أشكاله محل للنقاش خلال جلسة المحاكمة، وذلك لا يحصل أثناء أعمال التحقيق الإبتدائي، بل خلال مجلس القضاء مباشرة كون حياد القاضي الجنائي يوجب عدم إقامة قضائه أو تقرير حكمه إلا على ما كان في مجلسه، وذلك يشمل الدليل الرقمي والإلكتروني المتولد عن الحاسبات الآلية، ويتضمن إيضاً كل الأدلة المرتبطة بالجريمة الإلكترونية.[139]

أما بنسبة لحجية البريد الإلكتروني عندما يقوم أي شخص بإرسال أي رسالة، فالشخص المستقبل يكون لديه توقيع رقمي، والمستقبل فقط هو الوحيد الذي يستطيع استخدامه وهذا الرسالة من المحتمل أن تكون فيديو تحويلات بنكية، وصوت، والتوقيعات الإلكترونية تستخدم في تأمين المعلومات من خلال إدخال أختام توقيت الارسال في الرسائل المشفرة، ففي حالة محاولة تزوير هذا التوقيع فيكون هذا التزوير من الممكن الكشف عنه .[140]

إن تقدير حجية المخرجات يعود إلى اختلاف نظم الإثبات في تقديرها، حيث أن حجية الدليل الإلكتروني لا تثير الجدل في الأنظمة اللاتينية(المصري، السوري، اللبناني، الأردني، الفرنسي)، وذلك نتيجة للسلطات التي تتمته بها القاضي في تقدير هذه الأدلة، حيث أن محكمة النقض الفرنسية قضت بأن(أشرطة التسجيل الممغنطة التي تكون لها قيمة دلائل الإثبات يمكن أن تكون

---

[136] زايد، محمود صبحي محمد، مرجع سابق، ص40.

[137] المصري، نداء نائل، مرجع سابق، ص96.

[138] زروق ، محمد، حجية الدليل الإلكتروني ومشروعيته أمام أمام القاضي الجنائي ، مجلة القانون والإعمال العدد37، 2018، ص55.

[139] أحمد عبد الحكيم عبد الرحمن شهاب، شروط قبول الأدلة الإلكترونية أمام القضاء الجنائي الفلسطيني، مجلة الجهاد للدراسات القانونية والاقتصادية، المجلد7، العدد2، 2018، ص178.

[140] المصري ، نداء فايز نائل، مرجع سابق، ص97.

صالحة للتقديم أمام القاضي الجنائي)، وهكذا بالنسبة لإلمانيا، وتركيا، ولكسمبورغ، اليونان، البرازيل، ، حيث أن المخرجات الإلكترونية تخضع لتقدير القاضي والمشرع .[141]

وفي التشريع السعودي يعتبر الدليل الإلكتروني أو الرقمي قرينة عادية يستأنس بها في الإثبات، وتحولت إلى قرينة قوية بعد صدور نظام التعاملات الإلكترونية لكن بشروط يحددها النظام تختلف عن الشروط يتطلبها الدليل التقليدي، ويؤكد هذا قرار الهيئة العامة للمحكمة العليا التي نصت فيه على أن "الدليل الرقمي حجية معتبرة في الإثبات متى سلم من العوارض، ويختلف قوة وضعفا حسب الواقعة وملابساتها وما يحتف بها من قرائن".[142]

وتمت المساواة بين الدليل التقليدي والديل الرقمي في الإثبات وذلك بإصدار نظام الإثبات الذي نص على المساواة بشكل صريح، وذلك وفق نص المادة الخامسة والعشرين حيث ورد نص أنه يكون للدليل الرقمي الرسمي الحجية المقررة للمحرر الرسمي إذا استوفى الشروط المنصوص عليها في الفقرة 1 من المادة 25 ويكون الدليل الرقمي حجة على الكافة إذا كان مثبتا على يد موظف عام أو شخص كلف بخدمة عامة وذلك في حدود سلطته وإختصاصه.[143]

وذهبت التشريعات الإمريكية إلى اعتماد الدليل الرقمي وأصالته في الإثبات حيث نصت المادة (3\1001) على أن "إذا كانت البيانات المخزنة في حاسب أو آلة مشابهة فأن أية مخرجات طابعة منها أو مخرجات مقرونة برؤية العين تبرز انعكاساً دقيقاً للبيانات تعد بيانات أصلية "، وإيضاً قرر المشرع الأمريكي "أن النسخة طبق الأصل لها نفس قيمة الإثبات للنسخة الأصلية.[144]

