جامعة العربي التبسي-تبسة-الجزائر
كلية الحقوق و العلوم السياسية
- قسم الحقوق -

مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر
تخصص قانون جنائي وعلوم جنائية
بعنوان

جـرائم الـتزويـر الإلـكتـروني

إعداد الطالبة:
رفيدة حفظ الله

إشراف الدكتور:
سـعـاد أجـعـود

الاسـم واللـقـب	الـرتبة الـعلميـة	الصفة في البحث
لاميـة شعبـان	استاذ محاضر - ب -	رئيســـــــا
سعـاد أجعـود	استاذ محاضر - أ -	مشرفـا ومقـررا
صـابرة شعنبي	استاذ محاضر - ب -	منـــاقشـــا

السنة الجامعية:2021/2020

"الكلية لا تتحمل أي مسؤولية

لما يرد في المذكرة من آراء"

بسم الله الرحمن الرحيم

مكية

سورة العلق

ايا تها ١٩

بسم الله الرحمن الرحيم

اقرا باسم ربك الذى خلق ﴿١﴾ خلق الانسان من
علق ﴿٢﴾ اقرا وربك الاكرم ﴿٣﴾ الذى علم بالقلم ﴿٤﴾
علم الانسان ما لم يعلم ﴿٥﴾ كلا ان الانسان ليطغى ﴿٦﴾

شكر وعرفان

شكرا لله تعالى الذي أعطاني القوة و القدرة على

إنجاز عملي المتواضع هذا .

أوجه شكري إلى أستاذتي **أجعود سعاد** لتكرمها

بالإشراف على هذا العمل .

كما أتوجه بالشكر لباقي أعضاء اللجنة الأستاذتين :

شعبان لامية ، و **شعنبي صابرة** أن منحاني من وقتهما الثمين

لمناقشة هذا العمل المتواضع

كما أتوجه بالشكر إلى الأستاذ دلول الطاهر

الذي علمني طيلة الخمس سنوات

كما أتوجه بالشكر إلى جميع طلبة

كلية الحقوق و العلوم السياسية

وشكرا

إهداء

الشكر لله أولا و أخيرا الذي وفقني لإتمام هذا العمل و أرشدني

إلى طريق العلم و النجاح و أهدي هذا العمل إلى :

روح والدي رحمة الله عليه اسأل الله تعالى أن يسكنه فسيح جناته

وإلى تلك المرأة الصبورة التي علمتني أن لا حاجة لي عند مخلوق

و أن الله معي دائما إلى أمي التي ستبقى لي فخرا طوال حياتي

فاللهم أحفظها لي .

وإلى إخوتي : تقي الدين و حسام و نور اليقين

وإلى أحبهم على قلبي أخي الصغير ضياء لطالما كان بجانبي وساعدني لإتمام

هذا العمل أسال الله أن يحفظهم و يوفقهم في حياتهم.

وشكرا لصديقاتي في الدراسة سارة و لبنى و هيبة و سلمى و رانيا

وإلى كل عزيز على قلبي .

رفيدة

قائمة المختصرات

الجريدة الرسمية	ج ر
قانون العقوبات الجزائري	ق ع ج
قانون الإجراءات الجزائية الجزائري	ق إ ج ج
دون طبعة	د ط
دون سنة نشر	د س ن
دون بلد النشر	د ب ن
الجزء	ج
صفحة	ص

مقدمة

أصبحت نظم المعالجة الآلية للمعطيات المتمثلة في الحواسيب و الشبكات المعلوماتية أكثر انتشارا في كل المجالات و القطاعات التي تعتمد عليها بشكل أساسي في عملها وذلك لتميزها بالسرعة و الدقة في تجميع المعلومات و تخزينها و معالجتها ومن ثم نقلها و تبادلها بين الأفراد و الشركات و المؤسسات المختلفة داخل الدولة الواحدة أو بين عدة دول.

لكن هذا النظام أضحى عرضة للاعتداء و إساءة استخدامه الشيء الذي استتبعه ظهور أنماط جديدة من الاعتداءات على المعلومات المخزنة في بيئة افتراضية ليس هذا فحسب، بل سهلت ارتكاب بعض الجرائم التقليدية فازدادت هذه المخاطر تفاقما في ظل البيئة الافتراضية التي تمثلها شبكة المعلومات مما أفرز نوعا جديدا من الجرائم لم يكن معهودا من قبل عرفت بالجرائم المعلوماتية أو الإلكترونية.

ومن بين هذه الجرائم جريمة **التزوير الإلكتروني**، والذي **يعني به** تزوير المستندات و البيانات الموجودة على جهاز الكمبيوتر، و تزوير المعلومات بحيث يتم وضع معلومات بديلة للمعلومات الحقيقية، وهذه الجريمة تحتاج إلى خبرة فنية عالية، و ترتكب من مجرم غير تقليدي يتسم بالذكاء و السلطة اتجاه النظام المعلوماتي.

حيث تبرز **أهمية موضوع** جريمة التزوير الإلكتروني في أنه يعد من الموضوعات الهامة الجديدة التي لا تزال بكرا و لم تنل حظها من البحث، حيث اقتصرت أغلب الدراسات المنشورة على البحث في الجريمة المعلوماتية بصفة عامة، دون التركيز على البحث في هذا الموضوع بصفة مستقلة، بالإضافة إلى حداثة التقنيات الحديثة التي يستخدمها المجرم في إتيان سلوك التزوير الإلكتروني، وصعوبة اكتشاف الجريمة، وهذا ما لا نجده في التزوير التقليدي الذي يستخدم فيه المجرم وسائل بسيطة و في المتناول مما يسهل اكتشافه.

ونظرا لهذه الأهمية، فقد دفعني **لاختيار** هذا الموضوع جملة من الدوافع الشخصية أي الذاتية المتمثلة في الرغبة البحثية لمعرفة مدى إمكانية انطباق نصوص التزوير التقليدية على التزوير في المجال الإلكتروني في التشريع الجزائري وما يثيره من إشكاليات يجب

معالجتها في هذا البحث، إضافة إلى ذلك قلة الدراسات و الأبحاث القانونية في التشريع الجزائري بخصوص هذا الموضوع، إضافة إلى ذلك هناك دوافع موضوعية وذلك نتيجة لأهميته كما سبقت الإشارة إليها حيث تزداد مشكلة التزوير الإلكتروني صعوبة و تعقيدا يوما بعد يوم بسبب تنوع الأساليب التقنية الجد مستحدثة و بصفة خاصة من طرف الكثير من المشتغلين في الإدارات الحكومية الإلكترونية، إضافة إلى حجم الأضرار أو الخسائر المادية منها و المعنوية الناجمة عن هذه الجرائم.

ونتيجة لحداثة جريمة التزوير الإلكتروني فقدت انجرت عنه مشكلات تتعلق بكل من الجانب الموضوعي من خلال إمكانية تطبيق نصوص قانون العقوبات المتعلق بجريمة التزوير التقليدية على هذا النوع من الجرائم و الجانب الإجرائي من خلال إمكانية تطبيق الأحكام الإجرائية المتعلقة بجريمة التزوير التقليدية على جريمة التزوير الإلكتروني سواء في جمع الأدلة أو طرق إثباتها.

لذلك يمكن طرح التساؤل التالي: كيف عالج المشرع الجزائري والتشريعات المقارنة أحكام جريمة التزوير الإلكتروني ؟.

وتندرج تحت هذه الإشكالية إشكاليات فرعية تتمثل في:

- ما المقصود بالتزوير الإلكتروني ؟ وهل يختلف عن التزوير التقليدي ؟.
- فما تتمثل خصائص جريمة التزوير الإلكتروني و صوره ؟.
- هل يمكن تطبيق القوانين المنظمة لجريمة التزوير التقليدي على هذه الجريمة ؟

وللإجابة على هذه الإشكالية و ما يندرج تحتها من إشكاليات فرعية فقد اتبعت كل من **المنهج** الوصفي من خلال وصف جريمة التزوير الإلكتروني، و المنهج التحليلي من خلال تحليل النصوص القانونية المنظمة لجريمة التزوير الإلكتروني، و المنهج المقارن من خلال المقارنة في بعض النقاط بين التشريعات المقارنة.

فالهدف من وراء طرح هاته الإشكاليات ومحاولة معالجتها هو:

- التعرف على مفهوم جريمة التزوير الإلكتروني و تمييزها عن جريمة التزوير التقليدية.

- التعرف على خصائص جريمة التزوير الإلكتروني وطرق ارتكابها.

- بيان مدى تلاءم العقوبة المقررة للتزوير التقليدي مع التزوير الإلكتروني.

- التعرف على الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني.

وباعتبار أن **الدراسات السابقة** عبارة عن جهود بحثية متخصصة النظرية منها و التطبيقية التي ترتبط بمشكلة أو موضوع البحث سواء كانت في شكل رسائل أو أبحاث علمية منشورة، فقد وجدت دراسات سابقة لهذا الموضوع و المتمثلة في:

- التزوير الإلكتروني، أطروحة مقدمة لنيل شهادة دكتوراه علوم في الحقوق من طرف الطالبة لامية مجدوب، تخصص قانون جنائي، كلية الحقوق، جامعة باجي مختار، عنابة، لسنة 2017، تناولت فيها الباحثة الجريمة الإلكترونية بصفة عامة و جريمة التزوير الإلكتروني بصفة خاصة.

- جرائم التزوير الإلكتروني، دراسة مقارنة، أطروحة مقدمة لنيل دكتوراه العلوم في العلوم الإسلامية من طرف الطالب حفصي عباس، تخصص شريعة و قانون، كلية العلوم الإنسانية و العلوم الإسلامية، جامعة وهران 1 أحمد بن بله، لسنة 2015، تناول فيها الباحث هذه الجريمة من المنظور الديني و القانوني.

- التزوير الإلكتروني، مذكرة ماستر مقدمة من طرف الطالبة دالي خلود، تخصص القانون الجنائي الأساسي و العدالة الجنائية، كلية الحقوق، جامعة باجي مختار، عنابة، لسنة 2016، تناولت فيها الطالبة ماهية جريمة التزوير الإلكتروني و الأحكام القانونية لجريمة التزوير الإلكتروني.

أما بالنسبة لموضوعي فقد اعتمدت فيه على دراسة جريمة التزوير الإلكتروني بصفة خاصة دون التطرق إلى الجرائم الإلكترونية الأخرى من خلال الأحكام الموضوعية لهذه الجريمة المتمثلة في المفهوم و الخصائص و الأركان و الجزاءات المقررة لها، إضافة إلى

الأحكام الإجرائية لجريمة التزوير الإلكتروني من خلال الإجراءات المتبعة لجمع الأدلة في هذه الجريمة و طرق إثباتها.

وكل موضوع تعترضه عدة **صعوبات** مما تعيق الباحث في إكمال موضع بحثه، ومن بين هذه الصعوبات التي اعترضت موضوع بحثي:

– قلة المراجع المتخصصة الجزائرية لأنني اعتمدت في معظم بحثي على مراجع متخصصة مشرقية.

– يضاف إلى ذلك ندرة الأحكام القضائية الجزائرية في الموضوع إذ لم أحصل على أي حكم في هذا الموضوع رغم أن الجزائر من الدول العربية السباقة و الرائدة في مجال محاربة الإجرام الإلكتروني.

وقد ارتأيت عرض هذا الموضوع في **خطة** ثنائية مكونة فصلين في كل فصل مبحثين بالنسبة للفصل الأول فقد تضمن الأحكام الموضوعية لجريمة التزوير الإلكتروني، مقسما إلى مبحثين، تناولت في المبحث الأول مفهوم التزوير الإلكتروني وفي المبحث الثاني أركان جريمة التزوير الإلكتروني و الجزاءات المقررة لها.

وأما بالنسبة للفصل الثاني فقد تضمن الأحكام الإجرائية لجريمة التزوير الإلكتروني، مقسما إلى مبحثين، تناولت في المبحث الأول إجراءات جمع الأدلة في التزوير الإلكتروني و في المبحث الثاني إثبات جرائم التزوير الإلكتروني.

الفصل الأول :

الأحكام الموضوعية
لجريمة التزوير الإلكتروني

تمهيد وتقسيم:

إن جريمة التزوير الإلكتروني من أخطر صور غش المعلوماتية نظرا للدور الهام والخطر الذي أصبح يقوم به الحاسب الآلي، والذي اقتحم كافة المجالات، اعتمادا على هذه الآلات الحاسوبية ولهذا ظهرت الحاجة لتشريعات تواكبها من حيث الوقاية والمكافحة، لمواجهة السلوك الإجرامي في استخدامها.

ولهذا فإن ماهية التزوير الإلكتروني تستلزم بيان مفهومه كنقطة انطلاقه، ومن ثم دراسة الخصائص المميزة لهذه الجريمة وصورها وأركانها والجزاءات المقررة لها، حيث سأقسم هذا الفصل إلى مبحثين، سأتناول في الأول مفهوم التزوير الإلكتروني في حين أتطرق في الثاني لأركانه جريمة التزوير الإلكتروني والجزاءات المقررة لها.

المبحث الأول: مفهوم التزوير الإلكتروني.

أمام تزايد فرص الأشخاص للعبث والتلاعب في معطيات الحاسوب بتعديلها أو تبديلها أو تحويلها أضحت جريمة التزوير الالكتروني أو ألمعلوماتي من أكثر الجرائم الالكترونية انتشارا، فلا تكاد تخلو جريمة من جرائم نظم المعلومات من شكل من أشكال التزوير، هذه الأخيرة تكون محلا للاعتداء بتغير حقيقتها بقصد الغش في مضمونها والذي من شأنه إحداث أضرار بالغير.

لذلك يستلزم لبيان مفهوم التزوير الإلكتروني التطرق إلى تعريفه وتمييزه عن غيره من المصطلحات المشابهة له(المطلب الأول) وبيان خصائصه (المطلب الثاني).

المطلب الأول: تعريف التزوير الالكتروني وتمييزه عن غيره من المصطلحات المشابهة.

أصبحت جريمة التزوير الالكتروني أو ألمعلوماتي من أكثر الجرائم الالكترونية ذيوعا وخطورة ناهيك عن تشعب هذه الجريمة في نطاق الجريمة المعلوماتية، لذلك يتوجب تحديد مدلول هذه الجريمة وهذا لا يتأتى إلا بالرجوع إلى التعريف اللغوي لمصطلحاتها ثم التعريف الفقهي أو الاصطلاحي لها وهذا ما سيتم تناوله في الفروع التالية:

الفرع الأول: تعريف التزوير الإلكتروني.

من خلال هذا الفرع سيتم تعريف التزوير الإلكتروني لغويا وفقهيا وقانونا:

أولا – التعريف اللغوي:

لفظ مشتق من كلمة مزور وهو الكذب والتلفيق وإدخال الباطل وهو معنى واسع شامل لكل صنوف الغش.[1]

[1] جلال محمد الزغبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة)، دار الثقافة للنشر والتوزيع،عمان،2010 ص156.

– **التزوير لغة:** أما عن المدلول اللغوي لمصطلح معلوماتي أو بالأحرى عبارة معلومة فهي مشتقة من مصطلح "العلم" في اللغة العربية وكذلك مصطلح "معلم" أي الأثر الذي يستدل به على الطريق.

ثانيا – التعريف الفقهي:

لقد اختلفت آراء فقهاء القانون الجنائي حول تحديد تعريف التزوير الإلكتروني أو المعلومات ومن بين أهم هذه التعاريف ما يلي:

– عرف التزوير الإلكتروني بأنه "أي تغيير للحقيقة يرد على مخرجات الحاسوب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريق الطباعة أو كانت مرسومة عن طريق الراسم ويستوي في المحرر الإلكتروني أن يكون مدونا باللغة العربية أو لغة أخرى لها دلالتها ". كما قد يتم في مخرجات ورقية شرط أن تكون محفوظة على دعامة، كبرنامج منسوخ على أسطوانة وشرط أن يكون المحرر الإلكتروني ذا أثر في إثبات حق أو أثر قانوني معين.[1]

– وعرف كذلك بأنه التزوير الذي يتم بوسيلة معلوماتية في محرر معلوماتي، أو بوسيلة إلكترونية في محرر إلكتروني، وذلك ضمن الجريمة المعلوماتية التي عرفت بأنها سلوكا غير مشروع، أو غير مصرح به، ويتعلق بالمعالجة الآلية للبيانات أو نقلها، أو إساءة استخدام الحاسب الآلي على نحو مقصود.

– وكما عرفه الفقه بأنه كل تغيير في الحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية وذلك بغية استعمالها، كما عرف بأنه تغيير الحقيقة بأي وسيلة كانت سواء كان في إحداث نتيجة معينة.[2]

[1] لامية مجدوب، التزوير الالكتروني، أطروحة مقدمة لنيل شهادة دكتوراه علوم في الحقوق، تخصص قانون جنائي جامعة باجي مختار، عنابة، 2017، ص 30 .

[2] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت في التشريعات العربية، الزقازيق، مصر، 2009، ص 50 .

إذن هذه تعريفات مختلفة ومتعددة للتزوير الإلكتروني فقد يكون التزوير الإلكتروني نسخا للأقراص أو الدخول غير المشروع للشبكة أو التعديل في البيانات وغيرها من الوسائل المتعددة. [1]

تجدر الإشارة إليه انه يجب التفرقة بين التزوير الذي يقع في المعطيات أو المعلومات أو البيانات والتلاعب أو التزوير الواقع على البرامج، فإذا كان من الممكن تصور ذلك في الحالة الأولى، فان تزوير برامج الحاسب الآلي وقاعدة البيانات بكل صورها لا تخضع لقواعد التزوير الإلكتروني موضوع هذه الدراسة بل تعد جريمة تقليد المصنف طبقا للأمر رقم 03-05 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة، وهذا نفس الاتجاه الذي سلكته معظم التشريعات العالمية وأكدته الاتفاقية الدولية التربص في الفقرة الأولى من المادة 10 منها التي نصت على أنه "تتمتع برامج الحاسب الآلي سواء كانت بلغة المصدر أو بلغة الآلة بالحماية باعتبارها أعمالا أدبية بموجب معاهدة برن 1971". [2]

ثالثا – التعريف القانوني:

اتجهت أغلب التشريعات إلى إدخال هذا النوع المستحدث من التزوير في دائرة التجريم والعقاب، وفقا لنصوص عامة تجرم هذا التزوير، ليمتد حكم هذه النصوص ليشمل التزوير الحاصل في كافة صور هذه المحررات كالقانون الفرنسي، بينما البعض الأخر منها جرم بعض الصور لتزوير المحررات الالكترونية كالقانون المصري.

وتطور القانون الفرنسي في مجال تجريم التزوير في المحررات الالكترونية باعتباره من أخطر صور الغش في نطاق المعلوماتية، بسبب خطورة الدور الذي يقوم به الحاسب الآلي في الوقت الحاضر وفي كل المجالات، فقد أصبحت تتم من خلاله عمليات هائلة ترتب آثار قانونية خطيرة. [3]

---

[1] زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2011، ص 88.

[2] المرجع نفسه، ص 982.

[3] عبد الله بلقاسم، " الطبيعة الخاصة لجريمة التزوير في المحررات الالكترونية "، مجلة الدراسات القانونية المقارنة، المجلد 06، العدد 02، 2020، تيزي وزو، ص 981.

كما نص المشرع الجزائري على جريمة تزوير المحررات في المواد 214 إلى229 من قانون العقوبات حيث قسم هذه الجريمة إلى ثلاثة أقسام، قسم خاص بتزوير المحررات الرسمية، قسم خاص بتزوير المحررات العرفية والتجارية أو المصرفية، وقسم أورد فيه تزوير بعض الوثائق الإدارية والشهادات.

من خلال مختلف التشريعات المقارنة، فالتزوير في المحررات الالكترونية يعتبر بصفة عامة تزوير المعلومات والبيانات الموجودة على جهاز الكمبيوتر وتزوير المعلومات والمحررات، بحيث يتم وضع معلومات بديلة للمعلومات الحقيقية، وبالتالي فان طبيعة ومضمون هذه الجرائم الماسة بالمحررات الالكترونية تختلف تماما عن جرائم المحررات الورقية، هذا ما دفع بالتشريعات والقوانين الحالية إلى إدخال في تشريعاتها مثل هذه الأنماط من الجرائم في مواجهتها ومكافحتها هذا النوع من السلوك الإجرامي في تقنية المعلومات، لأن القوانين الحالية غير كافية لمواجهة هذا النوع من الجرائم سواء في مجال التجريم أو العقاب.[1]

الفرع الثاني: تمييز التزوير الإلكتروني عن غيره من المصطلحات المشابهة.