وبالنسبة لتشريعات الفلسطينية فقد حرصت على الأخذ بالأدلة الإلكترونية في القضاء الجنائي، وذلك من خلال قانون مكافحة الجرائم الإلكترونية، والمشرع يسمح باستخدام السندات والوسائل والسجلات الإلكترونية كحجية أمام القضاء وهو الذي يسهل إثبات حق الطرق الذي يرغب في الاحتجاج بها، ونصت المادة 37 من قانون مكافحة الجرائم الإلكترونية على "يعتبر الدليل الناتج بإي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو الشبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات".[145]

---

[141] المصري، نداء فايز نائل، مرجع سابق، ص98.

[142] عبد الجابر، زياد، حجية الدليل الرقمي في الإثبات، مجلة العلوم الإقتصادية والإدارية والقانونية، المجلد(6)، العدد(2)، 2022، ص141.

[143] عبد الجابر، زياد، مرجع سابق، ص141.

[144] محيي عبد العال، أسامة حسين، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية مجلة البحوث القانونية والإقتصادية، العدد(76)، 2021، ص688.

[145] انظر المادة(57) من قرار بقانون رقم(38) لسنة 2021 بتعديل قرار بقانون رقم(10) لسنة (2018).

يلاحظ من ذلك أن معظم التشريعات اتجهت إلى الأخذ بحجية الدليل الإلكتروني في الإثبات في القضاء الجنائي، إلا أن الأخذ بهذه الأدلة تحكمه عدة شروط وضوابط منها مبدأ افتراض البراءة وما يتفرع عن هذا المبدأ من آثار ونتائج، حيث يجب توافر شروط معينة في الدليل الإلكتروني حتى يتم استبعاد قرينة البراءة، ويجب على القاضي أن يصل إلى حد الجزم حتى يتم افتراض عكسها، كما يشترط أن تكون المخرجات الإلكترونية قد تمت مناقشتها وطرحها في الجلسة، فالقاضي لا يحكم بعلمه الشخصي إنما على الوقائع والأدلة التي ترد في ملف الدعوى، وعليه فأن شروط قبول المخرجات الإلكتروني في الإثبات تتجسد بالمشروعية واليقين والجزم والشفوية.[146] ويتفق الباحث مع توجه التشريعات بالأخذ بحجية الدليل الإلكتروني في الإثبات الجنائي، كون الجرائم ترتكب عن طريق الأنترنت فمن المهم أن يتم لجوء إلى الإثبات بهذه الأدلة .

الفرع الثاني: العقوبات المقررة لجريمة التزوير الإلكتروني

يتوجب علينا في البداية لتعرف على العقوبات المقررة لتزوير الإلكتروني الرجوع إلى الصيغ التشريعية التي جرمت التزوير، سواء عن طريق نصوص قانون العقوبات أو عن طريق نصوص خاصة، ونوضح فيما يلي العقوبات في التشريعات المقارنة والتشريع الفلسطينية.

عاقب التشريع المصري على التزوير الالإلكتروني بالحبس بغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مئة ألف جنيه أو بأحدى هاتين العقوبتين، وذلك في المادة(23) من قانون التوقيع الإلكتروني رقم (15) لسنة (2004) إلا أنه يجب مراعاة تطبيق العقوبة الأشد المنصوص عليها في قانون العقوبات أو أي قانون آخر.[147]

حيث نصت المادة (23) على "يعاقب بالحبس وبغرامة لا تقل على عشر آلاف جنيه ولا تتجاوز مئة ألف جنيه أو بأحدى هاتين العقوبتين كل من :

-أصدر شهادة تصديق إلكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة .

-أتلف أو عيب توقيعاً أو وسيطاً أو محرراً إلكترونياً أو زور شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحوير بإي طريق آخر .

-استعمل توقيعا أو وسيطا أو محررا إلكترونيا معيبا أو مزورا مع علمه بذلك .

-خالف أياً من أحكام المادتين (19)، (21) من هذا القانون .

---

[146] المصري، نداء فايز، مرجع سابق، ص100.

[147] غنيمي، وفاء غنيمي، عقوبة التزوير الإلكتروني، مجلة الزهراء، العدد الحادي والثلاثون، ص1481.