انطلاقا من اشتباه جريمة التزوير تبعا للنصوص التقليدية واقترابها من جرائم أخرى كالنصب والاحتيال باعتبارها من جرائم الكذب، يطرح نفس الإشكال فيما يتعلق باشتباه التزوير الإلكتروني بغيره من الجرائم الإلكترونية كالاحتيال الالكتروني والغش ألمعلوماتي وعليه هل يوجد فروقا بين هذه المصطلحات أم أنها مترادفة تؤدي إلى نفس المعنى؟.

للإجابة على هذا التساؤل لا بد من التطرق إلى من التزوير التقليدي وكذلك الغش ألمعلوماتي والاحتيال الإلكتروني على النحو التالي:[2]

أولا – التمييز بين التزوير الإلكتروني وجريمة التزوير التقليدية.

حيث أن تزوير البيانات الكترونيا يكون بالدخول بطريقة مشروعة أو غير مشروعة على قاعدة البيانات الموجودة في نظم المعلومات وتعديل البيانات سواء بإلغاء بيانات

[1] عبد الرحمان فرزات، "المعلوماتية وقانون العقوبات الواقع والآفاق"، مجلة المحامون السورية، السنة 6، العدد05و06 أيار، حزيران، 2001، ص 643.

[2] دالي خلود، " التزوير الالكتروني "، مذكرة ماستر، تخصص القانون الجنائي الأساسي والعدالة الجنائية، جامعة باجي مختار، عنابة، 2016، ص 12.

موجودة بالفعل أو بإضافة بيانات لم تكن موجودة من قبل وبالتالي صعوبة القبض على مرتكبيها، أو تحديدها، وان تم تحديد الموقع المستخدم في عمليات التزوير، فمن الصعوبة تحديد مكان مستخدم الموقع، وهذا على عكس جريمة التزوير التقليدية، التي ترتكب بوسائل تقليدية.

ثانيا – التمييز بين التزوير الإلكتروني والاحتيال الإلكتروني (المعلوماتي).

تعرف هيئة الأمم المتحدة الاحتيال المعلوماتي بأنه " إدخال البيانات أو محوها أو تعديلها أو برامج الحاسوب أو التدخل المؤثر في معالجة البيانات التي تسبب خسارة اقتصادية أو فقد حيازة ملكية شخص آخر، بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص آخر ".

وبالتالي فإن جريمة التزوير الإلكتروني تشبه جريمة الاحتيال المعلوماتي، من حيث صور ارتكاب الجريمة في كل منهما (إدخال بيانات، محوها، تعديلها).

فمرتكبي الاحتيال المعلوماتي هم عادة أشخاص لديهم سلطة في التعامل مع المعلومات التي يحتويها النظام المعلوماتي، حتى أنه قد أطلق على التحايل المعلوماتي أنه جريمة داخلية إشارة إلى حدوثه داخل المؤسسة المجني عليها وبواسطة أحد المنتمين إليها.

ثالثا – التمييز بين جريمة التزوير الإلكتروني والغش الإلكتروني.

إن الغش الإلكتروني يستهدف الجانب المعنوي للحاسب الآلي، إذ يعد سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها، كما يؤكد بعض الفقه أن الغش الإلكتروني هو مرادف لجرائم الكمبيوتر بصفة عامة إشارة إلى المظاهر الإجرامية التي يتصور ارتكابها في البيئة الإلكترونية أو المضرة الإلكترونية.

كما أن مصطلح الغش الإلكتروني هو مصطلح واسع فضفاض إلى درجة أنه قد يشغل حيزا واسعا من الأنشطة بعضها قد يرتبط بالحاسب الآلي وعليه يظهر بأن جريمة التزوير

الإلكتروني هي صورة عن جرائم الغش المعلوماتي أو بالأحرى نموذج عنها. [1]

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، ط1، دار الثقافة، عمان، 2008، ص 148.

المطلب الثاني: خصائص جريمة التزوير الإلكتروني.

للجريمة الالكترونية خصائص تتميز بها عن غيرها من الجرائم، ولذلك من أجل محاولة وضع النصوص الملائمة لمكافحة هذا النوع من الجرائم المستحدثة التي رافقت التطور التقني والمعرفي الذي يمر به عالمنا المعاصر بفضل تطور الحاسب الالكتروني، وسوف يتم تناول هذه الخصائص بشيء من التفصيل على النحو التالي:

الفرع الأول: ارتكاب الجريمة في أي مرحلة من مراحل تشغيل النظام.

مرحلة الإدخال، مرحلة المعالجة، مرحلة : ترتكب جريمة التزوير الإلكتروني في أي مرحلة من مراحل المعالجة الآلية وهي الإخراج، فأثناء مرحلة الإدخال يستطيع الجاني إدخال معلومات غير صحيحة، أو إدخال الوثائق الصحيحة أو المعلومات المطلوبة، إذ أن إدخال معلومات غير صحيحة للاعتداد بها على أنها معلومات صحيحة، أو ترك معلومات ضرورية بهدف تغيير الحقيقة، أو إدراج أسماء أشخاص غير موجودين حقيقة، وهي صورة من صور التزوير المعنوي.[1]

أما أثناء مرحلة المعالجة فيمكن إدراج تعديلات عن طريق التلاعب في برنامج نظام المعلومات وأثناء مرحلة الإخراج يمكن تغيير النتائج التي تم إدخالها ومعالجتها بطريقة صحيحة للدخول إلى نظام المعالجة الآلية من أجل تغيير الحقيقة.

الفرع الثاني: انعدام الأثر المادي للتزوير الإلكتروني.

تعد جريمة التزوير الإلكتروني جريمة فنية غير ملموسة لا تظهر آثارها ذلك أنها تتم من خلال الوصول إلى المعلومات عن طريق النظام المعلوماتي وتغيير مضمونها.

حيث يتميز التزوير في المحرر الالكتروني بعدم ترك أثر مادي على المحرر المزور كما هو الحال في المحرر الورقي، حيث قد تظهر آثار التغيير بالإضافة أو الحذف باستخدام أدوات أو مواد كيميائية، بينما لا تظهر هذه الآثار في النوع الأول حيث تتم الجريمة من خلال الوصول إلى المعلومات وتغيير مضمونها، فهي جريمة فنية غير

[1] برهوم الطاهر، " جرائم التزوير الالكتروني "، مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، جامعة العربي التبسي، تبسة، 2019، ص 09.

ملموسة، وصعوبة اكتشاف وإثبات الجرائم الالكترونية راجع لعدة أسباب، منها وسيلة التنفيذ التي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد، ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، لأنها تتطلب الماما خاصا بتقنيات الكمبيوتر ونظم المعلومات، بالتالي يصعب العثور على دليل مادي للجريمة وذلك يعود أساسا أن المجرم المعلوماتي يستخدم في ارتكابه لهذا النوع من الجرائم، وسائل فنية وتقنية معقدة، وفي أقل فترة ممكنة أين يقوم فيها بمحو الدليل والتلاعب به.[1]

الفرع الثالث: جريمة عابرة للحدود الوطنية.

إن الاستخدام الغير شرعي للحاسوب اتصف بالعالمية أو بالعابر للحدود الوطنية حيث أن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية، والفضائيات والانترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمرا ممكنا وشائعا.

حيث أن أغلب الجرائم المعلوماتية، ومن بينها التزوير الإلكتروني عن بعد، أين يكون للجاني فيها في دولة ما، والمجني عليه في دولة أخرى.

هذه الطبيعة التي تتميز بها الجريمة المعلوماتية كونها جريمة عابرة للحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام. [2]

الفرع الرابع: جريمة فادحة الأضرار.

حيث أشارت معظم الدراسات أن الأضرار الناجمة عن الجرائم التقليدية خصوصا عندما أصبحت مختلف المؤسسات المالية والبنوك والشركات تعتمد الحواسيب في تسيير شؤونها.

[1] عبد الله بلقاسم، مرجع سابق، ص983.

[2] محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، 2005، ص 36 .

الفرع الخامس: يرتكبها مجرم إلكتروني.

يطلق على المجرم الذي يرتكب جريمة التزوير الإلكتروني، والتي تعتبر من الجرائم المعلوماتية، المجرم المعلوماتي، حيث يتسم هذا الأخير بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية (المجرم التقليدي).

الفرع السادس: تحتاج إلى خبرات فنية عالية.

حيث لا ترتكب جريمة التزوير الإلكتروني بطريقة غير مدروسة، وإنما تتطلب إلماما كافيا بمهارات ومعارف فنية، كالمعرفة التقنية بالحاسب. أي انه يحتاج إلى ارتكابها إلى خبراء على درجة عالية من التخصص الآلي، وكيفية تشغيله واستخدامه والكفاءة في استخدام الحاسب الآلي والإنترنت.[1]

المطلب الثالث: صور جريمة التزوير الإلكتروني.

إن جريمة التزوير من أكثر الجرائم خطورة وانتشارا في جميع المجالات سواء كان ذلك وفقا للقواعد التقليدية الجنائية للتزوير أو حتى في مفهومه الحديث أو ما يعرف بالتزوير في المجال الالكتروني خاصة بعد الانتشار الواسع للحاسبات الآلية والانترنت وحلولها محل الأوراق أو المحررات في كل الهيئات المؤسسات العامة منها والخاصة.

حيث يتخذ التزوير الإلكتروني أشكالا عديدة لا يمكن حصرها كونها تخضع للتطور وكذا القصد من ارتكابها، وسأذكر من خلال هذا المطلب أهم صورها.

الفرع الأول: تزوير التوقيع الإلكتروني.

أولا – تعريف التوقيع الالكتروني

1- تعريف التوقيع الإلكتروني في التشريعات الوطنية:

- الأردن: تعرف المادة الثانية من قانون المعاملات الإلكترونية رقم 85 لسنة 2001 التوقيع الإلكتروني بأنه: " البيانات التي تتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي أو أية وسيلة أخرى مماثلة

[1] نهلا عبد القادر المومني، المرجع السابق، ص 51.

في رسالة معلومات أو مضافة علها أو مرتبطة بها ولها طابع يسمح بتحديد هوية الشخص الذي وقعها و يميز عن غيره من أجل توقيعه وبغرض الموافقة على مضمونه". [1]

- **مصر**: طبقا لما ورد بالقانون رقم 15 لسنة 2004 الخاص بتنظيم التوقيع الإلكتروني وبإنشاء هيئة صناعة تكنولوجيا المعلومات (المادة 1 / ج) فإنه يقصد بالتوقيع الإلكتروني: "كل ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع مفرد يسمح بتحديد شخص الموقع ويميزه عن غيره".

- **البحرين**: تعرف المادة الأولى من قانون التجارة الإلكترونية لسنة 2002 التوقيع الإلكتروني أو بأنه "معلومات في شكل إلكتروني فتكون موجودة في سجل إلكتروني أو مثبتة أو مقترنة به منطقيا، ويمكن للموقع استعمالها لإثبات هويته".

2- تعريف التوقيع الإلكتروني في الفقه.

تعددت التعريفات الفقهية لمفهوم التوقيع الإلكتروني، حيث عرف البعض التوقيع الإلكتروني بأنه "مجموعة من الإجراءات والوسائل التي يتبع استخدامها، عن طريق الرموز أو الأرقام إخراج رسالة إلكترونية تتضمن علامة مميزة لصاحب الرسالة المنقولة إلكترونيا".

وعرف البعض الآخر بأنه "إشارات أو رموز أو حروف مرخص بها من الجهة المختصة باعتماد التوقيع، ومرتبطة ارتباطا وثيقا بالتصرف القانوني، تسمح بتمييز شخص صاحبها وتحديد هويته، ويعبر -دون غموض- عن رضائه بهذا التصرف القانوني". [2]

[1] القانون رقم 15- 04 المؤرخ في 11 ربيع الثاني عام 1436 الموافق للفاتح من فبراير سنة 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين .

[2] عيسى غسان ربضي، القواعد الخاصة بالتوقيع الإلكتروني، ط 2، دار الثقافة للنشر والتوزيع، عمان،2002، ص55، 56.

3- تعريف التوقيع الإلكتروني في قانون الأونسترال النموذجي للتواقيع الإلكترونية:

في المادة الثانية بأنه "بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات". [1]

4- تعريف التوقيع الإلكتروني في التشريع الجزائري:

تم تعريفه في الفصل الثاني من القانون المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني في المادة الثانية تحت عنوان التعاريف على أنه: "بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق".

ثانيا - تزوير التوقيع الإلكتروني:

إن تزوير التوقيع الإلكتروني يختلف كل الاختلاف عن تزوير التوقيع التقليدي، فتزوير التوقيع التقليدي يعني قيام أحد الأشخاص بتقليد توقيع شخص آخر مما يعني أن التوقيع ذاته مختلف عن التوقيع الخاص بصاحبه وذلك لأن التوقيع المقلد لا يمكن أن يكون بذات خواص التوقيع الأصلي وبالتالي لا يمكن أن يكون متماثل معه.

بينما في جريمة تزوير التوقيع الإلكتروني يقوم الشخص بالحصول على منظومة التوقيع الإلكتروني الخاصة بشخص آخر وقيامه باستخدامها في توقيع مستندات إلكترونية فهنا نجد أن التوقيع الإلكتروني سليم مثله مثلما لو كان مالك منظومة التوقيع قد قام بالتوقيع بواسطتها، وإنما المشكلة تكمن هنا أن التوقيع تم بواسطة شخص آخر تحصل على تلك المنظومة عن طريق التجسس الإلكتروني أو التلصص أو أيا كانت الطريقة.[2]

الفرع الثاني: تزوير بطاقة الائتمان.

أولا- تعريف بطاقة الائتمان:

عرفت البطاقة الائتمانية بأنها "بطاقة مستطيلة الشكل تحمل اسم المؤسسة المصدرة لها وشعارها وتوقيعها ورقمها واسم حاملها ورقم حسابه وتاريخ صلاحيتها ".

[1] رياض فتح الله بصلة، جرائم بطاقة الإئتمان، ط1، دارالشروق، القاهرة، 1995، ص 122 .
[2] قانون الأونسترال النموذجي للتواقيع الالكترونية الصادر سنة 2001.

وعرفت بأنها "بطاقة بلاستيكية صغيرة الحجم تصدرها البنوك وأن منشأة التمويل تمنح لأشخاص لهم حسابات مصرفية وهي من أشهر الخدمات المصرفية الحديثة ".

كما عرفت بأنها "بطاقة بلاستيكية مزودة بشريط ممغنط ضيق، والذي يستخدم كوسيلة للتحكم في الدخول أو للتفويض ببدء المعاملة، في العامة يجري تشفير البيانات في ثلاث قنوات أفقية على امتداد شريط ".[1]

ثانيا – تزوير بطاقة الائتمان:

إن تزوير البطاقة الائتمانية يتم بصورتين: كلية وجزئية.

فالتزوير الكلي إما بنسخ المعلومات لاستعمالها في إنشاء بطاقات، أو بالتشفير، ذلك أن الحصول على هذه الأرقام بات ممكنا من خلال برامج يتم التسويق لها من خال شبكة الإنترنت فيقوم الجاني بإدخال رقم بطاقة صحيحة فيتولى البرنامج بتوليد أرقام بطاقات ائتمانية قد تصل إلى مائة رقم لبطاقة صحيحة منسوبة لمؤسسة بنكية واحدة، ثم إدماجها في بطاقة مقلدة أو تضمينها.

أما التزوير الجزئي لبطاقة الائتمان فيتم بالحصول على بطاقة ائتمان بطريقة غير مشروعة تكون منتهية الصلاحية أو ملغاة فيقوم الجاني بالتخلص من بياناتها البارزة ثم يوضع بدلا منها بيانات جديدة عن طريق آلة، ثم تضمينها أرقام حسابات ثم سرقة المعلومات الخاصة بها بطريقة غير مشروعة، وتتم هذه السرقة أثناء القيام بعمليات الشراء التي تتيحها التجارة الإلكترونية حيث تتطلب هذه العملية ملئ النموذج الإلكتروني بمعلومات البطاقة الائتمانية وخاصة الرقم السري.[2]

الفرع الثالث: التزوير عن طريق البريد الإلكتروني.

أولا– تعريف البريد الإلكتروني:

1– القانون الأمريكي: عرَف البريد الإلكتروني في القانون الصادر عام 1986، على أنه: "وسيلة اتصال يتم بواسطتها نقل المراسلات الخاصة عبر شبكة خطوط تلفزيونية

[1] برهوم الطاهر، مرجع سابق، ص 15، 16.
[2] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية 2006، ص 54.

عامة أو خاصة، وغالبا يتم كتابة الرسالة على جهاز الكمبيوتر، ثم يتم إرسالها إلكترونيا إلى كمبيوتر مورد الخدمة الذي يتولى تخزينها لديه، حيث يتم إرسالها عبر نظام خطوط التليفون إلى كمبيوتر المرسل إليه"

2- القانون الفرنسي: وجاء في التشريع الفرنسي في القانون الصادر في 22 يونيو 2004 بأنه، " كل رسالة سواء كانت نصية، أو صوتية، أو مرفق بها صور أو أصوات، ويتم إرسالها عبر شبكة اتصالات عامة، وتخزن على أحد خوادم الشبكة أو في المعدات الطرفية للمرسل إليه ليتمكن هذا الأخير من استعادتها ".

3- القانون المصري: وفي القانون المصري بشأن تنظيم التوقيع الإلكتروني ورد خاليا من تعريف البريد الإلكتروني، إلا انه أمر بحجية المحررات الإلكترونية التي تكون عن طريق التراسل بوسيلة إلكترونية ومنها البريد الإلكتروني.

4- القانون الجزائري: وفي القانون الجزائري، تم التعرض للبريد الالكتروني من خلال القانون رقم 04/18 المتضمن للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، كما أقر بحجية التعاملات الالكترونية، سواء عن طريق تبادل أو تراسل أو تعاقد، وطبعا من ضمن الوسائل "البريد الالكتروني ".

ثانيا- التزوير عن طريق البريد الالكتروني.[1]

يجب أن يكون التزوير للحقيقة قد وقع في محرر مكتوب عن طريق البريد الالكتروني، أي محرر موجود من الأصل , ولا يهم اللغة التي كتب بها المحرر سواء كانت العربية أو أية لغة أجنبية، وفي جرائم المعلوماتية فان البيانات المخزنة آليا سواء في ذاكرة الحاسب أو في أسطوانات ممغنطة أو أشرطة أو برامج غير مقروءة، ولا يمكن للمعنى الذي تحمله أن ينتقل عن طريق البصر أو المشاهدة، لأنها تسجل على هيئة نبضات الكترونية مثبتة على دعامة بشكل يسمح للحاسب فقط بقراءتها فيتم بواسطة البريد الالكتروني الوصول إلى هذه البيانات المخزنة والتلاعب فيها.

[1] حفصي عباس، مرجع سابق، ص 125، 126 .

المبحث الثاني: أركان جريمة التزوير الالكتروني والجزاءات المقررة لها:

لكل جريمة أركان لقيامها قانونا مما يترتب عنها الجزاء لمرتكبها وبالتالي من خلال هذا المبحث:

تناولنا الأركان العامة لجريمة التزوير الالكتروني، والمتمثلة في الركن الشرعي، الركن المادي، الركن المعنوي (المطلب الأول).

كما تناولنا أهم الجزاءات التي أقرها المشرع الجزائري للاعتداء على أنظمة معطيات الحاسب الآلي على كل من الشخص الطبيعي، وكذا الشخص المعنوي (المطلب الثاني).

المطلب الأول: أركان جريمة التزوير الالكتروني.

لكي تقع جريمة التزوير الإلكتروني، يجب أن تقوم على ركن شرعي، وركنين أساسيين، ركن مادي، قوامه تغيير الحقيقة في محرر بإحدى الطرق التي حددها القانون، تغييرا من شأنه أن يسبب ضررا للغير، وثالثهما ركن معنوي، يتخذ صورة القصد الجنائي، ويتحقق بانصراف إرادة الجاني إلى تغيير الحقيقة في المحرر، واتجاه نيته إلى استعمال المحرر فيما زور من أجله.[1]

الفرع الأول: الركن الشرعي في جريمة التزوير الالكتروني.