-توصل بأي وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني أو اخترق هذا الوسيط أو اعترضه أو عطله عن أداء وظيفته.[148]

وجعل هذا القانون العقوبة على جريمة التزوير الإلكتروني الحبس أو الغرامة أو التعويض أو الجمع بينهما أو التشهير وإلغاء التراخيص، وفي حالة التكرار يتم مضاعفة العقوبة .[149]

والتشريعات المصرية لم تضع نصوصا خاصة بتجريم التزوير الإلكتروني في قانون العقوبات بل كانت هناك بعض النصوص المتناثرة في القوانين وهذا يعتبر ضعف تشريعي، كما أن المشرع المصري لم ينص على الضرر في جريمة التزوير الإلكتروني وهو عنصر أساسي في عملية التزوير واكتفى بقول من زور أو عيب أو أتلف .

وفي التشريع الإماراتي تم تجريم بعض الجرائم المتصلة بتقنية المعلومات وجهاز الكمبيوتر في القانون الإتحادي الخاص، ومن الجرائم المتعلقة باستخدام الكمبيوتر جرم المشرع في المادة (4) فعل التوزير في مستند من مستندات الحكومة الإتحادية أو المحلية أو المؤسسات العامة الإتحادية والمحلية المعترف بها في نظام معلوماتي قانوناً، حيث تم تشديد العقوبة في هذا الحالة وهي السجن المؤقت، وإذا وقع التزوير في مستند غير صادر عن هذه الجهات يعاقب بالحبس والغرامة أو إحدى هاتين العقوبتين، وقد نصت المادة (4) على "يعاقب بالسجن المؤقت كل من زور مستنداً من مستندات الحكومة الإتحادية أو المحلية أو الهيئات أو المؤسسات العامة الإتحادية والمحلية معترفا به في نظام معلوماتي ".[150]

شدد المشرع الإماراتي العقوبة في حالة تزوير مستندات حكومية ذات طبيعة معلوماتية، رغبة منه في مكافحة هذا النوع من الجرائم التي تتسم بالخطورة، وذلك بالمقارنة مع الجرائم التي تقع على المستندات العادية كونه أي اعتداء على المستندات ينزع الثقة التي يتمتع بها وأنه يتمتع بالحجية التامة في العلمية الإثباتية، ولهذا المشرع الإماراتي شدد على مكافحة تلك الجرائم.[151]

وجرمت التشريعات الأردنية في قانون الجرائم الإلكترونية رقم (27) لسنة 2015 الإفعال التي لها علاقة بالجريمة الإلكترونية عن طريق إستخدام جهاز الحاسوب، حيث نصت المادة(4) على "يعاقب كل من أدخل أو نشر أو استخدم قصدا برنامجا عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير

---

148 انظر المادة (23) من قانون التوقيع الإلكتروني المصري لاقم(15) لسنة 2004.
149 غنيمي، وفاء غنيمي، مرجع سابق، ص1482.
150 انظر المادة(4) من قانون مكافحة جرائم تقنية المعلومات الإماراتي ، رقم2\2006.
151 الجبوري ، عمر عبد السلام، مرجع سابق، ص36.

أو نقل أو نسخ أو التقاط او تمكين الاخرين من الاطلاع على بيانات أو معلومات أو اعاقة أو تشويش أو ايقاف أو تعطيل عمل نظام معلومات أو الوصول إليه أو تغيير موقع الكتروني أو إلغائه أو اتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفة أو انتحال شخصية مالكه دون تصريح بالحبس مدة لا تقل على ثلاثة شهور وبغرامة لا تقل على 200 دينار أردني ولا تزيد على 1000 دينار".[152]

والقانون شدد في العقوبات على من ينشر أو يرسل عن طريق شبكة المعلومات أو أنظمة المعلومات عمدا كل ما هو مقروء أو مسموع أو مرئي ويشتمل عملا إباحي أو متعلقا بالاستغلال الجنسي من لم يتم الثامنة عشره من عمره بالحبس لمدة لا تقل على 3 شهور ولا تزيد عن سنة وبغرامة لا تقل على 300 دينار ولا تزيد على 5 آلاف دينار ".[153]

والتشريع الفلسطيني جرم التزوير الإلكتروني في القرار بقانون بشأن مكافحة الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، حيث نصت المادة(11) على"كل من زور مستنداً إلكترونياً رسميا من مستندات الدولة أو الهيئات أو المؤسسات العامة معترفا به قانونا في نظام معلوماتي، يعاقب بالسجن مدة لا تقل على خمس سنوات، وبغرامة لا تقل على ثلاثة الاف دينار أردني، ولا تزيد على خمسة الاف دينار اردني، أو ما يعادلها بالعملة المتداولة قانونا ".[154]

حيث نصت في هذا المادة على عقوبة التزوير الإلكتروني في المستندات الرسمية وشددت العقوبة عليها بالمقارنة مع عقوبة التزوير في المستندات غير رسمية حيث نصت الفقرة الثانية من ذات المادة على ما يلي"إذا وقع التزوير فيما عدا ذلك من المستندات، وكان من شأن ذلك إحداث الضرر، يعاقب بالحبس أو غرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونا، أو بكلتا العقوبتين."[155]

وتتفق التشريعات العربية مع التشريع الفلسطيني في أنها لم تضع نصوص خاصة في قانون العقوبات لتجريم التزوير الالكتروني أنما تم النص عليه في قوانين مستقلة كما أنها تشابهت في أنها عاقبت على التزوير في المستندات الرسمية بعقوبة أشد، وذلك حرصا منها على مكافحة هذا

---

[152] انظر المادة(4) من قانون الجرائم الإلكترونية الأردني رقم(27) لسنة 2015.

[153] الجبوري ، عبد السلام، مرجع سابق، ص37.

[154] انظر المادة(11) من القرار بقانون رقم(38) لسنة 2021 بتعديل قرار بقانون رقم(10) لسنة (2018) بشأن مكافحة الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات..

[155] انظر المادة(11) من القرار بقانون رقم(38) لسنة 2021 بتعديل قرار بقانون رقم(10) لسنة (2018) بشأن مكافحة الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

النوع من الجرائم الذي يمس الدولة ومصلحتها حيث تعتبر هذه الجرائم من أخطر الجرائم التي ترتكب.

كما وجرمت الفقرة الثالثة من ذات المادة التزوير في المستندات حيث نصت على"كل من استعمل المستند المزور مع علمه بتزويره يعاقب بالعقوبة المقررة لجريمة استعمال السند المزور وفق قانون العقوبات النافذ".[156]

وجرمت التشريعات الفلسطينية تزوير التواقيع الإلكترونية وذلك من خلال إتلافها أو تعييبها أو اصطناعها أو تحويرها، ونصت الفقرة (4) من ذات القانون على "كل من زور أو تلاعب بتوقيع أو أداة أو أنظمة توقيع إلكترونية رسمية، سواء تم ذلك باصطناعه أو إتلافه أو تعييبه أو تعديله أو تحويره، أو بإي طريقة أخرى تؤدي إلى تغيير الحقيقة في بياناته أو معلوماته، يعاقب بالسجن مدة لا تقل على خمس سنوات وبغرامة لا تقل على ثلاثة آلاف دينار أردني، ولا تزيد على خمس آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً."[157]

كما وعاقبت الفقرة الخامسة على تزوير في غير التواقيع الرسمية حيث نصت على "إذا وقع التزوير أو التلاعب فيما عدا ذلك من التواقيع الإلكترونية المذكورة في الفقرة (4) من هذه المادة، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانونا، أو بكلتا العقوبتين".[158]

ونلاحظ إيضا هنا أن المشرع الفلسطيني يشدد في العقوبة على التزوير في التواقيع الإلكترونية الرسمية حيث عاقب عليها بالحبس مدة لا تقل على خمس سنوات، وبغرامة لا تقل على ثلاث الاف دينار أردني ولا تزيد على خمس آلاف دينار أردني، مقارنة بالتزوير في التواقيع الغير رسمية حيث عاقب عليها بالحبس أو بغرامة لا تقل مائتي دينار أردني ولا تزيد على ألف دينار أردني، وذلك حرصا من المشرع على مكافحة هذا النوع من الجرائم الذي يمس مصلحة الدولة ويشكل اعتداء عليها.