الركن الشرعي للجريمة هو تطبيق مبدأ لا جريمة ولا عقوبة إلا بنص، معنى ذلك أنه للعقاب على الجريمة لابد أن يتطابق الفعل الإجرامي للجاني مع قاعدة قانون العقوبات على نحو من الدقة والوضوح بحيث لا يدع مجالا لاختلاف الرأي في مضمونه ومعناه.

[1] برهوم الطاهر، مرجع سابق، ص 15، 16.

أولا: جريمة التزوير في القانون الجزائري.

نص المشرع الجزائري على جريمة التزوير في المواد من 197 إلى 241 ق. ع والذي تناول فيها بالتنظيم أحكام وعقوبات التزوير في المحررات الرسمية أو العمومية، وكذلك المحررات العرفية أو التجارية أو المصرفية، وكذلك التزوير في بعض الوثائق الإدارية والشهادات.[1]

كما نص على أنه لقيام جريمة التزوير أن يكون تغيير الحقيقة في محرر، وهذا ما نصت عليه نصوص المواد 214 الى 229 ق.ع الجزائري التي تشير إلى حصول التزوير في المحررات العمومية أو الرسمية، أو في المحررات العرفية، أو التجارية، أو المصرفية أو في بعض الوثائق الإدارية والشهادات.

كما أن المشرع الجزائري قد حدد طرق التزوير، علي سبيل الحصر علي خلاف المشرع الفرنسي الذي لم يقوم بتحديد هذه الطرق، وإنما عاقب على التزوير الذي يحدث في محرر أيا كانت طريقة التزوير التي لجأ إليها الجاني، كذلك يتبين أن المشرع الجزائري بتناوله للتزوير في المحررات لم يتعرض بعد لمعالجته بنصوص قانونية أو إجراءات أخرى في نطاق المعالجة الآلية للبيانات مثل غيره من الجرائم المعلوماتية.

ثانيا: ضرورة تعديل النص التجريمي.

نأمل أن يشمل المشرع الجزائري هذه الجريمة (جريمة التزوير الإلكتروني) بتنظيم خاص استنادا إلى ما لها من أهمية وطبيعة خاصة تتعلق بالأسلوب الإجرامي المتبع في ارتكابها أو بالمحل الذي ترد عليه تلك الجرائم اقتداء بمشرعي الدول المتقدمة التي انتهجت سبيل النصوص والمواد المستقلة التي تعالج هذه الظاهرة الإجرامية من ناحية التنظيم والأحكام والإجراءات والعقاب فلقد أصدر المشرع الفرنسي قانون 5 يناير 1988 المعدل بقانون العقوبات الصادر سنة 1994، والذي يتعلق بالغش المعلوماتي وحدد الجرائم التي يمكن أن تتعرض لها المعلوماتية ومنها جريمة التزوير في الوثائق المعالجة آليا.[2]

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج 2، دار هومة، ط 14، الجزائر، 2013، ص 408.
[2] دالي خلود، مرجع سابق، ص 62 .

الفرع الثاني: الركن المادي في جريمة التزوير الإلكتروني.

يعد الركن المادي المظهر الخارجي للجريمة، فلا عقوبة على الأفعال المادية التي لا تقوم على أساس التطابق بينها وبين نصوص التجريم، كما أنه لا يعاقب على النوايا السيئة ما لم تظهر إلى الوجود أو العالم الخارجي، ويقصد بالركن المادي لجريمة التزوير في المحررات الالكترونية بأنه لا يعاقب على النوايا السيئة ما لم تظهر إلى الوجود أو العالم الخارجي، ويقصد بالركن المادي لجريمة التزوير في المحررات الالكترونية بأنه تحريف أو تغيير للحقيقة في محرر الكتروني أو تغيير للحقيقة في محرر الكتروني أو تغيير البيانات بما يخالف الحقيقة، ويكفي أن يكون تغيير الحقيقة جزئيا أو كليا، بالتالي لا يختلف الركن المادي في جريمة تزوير المحرر الالكتروني عن الركن المادي في جريمة تزوير المحرر التقليدي الورقي من حيث عناصره.

لذلك فان صور الركن المادي لجريمة التزوير الإلكتروني لا تخرج عن صور الركن المادي في التزوير التقليدي إلا أنه يختلف عنه من حيث محله والطرق التي يتم بها، فجوهر التزوير في كلاهما هو تغيير الحقيقة.

أولا: تغيير الحقيقة.

التزوير عبارة عن تغيير الحقيقة، فإذا كان المحرر لا يشتمل على شيء من الكذب، بل كان يتضمن أمور حقيقية، فلا تزوير ولا عقاب، ولو كان الذي حرره قد قصد تغيير الحقيقة والإضرار بالغير، وبمعنى آخر يقصد بتغيير الحقيقة، إنشاء حقيقة مخالفة أو تحريف حقيقة قائمة، فجوهر تغيير الحقيقة اذن الزيف والكذب.[1]

وينصب تغيير الحقيقة المحصورة من صور الركن المادي لجريمة التزوير الإلكتروني على المعلومات والبيانات مهما كانت طبيعتها سواء كانت صورا أو رموزا أو علامات وذلك باستخدام الحاسب الآلي.

كما قد ينصب التغيير للحقيقة على بيانات المستند المعلومات، وفي هذه الحالة نكون أمام إنشاء مستند معلوماتي جديد ومزور بطريق الاصطناع، مثل قيام الجاني بعمل

[1] دالي خلود، مرجع سابق، ص 62 .

بطاقة ائتمانية جديدة باسم مزور، وتحمل نفس بيانات البطاقة الأصلية، ونفس الرقم السري، ورقم الكود الخاص بها، مما يتاح للجاني التعامل بها عن طريق أجهزة الدفع الآلي للنقود، واستخراج الجاني بطاقة الرقم القومي الخاصة بشخص حقيقي مع استبدال الصورة الأصلية بصورة مزورة خاصة بالجاني.

ولقد عبر قانون العقوبات في المواد من(214-218) عن أن العلة في العقاب على التزوير هو تغيير الحقيقة في المحررات على نحو يزعزع الثقة في المحررات الرسمية، أو يؤدي للمساس بحقوق الأفراد، غير أنه لا يكفي لاعتبار الشخص مزورا أي يغير الحقيقة بطريقة ما، ولكن يجب أن يتم ذلك بطريقة من الطرق التي حددها القانون، وعلة ذلك هو حرص المشرع على حصر الدائرة التي تعتبر تغيير للحقيقة فيها تزويرا، حتى لا يصبح كل كذب مكتوب تزويرا. ولقد ورد النص على طرق التزوير في المواد (214) من قانون العقوبات.[1]

ثانيا: محل الجريمة (المحرر الإلكتروني).

المحرر أو السند الكتابي وفقا لمصطلح القانون الأردني هو محل جريمة التزوير الذي ينصب عليه الفعل أو النشاط الإجرامي المكون لجريمة التزوير والمتمثل في تغيير الحقيقة، وبالتالي يعتبر المحرر هو المال أو المصلحة التي يقع بارتكاب الجريمة عدوان لها، ويرمي القانون إلى حمايتها بالجزاء الجنائي، وهذه المصلحة هي في جريمة التزوير الثقة العامة في المظهر القانوني للمحررات التي يشملها القانون بحمايته.[2]

- هناك جانب من الفقه عرف المحرر الإلكتروني بأنه الدعامة أو الوعاء إن حمل فكرة، أو يمكن أن ينتج عنها دليلا على حق أو واقعه ذات آثار قانونية، والدعامة هي الأقراص الإلكترونية التي تسجل عليها المعلومات عن طريق مغنطتها بشكل يرمز إلى كتابة غير مرئية مدونة بلغة الآلة التي تعتمد على نظام التشفير.

- أما الجانب الآخر من الفقه، فقد عرف المحرر الإلكتروني بأنه معلومات تم إنشاؤها أو تخزينها أو استلامها بوسيلة إلكترونية أو ضوئية أو رقمية أو صوتية مادامت تتضمن

[1] فتيحة عمارة، " جريمة التزوير الالكتروني "،مجلة القانون والمجتمع، المجلد 07، العدد 01، السنة 2019 .
[2] عامر محمود الكسواني، التزوير المعلوماتي للعلامة التجارية، دار الثقافة للنشر والتوزيع، عمان، 2010، ص155.

إثبات واقعة أو تصرف قانوني محدد، ويتضمن توقيع إلكتروني ينسب هذه الواقعة أو التصرف لشخص محدد.

ثالثا: طرق التزوير الالكتروني.

هناك نوعان من التزوير (مادي، معنوي):

1- التزوير المادي:

يقصد بالتزوير المادي ما يترك أثرا ماديا على العبث في المحرر، وقد يتبين هذا الأثر بالحواس المجردة، وقد لا يتبين إلا بالاستعانة بالخبرة الفنية.[1]

حيث وردت في قانون العقوبات الجزائري على سبيل الحصر في المواد 214 و215، إذ نصت المادة 214 على صور التزوير المادي بقولها: "يعاقب بالسجن المؤبد كل قاض أو موظف أو قائم بوظيفة عمومية ارتكب تزويرا في المحررات العمومية أو الرسمية أثناء تأدية وظيفته ".

أ- **إما بوضع توقيعات مزورة:** ويقصد بوضع إمضاء مزور، توقيع الشخص بإمضاء غير إمضاءه، وليس له حق التوقيع بيه مثل إمضاء الجاني محررا باسم شخص أخر، أو باسم شخص خيالي.

وقد يقوم البعض بتزوير بعض المحررات الالكترونية، لاستخدامها في الاحتيال على الأشخاص في محاولة لإيهامهم بصحة هذه المحررات، وبذلك فإن في هذا واقعتين:

الأولى: واقعة التزوير في المحرر الالكتروني، والثانية هي واقعة الاحتيال والنصب بهذا التزوير لسلب ثروة الغير.

ب- التقليد في الكتابة: يراد بالتقليد محاكاة خط اليد، **أي** إنشاء محرر على مثال محرر آخر **مثل** أن تكون الكتابة متشابهة ولا يشترط في التقليد أن يكون متقنا، بل يكفي أن

[1] دالي خلود ، التزوير الإلكتروني ، مذكرة ماستر ، تخصص القانون الجنائي الأساسي و العدالة الجنائية ، جامعة باجي مختار ، عنابة ، 2016 ، ص88.

يكون على درجة من التشابه يحمل القارئ على الاعتقاد بأن المحرر قد صدر عن الشخص الذي قلدت كتابته.

ج- التغيير في الكتابة: مثل حذف جزء من المحرر أو شطب كلمة أو جملة منه أو إضافة شيء إليه.

د- الاصطناع: وهذا ما نصت عليه المادة 216 الفقرة 02 ق ع ج إذ يقوم الجاني بافتعال سند لنفسه. هناك فرق بين الاصطناع والتقليد ففي الأول لا يشترط التشابه بين خط المتهم وخط غيره عكس التقليد، وذلك لأنه يصنع محررا جديدا بكامله ' بينما التقليد يعالج جزء من المحرر.

2- التزوير المعنوي:

نصت عليه المادة 215 ق ع ج والمتعلقة بتزييف جوهر المحررات أو ظروفها بطريق الغش وكتابة اتفاقات خلاف التي دونت وأمليت من قبل الأطراف، وتقرير وقائع كاذبة بصورة وقائع صحيحة، والشهادة كذبا بوقائع غير معترف بها في صور وقائع معترف بها وإسقاط أو تغيير الإقرار عمدا.

رابعا: الضرر.

الضرر هو عنصر جوهري في جريمة التزوير، إذ لا يكفي اكتمال الركن المادي في هذه الجريمة تغيير الحقيقة في محرر، وأن يحدث هذا التغيير بإحدى الطرق التي بينها القانون، وإنما ينبغي أن يكون من شأنه أن يسبب ضررا للغير.[1]

ويقع الضرر بتمام التحريف المفتعل للحقيقة، ثم استخدام تلك الصورة الجديدة للحقيقة، سواء من قبل الفاعل أو حتى من قبل الغير، الذي يعتمد في بناء قراره على هذه الحقيقة المفتعلة بفعل الفاعل والتي يجهل زيفها.

[1] ايهاب فوزي السقا، مرجع سابق، ص 56.

وبالتالي فان بقاء الحقيقة المفتعلة المحرفة مخزنة في نطاق معالجة آلية للبيانات والمعلومات لا يعني عدم وجود الجريمة، ذلك أن تحقق الضرر أمر محتمل هنا، والمشرع لا يشترط لقيام المسؤولية تحقق الضرر بل احتمال تحققه يكفي. [1]

ثم إن تقنيات نظم المعلومات والاتصالات اليوم أتاحت مجالا واسعا، وبنت مجتمعا الكترونيا عاما يحتاج إلى انسياب كبير للمحررات الالكترونية بصورتها المخزنة على الشبكة أو نظم المعلومات، وبالتالي فان أمر وجود الضرر ممكن طالما وجد المحرر الالكتروني، والى حدود استعماله ووضعه الغاية المرجوة منه.

ويستوي أن يكون الضرر الذي يلحق المجني عليه من فعل التزوير ضرر مادي أو معنوي أو اجتماعي وقع فعلا أو على أقل تقدير ممكن الوقوع.

الفرع الثالث: الركن المعنوي في جريمة التزوير الالكتروني.

جرائم التزوير الالكتروني هي جرائم عمدية قوام ركن العمد فيها القصد الجنائي، ولذلك يلزم تواصل القصد الجنائي في صورتيه العامة والخاصة.

– فالقصد الجنائي العام يتطلب علم الجاني بكافة الأركان والعناصر القانونية الداخلة في نموذج جريمة التزوير واتجاه إرادته الى الفعل المكون للتزوير. [2]

فجريمة التزوير الالكتروني التي تتم عن طريق الحاسب الآلي يجب أن يكون فيها الجاني عالما بأنه يغير الحقيقة في المحرر المعلوماتي، وأن هذا التغير من شأنه إحداث ضرر محقق أو من المحتمل حدوثه، فلا مجال للتزوير إذا ثبت أن الجاني قد أهمل تحري الحقيقة فإذا أثبت أنه يجهل بأمر تزويره، أو أنه كان يجهل تحريره فينتفي القصد الجنائي. [3]

– أما القصد الجنائي الخاص فيتمثل في نية الجاني ويشترط توافرها لدى الجاني حتى يمكن مساءلته قانونا، حيث يتطلب المشرع الفرنسي في جريمة التزوير في المستندات

[1] جلال محمد الزغبي، أسامة أحمد المناعسة، مرجع سابق، ص 160.
[2] محمد علي العريان، مرجع ص 143.
[3] حفصي عباس، مرجع سابق، ص 78.

المعلوماتية قصد جنائي خاص يتمثل في اتجاه نية الجاني إلى إحداث ضرر سواء حقيقي أو احتمال حدوثه.

في حين أن قانون العقوبات الجزائري في مادته 394 مكرر 1 لا يتطلب توافر قصد لدى الجاني لكي تقوم جريمة التلاعب بالمعطيات إنما يكتفي بتوافر القصد العام فقط.[1]

في حين هناك بعض التشريعات تتطلب توافر قصد خاص في جريمة التلاعب بالمعطيات كقصد الإضرار بالغير، وقصد تحقيق ربح غير مشروع للجاني أو للغير مثل التشريع البرتغالي والفنلندي والتركي، إلا أن هذا كان محل انتقاد لأنه يؤدي إلى التضييق من نطاق تطبيق واستبعاد الحالات التي لا تتجه فيها نية الفاعل إلى تحقيق ذلك الربح.

المطلب الثاني: الجزاءات المقررة لجريمة التزوير الالكتروني.

أحدث المشرع الجزائري قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات (القانون 04 – 15) المؤرخ في 10 نوفمبر 2004 المتضمن تعديل قانون العقوبات.

لكن المشرع الجزائري ركز على الاعتداءات الماسة بالأنظمة المعلوماتية، وأغفل الاعتداءات الماسة بمنتوجات الإعلام الآلي والمتمثلة في التزوير الإلكتروني (الحذف، الإزالة، التعديل بطريق الغش) وهذا من خلال الفروع التالية:

الفرع الأول: بالنسبة للشخص الطبيعي.

أقر قانون العقوبات الجزائري في هذا القسم جزاءات على مرتكبي هذه الجرائم، وتتمثل في عقوبات أصلية (الحبس والغرامة)، وأخرى عقوبات تكميلية.

[1] محمد خليفة، مرجع سابق، ص 187.

أولا- العقوبات الأصلية:

وهي العقوبات التي يجوز للقاضي بعد ثبوت الإدانة أن يحكم بها دون أن تقترن بعقوبة أخرى، وقد تكون بدنية كالإعدام أو سالبة للحرية كالسجن والحبس، وإما أن تكون مالية كالغرامة وهي الواردة في المادة في المادة الخامسة من قانون العقوبات الجزائري.[1]

- نصت المادة 394 مكرر 1 على " كل من أخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال، أو عدل بطريق الغش المعطيات التي يتضمنها، بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 إلى 2.000.000 دج.

- كما تنص المادة 394 مكرر 2 ق ع ج على الاعتداء العمدي على المعطيات، حيث أنه طبقا لنص هذه المادة فالعقوبة المقررة للاعتداء العمدي على المعطيات الموجودة داخل النظام هي الحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500.000 دج إلى 2.000.000 دج، أما العقوبة المقررة لاستخدام المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية، وكذا حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة بالأنظمة المعلوماتية العقوبة المقررة هي الحبس من شهرين إلى ثلاث (3) سنوات، وغرامة من 1.000.000 دج إلى 5.000.000 دج.

ثانيا- العقوبات التكميلية:

وهي تلك العقوبات التي لا يجوز للقاضي أن يحكم بها مستقلة عن العقوبة الأصلية إلا إذا نص القانون على سبيل الحصر في المادة 9 ق ع ج.[2]

- حيث جاءت المادة 394 مقرر 6 من قانون العقوبات الجزائري بعقوبات تكميلية إلى جانب العقوبات الأصلية، حيث نصت على ما يلي: " مع الاحتفاظ بحقوق الغير حسن النية، يحكم مصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها ".

---

[1] انظر المادة 5 من الأمر رقم 66 – 155 المؤرخ في 1966/06/08 المعدل والمتمم المتضمن قانون العقوبات الجزائري، ج ر، عدد 49، المؤرخة في 11 يونيو 1966.

[2] انظر المادة 9، ق ع ج.

1- المصادرة:

المصادرة قد تكون عامة أو خاصة، فأما المصادرة الخاصة والتي نصت عليها المادة 15 من قانون العقوبات الجزائري (المصادرة هي الأيلولة النهائية، إلى الدولة أو مجموعة أموال معينة، أو ما يعادل قيمتها عند الاقتضاء)، وبالتالي فهي نزع ملكية مال معين من أموال المحكوم عليه، وإضافتها إلى ملكية الدولة، أما المصادرة العامة فهي نزع سائر أموال المحكوم عليه وإضافتها إلى ملكية الدولة، أما بالنسبة إلى المصادرة في جرائم المعطيات، فيبدو من خلال نص المادة 394 مكرر 6 السالفة الذكر بأنها عقوبة تكميلية وجوبية، إذ أنها لم تخير القاضي بين الحكم أو عدم الحكم بها، فليست له سلطة تقديرية في ذلك وإنما يجب عليه الحكم بها.

- شروط تطبيق المصادرة:

من خلال المادة 394 مكرر 6[1] فإن شروط تطبيق المصادرة كالتالي:

- أن يحكم على المتهم بالعقوبة الأصلية لإحدى الجرائم الواقعة على معطيات الحاسب الآلي، أي عقوبة الحبس والغرامة.

- أن تكون الأشياء التي يحكم بمصادرتها قد استخدمت في ارتكاب الجريمة.

- أن تكون الأشياء التي يحكم بمصادرتها مضبوطة فعلا وذلك بكونها تحت يد السلطة القضائية، سواء قدمها الجاني من تلقاء نفسه، أو ضبطتها الشرطة.

- يجب ألا تخل المصادرة بحقوق الغير حسنة النية، والغير هو كل أجنبي عن الجريمة تماما، ولم يكن قد أدين بوصفة فاعلا أو شريكا، وتثبت ملكيته للشيء المضبوط، ويعتبر حسن النية، لأنه لا يتوافر لديه قصد أو خطأ بالنسبة لها.

2- الغلق:

من خلال المادة 394 مكرر6 نجدها نصت على عقوبة الغلق، وتشمل عقوبة الغلق

[1] أنظر المادة 394 مكرر 6 من الأمر 66-155 المتعلق بقانون العقوبات المعدل والمتمم.