---

156 انظر المادة(11) من القرار بقانون رقم(38) لسنة 2021 بتعديل قرار بقانون رقم(10) لسنة (2018) بشأن مكافحة الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

157 انظر المادة(11) من القرار بقانون رقم(38) لسنة 2021 بتعديل قرار بقانون رقم(10) لسنة (2018) بشأن مكافحة الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

158 انظر المادة(11) من القرار بقانون رقم(38) لسنة 2021 بتعديل قرار بقانون رقم(10) لسنة (2018) بشأن مكافحة الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

الفرع الثالث: مشروعية الدليل الإلكتروني

المشروعية يقصد بها "ضرورة اتفاق الإجراء مع القواعد القانونية والأنظمة الثابتة في وجدان المجتمع، ومشروعية الأدلة الجنائية غير مقتصرة على المطايقة مع القواعد القانونية بل يجب أن تراعي حقوق الإنسان وحرياته، وحسن الآداب التي استقر عليها المجتمع .[159]

ونص القانون الأساسي الفلسطيني على ضمان حقوق المتهم وحرياته الأساسية ملزمة وواجبة الاحترام وذلك بنص المادة(10)، ونصت المادة(17) على [160]"للمساكن حرمة لا يجوز مراقبتها إلا بناء على إذن قضائي مسبب ووفقاً لإحكام القانون، ويقع باطل كل ما يترتب على مخالفة نصوص هذه المادة، كما ونصت المادة (273) من قانون الإجراءات الجزائية على "تحكم المحكمة في الدعوى حسب القناعة التي تولدت لديها بكامل حريتها، ولا يجوز لها أن تبني حكمها على أي دليل لم يطرح في الجلسة أو تم التوصل إليه بطريق غير مشروع "، وحظر القانون كل مساس بحقوق الإنسان وحرياته من أعمال القبض والتفتيش إلا بأمر قضائي .

أن إجراءات الحصول على الأدلة المتعلقة في الجريمة الإلكترونية يجب أن يندرج تحت الإطار العام الذي نص عليه القانون الأساسي وقانون الإجراءات الجزائية، وكل دليل مستمد بطريقة غير مشروعة يقع باطل ويكون مخالف لنظام العام، فالإجراء الباطل يمتد بطلانه للإجراءات اللاحقة له .[161]

وفي بريطانيا الشرطة قامت بتركيب أجهزة تنصت على خط هاتف أحد الشاكيات بناء على موافقتها، والشاكية قامت بإجراء مكالمة هاتفية مع الشخص الذي تشك في ارتكابه للجريمة، وتم تسجيل المكالمات التي تضمنت مواضيع تدين المدين، والقاضي استبعد التسجيلات على أساس أنها شرك خداعي .[162]

وفي التشريع الفلسطيني نصت المادة (51) من قانون الإجراءات الجزائية الفلسطيني على "للنائب العام أو أحد مساعديه أن يضبط لدى مكاتب البرق أو البريد الخطابات والرسائل والجرائد والمطبوعات والطرود والبرقيات المتعلقة بالجريمة وشخص مرتكبها."فهذه المادة نصت على السماح لنائب العام بضبط الرسائل للحصول على دليل متعلق بالجريمة .[163]

---

[159] أحمد ، عبد الرحمن شهاب ، شروط قبول الأدلة الإلكترونية أمام القضاء الجنائي الفلسطيني، مجلى الإجتهاد للدراسات القانونية، المجلد(7)، العدد(2)، 2018، ص175.

[160] انظر المادة(17) من قانون الإجراءات الجزائية الفلسطيني رقم(3) لسنة(2001).

[161] أحمد، عبد الرحمن شهاب، مرجع سابق، ص176.

[162] محمد الزورق، حجية الدليل الإلكتروني وحجيته أمام القاضي الجنائي، مجلة القانون والأعمال، المجلد37، العدد37، 2018، ص58.

[163] انظر المادة(51) من قانون الاجراءات الجزائية الفلسطيني رقم(3) لسنة (2001).

ونصت المادة (34) من قانون الجرائم الالكترونية "1.لقاضي الصلح أن يأذن لنائب العام أو أحد مساعديه بمراقبة الاتصالات والمحادثات الالكترونية، وتسجيلها والتعامل معها للبحث عن دليل مادي متعلق بجناية أو جنحة معاقب عليها بالحبس مدة لا تقل عن سنة، لمدة (15) عام و قابلة للتجديد مرة واحدة بناء على توافر دلائل جدية .....".[164]

وفي اليابان أصدرت محكمة مقاطعة حكماً أقرت فيه مشروعية التنصت للبحث عن دليل، ويرى الفقه الياباني أن الدليل الجنائي الذي تم الحصول عليه بطرق مشروعة يجب أن مستبعد حيث أنه من الطرق غير مشروعة الغش والتدليس والخداع للحصول على الدليل الالكتروني .[165]

وقضت محكمة النقض الفلسطينية في قرار لها رقم 255\2021 واعتبرت فيه الدليل الالكتروني مقبولا بشرط أن يتم جمعه وتوضيحه وفقاً للإجراءات القانونية المحددة، حيث أظهر القرار أهمية الالتزام بالإجراءات الصحيحة لضمان قبول الدليل الإلكتروني.

---

[164] أنظر المادة(34) من قانون الجرائم الالكترونية الفلسطيني .

[165] محمد الزورق، مرجع سابق، ص58.

الخاتمة

تم الحديث في هذه الدراسة عن التزوير الإلكتروني، إحدى الجرائم الإلكترونية التي ترتكب بواسطة الأنترنت وتعد من أخطرها حيث تناولت في الفصل الأول الحديث عن ماهية هذه الجريمة وخصائصها وأنواعها، وفي الفصل الثاني تم التطرق إلى المواجهة التشريعية لهذه الجرائم والتصدي لها وبيان العقوبات المفروضة عليها في التشريع الفلسطيني والتشريعات الأخرى.

وتوصلت هذه الدراسة إلى مجموعة من النتائج والتوصيات:

1.التزوير الإلكتروني يعد من الجرائم المستحدثة التي ظهرت في الآونة الأخيرة، نتيجة التقدم العلمي والتكنولوجي كما أن التزوير الإلكتروني يشكل خطورة لصعوبة اكتشافه من قبل المحققين كونه لا يترك أي أثر مادي.

2.يتميز التزوير الالكتروني بمجموعة من الخصائص ميزته عن غيره من الجرائم منها أنه من الجرائم العابرة للحدود، وهنا تثار مشكلة الاختصاص المكاني .

3.أن التزوير في المستندات الالكترونية يحتاج إلى خبرة أكثر من التزوير في المستندات الورقية، بالتالي تكون صعوبة الكشف عنه أكبر وأكثر تعقيداً

4.أفردت التشريعات العربية قوانين مستقلة لمواجهة جرائم الأنترنت ومن ضمنها التزوير الإلكتروني ومن بينها التشريع الفلسطيني على العكس من التشريعات الأجنبية كالتشريع الفرنسي الذي نص على تجريمه في قانون العقوبات.

5.ضعف الخبرات الفنية والتقنية لدى الضابطة القضائية، للبحث والتقصي عن جرائم التزوير الإلكتروني، وعدم وجود أجهزة كافية تساعد في تتبع الجاني الإلكتروني.

6. جريمة التزوير الإلكتروني تتطلب بالاضافة إلى الأركان الأساسية، وجود ركن خاص. فالأركان الأساسية للتزوير الإلكتروني هي الركن المادي والمتمثل في تغيير الحقيقة، والركن المعنوي والمتمثل في اتجاه إرادة المتهم نحو ارتكاب جريمة التزوير. وبالإضافة إلى هذه الأركان، يتطلب التزوير الإلكتروني أيضًا إحداث ضرر من خلال هذا التزوير.

7.جرائم التزوير الإلكتروني تقع على بيئة افتراضية تعتمد على النبضات الإلكترونية وليس على الوثائق والمستندات المكتوبة، فهي تتم عن طريق الحاسب الآلي، كما أن بيانات الحاسب الآلي يمكن العبث بها وتغييرها في بضع لحظات.

8.شددت التشريعات الفلسطينية على عقوبة التزوير في المستندات الرسمية كونه يمس أمن الدولة، كما جرمت تزوير التوقيعات الإلكترونية وأفردت لها عقوبة خاصة في قانون الجرائم

الالكترونية وذلك وفقاً للمادة (11) من القرار بقانون بشأن الجرائم الالكترونية رقم (10) لسنة (2018).

التوصيات

1.إجراء تعديل على قرار بقانون رقم (10) لسنة (2018) المطبق بحيث يتم النص على تجريم التزوير الإلكتروني بشكل واضح ودقيق مع توضيح الأركان الأساسية لقيام جريمة التزوير الإلكتروني .

2.تشديد العقوبة على مرتكبي الجرائم الإلكترونية وخاصة التزوير الإلكتروني في المستندات الرسمية التي تخص الدولة والنص على ذلك في القرار بقانون بالإضافة الى توضيح الظروف المخففة في حال قيام جريمة التزوير الإلكتروني .

3.تفعيل دور الذكاء الاصطناعي في الكشف عن الجريمة الإلكترونية لما له من دور في الكشف عن الحقيقة والتوصل للجناة والعمل على تطوير هذه الآليات لاستخدامها في الكشف عن الجريمة

4.وضع معايير لمكافحة جريمة التزوير الإلكتروني يمكن اتباعها من قبل المؤسسات الأمنية وتقييم هذه المعايير باستمرار لضمان فعاليتها.