المواقع ومحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.

– المقصود بالمواقع التي استعملت في ارتكاب الجريمة، هي تلك المواقع التي تقدم خدمات تسمح بالدخول غير المصرح به لمختلف الأنظمة أو تسمح بالتلاعب بالمعطيات حيث هناك مواقع تقوم بتعليم كيفية تصميم المعطيات غير المشروعة وتوفرها وتنشرها وتتجر فيها.

– المقصود بالمحل أو مكان الاستغلال، وهو المكان الذي استعمله الجناة في ارتكاب جريمتهم وكان يحوي الأجهزة التي استعملت في عملية الدخول غير المصرح به أو في عملية التلاعب بالمعطيات أو في عملية التعامل في معطيات غير مشروعة.

ثالثا – الظروف المشددة:

تنص المادة 394 مكرر فقرة 2 و3 على ظروف تشدد به عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام، ويتحقق هذا الظرف عندما ينتج عن الدخول والبقاء إما بحذف أو تغيير المعطيات التي يحتويها النظام وإما بحذف أو تغيير المعطيات التي يحتويها النظام و إما تخريب نظام إشغال المنظومة.[1]

في الحالة الأولى تضاعف العقوبات المقررة في الفقرة الأولى من المادة 394 مكرر وفي الحالة الثانية تكون العقوبة الحبس من ستة أشهر إلى سنتين، والغرامة من 50000 إلى 150000دج.

وهذا الظرف المشدد هو ظرف مادي يكفي أن تقوم بينه وبين الجريمة الأساسية، وهي جريمة الدخول والبقاء غير المشروع علاقة سببية للقول بتوافره.

وتنص المادة 394 مكرر 3 على أن تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد.

وقد ركزت المادة السابقة على مؤسسة الدفاع الوطني نظرا لأهمية هذه المؤسسة ودورها في الحفاظ على سلامة التراب الوطني والأمن العام.

[1] أنظر المادة 394 مكرر من الأمر رقم 66-155 المتضمن قانون العقوبات، المعدل والمتمم.

– بالإضافة للمؤسسات الخاضعة للقانون العام.

– كذلك بالنسبة للشخص المعنوي، فإنه إذا ارتكب إحدى الجرائم السابقة على إحدى الجهات العامة فتضاعف الغرامة مرتين، إذ تضاعف إلى خمسين مرات عما هو مقرر على الشخص الطبيعي لأن الجريمة ارتكبت من شخص معنوي، ثم يضاعف ذلك إلى ضعفين لأن الجريمة ارتكبت ضد إحدى الجهات العامة، وبالتالي فمجموع ذلك هو مضاعفة الغرامة إلى عشرة أضعاف عما هو مقرر على الشخص العادي.

الفرع الثاني: بالنسبة للشخص المعنوي.

تقوم المسؤولية الجزائية للشخص المعنوي طبقا للمادة 12 من الاتفاقية الدولية للإجرام المعلوماتي، بحيث يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا، كما سأل عن الجريمة التامة أو الشروع فيها، كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أعضائه أو ممثليه.

بالإضافة إلى قيام المسؤولية الجزائية للشخص المعنوي، تقوم المسؤولية الجزائية في حق الأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة.

كما أن المشرع الجزائري قد أقر في التعديل الأخير لقانون العقوبات المسؤولية الجزائية للشخص المعنوي، وذلك في نص المادة 18 مكرر من القانون 15/04 المتضمن قانون العقوبات.

أولا– العقوبات الأصلية:

اعترف المشرع الجزائري بالمسؤولية الجنائية للشخص المعنوي وذلك في التعديل الذي أجري سنة 2004 على قانون العقوبات في المادة 18 مكرر.[1]

– العقوبات المقررة للشخص المعنوي في مواد الجنايات والجنح هي:

1– الغرامة: تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

[1] أنظر المادة 18 مكرر من الأمر رقم 66-155 المعدل والمتمم.

ثانيا – العقوبات التكميلية:

بالإضافة إلى العقوبات الأصلية المطبقة على الشخص المعنوي، قد أقر المشرع عقوبات تكميلية تطبق عليه، وقد أوردها في المادة 18 مكرر في الفقرة الثانية وهي:

– حل الشخص المعنوي.

– غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات.

– الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات.

– المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز خمس سنوات.

– المصادرة.

– نشر وتعليق حكم أو قرار الإدانة.

الوضع تحت الحراسة لمدة لا تتجاوز خمس سنوات.

عقوبة الاشتراك والشروع في الجريمة:

تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة 394 مكرر 5 بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية، ولم يخضعها لأحكام المادة 186 من قانون العقوبات المتعلقة بجمعية الأشرار، حيث تنص المادة 394 مكرر5 من قانون العقوبات على "كل من يشارك في مجموعة أو في اتفاق سالف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها.[1]

من خلال استقراء نص المادة أعلاه نجد أن المشرع الجزائري لم يخرج عن القواعد العامة لعقوبة الشريك حيث رصد لها نفس عقوبة الجريمة التامة ذلك أن جرائم الاعتداء على نظم المعالجة الآلية للمعلومات، أغلبها تتم في شكل جماعات، وإن كان لم يسبق بيت هاته المجموعة على ارتكاب هذه الجريمة، ولكن النتيجة الجرمية تبين اتفاق ضمني

[1] دالي خلود، مرجع سابق، ص 86 .

بين أفراد المجموعة، إذ أن هذه الجرائم لا تتطلب اجتماع حقيقي فيما بين شخصين أو أكثر وإنما يتصور الاتفاق الجنائي بمجرد انتقال كلمة السر من شخص إلى آخر، وإن لم يكن بينهما معرفة سابقة.

– لجريمة الاتفاق الجنائي في جرائم المعطيات ركنان ركن مادي، وركن معنوي هو القصد الجنائي.

بالنسبة للركن المادي فيتكون من ثلاث عناصر: فعل الاتفاق، وموضوع الاتفاق، وتعدد المتفقين، **ففعل الاتفاق** هو انعقاد إرادتين أو أكثر واجتماعهما على موضوع معين، والاتفاق بطبيعته له مظهر مادي ملموس إذ يفترض تعبير كل واحد من أطرافه عن إرادته بحيث يعلم بها زملائه في الاتفاق فيتحقق لهم أن كل واحد من أطرافه يعبر عن إرادته وبالتالي يتحقق لهم أن إرادتهم تسير في اتجاه واحد وتتلاقى عند موضوع معين. [1]

كما أن المادة 394 مكرر 5 فإن المشرع الجزائري يتطلب للعقاب على الاتفاق أن يكون مجسدا بفعل أو عدة أفعال مادية، والمتمثلة في الأعمال التحضيرية، كأن يقوم المتفقون باقتناء برامج خبيثة كالفيروسات أو برامج اختراق يتم من خلالها الدخول غير المشروع لأنظمة الحاسبات الآلية، أو اقتناء كتب تشرح كيفية القيام بتلك الجرائم، أما **موضوع الاتفاق** فهو أعمال التحضير والإعداد لتلك الجرائم المنصوص عليها في المواد 394 مكرر والخاصة بالدخول والبقاء غير المصرح بهما و394 مكرر1 والخاصة بالتلاعب بالمعطيات، والمادة 394 مكرر2 والخاصة بالتعامل في المعطيات غير المشروعة، حيث يكتسب الاتفاق صفته الجنائية ولو كانت الأعمال في ذاتها مشروعة.

أما بالنسبة للركن المعنوي فإن جريمة الاتفاق هي جريمة عمدية لابد لقيامها توافر القصد الجنائي العام الذي يقوم على العلم، والإرادة.

يقصد بالعلم أن يعلم كل عضو في الاتفاق بماهية الفعل أو الأفعال موضوع الاتفاق وبأنها غير مشروعة، ويترتب على ذلك أن من يجهل الغرض من الاتفاق، وهو ارتكاب جناية أو جنحة أو التحضير لهما لا يعد القصد الجنائي متوافر لديه أي أن انعدام

[1] محمد خليفة، الحماية الجنائية للحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الاسكندرية، 2007، ص 114 .

العلم بموضوع الاتفاق الجنائي لدى أحدهما يؤدي إلى عدم قيام جريمة الاتفاق الجنائي وبالتالي انتقاء مسؤوليتهما معا.

أما الإرادة فيجب أن تتوافر لشخصين على الأقل للدخول في الاتفاق، وأن يقوم كل واحد فيهم بالدور الذي سيعهد به إليه فلا بد أن تكون هذه الإرادة جادة، وإذا كانوا شخصين فإن انتفاء الإرادة الجادة لدى أحدهما ينفي الجريمة عن كليهما.[1]

– نصت المادة 30 من قانون العقوبات الجزائري على المحاولة، فنصت على " كل محاولة لارتكاب جناية تبتدئ بالشروع في تنفيذ الجناية أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أو يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى ولو لم يكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها ".

أما الشروع في الجنح لا يعاقب عليه، إلا بنص وبذلك نجد أن المشرع الجزائري، قد تبنى فكرة العقوبة على الشروع في ارتكاب الجنح الماسة بنظام المعالجة الآلية للمعطيات وذلك من أجل حماية هذا النظام.

في حين أن بعض التشريعات الأخرى بما فيها التشريع الفرنسي، قد أخرج جنحة الاتفاق الجنائي لتحضير جرائم ماسة بالأنظمة المعلوماتية من نطاق الشروع لأنها تعتبر أن في ذلك مساس بالنظرية العامة في القانون الجنائي، لأن التحضير للجرائم الذي يتم في إطار اتفاق أو مجموعة تشكل في حد ذاتها محاولة أو عمل تحضيري مما يؤدي إلى تبني فكرة الشروع في الشروع.[2]

[1] محمد خليفة، مرجع سابق، ص117 .

[2] خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، عين مليلة، 2010، ص130.

خلاصة الفصل الأول :

من خلال ما تم توضيحه في مفهوم التزوير الالكتروني، يتضح بأن المشرع الجزائري لم يطور النصوص الجنائية الخاصة بالتزوير حيث اكتفى بالتزوير التقليدي دون اعتماد التزوير الالكتروني على غرار التشريعات المقارنة.

كما أن الأحكام المتعلقة بالتزوير التقليدي في المادة 214 ق ع ج لا تنطبق على التزوير في المجال الإلكتروني، لاختلاف محل الجريمة في كلا الجريمتين.

أما بالنسبة لجريمة التلاعب بمعطيات الحاسب الآلي ومدى انطباقها على أحكام التزوير الالكتروني في التشريع الجزائري، سواء تم التلاعب بالمعلومات في شكل الإدخال أو التعديل أو الإزالة للمعلومات بغَض النظر عن نوعها، نعتقد بأنها تمثل صورة حقيقية أو مثلى للتزوير في البيئة الالكترونية ذلك أن التزوير قد يحدث سواء في مرحلة إدخال المعطيات أو المعلومات أو معالجتها أو استرجاعها أو حتى نقلها أو تبادلها بشكل الكتروني.

بالإضافة إلى أن القانون 15-04 المتعلق بالتوقيع والتصديق الالكترونيين لم يكفل الحماية اللازمة لهذا التوقيع من مخاطر التزوير أو التلاعب به.

الفصل الثاني:
الأحكام الإجرائية لجرائم التزوير الالكتروني

تمهيد وتقسيم:

في الفصل السابق تم التطرق للحماية الجنائية للمعاملات الإلكترونية من الجانب الموضوعي وهذا غير كافي لذلك وجب التطرق إلى الجوانب الإجرائية كذلك من خلال قانون الإجراءات الجزائية الذي ينظم ويضبط المتابعات الجزائية منذ ارتكاب الجريمة إلى غاية النطق في الحكم وهو ما يعرف بالدعوى العمومية، وعلى هذا الأساس سوف أطرق في هذا الفصل إلى خصوصية المتابعة الجزائية في التزوير الإلكتروني، حيث يتم تناول إجراءات جمع الأدلة في التزوير الإلكتروني (المبحث الأول) وإثبات جرائم التزوير الإلكتروني (المبحث الثاني) .

المبحث الأول: إجراءات جمع الأدلة في التزوير الإلكتروني.

أصبح الدليل الجنائي التقليدي لا يتفق بشكل عام مع طبيعة الجريمة الإلكترونية حتى يستطيع القاضي أن يبنى القناعة الكاملة في الإثبات، ولهذا ظهرت طائفة جديدة من الأدلة تتفق مع طبيعة الوسط الذي ارتكبت فيه الجريمة وهو الدليل الإلكتروني الذي يستطيع القاضي بموجبه أن يبني قناعته ويصدر قراره، فدلي التزوير يأتي من إثبات تغيير الحقيقة في المحرر الذي يقع عليه وتطبيق ذلك على الجريمة المعلوماتية فإنه يمكن أن نثبت بالأدلة التقنية الناتجة عن الوسائل التقنية، لذلك يتم دراسة الإجراءات التقليدية (المطلب الأول)، والإجراءات الحديثة (المطلب الثاني) .

المطلب الأول: الإجراءات التقليدية .

نظم المشرع كيفية استنباط الدليل عن طريق إجراءات تتبع وصولا إلى هذه الغاية، وأهم هذه الإجراءات كما بينها القانون، هي المعاينة والتفتيش، وضبط الأشياء، سماع الشهود وندب الخبراء، وهي تستخدم صفة عامة لجم الدليل في جميع الجرائم التقليدية منها والمستحدثة، إلا أن دورها يكون بين المد في الجرائم الأولى والجزر في الثانية، وهو ما سوف نلاحظه في الفروع المتقدمة من هذا المطلب .

الفرع الأول: الإجراءات المادية .

يقصد بالإجراءات المادية تلك القواعد الشكلية ذات الطابع المادي والتي تتم في الغالب عن نتائج مادية ملموسة أو محسوسة، وتتمثل هذه الإجراءات في المعاينة، التفتيش والضبط.

أولا: المعاينة:[1] عرف جانب من الفقه المعاينة بأنها: "رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة "، وهي إجراء يتطلب سرعة الانتقال إلى محل الواقعة الإجرامية لمباشرتها وذلك لإثبات حالته وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى فاعلها، وقد نص المشرع على المعاينة في مرحلة جمع الاستدلالات بموجب نصوص المواد 12، 16، 17، 18 من ق إ ج ج، وذلك في

[1] أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2015، ص135.

إطار حصر وضبط مهام الضبطية القضائية في الحالات العادية والاستثنائية المتمثلة في حالة التلبس والإنابة القضائية.

الأصل في المعاينة أنها إجراء من إجراءات التحقيق وهذا ما جاء بموجب نص المادة 79 من ق إ ج ج وتبعا لذلك ففي غير حالات التلبس التي نص عليها القانون يجب أن تقوم بها سلطات التحقيق بنفسها أو تندب لذلك ضباط الشرطة القضائية .

كما أن لقاضي الحكم إذا لم يقتنع بالنتائج التي تمخضت عنها المعاينة والتي قام بها الضبط القضائي أو جهات التحقيق، جاز له أن يأمر بمعاينة من تلقاء نفسه أو بناء على طلب أحد الخصوم .

1- كيفية إجراء المعاينة التقنية لمسرح الجريمة:

عند وقوع جريمة تزوير في المجال الإلكتروني يتعين الانتقال إلى مسرح الجريمة الذي يعد حجر الزاوية في التحقيق القضائي ومكمن الأدلة، على أن ما يميز مسرح الجريمة الإلكترونية على غرار التزوير أن له مسرحان:

- **مسرح تقليدي:** ويقع خارج بيئة الحاسوب والإنترنت، ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أية جريمة تقليدية، قد يترك فيها الجاني آثار عدة، كالبصمات وبعض متعلقاته الشخصية أو وسائط تخزين رقمية.[1]

- **مسرح افتراضي:** ويقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الانترنت، في ذاكرة الأقراص الصلبة الموجودة بداخله، فإذا كانت عملية الانتقال لمعاينة المسرح التقليدي تتم بطريقة محسوسة مادية فعلية فالأمر مختلف بالنسبة للبيئة الافتراضية، حيث يستطيع القائم بجمع الأدلة سواء كان قاضي التحقيق، أو ضابط الشرطة القضائية أن يقوم بالمعاينة وهو جالس في مكتبه من خلال الحاسوب الموجود في مكان عمله، كما يمكنه اللجوء إلى الخبرة القضائية، أو إلى مقهى الإنترنت أو مزودي خدمات الإنترنت لإجراء المعاينة ونتيجة لاختلاف مسرح الجريمة

[1] أشرف عبد القادر قنديل، مرجع سابق، ص 138 .

الإلكترونية عن غيره من الجرائم لكون هذا النوع من الجرائم يتميز بوجود الأدلة الإلكترونية ذات الطبيعة غير المرئية، لذلك ينبغي تعامل خاص معه ويكون ذلك من خلال إتباع عدة قواعد فنية قبل الانتقال إلى مسرح الجريمة الإلكترونية أبروها ما يلي:[1]

- توفير معلومات مسبقة عن مكان الجريمة .
- إعداد خريطة للموقع الذي يتم الإدارة عليه .
- إعداد فريق التفتيش من المتخصصين .
- الحصول على الاحتياجات الضرورية من أجهزة وبرامج للاستعانة بها في الفحص والتشغيل .
- تأمين التيار الكهربائي من الانقطاع المفاجئ .

ومن الإجراءات التي يتعين إتباعها عند إجراء المعاينة ما يلي:

- القيام بتصوير جهاز الحاسب الآلي الذي ترتكب عن طريق الجرائم.
- العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام، والآثار الإلكترونية التي يخلفها ولوج النظام أو التردد على الموقع بشبكة المعلومات، وبوجه خاص السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي يتم عن طريقه الولوج الى النظام أو الموقع أو الدخول معه في حوار.
- عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة وذلك قبل إجراء الاختبارات اللازمة للتيقن من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة.
- القيام بحفظ المستندات الخاصة بالإدخال وكذلك مخرجات الحاسوب الورقة ذات الصلة بالجريمة ورفع ما قد يوجد عليها من بصمات أو آثار مادية .
- ربط الأقراص الكومبيوترية التي ربما تحمل الأدلة، مع جهاز يمنع الكتابة أو التسجيل عليها مما يتيح للمحققين قراءة بياناتها من دون تغييرها .

[1] لامية مجدوب، مرجع سابق، ص 167.

- التحفظ على محتويات سلة المهملات، والقيام بفحص الأوراق والشرائط والأقراص الممغنطة المحطمة المتواجدة فيها، ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.

- الاستعانة بأهل الخبرة الفنية في المجال ألمعلوماتي كلما اقتضى الأمر ذلك.[1]

ثانيا: التفتيش:

التفتيش إجراء من إجراءات التحقيق يستهدف البحث عن الحقيقة في مستودع السر، لذلك يعتبر من أهم إجراءات التحقيق في كشف الحقيقة لأنه غالبا ما يسفر عن أدلة مادية تؤيد نسبة الجريمة إلى المتهم.

والتفتيش ليس غاية في حد ذاته، وإنما هو وسيلة لغاية تتمثل فيما يمكن الوصول من خلاله إلى أدلة مادية تسهم في بيان وظهور الحقيقة، حيث يساهم التفتيش داخل المنظومة المعلوماتية في ظهور حقيقة الجريمة الإلكترونية بصفة عامة والتزوير بصفة خاصة، ونظرا لصعوبة إجراء التفتيش في البيئة كون محله عبارة عن نظم الحاسوب والإنترنت، فقد حضه المشرع الجزائري بقواعد خاصة ورد ذكرها بنص المادة 05 من القانون 09-04 المؤرخ في 2009/08/05، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها إلى جانب القواعد العامة المتعلقة بالتفتيش الوارد ذكرها في قانون الإجراءات الجزائية.

أ- مدى قابلية مكونات وشبكات الحاسوب للتفتيش:

تتكون نظم الحاسوب من مكونات مادية ومكونات منطقية، كما أنه تربطه بغيره من الحاسبات شبكات اتصال بعدية على المستوى المحلي أو الدولي وللوقوف على مدى صلاحية مسح جرائم نظم الحاسوب للتفتيش لا بد من التفرقة بين ثلاث حالات هي:

- تفتيش المكونات المادية للحاسوب:

في الواقع أن تفتيش المكونات المادية للحاسوب بأوعيتها المختلفة بحثا عن شيء يتصل بجريمة إلكترونية وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، يدخل في نطاق التفتيش طالما تم وفقا للإجراءات القانونية المقررة، يمكن أن حكم تلك المكونات

[1] عبد الفتاح بيومي حجازي ، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دار النهضة العربية، القاهرة، مصر ، 2009، ص 587.