5.تعزيز التعاون بين الدول لتبادل المعلومات والخبرات في مجال مكافحة التزوير الإلكتروني .

قائمة المصادر والمراجع

القوانين

قانون مكافحة جرائم تقنية المعلومات الاماراتي رقم (2) لسنة 2006.

قانون التوقيع الإلكتروني المصري رقم (15) لسنة (2004).

قانون العقوبات الأردني رقم(16) لسنة (1960).

قانون العقوبات العراقي (111) لسنة (1969).

قانون البينات الفلسطيني رقم(4) لسنة 2001.

المادة (1) من قانون التوقيع الالكتروني والمعاملات الالكترونية العراقي رقم(78)، 2012.

القرارات القضائية

محكمة النقض، قرار رقم(401)، الصادر في تاريخ 5 يناير، 2021.

الكتب

أيمن، محمد الظاهر، الجرائم الالكترونية وإجراءاتها وطرق إثباتها، الطبعة الأولى، 2024.

ابراهيم، خالد ممدوح، فن التحقيق في الجرائم الالكترونية، دار الفكر الجامعي، 2009.

الرسائل العلمية

رسائل الدكتوارة

عزيزة، رابحي، الأسرار المعلوماتية وحمايتها الجزائية، رسالة دكتوراة، جامعة أبو بكر، بلقايد، تلمسان، 2018.

رسائل الماجستير

علي، حنان محمد حسن، مبدأ أقليمية القانون الجنائي في القانون والشريعة، رسالة ماجستير، جامعة الخرطوم، السودان، 2008.

المصري، نداء فايز نائل، خصوصية الجرائم المعلوماتية، رسالة الماجستير، جامعة النجاح الوطنية، نابلس، فلسطين، 2017.

عموري، أشرف أحمد مصطفى، التفتيش في الجرائم الإلكترونية، رسالة ماجستير، مقدمة لجامعة القدس، أبو ديس، فلسطين، 2018.

عوني، رمزي، المعاينة الجنائية ودورها في الإثبات الجنائي، رسالة ماجستير، جامعة النجاح الوطنية، نابلس، فلسطين، 2019.

الجبوري، عمر عبد السلام، جريمة التزوير الالكتروني في التشريع الاردني، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، 2017.

خليل، أحمد حمد حسن، جريمة التزوير في التشريع الفلسطيني، رسالة ماجستير، الجامعة الاسلامية، غزة، 2015.

رائدة، باديس، جريمة التزوير في المحررات الالكترونية، رسالة ماجستير، جامعة العربي بن مهيدي، الجزائر، 2017.

العفيفي، يوسف خليل، الجرائم الالكترونية في التشريع الفلسطيني، رسالة ماجستير، الجامعة الاسلامية، غزة، 2013.

الطاهر، برهوم، جرائم التزوير الالكتروني، رسالة ماجستير، جامعة العربي التبسي، ، التبسة، 2019.

علي، بلعيشة، الحماية الجنائية للمستند الالكتروني، رسالة ماجستير، جامعة عبد الحميد بن باديس مستغانم، قسم القانون العام، الجزائر، 2019.

مقالات المجلات

أحمد، عبد الرحمن شهاب، شروط قبول الأدلة الإلكترونية أمام القضاء الجنائي الفلسطيني، مجلى الإجتهاد للدراسات القانونية، المجلد(7)، العدد(2)، 2018.

العارضي، فرقد عبود، جريمة التزوير الالكتروني، مجلة الكوفة للعلوم القانونية والسياسية، موقع دار المنظومة، المجلد(5)، العدد(13).

غنيمي، وفاء، عقوبة التزوير الالكتروني، مجلة الزهراء، العدد الحادي والثلاثون، 2021.

عبد الجابر، زياد، حجية الدليل الرقمي، مجلة العلوم الإقتصادية والإدارية والقانونية، المجلد(6)، العدد(2)، 2022.

محيي، عبد العال، أسامة حسين، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية، مجلة البحوث القانونية والإقتصادية، العدد(76)، 2021.

أحمد، عبد الحكيم، عبد الرحمن شهاب، شروط قبول الأدلة الإلكترونية أمام القضاء الجنائي الفلسطيني، مجلة الجهاد للدراسات القانونية والإقتصادية، المجلد (7)، العدد 2، 2018.