يتوقف على طبيعة المكان الموجود فيه، سواء من الأماكن العامة أو الأماكن الخاصة إذ أن لصفة المكان أهمية خاصة في مجال التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمة، فلا يجوز تفتيشها إلا في المجالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانونا في أغلب التشريعات الجنائية كالقانون المصري، أما بالنسبة للقانون الجزائري فقد ورد ذكره بموجب نص المادة 05 من القانون 09-04 التي تجيز تفتيش منظومة معلوماتية أو جزء منها 58أو منظومة تخزين معلوماتي في إطار قانون الإجراءات الجزائية، وبالرجوع إلى هذا الأخير نجده قد أورد قاعدة عامة بموجب نص المادة 81 منه التي تجيز التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة، كما تقرر المادة 64 من ذات القانون بعض الضمانات حيث تنص على أنه لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات مكتوب بخط يد صاحب الشأن، فإن كان يجيد الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه مع ذكر ذلك بالمحضر، وتطبق فضلا على ذلك أحكام المواد 44 إلى 47 من ق.إ.ج.ج .

غير أن المشرع أورد استثناء على هذه المادة بموجب القانون 06-22 المؤرخ في 2006/02/20 المعدل لقانون الإجراءات الجزائية، حيث استثنى تطبيق هذه الضمانات على طائفة من الجرائم المذكورة بنص المادة 47 فقرة 3 والمادة 47 مكرر من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات حيث أجاز إجراء التفتيش في كل محل سكني أو غير سكني وفي كل ساعة من النهار والليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص دون الإخلال بقواعد ضمان احترام السر المهني من قبل بعض الأشخاص كالمحامين والموثقين والأطباء ومقرات وسائل الإعلام والاتصال وهذا ما جاء ذكره في المادة 45 في فقرتها الأخيرة من ق.إ.ج.ج .[1]

أما عن مسألة تفتيش الأشخاص فقد ورد ذكرها ضمن أحكام قانون الجمارك بموجب نص المادة 42 منه في إطار التحقيق الجمركي، كما أنه يجوز تفتيش الشخص

[1] أحمد الشافعي، البطلان في قانون الاجراءات الجزائية، دراسة مقارنة، ط 4، دار هومة، الجزائر، 2005، ص 262 .

حالة القبض عليه في جناية أو جنحة متلبس بها أو تنفيذا لأمر القبض، كما يجوز تفتيش الشخص كإجراء مكمل لتفتيش المساكن كلما دعت مقتضيات إجرائية أو قامت دلائل قوية على حيازته أدلة تتعلق بجريمة التزوير الإلكتروني أما فيما يخص مسألة تفتيش الأنثى فلم يفرق المشرع الجزائري بين الجنسين، وقد جرى العرف أن يتم تفتيش الأنثى بواسطة الأنثى احتراما وحفاظا على عورتها وإلا ترتب على ذلك قيام المسؤولية الجنائية عن هتك العرض حسب ما جاء في نص المادة 335 من قانون العقوبات الجزائري.[1]

- تفتيش المكونات الغير مادية للحاسوب:

إن تفتيش المكونات الغير مادية للحاسبة الإلكترونية أثار خلافا كبيرا في الفقه بشأن جواز تفتيشها وكما يلي:

الرأي الأول: يرى جواز ضبط البيانات الإلكترونية بمختلف أشكالها، ويستند هذا الرأي في ذلك إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط (أي شيء) فإن ذلك يجب تفسيره بحيث يشمل بيانات الحاسبة المحسوسة وغير المحسوسة، لأن الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد كشف الحقيقة فان المفهوم يمتد ليشمل البيانات الإلكترونية بمختلف أشكالها.[2]

الرأي الثاني: على نقيض الرأي الأول يرى بعدم انطباق المفهوم المادي على بيانات الحاسبة غير المرئية أو غير الملموسة، ولذلك فإنه يقترح مواجهة هذا التصور التشريعي بالنص صراحة على تفتيش الحاسبة الإلكترونية لا بد أن يشمل (المواد المعالجة عن طريق الحاسبة الإلكترونية أو بيانات الحاسبة الإلكترونية).

الرأي الثالث: في مقابل الرأيين أعلاه فإن هذا الرأي قد نأى بنفسه عن البحث عما إذا كانت كلمة شيء تشمل البيانات المعنوية لمكونات الحاسبة الإلكترونية، أم لا، فذهب إلى أن النظرة في ذلك يجب أن تستند إلى الواقع العملي والذي يتطلب أن يقع الضبط على بيانات الحاسبة الإلكترونية إذا اتخذت شكلا ماديا.

---

[1] عبد الله أو هايبية، "شرح قانون الاجراءات الجزائية الجزائري"، التحري والتحقيق، دار هومة، الجزائر، 2005، ص262 .

[2] دالي خلود، مرجع سابق، ص 106.

أما عن موقف المشرع الجزائري فقد حذا حذو التشريعات السابقة إذ اقر تفتيش المعطيات المعلوماتية بموجب نص المادة 05 من القانون 09-04 التي تحيز تفتيش المنظومة المعلوماتية، وفي هذا الصدد صرحت الاتفاقية الأوروبية في شأن جرائم تقنية المعلومات بحق الدول الأعضاء في تفتيش النظم المعلوماتية في إطار القوانين الجزائية وذلك من خلال نص الفقرة الأولى من المادة 19 من القسم الرابع لها.[1]

أما فيما يخص الإشكال حول مدى مشروعية تفتيش وضبط المراسلات أو الاتصالات الإلكترونية، فيتضح أن المشرع الجزائري قد تنبه إلى هذه المسألة بمعنى عدم جدوى الأساليب التقليدية في البحث والتحري والتحقيق، حيث استحدث إجراءات جديدة ألا وهي اعتراض المراسلات وتسجيل الأصوات والتقاط الصور وذلك بموجب نص المادة 65 مكرر 5 بمناسبة تعديل قانون الإجراءات الجزائية بموجب القانون 6-22 السالف الذكر وفقا لضمانات موضوعية وإجرائية خاصة لضمان عدم المساس بحرمة الحياة الخاصة.

- تفتيش شبكات الحاسب:

تعد هذه المسألة من المشكلات العالقة التي تواجه اجراء التفتيش نتيجة لطبيعة التكنولوجيا الرقمية، التي تعمل على توزيع المعلومات المحتوية على أدلة عبر شبكات حاسوبية في أماكن مجهولة بعيدة كليا عن الموقع المادي للتفتيش، فقد يكون الموقع الفعلي للبيانات داخل اختصاص فضائي آخر أو حتى في بلد أجنبي، وعليه فهل يمتد تفتيش الحاسوب إلى الأجهزة المرتبطة به سواء داخل الإقليم أو خارجه ؟

للإجابة على هذا الإشكال علينا التفرقة بين الفرضيتين الآتيتين:

1- اتصال حاسب المتهم بحاسب آخر موجود في مكان آخر داخل إقليم الدولة:

لا تزال هذه المسألة عالقة في بعض القوانين الإجرائية العربية كمصر وسوريا ولبنان، في حين وجدت الكثير من التشريعات حلا لها كالتشريع الأمريكي والفرنسي، وكذلك الجزائري حيث أجاب القانون 09-04 على هذه المسألة بموجب المادة 05 في فقرتها الثانية، التي أقرت أنه اذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات

[1] لقد عرف المشرع الجزائري الاتصالات الإلكترونية بموجب نص المادة 02 الفقرة (و) من القانون 04 تحت عنوان مصطلحات بأنها: "تراسل أو استقبال علامات أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أية وسيلة إلكترونية ".

المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الولوج اليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة بعد إعلام السلطة القضائية المختصة مسبقا بذلك.[1]

2- اتصال حاسب المتهم بحاسب آخر موجود خارج الدولة:

قد يقوم الجناة بتخزين بياناتهم في أنظمة تقنية خارج الدولة التي يقيمون فيها، مستخدمين في ذلك شبكة الاتصال البعدية بغية إخفاء جرائمهم أو إعاقة التحقيق بشأنها أو عرقلة الوصول إلى الدليل التقني الخاص بها، أما عن موقف المشرع الجزائري من مسألة التفتيش عن بعد، فقد تدارك الأمر بموجب دائما نص المادة 5 في فقرتها الثالثة من القانون 09-04 وذلك بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية وفقا لمبدأ المعاملة بالمثل مقتديا بذلك بالمشرع الفرنسي.

ب- شروط التفتيش في البيئة الإلكترونية:

يقوم إجراء التفتيش على جملة من الشروط والضمانات بهدف تحقيق الموازنة بين مصلحة المجتمع في العقاب وضمان حقوق الأفراد وحرياتهم، وعليه فيما تتمثل هذه الشروط في:

- الشروط الموضوعية للتفتيش:

يقصد بها تلك الضوابط اللازمة لإجراء تفتيش صحيح في البيئة الإلكترونية وهي سابقة له عادة، ويمكن حصرها في النقاط التالية:

1- سبب التفتيش في البيئة الإلكترونية:

يتمثل سبب التفتيش في السعي نحو الحصول على دليل ضمن تحقيق قائم، من أجل الوصول إلى حقيقة الحدث ويتحقق هذا السبب بوقوع جريمة إلكترونية بالفعل، سواء كانت جناية أو جنحة مثل جريمة التزوير الإلكتروني أو التلاعب بالمعطيات، وهي الجنحة المقررة بموجب المادة 394 مكرر 1 من قانون العقوبات الجزائري، وكذلك اتهام

[1] لامية مجدوب، " إجراء التفتيش في التزوير الإلكتروني "، مجلة التواصل في الاقتصاد والإدارة والقانون، المجلد25 العدد 03، 2019، عنابة، ص 113.

شخص أو أشخاص معينين بارتكاب هذه الجريمة، أو المشاركة فيها ومثال ذلك ارتباط عنوان إنترنت بروتوكول الخاص بجهاز الحاسوب الذي يحتوي على صور وبيانات مزورة، برقم حساب المتهم لدى مزود الخدمات ووجود رقمين للهاتف لديه يستخدمان في ذلك، يتحقق سبب التفتيش أيضا يتوافر أمارات قوية أو قرائن على وجود بيانات أو معدات معلوماتية تفيد في كشف الحقيقة.

2- محل التفتيش في البيئة الإلكترونية:

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره، والسر الذي يحميه القانون هو ذلك المستودع في محل له حرمة كالمسكن أو الشخص أو الرسائل. ومحل التفتيش في الجريمة الإلكترونية هو الحاسوب والشبكة التي تشمل مكوناتها الخادم والمزود الآلي والمضيف والملحقات التقنية. سبق وأن أشرنا إلى مدى قابلية المكونات المادية والمعنوية للحاسوب فضلا عن شبكات الاتصال الخاصة به إلى التفتيش، وموقف التشريعات المقارنة من ذلك، فلا مجال لتكرار ذلك.[1]

3- السلطة المختصة بإجراء التفتيش:

تختلف الجهة المختصة بالقيام بإجراء التفتيش باختلاف الأنظمة الجزائية، ففي التشريع المصري مثلا يعهد به إلى النيابة العامة بخلاف التشريع الجزائري والفرنسي اللذان يعهدان به إلى قاضي التحقيق كقاعدة عامة إلا أنه هناك استثناءات حيث يمكن لضباط الشرطة القضائية القيام بالتفتيش في حالتين هما:

- حالة التلبس أو الجرم المشهود في الجنايات والجنح .

- حالة الإنابة القضائية أو في حالة الإذن من قبل قاضي التحقيق، أو وكيل الجمهورية لضباط الشرطة القضائية بتفتيش منزل المتهم وهذا ما جاء في نص المادة 44 من ق.إ.ج.ج، كما أن هذه المادة في فقرتها الثالثة قد حددت شروط إذن التفتيش حتى يكون صحيحا بأن يكون مكتوبا ويتضمن تكييف الجريمة موضوع البحث وتحديدها بدقة وعنوان الأماكن التي سيتم تفتيشها وإجراء الحجز أو الضبط تحت طائلة البطلان.

- الشروط الشكلية للتفتيش في البيئة الإلكترونية:[2]

[1] أشرف عبد القادر قنديل، مرجع سابق، ص .149

[2] لامية مجدوب، التزوير الالكتروني، مرجع سابق، 177.

إضافة إلى الشروط الموضوعية لصحة إجراء تفتيش نظم المعلومات، يجب مراعاة الشروط الشكلية والمتمثلة في ما يلي:

أ- الحضور الضروري لبعض الأشخاص أثناء التفتيش:

فبالنسبة لتفتيش الأشخاص لم يشترط القانون ذلك أما تفتيش المساكن، وما في حكمها فقد أكد القانون الإجرائي على ضرورة حضور شاهدين وإذا كان القائم بالتفتيش قاضي التحقيق أو ضابط الشرطة القضائية من غير الموظفين الخاضعين لسلطتها، متى تعذر حضور المتهم أو ممثله أو امتنع أو كان هاربا، غير أن التفتيش في البيئة الإلكترونية لا يتطلب هذا الشرط، حيث أن المشرع الجزائري استغنى عنه في مجال تفتيش الجريمة المعلوماتية، وذلك بموجب نص المادة 45 في فقرتها الأخيرة مع مراعاة ما جاء في نص المادة 47 مكرر من قانون الإجراءات الجزائية الجزائري.

ب- الميعاد الزمني لإجراء التفتيش في البيئة الإلكترونية:

إذا كانت القاعدة العامة في التشريع الإجرائي الجزائري أن إجراء تفتيش المساكن يتم في وقت محدد من الساعة الخامسة صباحا حتى الثامنة مساء وهذا ما أقرته المادة 47 من ق.إ.ج.ج، غير أنه ورد استثناء يجيز إجراء التفتيش ليلا نهارا في بعض الجرائم منها جرائم نظم المعلومات وهذا ما ورد ذكره بموجب نص المادة 47 في فقرتها الثالثة حفاظا على خصوصية هذه الجريمة وتبعاتها.

ج- محضر التفتيش في البيئة لإلكترونية:

لم يستلزم القانون شكلا معينا في محضر التفتيش لذلك لا يشترط لصحته سوى ما تتطلبه بقية المحاضر القضائية الأخرى كأن يكون مكتوبا باللغة الرسمية وأن يحمل تاريخ تحريره وتوقيع محرره وأن يحوي كافة الإجراءات التي تم القيام بها سواء تم التحصل على أدلة أم لا، كما يستلزم تحريره إحاطة قاضي التحقيق بتقنية المعلومات وأن يستعين بذوي الاختصاص وأهل الخبرة الفنية كذلك مقدمي الخدمات في تحرير مسودة محضر التفتيش والمحافظة على الأدلة الإلكترونية من أي تلف أو ضياع.

ثالثا: الضبط:

يختلف الضبط في الجريمة الإلكترونية عن الضبط في غير ذلك من الجرائم من حيث المحل، وذلك بسبب أن الأول يرد على أشياء ذات طبيعة معنوية وهي البيانات،

المراسلات، والاتصالات الإلكترونية، أما الثاني فيرد على أشياء مادية منقولة كانت أم عقارات، وقد أثارت هذه الطبيعة المعنوية للبيانات جدلا فقهيا واختلافا تشريعيا حول مدى إمكانية ضبطها خاصة إذا كانت مجردة من الدعامة المادية المثبتة عليها.[1]

وتجدر الإشارة إلى أن الضبط قد يرد على عناصر معلوماتية منفصلة مثل الديسكات والأسطوانات الممغنطة، وهنا لا تثور أي مشكلة قانونية عند القيام بالضبط، ولكن الصعوبة تثار عندما يلزم ضبط النظام كله أو الشبكة كلها، ذلك لأنها تحتوي غلى عناصر لا يمكن فصلها، ومع ذلك يتعين ضبطها لأنها تتضمن عناصر مهمة للإثبات في الجريمة.

الفرع الثاني: الإجراءات الشخصية.

يقصد بالإجراءات الشخصية تلك القواعد الإجرائية أو الشكلية التقليدية ذات الطبيعة الشخصية، لأنه غالبا ما يتوسط فيها الشخص بين القيام بالإجراء والحصول على الدليل المستنبط منها وتتمثل هذه الإجراءات في الشهادة والخبرة الفنية، أما عن عملية التسرب باعتبارها أيضا من الإجراءات الشخصية ورغم أنها تعد إجراء مستحدث من قبل المشرع الجزائري غير أنها لاحقا ضمن الإجراءات المستحدثة لمقتضيات الدراسة ولإزالة أي غموض قد يعتريها .

أولا- الشهادة: هي الأقوال التي يدلي بها غير الخصوم أمام سلطات التحقيق أو الحكم أو جهاز القضاء بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى المتهم أو براءته منها. [2]

أما الشاهد ألمعلوماتي هو كذلك الشخص الفني صاحب الخبرة والتخصص في تقنية علوم الحاسب الآلي وشبكات الاتصال والذي تكون لديه معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للمعطيات متى كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله، يطلق على هذا الشاهد اسم الشاهد المعلوماتي نسبة للجريمة المعلوماتية وتمييزا له عن الشاهد في الجرائم التقليدية .

[1] أشرف عبد القادر قنديل، مرجع سابق، ص 154، 155

[2] لامية مجدوب، التزوير الالكتروني، مرجع سابق، ص 184 .

- التزامات الشاهد المعلوماتي:

يقع على عاتق الشاهد المعلوماتي أن يقدم إلى ضابط الشرطة القضائية أو جهات التحقيق أي معلومات جوهرية لازمة للدخول أو الولوج إلى نظام المعالجة الآلية للبيانات بحثا عن أدلة يمكن أن تثبت جرائم التزوير في البيئة الإلكترونية.

كما يقع على عاتق الشاهد ثلاث التزامات رئيسية وهي: الحضور أمام الجهة التي استدعته، حلف اليمين، وأخيرا الإدلاء بشهادته وهذا ما سيأتي توضيحه في النقاط التالية:

1- حضور الشاهد: ويقصد به تقدم أو حضور الشاهد بنفسه شخصيا في المكان والزمان المحددين لسماع شهادته والبقاء في هذا المكان حتى يؤذن له بالانصراف، وعادة يكون ذلك بناء على تكليف بالحضور يعلن إليه بواسطة أحد المحضرين أو يتم ضباط الشرطة القضائية، وفي حالة الإخلال بهذا الالتزام يتم إجباره على الحضور ولو اقتضى الأمر استعمال القوة العمومية وهذا ما نصت عليه المادة 97 فقرة 02 من ق.إ.ج.ج.[1]

2- حلف اليمين: لقد ألزم المشرع كل شاهد بحلف اليمين قبل أدائه للشهادة منه القاضي اقتناعه، كما يعطي لها قيمتها القانونية من جهة، وجدير بالذكر أن المشرع الجزائري قد حدد صيغة اليمين مثله مثل المشرع الفرنسي هذا الأخير جعل صيغة اليمين تختلف باختلاف المحاكم وهي حتمية ويترتب على مخالفتها البطلان، كما أن الالتزام بأداء اليمين من النظام العام لا يمكن للشاهد الامتناع عن أدائها أو أن يطلب من القاضي إعفاءه منها .[2]

3- الإدلاء بالشهادة: يعد هذا الإلزام جوهر مهمة الشاهد وأهم التزام في شهادته على الإطلاق وينطوي هذا الالتزام في واقع الأمر على واجبين يتحملهما الشاهد وهما:

- الواجب الأول: الالتزام بالتحدث والتكلم عكس المتهم فلا يمكنه أن يسكت، إذ يتوجب عليه الإدلاء بشهادته، إلا إذا كان ملزم قانونيا بكتمان السر المهني كالأطباء والمحامين وغيرهم ممن لهم مبرر قانوني، أما الإخلال بهذا الواجب يترتب عنه الحكم على هذا

[1] تنص المادة 97 في فقرتها 02 من ق.إ.ج.ج على ما يلي: "و إذا لم يحضر الشاهد فيجوز لقاضي التحقيق بناء على طلب وكيل الجمهورية جبرا بواسطة القوة العمومية الحكم عليه بغرامة من 200 إلى 2000 دج".

[2] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، 2010، ص 133.

الشخص بغرامة من 1000 إلى 10000 دج والحبس من شهر إلى سنة أو بإحدى هاتين العقوبتين وهذا ما جاء ذكره بموجب نص المادة 98 من ق.إ.ج.ج.

– الواجب الثاني: يتمثل في واجب قول الحقيقة كما هي أي قول الحقيقة كاملة، ذلك أن المشرع الجزائري قد أقر عقوبة شهادة الزور بموجب نص المادة 232 من قانون العقوبات الجزائري.[1]

ثانيا– الخبرة التقنية:

وهي الاستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته نحو الوسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوفر لديه، فهي وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الدلائل أو الأدلة.[2]

1– اختيار الخبراء:

يتم اختيار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة وهذا ورد ذكره بموجب نص المادة 144 ق إ ج ج، ودون الالتزام بترتيب معين تبعا لثقة المحقق أو القاضي، وتحدد الأوضاع التي يجري بها قيد الخبراء أو شطب أسمائهم بقرار من وزير العدل، كما يمكن استثناء اختيار خبراء ليسوا مقيدين في هذه الجداول بقرار مسبب يتضمن أسباب ودوافع ذلك، كما أن المشرع ترك للقاضي حرية ندب خبير وأحد أو أكثر وهذا ما جاء في نص المادة 147 ق إ ج ج .[3]

2– واجبات الخبير:

– حلف اليمين حتى يكون تقرير الخبير صحيحا ومنتجا قانونا يجب أن يقوم الخبير بأداء اليمين وذلك لدفع هذا الأخير إلى قول الصدق والحقيقة الأمانة والنزاهة في عمله (المادة 145 ق إ ج ج).[4]

– خضوع الخبير للرقابة القضائية، أي تحت رقابة القاضي الذي أمر بإجراء الخبرة.

– قيام الخبير بأعمال الخبرة اللازمة بنفسه.

---

[1] تنص المادة 232 من ق ع ج على ما يلي: " كل من شهد زورا في مواد الجنايات سواء ضد المتهم أو لصالحه يعاقب بالسجن من خمس سنوات إلى عشر سنوات ".

[2] لامية مجدوب، مرجع سابق، ص 189.

[3] المرجع نفسه، ص 190

[4] أنظر المادة 145 من ق إ ج ج.

- إيداع التقرير الفني خلال المدة المحددة له.

المطلب الثاني: الإجراءات الحديثة لجمع الأدلة في التزوير الالكتروني:

من خلال ما سبق يتبن بأن الإجراءات التقليدية لجمع الدليل التقني وإثبات جرائم التزوير الالكتروني غير كافية وغير مجدية مما يتطلب اللجوء إلى إجراءات حديثة تفي بالغرض، حيث أصدر المشرع الجزائري القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، حيث استحدث الفصل الرابع من الباب الثاني من الكتاب الأول تحت عنوان " في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور "أو الترصد الالكتروني، وكذلك الفصل الخامس منه تحت عنوان " في التسريب" أو الاختراق وبعد ذلك أصدر المشرع الجزائري القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، حيث استحدث إجراءين هامين الأول حول المراقبة الالكترونية والثاني حول حفظ المعطيات المتعلقة بحركة السير وهذا ما سيأتي بيانه في ما يلي :

الفرع الأول: الإجراءات المستحدثة بموجب قانون الإجراءات الجزائري:

من خلال ما تم استحداثه في قانون الإجراءات الجزائية بموجب القانون 06-22:

أولا- اعتراض المراسلات وتسجيل والتقاط الأصوات والصور:

من خلال المواد 65 مكرر 5 إلى غاية 65 مكرر 10 من القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 فان المقصود باعتراض المراسلات هي عبارة عن بيانات قابلة للإنتاج، التوزيع التخزين، الاستقبال، الإرسال والعرض، بمعنى إباحة إمكانية التصنت على المحادثات الهاتفية واعتراض المراسلات سواء تلك التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، إضافة إلى التقاط وتثبيت وتسجيل وبث الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن عامة أو خاصة بغض النظر عما يتخلل هذه الاتصالات من أحاديث شخصية وغيرها.[1]

[1] لامية مجدوب، مرجع سابق، ص 193.

إضافة إلى التقاط صور لشخص أو أشخاص يتواجدون في أماكن معينة، ولا يقتصر الاعتراض على المراسلات المكتوبة بل يمتد إلى كل الرسائل المكتوبة أو المصورة أو الالكترونية وكل ما تفرزه الأجهزة التقنية المعاصرة عبر الهاتف الثابت أو المنقول أو التلغراف أو الفاكس أو التلكس أو الإنترنت وغيرها من الوسائل التقنية الحديثة.

1- موقف التشريعات المقارنة من هذه الإجراءات:[1]

حاولت العديد من الدول سد الفراغ التشريعي في هذا المجال ومنها:

بالنسبة لفرنسا ليم يتردد القضاء الفرنسي في القول بشرعية وقانونية هذه الإجراءات، حيث أكدت محكمة النقض الفرنسية شرعية التنصت التليفوني الذي يأمر به قاضي التحقيق شريطة ألا يقترن ذلك بحيلة فنية أو بمخالفة لحق الدفاع أي حظر التنصت على الخط الهاتفي لمحامي المتهم.

كما لجأ المشرع إلى التدخل مرة أخرى لإضفاء الشرعية على استعمال الأساليب الحديثة للتحري لاحقا وذلك بإصدار القانون رقم 04-202 الصادر في 2004/03/09 المعدل والمتمم لقانون الإجراءات الجنائية الفرنسي، حيث أورد بابا كاملا يتعلق بهذه الإجراءات الجديدة وذلك وفق ضمانات وشروط معينة .

وبالنسبة لهولندا فيجيز القانون لقاضي التحقيق أن يأمر بالتنصت على شبكات اتصالات الحاسب الآلي إذا كان الغرض من ذلك ضبط جرائم خطيرة ويمكن أن تتم المراقبة أيضا على التلكس والفاكس ومختلف طرق نقل البيانات.

أما في المشرع المصري حيث أكد الدستور المصري على الحق في خصوصية الحياة الخاصة بموجب نص الادة 45 منه، وبالتالي لا يجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر مسبب ولمدة محددة وفقا لأحكام القانون، حيث إذا كانت مصلحة التحقيق تقتضي اللجوء في بعض الأحيان إلى مراقبة الأحاديث الخاصة وتسجيلها فقد يجوز ذلك بشروط معينة طبقا للمادتين 25 و206 من قانون الإجراءات

[1] لامية مجدوب، مرجع سابق، ص 199 .

الجزائية المصري وجاءت هذه الإضافة بموجب القانون رقم 37 لسنة 1972 المسمى بقانون الحريات.[1]

وأما المشرع المغربي فقد حذا حذو باقي التشريعات المقارنة التي أخذت بهذه الإجراءات، كما مكن الوكيل العام للملك من إصدار أمرا بالتقاط المكالمات الهاتفية وجميع الاتصالات الأخرى بعد تقديم التماس كتابي إلى الرئيس الأول لمحكمة الاستئناف ما عدا في حالة الاستعجال .

2- موقف المشرع الجزائري:

بالنسبة للمشرع الجزائري فقد ساير التطورات التي عرفها المجتمع الدولي في مجال الإعلام والاتصالات، وكانت بداياته الأولى من خلال المصادقة على معظم الاتفاقيات الدولية المتعلقة بالإرهاب الدولي ومكافحته والتخريب، والجريمة المنظمة العابرة للحدود الوطنية والجريمة المعلوماتية، وكان لزاما عليه أن يستتبع ذلك بآليات قانونية تكفل ضبط مرتكبي هذه الجرائم والتحري عنهم وهذا ما جسده فعلا من خلال القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية الذي تضمن جملة من الإجراءات الحديثة المتعلقة بتسجيل المكالمات واعتراضها والتقاط الصور فضلا عن اجراء التسرب.[2]

فإنه لا يمكن لضباط وبالرجوع إلى نص المادة 65 مكرر05 من ق إ ج ج الشرطة اللجوء إلى هذا الإجراء إلا بعد الحصول على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي لمدة أربعة أشهر قابلة للتجديد ويجب أن يشمل الإذن المسلم لضباط الشرطة القضائية جميع العناصر المتعلقة بنوع الجريمة التي اقتضت ضرورة التحري أو التحقيق القضائي وطبيعة المراسلة والاتصال.

أما بالنسبة للجرائم التي يجوز فيها الاعتراض وهي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الالكترونية، جرائم الصرف، جرائم الإرهاب،

---

[1] أنظر المادة 65 مكرر05 من ق إ ج ج .

[2] أحمد محمد حسان، " الحماية القانونية للمحادثات الهاتفية والشخصية ضد التنصت والتسجيل الصوتي، " مجلة كلية الدراسات العليا، دون عدد، دون تاريخ، ص 319.

تبييض الأموال وجرائم الرشوة والفساد.

ثانيا- التسرب:

هذا الإجراء أدرجه المشرع الجزائري بموجب القانون رقم 06-22 المتعلق بقانون الإجراءات الجزائية في الفصل الخامس منه تحت عنوان: " التسرب" من المادة 65 مكرر 11 إلى غاية المادة 65 مكرر 18 .

يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم بأنه فاعل معهم أو شريك لهم، حيث يجوز له الاستعانة بهوية مستعارة، كما يمكنه ارتكاب الأفعال المتعلقة بالجريمة دون أن يتابع من أجلها .

ويمكن تصور عملية التسرب في نطاق جرائم التزوير الالكتروني عن طريق دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي واشتراكه مثلا في محادثات غرف الدردشة أو حلقات النقاش والاتصال المباشر إضافة إلى الولوج إلى الأنظمة المعلوماتية والمشاركة في عمليات التلاعب بالمعطيات وتزويرها وكل عملية تمكنه من تنفيذ أو تسهيل هذه الجرائم، كما يجوز له استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال.[1]

إلا أنه يشترط ألا يقوم هذا العون أو الضابط بتحريض المجرمين، وذلك تحت طائلة البطلان إذا ثبت أنها تشكل تحريضا، وهذا ما ورد في نص المادة 65 مكرر 2/12 من ق إ ج ج .

ويجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهدا عن العملية .

1- شروط صحة عملية التسرب:

[1] مراد، اجراءات التحقيق المستحدثة في قانون الإجراءات الجزائية الجزائري عملية التسرب في المادة الجزائية، الجزء الأول، الطبعة الأولى، سلسلة للمعارف القانونية والقضائية، دار نشر المعرفة، الرباط، المغرب، 2013، ص 166.

إن عملية التسرب إجراء يتطلب اتخاذ كثيرا من الحيطة والحذر، لذلك أحاطه المشرع الجزائري بجملة من الشروط وهي كما يلي:[1]

– صدور عملية التسريب بإذن قضائي: طبقا للمادة 65 مكرر 11 من ق إ ج ج التي تنص: ".....يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية أن يأذن تحت إذن ..." وذلك لحماية الحقوق الأساسية المكرسة دستوريا وعليه لا يمكن قيام ضابط الشرطة القضائية الانفراد والقيام بالعملية لوحده دون الرجوع إلى الجهاز القضائي المختص.

– أن يكون الإذن مكتوبا: طبقا للمادة 65 مكرر15 من ق إ ج ج بقولها: " يجب أن يكون الإذن المسلم طبقا للمادة 65 مكرر 11 أعلاه مكتوبا.. تحت طائلة البطلان" .

– ذكر اسم الضابط: يجب توفر مواصفات في القائم بعملية التسرب كشدة الملاحظة قوة الذاكرة والسرعة في الحركة والصبر والمثابرة والذكاء والشجاعة ...الخ وضرورة ذكر اسم الضابط المشرف أو المسؤول عن العملية وهويته الكاملة. [2]

– مدة عملية التسرب: لقد تم تحديدها بموجب نص المادة 65 مكرر 15 الفقرة الثالثة منها من ق إج ج على أن لا تتجاوز أربعة أشهر ويمكن تجديدها حسب مقتضيات التحري أو التحقيق ضمن الشروط الشكلية والزمنية، وفي نفس الوقت أجاز القانون للقاضي الذي رخص بإجرائها أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة، كما نصت المادة 65 مكرر17 من ق إج ح على أنه يمكن للعون المتسرب أن يواصل نشاطه غير القانوني الوارد في نص المادة 65 مكرر14 من القانون نفسه مع إعفائه من المسؤولية الجزائية لمدة لا تتجاوز أربعة أشهر على أن يخطر القاضي مصدر الرخصة في أقرب الآجال، أما إذا لم يتمكن العون المتسرب من إيقاف نشاطه خلال المدة المذكورة في ظروف تضمن أمنه يمكن للقاضي أن يرخص بتمديدها لمدة أربعة أشهر أخرى.

– إبقاء الإذن بالتسرب خارج ملف الإجراءات إلى غاية نهاية العملية: حفاظا على السرية التامة المطلوبة والتي حصرها المشرع بين القاضي الآمر بها وضابط الشرطة القضائية المشرف على عملية التسرب وكذلك الضابط أو العون المتسرب.

[1] عبد الرحمان خلفي، محاضرات في الإجراءات الجزائية، الطبعة الثانية، دار الهدى، عين مليلة، 2012، ص 74

[2] نفس المرجع، ص 168

- التسبيب .
- نوع الجريمة .

الفرع الثاني: الإجراءات المستحدثة بموجب القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما:

من خلال ما تم استحداثه في القانون 09-04 المؤرخ في 2009/08/05 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما:

أولا- مراقبة الاتصالات الإلكترونية في حينها:

نصت المادة 03 من القانون 09-04 على ما يلي: "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع الترتيبات التقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها ".

والمقصود بمراقبة الاتصالات الإلكترونية في الفقه الجنائي هي مراقبة شبكة الاتصالات، أوهي ذلك العمل الذي يقوم به المراقب باستخدام التقنية التكنولوجية لجمع معطيات ومعلومات عن المشتبه فيه سواء كان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر ".

باستقراء هذين التعريفين يتضح أن المراقبة الإلكترونية تعد من بين التدابير الماسة بحق الإنسان في سرية مراسلاته واتصالاته الخاصة بما فيها الإلكترونية مثل البريد الإلكتروني. لذلك تفطن المشرع الجزائري حيث سن قواعد قانونية تعمل على توفير قدر كبير من الحماية الجزائية لسرية الاتصالات الخاصة للأفراد، حيث عاقب لأول مرة على ذلك متأثرا بنظيره الفرنسي، على اعتراض الاتصالات دون إذن بذلك بموجب نص المادة 303 مكرر المضافة بموجب القانون 23/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون العقوبات.[1]

[1] تنص المادة 303 مكرر من ق ع ج على ما يلي: " يعاقب بالحبس من 6 أشهر إلى ثلاث سنوات وبغرامة من 50.000 إلى 300.000 دج كل من تعمد المساس بحرمة الحياة للأشخاص بأي تقنية كانت وذلك بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه .
بالتقاط أو تسجيل أو نقل صورة للشخص في مكان خاص بغير إذن صاحبها أو رضاه ".

1- تنفيذ الإجراء تحت سلطة القضاء وبإذن منه:

بمعنى أن السلطة القضائية هي الجهة المختصة بإصدار هذا الإذن، وذلك لإضفاء الشرعية على كل الإجراءات المتخذة في هذا الشأن من قبل ضباط الشرطة القضائية وهذا ما أكده المشرع الجزائري بموجب الفقرة الأخيرة من المادة الرابعة 04 من القانون09-04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما التي لا تجيز إجراء المراقبة إلا بإذن مكتوب من السلطة القضائية المختصة.[1]

2- الضرورة القصوى للقيام بالمراقبة:

أي أن تكون هناك معلومات كافية تنبأ عن احتمال حدوث اعتداء على منظومة معلوماتية على نحو يهدد النظام العام والدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو أن هناك معلومات تنتقل في الفضاء الإلكتروني تنذر بوقوع اعتداء على أمن الدولة، وفي هذا الغرض يتم الترخيص أو الإذن بتنفيذ إجراء المراقبة الإلكترونية .

3- الجرائم التي يجوز فيها إجراء المراقبة الإلكترونية:

نص المشرع الجزائري صراحة بموجب المادة الرابعة 40 من القانون 09-04 على الحالات التي يجوز فيها مراقبة الاتصالات الإلكترونية وهي مذكورة على سبيل الحصر .

ثانيا- حفظ المعطيات المتعلقة بحركة السير:

أكد المشرع الجزائري على هذا الإجراء بموجب نص المادة العاشرة 10 من الفصل الرابع من القانون رقم 09-04 تحت عنوان "التزامات مقدمي الخدمات " كما يلي: " في إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية ...وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أعلاه تحت تصرف السلطات المذكورة ..."

[1] تنص المادة 04 من القانون 09-04 على: "...لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة ..."

حيث عرف المشرع الجزائري مزود أو مقدم الخدمة بموجب الفقرة (د) من المادة الثانية من القانون 09-04 المذكور سابقا بأنه: " أي كيان عام أو خاص يقدم لمستعملي خدماته ضمانة القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات.

وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها."

يقصد بحفظ المعطيات: " قيام مزود الخدمات بتجميع المعطيات المعلوماتية وحفظها وحيازتها في أرشيف، وذلك بوضعها في ترتيب معين والاحتفاظ بها في المستقبل في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش وغيره ."

الملاحظ أنه ليست كل المعطيات المعلوماتية محل اعتبار من قبل المشرع، بل إنه قد حدد المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمات بمعطيات المرور كما سماها "حركة السير " وقد عرف هذه الأخيرة بموجب نص المادة الثانية في فقرتها الخامسة من القانون 09-04، بأنها: "أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزء في حلقة الاتصالات توضح مصدر الاتصال والوجهة المرسل اليها والطريق الذي سلكه ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة ".[1]

1- مسؤولية مزودي الخدمات:

فضلا عن الالتزامات السابقة الواردة على عاتق مزودي الخدمات، فهناك التزامات أخرى مذكورة في دفتر الشروط الخاص بهم، لأن مستعملي هذه الوسائل يتعاملون مع هيئات معينة، ولديهم دفتر شروط يتضمن كل الالتزامات الواقعة على عاتقهم، فمتى تخلوا عنها أو امتنعوا عن تنفيذها، فتطبق عليهم عقوبات كسحب الرخصة، إضافة إلى عقوبات إدارية أخرى، وتطبق عقوبات جزائية على أحد مستخدمي هذه الوسائل إذا قصر أو أهمل كحالة التقاعس عن حفظ المعطيات، وتتراوح العقوبة بين 06 أشهر إلى 05 سنوات والغرامة المالية التي تتراوح بين 50.000 ألف إلى 500.000 دج أما الشخص المعنوي فيعاقب بالعقوبات المقررة له وفقا لقانون العقوبات الجزائري .

[1] لامية مجدوب، مرجع سابق، ص 219 .

المبحث الثاني: إثبات جرائم التزوير الإلكتروني .

غالبا ما يحدث فعل التزوير في المجال الإلكتروني دون علم المجني عليه، مثلا كدخول بعض المواقع الإلكترونية وتزوير بعض المعطيات الخاصة بها، ذلك أن موضوع الإثبات الجنائي في الجرائم الإلكترونية ينطوي على حد كبير من الصعوبة والتعقيد في غياب قانون الإثبات أو لانعدام نصوص قانونية ترسم الإطار أو الأساس القانوني للنظرية العامة للإثبات الجنائي .

حيث سيتم تناول الإثبات الجنائي في البيئة الإلكترونية من خلال دراسة طرق الإثبات (المطلب الأول)، وضوابط سلطة القاضي الجنائي في قبول الدليل الإلكتروني (المطلب الثاني).

المطلب الأول: طرق الإثبات.[1]

لقد أقر المشرع الجزائري مبدأ حرية الإثبات في المسائل الجنائية بموجب نص المادة 212 من ق إ ج ج التي تنص: " يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي نص فيها القانون على غير ذلك وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي ".

كما أن للمحكمة أن تأمر من تلقاء نفسها أثناء نظر الدعوى وفي أي مرحلة من مراحل المحاكمة بتقديم أي دليل تراه لازما لإظهار الحقيقة، كما أن للمحكمة أن تأمر من تلقاء نفسها أثناء نظر الدعوى وفي أي مرحلة من مراحل المحاكمة بتقديم أي دليل تراه لازما لإظهار الحقيقة، كما أن النيابة العامة تملك الحرية المطلقة في إثبات الجريمة وإسنادها للمدعي عليه، بجميع طرق الإثبات وتنطبق على كافة الجرائم أمام مختلف الجهات القضائية بما فيها التزوير الإلكتروني كنموذج عن الجرائم الإلكترونية عدا الأحوال التي نص فيها القانون على خلاف ذلك .