زروق، محمد، حجية الدليل الإلكتروني ومشروعيته أمام القضاء الجنائي، مجلة القانون والأعمال، العدد(37)، 2018.

خليفة، فتيحة، مهداوي محمد صالح، مجلة الدراسات القانونية، المجلد(8)، العدد(2)، 2022.

زايد، محمود صبحي محمد، حجية الدليل الإلكتروني في الإثبات الجنائي وسلطة القاضي في تقديره، مجلة بنها للعلوم الإنسانية، العدد1، الجزء2، 2022.

حميدي، أميمة خديجة، امكانية تفعيل مبدأ العالمية على الجريمة الإلكترونية، مجلة الحقوق والحريات، المجلد(10)، العدد(1)، 2022.

احمد، جمال زين العابدين، الاختصاص القضائي واجراءات التحقيق في الجرائم الالكترونية، مجلة مستقبل للعلوم الاجتماعية، العدد الرابع، 2021.

المساعدة، أنور محمد صدقي، اشكالية الاختصاص في الجرائم الالكترونية، المجلة الدولية للقانون، جامعة قطر، المجلد2، العدد4، 2018.

طالب، لينداً، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، العدد(16)، 2017.

مصطفى، عبد الباقي، التحقيق في الجريمة وإثباتها في فلسطين، مجلة علوم الشريعة والقانون، المجلد(45)، العدد(4)، 2018.

المطيري، بندر صياح، جريمة التزوير الالكتروني، مجلة رماح للبحوث والدراسات، المجلد(88)، 2023.

نفطي، عبد العزيز، جريمة التزوير في بطاقات الإئتمان، مجلة العلوم السياسية والقانونية، جامعة الوادي، المجلد(13)، العدد(1)، 2022.

الحنيص، عبد الجبار، الحماية الجزائية لبطاقات الائتمان الممغنطة من التزوير، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد(24)، العدد الثاني، 2008.

مشري، راضية، جريمة تزوير التوقيع الالكتروني، حوليات جامعة قالمة للعلوم الاجتماعية والإنسانية، العدد(20)، جوان، 2017.

فريحة، حسين، الجرائم الالكترونية والانترنت، مجلة المعلوماتية، موقع دار المنظومة، العدد السادس والثلاثون، المجلد (36)، 2011.

بن يوسف، إدريس، أساليب التزوير وكشفها عن طريق عملية الاستكتاب، مجلة الملف، جامعة العربي التبسي، تبسة، كلية الحقوق، 2019.

الأبحاث المنشورة

الغالبي، رامي، أحمد كاظم جريمة تزوير التوقيع الالكتروني، بحث منشور.

بنعومر، زينب، جريمة تزوير المستندات الالكترونية، بحث منشور، المعهد العالي للقضاء، المملكة السعودية، 2009.

رحيمة، نمديلي، 25\مارس\2017، خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة، مركز جيل البحث العلمي.

السيراني، عبدالله، سعود، فاعلية الاساليب المستخدمة في اثبات جريمة التزوير، (جامعة نايف العربية للعلوم الأمنية)، الرياض، 2011.

المقابلات الشخصية

سفيان، موسى، حسن أبو زهيرة، 22\3\2024، رئيس نيابة مكافحة الجرائم الالكترونية، نيابة الجرائم الالكترونية، الساعة الواحدة ظهراً، مكتب رئيس نيابة مكافحة الجرائم.

Abstract

This thesis discusses electronic forgery, one of the most dangerous crimes committed through computers and the internet. The severity of this crime increases daily due to the significant advancements in technology and the pervasive use of computers and the internet, which have come to dominate various aspects of life. This study aims to explore the position of Palestinian legislation on this crime, examining its alignment with other legal frameworks. It also assesses whether the Palestinian legislator has successfully established penalties commensurate with the seriousness and severity of this crime, given that forgery crimes do not only affect specific sectors but also pose a threat to the social and economic order of the state.

Moreover, this thesis seeks to investigate and clarify the types of electronic forgery crimes, determine their scope, compare them with other legislations, and identify the shortcomings within Palestinian laws. The study also examines the role of procedural and substantive legal texts and their application to electronic forgery crimes. A descriptive, analytical, and comparative approach was employed to derive findings relevant to the subject of the study.

One of the key conclusions reached is that electronic forgery is a newly emerged crime resulting from scientific and technological advancements. In addition, electronic forgery poses significant risks due to the difficulty of detection by investigators, as it leaves no material trace.