الفرع الأول: مدى فعالية طرق الإثبات في التزوير الإلكتروني .

في هذا الفرع سيتم التطرق إلى الطرق الأكثر ملائمة للإثبات جرائم التزوير الإلكتروني ومدى فعاليتها والمتمثلة في:

[1] لامية مجدوب، مرجع سابق، ص 232 .

أولا- الاعتراف:

هو إقرار المتهم على نفسه بصحة التهمة المسندة إليه، فهو عمل إرادي ينسب به المتهم نفسه بأنه قام بارتكاب الوقائع المكونة للجريمة كلها أو بعضها، وقد يكون شفويا أو مكتوبا وكلاهما كافي في الإثبات، طبقا للمادة 213 من قانون الإجراءات الجزائية الجزائري، كما أن معظم القوانين لم تنظم شكلا خاصا بالاعتراف الصادر من المتهم، إلا أنه يجب أن يكون هذا الاعتراف في شكل واضح ويجب أن يكون كتابة أو شفاهة، فلا يجوز استنتاجه ولا يكون ضمنيا ولا يؤخذ بسكوت المتهم بأنه اعتراف، إلا أنه لا يجب أن يوقع المتهم على الاعتراف فقد يرفض أن يوقع والمحكمة في جميع حالات الاعتراف أن تتحرى الدقة الشديدة في اعتراف المتهم ويجب عليها أن تنتبه من واقع وظروف الواقعة.[1]

وبالتالي فإن الاعتراف ليس سيد الأدلة لأنه يمكن نسبة الجريمة لغر مرتكبها الحقيقي إراديا، لذلك هو شأنه شأن بقية الأدلة، فمثلا حال حدوث جريمة تزوير الكتروني وقيام أكثر من شخص بالاعتراف بارتكابها ففي هذا الفرض فإن الاعتراف وحده لا يكفي بل يتطلب التدخل في بناء الإدانة على ضوء كيفية القيام بفعل التزوير في المجال الالكتروني وعليه إذا فشل المتهم في الإدلاء بكيفية قيامه بالتزوير أو كانت معلوماته غير دقيقة، فإن الاعتراف لا يكفي لإدانته نظرا لأن الحاسوب والانترنت يسمحان بدخول أكثر من شخص واحد على أي موقع وفي ذات الوقت دون أن يمكن أحدهم من رصد الآخر.[2]

ثانيا- المحررات:

وهي الأدلة الكتابية التي لا يمكن دحضها أو ردها بعد التأكد من صحتها حيث تفرض على المتهم الاعتراف بالتهمة الموجهة إليه وعدم التهرب من العقوبة المقررة له، فقد أعطى القانون سلطات واسعة لضباط الشرطة القضائية خاصة في جرائم التلبس، لحجز كل ما من شأنه أن يستعمل أو كان قد استعمل فعلا في ارتكاب الجريمة.

تجدر الإشارة إليه أن المحررات في مفهوم طرق الإثبات متنوعة تبعا للجهة المصدرة لها أو مضمونها أو نوعها فهناك المحاضر، التقارير، الأحكام، القرارات

---

[1] سارة غادري، الأدلة القولية الشهادة والاعتراف ودورها في الإثبات الجنائي، مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة المسيلة، ص 2014، ص 34 .

[2] منى فتحي أحمد عبد الكريم، الجريمة عبر الشبكة الدولية للمعلومات صورها مشاكل إثباتها، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق، جامعة القاهرة، 2008، ص 138 .

القضائية والعقود بمختلف أنواعها الرسمية منها والعرفية وغيرها وعموما يمكن القول أن المحررات بمختلف صورها، تعد كغيرها من طرق الإثبات أي تخضع للسلطة التقديرية للقاضي.

فمثلا تعد المحاضر المحررة من طرف ضباط الشرطة القضائية بما تحويها من معلومات وبيانات التي تم تحريرها بمناسبة قيامهم بأعمالهم كالانتقال للمعاينة، أو سماع الأقوال فكلها تعد مجرد استدلالات طبقا لنص المادة 215 ق إ ج ج.[1]

فهذه المحاضر ليست لها أي حجية أمام القضاء أو بالأحرى تبقى حجيتها بسيطة يمكن دحضها بما يخالفها وهذا ما ورد ذكره بموجب نص المادة 216 من نفس القانون.

غير أن المشرع أعطى للمحاضر الجمركية حجية في الإثبات إلى حين يطعن فيها بالتزوير وهذا ما نصت عليه المادة 254 الفقرة الأولى والثانية من قانون الجمارك الجزائري.[2]

ثالثا- الخبرة:

الخبرة هي إجراء يستهدف استخدام قدرات شخص الفنية أو العلمية والتي لا تتوافر لدى رجال القضاء من أجل الكشف عن دليل أو قرينة تفيد في معرفة الحقيقة بشأن وقوع الجريمة ونسبتها إلى المتهم أو تحديد ملامح شخصيته الإجرامية ولهذا فإن للخبرة التقنية في مجال الجريمة المعلوماتية أهمية بالغة حيث أنه لا يستطيع التعامل مع هذه الجريمة إلا شخص ذو دراية وخبرة في مجال الشبكات .

ونظرا لأن الجريمة المعلوماتية لها خصوصيتها فإن الخبير المعلوماتي لابد أن تتوافر لديه المقدرة الفنية والإمكانيات العلمية والفنية في المسألة موضوع الخبرة ولا يكفي في ذلك حصول الخبير على شهادة علمية بل يجب مراعاة الخبرة العملية لأنها هي التي تحقق الكفاءة الفنية من أجل كشف الغموض عن الجريمة أو تجميع أدلتها والتحفظ عليها

[1] تنص المادة 215 من ق إ ج ج على ما يلي: " لا تعتبر المحاضر والتقارير المثبتة للجنايات أو الجنح إلا مجرد استدلالات ما لم ينص القانون على خلاف ذلك ".

[2] تنص المادة 254 من قانون الجمارك الجزائري على ما يلي: " تبقى المحاضر الجمركية المحررة من طرف عونينمحلفين على الأقل من بين الأعوان المذكورين في المادة 241 من هذا القانون صحيحة ما لم يطعن فيها بتزوير المعاينات المادية ...".

ومساعدة المحقق في ايجاد جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق.[1]

رابعا- الشهادة:

يمكن تصور الشهادة في الجريمة المعلوماتية مثلا من خلال، شهادة شخص على آخر حدثت أمامه الجريمة كصديق شاهد رفيقه أثناء قيامه بكتابة بعض الوثائق المزورة إلكترونيا .

خامسا- المعاينة:

يقصد بالمعاينة انتقال ضباط الشرطة القضائية أو قاضي التحقيق الانتقال إلى أماكن وقوع الجريمة للمعاينة وضبط ما قد يعثر عليه من آثار وسماع ما قد يجده من شهود في عين المكان قبل أن يقع التأثير عليهم من المتهم أو من أطراف أخرى وهو ما قرره المشرع الجزائري في المادة 79 ق إ ج ج .

وتتم المعاينة في الجريمة المعلوماتية المرتكبة عبر الإنترنت كأي جريمة أخري عن طريق الانتقال إلى محل الواقعة الإجرامية إلا أن الانتقال هناك لا يكون إلى العالم المادي وإنما إلى العالم الافتراضي أو عالم الفضاء الإلكتروني .

وحتى تكون المعاينة صحيحة لابد على قاضي التحقيق أن ينتقل إلى مكان وقوع الجريمة بصحبة كاتبه بعد إخطار وكيل الجمهورية المختص إقليميا بجميع الإجراءات اللازمة .

سادسا- القرائن:

إن القرائن بأنواعها تعد من طرق الإثبات غير المباشرة أي التي لا تنصب دلالتها على الواقعة المراد إثباتها وإنما على واقعة أخرى تسبقها أو نتيجتها بمحض اللزوم العقلي، حيث هناك قرائن ينشئها القانون وتسمى قرائن قانونية وتنقسم إلى نوعين مطلقة لا تقبل إثبات العكس كافتراض العلم بالقانون بمجرد نشره في الجريدة الرسمية، وقرينة بسيطة يمكن إثبات عكسها كقرينة الدفاع الشرعي، وهناك قرائن يقيمها القضاء وتسمى القرائن القضائية أي يستخلصها القاضي من الوقائع الثابتة أمامه بطريق الاستنتاج كأن

[1] ابتسام يغو، اجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة تكميلية لنيل شهادة ماستر في القانون- تخصص قانون جنائي للأعمال، جامعة العربي بن مهيدي، أم البواقي، 2016، ص 21.

يستخلص اشتراك عدة أشخاص في الجريمة لوجودهم في مسرحها وقت ارتكابها حاملين منتجتها.[1]

الفرع الثاني: الإثبات العلمي .

أصبحت الخبرة تلعب دورا رائدا لا يستهان به على حساب الوسائل الأخرى والسؤال الذي يمكن طرحه ما هو مفهوم الأدلة العلمية والدليل الإلكتروني في إثبات التزوير الإلكتروني؟.

أولا- المقصود بالأدلة العلمية:

يقصد بالدليل العلمي ذلك الدليل المتحصل من الأجهزة والوسائل العلمية الحديثة فالدليل العلمي هو النتيجة التي تسفر عنها التجارب العلمية والمعملية والأساليب التي يقوم بها مختص فنيا، ألا وهو الخبير.

حيث يحتل الدليل العلمي مكانة مرموقة في العصر الحديث بين أدلة الإثبات الجنائي الأخرى، ويلعب دورا هاما وفعالا في عملية الإثبات العلمي لكشف حقيقة الجريمة.

ثانيا- الدليل الإلكتروني كدليل علمي:

تتنوع الأدلة العلمية تبعا لمجالات استخدامها ومن بين أهم صور الدليل العلمي الأكثر انتشارا الدليل الإلكتروني أو التقني أو الرقمي موازاة مع الجريمة الإلكترونية وعليه ما هو مفهوم هذا الدليل ؟ وما مدى مشروعيته في إثبات جرائم التزوير في البيئة الإلكترونية ؟.

1- تعريف الدليل الإلكتروني:

عرف الدليل الإلكتروني بأنه: "الدليل الذي يجد أساسا له في العالم الافتراضي ويقود إلى الجريمة فهو كل بيانات يتم إعدادها أو تخزينها بشكل إلكتروني بحيث يمكن الحاسوب من إنجاز مهمة ما ".

[1] لامية مجدوب، مرجع سابق، ص 236 .

كما عرف كذلك بأنه الدليل المأخوذ من أجهزة الحاسوب ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية، من الممكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء.

ويمكن تعريفه بأنه "الدليل الذي تم الحصول عليه بواسطة التقنية الفنية الإلكترونية من معطيات الحاسوب وشبكة الإنترنت والأجهزة الإلكترونية الملحقة، والمتصلة به، وشبكات الاتصالات من خلال إجراءات قانونية لتقديمها للقضاء كدليل إلكتروني جنائي يصلح لإثبات الجريمة ".[1]

بعد استعراضها للتعريفات التي قيلت بشأن الدليل الإلكتروني، نلاحظ في البداية أنها متقاربة من بعضها البعض، وأنها حاولت استيعاب هذا النوع المستحدث من الدليل بالرغم من حداثته، وارتباطه بالتقنية الرقمية، إلا أن هناك بعض النقد الموجه لهذه التعريفات.[2]

2- خصائص الدليل الإلكتروني:

إن البيئة الرقمية التي يعيش فيها الدليل الإلكتروني بيئة متطورة بطبيعتها، فهي تشمل على أنواع متعددة من البيانات الرقمية تصلح منفردة أو مجتمعة لكي تكون دليلا للإدانة أو البراءة، وقد انعكس هذا العالم الرقمي على طبيعة هذا الدليل مما جعله يتصف بعدة خصائص ميزته عن الدليل الجنائي التقليدي وهي كالتالي:

- الدليل الإلكتروني ليس أقل من الدليل المادي فحسب، بل تصل إلى درجة التخيلية في شكلها وحجمها ومكان تواجدها غير المعلن لأنه من قبيل الأدلة الفنية والعلمية المستمدة من الأجهزة .

- يعتبر الدليل الإلكتروني دليلا غير ملموس فهو ليس دليلا ماديا، وإنما هو تلك المجالات المغناطيسية أو الكهربائية، حيث أن ترجمة الدليل الإلكتروني واخراجه في شكل مادي ملموس لا يعني أن هذا التجمع يعتبر هو الدليل، بل هذه العملية تعتبر عملية نقل تلك المجالات من طبيعتها الإلكترونية إلى الشكل الذي يمكن الاستدلال بها على معلومة معينة .

---

[1] دالي خلود، مرجع سابق، ص 92 .

[2] أشرف عبد القادر قنديل، مرجع سابق، ص 124 .

– الدليل الإلكتروني يصعب التخلص منه، وتعد من أهم خصائصه، بل إنه يمكن اعتبار هذه الخاصية ميزة يتمتع بها الدليل الرقمي عن غيره من الأدلة التقليدية، حيث يمكن التخلص بكل سهولة من الأوراق والأشرطة المسجلة إذا حملت في ذاتها إقرار بارتكاب شخص لجرائم وذلك بتمزيقها أو حرقها، كما يمكن أيضا التخلص من بصمات الأصابع بمسحها من موضعها، بالإضافة إلى أنه في بعض الدول أو الغربية يمكن التخلص من الشهود بقتلهم أو تهديدهم بعدم الإدلاء بالشهادة. [1]

– الدليل الإلكتروني ذو طبيعة تقنية، هذه الخاصية ترجع للبيئة التي يعيش فيها الدليل الإلكتروني ويستوحى منها وهي بيئة تقنية أو رقمية أو افتراضية بحته في نطاق الجرائم الإلكترونية وهذه البيئة تتمثل في أجهزة الحاسب الآلي وملحقاته والخوادم والمضيفات والشبكات بمختلف صورها، ذلك أن الأدلة الرقمية لا تشبه الأدلة العادية أو التقليدية، كونها نبضات رقمية أو كهرومغناطيسية لا يمكن ضبط شكلها أو حجمها أو مكان وجودها، فهي ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان إلى آخر عبر شبكات الاتصال متعدية بذلك المكان والزمان .[2]

– يمكن استخراج نسخ من الدليل الإلكتروني مطابقة للأصل ولها نفس القيمة العلمية والحجية الثبوتية، الشيء الذي لا يتوافر في الدليل التقليدي، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقدان والتلف والتغيير عن طريق عمل نسخ طبق الأصل في الدليل .

– يمكن من خلال استخدامه رصد المعلومات عن الجاني وتحليلها، حيث إن الدليل الإلكتروني يمكن من تسجيل تحركات الفرد وسلوكياته، ولذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل التقليدي.

المطلب الثاني: ضوابط سلطة القاضي الجنائي في قبول الدليل الإلكتروني وتقديره .

الدليل الإلكتروني شأنه شأن باقي الأدلة الأخرى يخضع لنفس القواعد المقررة لباقي الأدلة، سواء كانت هذه القواعد تتعلق بسلطة القاضي الجنائي في قبول الدليل الإلكتروني، أو تتعلق بسلطته في تقدير هذا النوع من الدليل، ذلك أن القاضي لا يقدر إلا

[1] أشرف عبد القادر قنديل، مرجع سابق، ص 127 .
[2] عائشة بن قارة، مرجع سابق، ص 62 .

الدليل المقبول، ولا يكون مقبولا إلا بعد التقين من مراعاة الدليل الإلكتروني أي آثار قانونية .

وبالنظر إلى الطبيعة الخاصة التي يتميز بها الدليل الإلكتروني، وما قد يصاحب الحصول عليه من خطوات معقدة، فإن قبوله في الإثبات قد يثير العديد من المشكلات، حيث أن مستودع هذه الأدلة هو الوسائل الإلكترونية.

الفرع الأول: أساس قبول وتقدير الدليل الإلكتروني في إثبات جرائم التزوير الإلكتروني.

أولا- أساس قبول الدليل الإلكتروني في إثبات جرائم التزوير الإلكتروني:

إن تحديد الأساس الذي يقوم عليه مسألة قبول الدليل الإلكتروني في الإثبات الجنائي تتوقف على نوع أو طبيعة نظام الإثبات السائد في تلك الدولة ومعلوم أن نظم الإثبات الجنائي ثلاثة وهي كالتالي:

- **النظام الأول:** يتمثل في مبدأ حرية الإثبات، ومنها سلطة القاضي في قبول جميع الأدلة، وهذا تكون جميع طرق الإثبات مقبولة، ما لم يستبعد المشرع بعضها صراحة، كاستبعاد المراسلات بين المتهم ومحاميه مثلا .وهذا ما أخذ به المشرع الجزائري كأصل عام من خلال المادة 212 من ق إ ج ج، كما أخذ به نظيره المصري بموجب المادة 291 من قانون الإجراءات الجزائية المصري تأثرا بالمشرع الفرنسي الذي جسد من خلال نص المادة 427 من قانون الإجراءات الجزائية الفرنسي وبالرجوع لنص المادة 212، حيث يتميز هذا النظام بعم تحديد الأدلة، بمعنى أن الخصوم لهم الحرية في الالتجاء إلى أي دليل يمكنهم من إثبات ادعاءاتهم، كما أن هذا النظام يخول للقاضي سلطة تقييم الأدلة دون أن يفرض عليه قيدا أو شرطا .

- **النظام الثاني:** يتمثل في نظام الإثبات القانوني أي المقيد، حيث تحدد الأدلة التي يجوز للقاضي الجنائي قبولها، كالقانون الهولندي من قانون الإجراءات الجزائية والقانون الألماني الذي يحدد على سبيل الحصر وسائل الإثبات التي يتعين على القاضي قبولها وهو ما أخذ به المشرع الجزائري كاستثناء من خلال المادة 212 من [1]ق إ ج ج .

[1] أنظر المادة 212 من ق إ ج ج .

- **النظام الثالث:** ويتمثل في النظام المختلط والمتمثلة في القوانين الأنجلوسكسونية حيث تقيد من حرية الإثبات في مرحلة الفصل في مسألة الإدانة أو البراءة، أما في مرحلة تحديد العقوبة فيسود مبدأ حرية الإثبات.

1- مبدأ حرية الإثبات الجنائي كأساس لقبول الدليل الإلكتروني:

تعتبر حرية الإثبات في المسائل الجنائية من المبادئ المستقرة في نظرية الإثبات الجنائي، وذلك بخلاف المسائل المدنية حيث يحدد القانون سلفا وسائل الإثبات وقواعد قبولها وقولها.

كما تم الإشارة من قبل بأن المشرع الجزائري أخذ بمبدأ حرية الإثبات الجنائي في المادة212 من ق إ ج ج بقولها: " يجوز إثبات الجرائم بأي طريق من طرق الإثبات".

وذلك للأسباب التالية:

- إن موضوع الإثبات في الدعوي العمومية يرد على وقائع قانونية تنتمي إلى الماضي، لذلك لابد للمحكمة أن تستعين بكل الوسائل الممكنة كي تعيد لها رواية ما حدث.
- من المسلم به أن قرينة البراءة تلقي عبء الإثبات كلية على عاتق سلطة الاتهام مما جعلت مهمة هذه الأخيرة جد صعبة.
- إن طبيعة المصلحة التي تحميها الدعوى الجنائية تختلف عن تلك التي تحميها الدعوى المدنية.
- مبدأ حرية الإثبات يعد بمثابة إقرار ضمني من المشرع بعدم قدرة الأدلة التقليدية والتي لو تم حصرها كأدلة إثبات على مواجهة الجرائم المستحدثة ومنها الجريمة الإلكترونية.

وعليه يتضح أنه بأنه يجوز للقاضي الاستناد إلى الدليل الإلكتروني في إثبات جرائم التزوير في البيئة الإلكترونية تحديدا وكافة الجرائم الإلكترونية الأخرى، إذا تم احترام ضابط المشروعية ذلك أن الحرية هنا لا يقصد بها إمكانية اللجوء إلى وسائل غير قانونية ويترتب على ذلك عدم مشروعية الدليل الإلكتروني.[1]

2- النتائج المترتبة على تطبيق مبدأ حرية الإثبات الجنائي:[2]

[1] لامية مجدوب، مرجع سابق، ص 247 .

[2] أشرف عبد القادر قنديل، مرجع سابق، ص 197 .

إن إعمال مبدأ حرية الإثبات الجنائي يجعل القاضي الجنائي يتمتع بدور إيجابي في توفير وقبول وتقدير الدليل الجنائي بما في ذلك الدليل الإلكتروني.

- الدور الإيجابي للقاضي الجنائي في توفير الدليل الإلكتروني:

ويقصد به عدم التزام القاضي بما يقدمه له أطراف الدعوى من أدلة، وإنما له سلطة بل وواجب عليه أن يبادر من تلقاء نفسه إلى اتخاذ جميع الإجراءات لتحقيق الدعوى والكشف عن الحقيقة الفعلية فيها .

وتجدر الإشارة أن المقصود بالقاضي ليس هو قضاء الحكم فحسب، وإنما يشمل أيضا قضاء التحقيق باعتبار أن مشكلة الإثبات قد تثور في أي مرحلة تمر بها الدعوي الجنائية بل يمكن أن تثور قبل ذلك أي في مرحلة جمع الاستدلالات أيضا.

- الدور الإيجابي للقاضي الجنائي في قبول الدليل الإلكتروني:

أن القاضي الجنائي أول ما يتأكد منه في هذه المرحلة – مرحلة قبول الدليل – هو مدى مشروعيته (الدليل الإلكتروني)، وذلك قبل الوصول إلى المرحلة الأخيرة ألا وهي مرحلة تقدير الدليل، لأن القاضي الجنائي لا يقدر إلا الدليل المقبول، ولا يكون كذلك إلا إذا كان مشروعا .

ثانيا- سلطة القاضي الجنائي في تقدير الدليل الإلكتروني:

رأينا أن القاضي الجنائي يتمتع بسلطة قبول أي دليل بما في ذلك الأدلة الإلكترونية وفي مقابل ذلك فإنه يتمتع كذلك بحرية تقدير ذلك الدليل، لكن المشرع الجزائري وضع ضوابط لهذه السلطة في تقدير الدليل وهي:

1- الضوابط المتعلقة بمصدر الاقتناع:

إن القاضي الجنائي ليس حرا في تقدير أي دليل إلكتروني، بل هو حر فقط في تقدير الدليل الإلكتروني المقبول في الدعوى، أي تم الحصول عليه بطريق مشروع وعليه فإن مسألة قبول الدليل ينبغي أن تحظى بفحص ودراسة سابقة على حرية القاضي في تقدير الدليل الإلكتروني.[1]

[1] عائشة بن قارة مصطفى، مرجع سابق، ص 267 وما يليها .

كما لا يجوز للقاضي أن يبني حكمه على أدلة لم تطرح لمناقشة الخصوم في الجلسة طبقا للمادة 212 فقرة 02 من ق إ ج ج بقولها: "ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت فيها المناقشة حضوريا أمامه".

2- الضوابط المتعلقة بالاقتناع ذاته:

وذلك من خلال مبدأ الاقتناع الشخصي للقاضي الجزائي، حيث يتيح للقاضي حرية كبيرة في تقدير أدلة الإثبات بما فيها الدليل الإلكتروني ويلزم لصحة سلامة اقتناع القاضي بالدليل أن يكون مبنيا على الجزم واليقين، وأن يكون متلائما مع مقتضيات العقل والمنطق.

- بلوغ الاقتناع القضائي درجة اليقين:

وهذا اليقين هو يقين قضائي وليس يقين شخصي، فيجب أن يصدر حكم القاضي بناء على اقتناع يقيني بصحة ما ينتهي إليه م وقائع لا مجرد الظن والاحتمال، إذ أن الشك يفسر لصالح المتهم، أخذا بقاعدة أساسية أن الأصل في الإنسان البراءة.

فالجزم بوقوع جريمة التزوير الإلكتروني ونسبتها للمتهم يتطلب نوعا جيدا من المعرفة، وهي المعرفة العلمية للقاضي بالمسائل المعلوماتية ولا سبيل له في ذلك سوى الاستئذان برأي الخبير إذا ما اطمأن إليه واقتنع به.

- ملائمة الاقتناع القضائي لمقتضيات العقل والمنطق:

بمعنى أن يكون الدليل الإلكتروني مؤديا إلى ما رتبه الحكم دون تعسف في الاستنتاج أو تنافر مع متطلبات العقل والمنطق.

ومع ذلك تجدر الإشارة إلى أن تقييد القاضي الجنائي عند تقديره للدليل الإلكتروني بضوابط معينة سواء كانت لضمانة منع الاستبداد والتحكم، بل لابد من ضمانة أخرى أشد من سابقيها، لتجعل سلطة القاضي الجنائي التقديرية تدور في إطار معتدل بهدف الوصول إلى الحقيقة الواقعية باعتبارها غرض الدعوى الجنائية وتتمثل هذه الوسيلة في رقابة المحكمة العليا على سلطة القاضي الجنائي التقديرية.[1]

[1] عائشة بن قارة مصطفى، مرجع سابق، ص 510.

الفرع الثاني: القيود الواردة على حرية القاضي الجنائي في قبول الدليل الإلكتروني.

الواقع أن حرية القاضي الجنائي في هذا الشأن لا يمكن أن تكون مطلقة من كل قيد، لأن السلطة المطلقة مفسدة مطلقة، لذا كان من الضروري رسم ضوابط وأطر معينة يتعين أن تمارس هذه السلطة في نطاقها بحيث لا تنحرف عن الغرض الذي يبغيه المشرع من ورائها.

ونتيجة لذلك حددت أغلب التشريعات الأدلة التي تقبل في إثبات بعض الجرائم بحيث لا يجوز الإثبات بغيرها، كأدلة إثبات جريمة الزنا مثلا، وهناك قيد عام يحد من حرية القاضي في قبول الدليل الجنائي عامة، والدليل الإلكتروني خاصة في إثبات جرائم التزوير في المجال الإلكتروني وهو أن يكون قد تم، وتتمثل هذه القيود فيما يلي: الحصول عليه بطريقة مشروعة.[1]

أولا- قيد مشروعية طريقة الحصول على الدليل الإلكتروني:

تخضع قواعد الإثبات الجنائي لمبدأ المشروعية ومقتضاه أن الدليل الجنائي بما يتضمنه من أدلة مستخرجة من وسائل إلكترونية كالكمبيوتر مثلا، لا يكون مشروعا ومن ثم مقبولا في الإثبات، إلا إذا جرت عملية البحث عنه والحصول عليه وإقامته أمام القضاء في إطار أحكام القانون واحترام قيم العدالة وأخلاقياتها التي يحرص على حمايتها.

وبالتالي لا يجوز للقاضي الجنائي أن يقبل في إثبات إدانة المتهم بالتزوير دليلا إلكترونيا تم الحصول عليه من تفتيش لنذام معلوماتي باطل، وذلك إثر صدور إذن بالتفتيش من جهة غير مختصة أو لم تكن جريمة التزوير الإلكتروني لم تقع بالفعل، كما يقر الفقه والقضاء الجنائي بعدم المشروعية متى كانت طريقة الحصول على الدليل الإلكتروني تتعارض مع القواعد العامة للإجراءات الجنائية والمبادئ العامة للقانون الجنائي كالقواعد والأسس التي توجب احترام قيم العدالة وأخلاقياتها والنزاهة في الحصول على الأدلة واحترام حقوق الدفاع .

[1] أشرف عبد القادر قنديل، مرجع سابق، ص 206.

حيث نصت المادة 336 من قانون الاجراءات الجزائية المصري على أنه: "إذا تقرر بطلان أي إجراء، فإنه يتناول جميع الآثار التي تترتب عليه مباشرة، ويلزم إعادته متى أمكن ذلك ".

وهي نفس القاعدة المتبعة في قانون الإجراءات الجزائية الجزائري، حيث نصت المادة 157 فقرة1 منه على أن: "تراعى الأحكام المقررة في المادة المتعلقة باستجواب المتهمين والمادة 105 المتعلقة بسماع المدعي المدني وإلا ترتب على مخالفتها بطلان الإجراء نفسه وما يتلوه من إجراءات ..."

ثانيا- القيود المستمدة من نصوص قانونية خاصة:

وهي الأدلة المحددة بنصوص قانونية خاصة فلا يجوز للقاضي دحضها وعدم الأخذ بها حيث تقيد حرية الأُثبات الجنائي كما تقيد مبدأ الاقتناع الشخصي للقاضي الجنائي ومثال ذلك جريمة الزنا بموجب المادة 341 ق ع ج وتتمثل في ثلاث أدلة وهي: محضر قضائي يحرره أحد رجال الضبط القضائي عن حالة التلبس، وإما، وعليه إقرار وارد في رسائل أو مستندات صادرة عن المتهم أو إما إقرار قضائي لا يمكن قبول أدلة أخرى غير ما أقرته المادة 341 من ق ع ج ولو كان دليلا الكترونيا سواء في شكل صور فيديو أو رسالة إلكترونية أو عن طريق البريد الإلكتروني.[1]

بالإضافة إلى قيد إثبات المسائل غير الجنائية أو الأولية التي تطرح على المحكمة الجنائية حيث يكون الفصل فيها ضروريا للفصل في الدعوى العمومية، فذلك يخضع للقانون الخاص بتلك المسائل الأولية سواء كانت مدنية أو تجارية أو أحوال شخصية أو غيرها وهذا تطبيقا للقاعدة القائلة بأن قواعد الإثبات إنما ترتبط بالموضوع الذي ترد عليه لا بنوع المحكمة المعروضة عليها.

نعتقد أنه يمكن للقاضي الجنائي الاستعانة بالدليل الإلكتروني في إثبات المسائل الأولية خاصة المدنية والتجارية ذلك أن المشرع نظم في مختلف الدول المقارنة

[1] تنص المادة 341 من ق ع ج على ما يلي: " الدليل الذي يقبل عن ارتكاب الجريمة المعاقب عليها بالمادة 339 يقوم إما على محضر قضائي يحرره أحد رجال الضبط القضائي عن حالة تلبس وإما بإقرار وارد في رسائل أو مستندات صادرة عن المتهم وإما بإقرار قضائي ".

المعاملات الإلكترونية وسبل إثباتها وأعطى للمحررات الإلكترونية حجية تامة شأنها شأن المحررات الورقية.

خلاصة الفصل الثاني:

كخلاصة لهذا الفصل يمكن القول بأن الجرائم الإلكترونية بصفة عامة وجريمة التزوير الإلكتروني بصفة خاصة، كغيرها من الجرائم الأخرى تخضع إلى قواعد إجرائية تقليدية طبقا لقانون الإجراءات الجزائية سواء كانت مادية أو شخصية والمتمثلة في المعاينة والتفتيش والضبط والشهادة والخبرة بالإضافة إلى الإجراءات المستحدثة والمتمثلة في اعتراض المراسلات وتسجيل والتقاط الأصوات والصور والتسرب، إلا أنها تختلف عن باقي الجرائم في بعض الأحكام الإجرائية طبقا للقانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما .

أما بالنسبة لطرق إثبات جرائم التزوير الإلكتروني فهي خاضعة لنفس طرق الإثبات المعروفة المتمثلة في الاعتراف والمحررات والخبرة والشهادة والمعاينة والقرائن إلا أن أهم طريق للإثبات في هذه الجرائم هي الخبرة والدليل العلمي والإلكتروني.

الخاتمة

الخاتمة

في ختام هذه الدراسة التي حاولنا من خلالها تسليط الضوء على جريمة من أهم الجرائم الإلكترونية وهي جريمة التزوير الإلكتروني ، التي تدخل فيها الوسائل الإلكترونية بشكل كبير ، وتتعاظم أهميتها كل يوم ، نظرا لانتشار استخدام المحررات الإلكترونية على مستوى الأفراد و المؤسسات توصلنا إلى الإجابة على الإشكالية الرئيسية لهذا الموضوع وهي أن النصوص الجنائية الحالية مازالت قاصرة على تغطية كل صوره سواء على المستوى الموضوعي أو الإجرائي و أنها بحاجة إلى تعديل أو تحيين يواكب التطورات و المستجدات في المجال الإلكتروني و التي تكون عرضة للتزوير المعلوماتي أو الإلكتروني.

ولقد خرجت بمجموعة من النتائج و التوصيات وهي كالتالي :

أولا : النتائج .

- تتميز جريمة التزوير الإلكتروني عن جريمة التزوير التقليدي في صعوبة الكشف عنها .

- تكتسب جريمة التزوير الإلكتروني طبيعة عالمية أي أنها جريمة عابرة للحدود الوطنية .

- يرتكبها أشخاص غير عاديين أي يرتكبها مجرم إلكتروني يتميز بمهارات وسمات كالاحترافية في استخدام الحاسب الآلي .

- لم يول المشرع الجزائري اهتماما واضحا لجرائم التزوير الإلكتروني رغم أنها من أكثر الجرائم الإلكترونية انتشارا و ذيوعا ، حيث لم يفرد نصوص خاصة بالتزوير الإلكتروني، ولم يقم حتى بتعديل نصوص قانون العقوبات التقليدية الخاصة بالتزوير مثلما فعل المشرع الفرنسي حيث عدل نص المادة 441 من قانون العقوبات الفرنسي و أدرج فيها كل أشكال التزوير ووسائله التقليدية منها و المستحدثة.

- كما أن جريمة التلاعب بمعطيات الحاسب الآلي التي جرمها المشرع الجزائري بموجب نص المادة 394 مكرر01 من قانون العقوبات الجزائري هي الصورة المثلى والحقيقية للتزوير في البيئة الإلكترونية في التشريع الجزائري.

- كما أنه من حيث العقوبة التي هي مقررة للتزوير التقليدي لا تحقق الغاية من فرضها وتطبيقها على المجرم الإلكتروني لأن جريمة التزوير الإلكتروني أشد خطورة من جريمة التزوير الإلكتروني ولها طبيعة خاصة.

- عدم كفاية الإجراءات التقليدية أو المستحدثة في إثبات جرائم التزوير الإلكتروني المنصوص عليها في قانون الإجراءات الجزائية الجزائري.

- استحدث المشرع الجزائري جملة من الإجراءات بشأن ملاحقة هذه الفئة من الجرائم بموجب القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما ، كالتفتيش والحجز في المنظومة المعلوماتية إضافة إلى إجراء المراقبة الإلكترونية كوسيلة وقائية قانونية إضافة إلى إجراء حفظ المعطيات المتعلقة بحركة السير .

- تمتع القاضي الجزائي بدور ايجابي من حيث تقدير القيمة القانونية للدليل الإلكتروني و خضوعه للسلطة التقديرية شأنه شأن باقي الأدلة .

ثانيا : التوصيات .

- استحداث سلطات مختصة لمكافحة جريمة التزوير الإلكتروني .

- تعديل نصوص قانون العقوبات الجزائري التقليدية الخاصة بالتزوير .

- وضع قواعد قانونية صارمة تتلاءم مع طبيعة هذه الجريمة .

- ضرورة القيام بإعداد دورات تدريبية بصفة منتظمة لرجال الشرطة القضائية والمحققين والقضاة و الخبراء لكيفية التعامل مع الجرائم الإلكترونية عموما والتزوير الإلكتروني خصوصا.

- تعديل قانون الإجراءات الجزائية في طرق الطعن لتتلاءم مع الجرائم الإلكترونية .

تم بحمد الله تعالى و فضله و كرمه أرجو أن ينال رضاءكم

وشكرا.

قائمة المصادر والمراجع

أولا: قائمة المصادر

النصوص القانونية

1- القوانين:

01 – قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية الصادر سنة 2001 .

02- القانون رقم 17-04، المؤرخ في 16 فبراير سنة 2017، المعدل والمتمم للقانون رقم 79-07 المؤرخ في 21 يوليو 1979، المتضمن قانون الجمارك، الجريدة الرسمية، العدد 11 ،المؤرخة في 19 فبراير سنة 2017 .

03- القانون رقم 09-04، المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتهما، الجريدة الرسمية، العدد 47، المؤرخة في 16 أوت 2009 .

04- القانون رقم 15-01، المؤرخ في 01 فيفري 2015، المتضمن القواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، الجريدة الرسمية، العدد 06، المؤرخة في 10 فيفري 2015 .

05- القانون رقم 18- 04، المؤرخ في 10 مايو 2018، المتضمن القواعد العامة المتعلقة بالبريد و الاتصالات الإلكترونية، الجريدة الرسمية، العدد27، المؤرخة في 13 مايو سنة 2018 .

2- الأوامر:

01- الأمر رقم 66-155، المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات الجزائري، المعدل و المتمم، الجريدة الرسمية، العدد 49، المؤرخة في 11 يونيو 1966.

02- الأمر رقم 66-155، المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية الجزائري، المعدل و المتمم، الجريدة الرسمية، العدد 48، المؤرخة في 10 يونيو 1966 .

03- الأمر رقم 03-05، المؤرخ في 19 يوليو 2003، المتعلق بحقوق المؤلف و الحقوق المجاورة، الجريدة الرسمية، العدد 44، المؤرخة في 23 يوليو 2003 .

ثانيا: قائمة المراجع باللغة العربية .

1- المؤلفات:

1-1- المؤلفات العامة:

01- أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الطبعة 14 ،الجزء 2، دار هومة، الجزائر، 2013 .

02 - أحمد الشافعي، البطلان في قانون الإجراءات الجزائية -دراسة مقارنة-، الطبعة الرابعة، دار هومة، الجزائر، 2005 .

03- عبد الرحمان خلفي، محاضرات في الإجراءات الجزائية، الطبعة الثانية، دار الهدى، عين مليلة، الجزائر، 2012 .

04- عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري -التحري و التحقيق-، دار هومة، الجزائر، 2005 .

1-2- المؤلفات المتخصصة:

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

02- أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2015 .

03- إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2007 .

04- جلال محمد الزغبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية -دراسة مقارنة- ،دار الثقافة للنشر و التوزيع، عمان، 2010 .

05- حسني مراد، إجراءات التحقيق المستحدثة في قانون الإجراءات الجزائية الجزائري (عملية التسرب في المادة الجزائية)، الجزء الأول، الطبعة الأولى، سلسلة المعارف القانونية و القضائية، دار نشر المعرفة، الرباط، المغرب، 2013 .

06- رياض فتح الله بصلة، جرائم بطاقة الائتمان، الطبعة الأولى، دار الشروق، القاهرة، مصر، 1995 .

07- زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدى للطباعة و النشر و التوزيع، عين مليلة، الجزائر، 2011 .

08- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري و المقارن، دار الجامعة الجديدة، الإسكندرية، مصر ،2010 .

09- عامر محمود الكسواني، التزوير المعلوماتي للعلامة التجارية، دار الثقافة للنشر و التوزيع، عمان، 2010 .

10- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دار النهضة العربية، القاهرة، مصر، 2009 .

11- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر و الإنترنت في التشريعات العربية، الزقازيق، مصر، 2009 .

12- عيسى غسان ربضي، القواعد الخاصة بالتوقيع الإلكتروني، الطبعة الثانية، دار الثقافة للنشر و التوزيع، عمان، 2012 .

13- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2004.

14- محمود أحمد عبابنة، جرائم الحاسوب و أبعادها الدولية، دار الثقافة، عمان، 2005.

15- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، مصر، 2006.

16- نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة، عمان، 2008.

2- الأطروحات و المذكرات:

2-1- الأطروحات:

01- حفصي عباس، جرائم التزوير الإلكتروني (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في العلوم الإسلامية، تخصص شريعة و قانون، جامعة وهران 1، 2015 .

02- لامية مجدوب، التزوير الإلكتروني، أطروحة مقدمة لنيل شهادة دكتوراه علوم في الحقوق، تخصص قانون جنائي، جامعة باجي مختار، عنابة، 2017 .

03- متى فتحي أحمد عبد الكريم، الجريمة عبر الشبكة الدولية للمعلومات صورها مشاكل إثباتها، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق، جامعة القاهرة، 2008 .

2-2- المذكرات:

01- ابتسام يغو، إجراءات المتابعة الجزائية في الجريمة المعلوماتية، مذكرة تكميلية لنيل شهادة الماستر في القانون، تخصص قانون جنائي للأعمال، جامعة العربي بن مهيدي، أم البواقي، 2016 .

02- برهوم الطاهر، جرائم التزوير الإلكتروني، مذكرة مقدمة لنيل شهادة الماستر، تخصص قانون جنائي و علوم جنائية، جامعة العربي التبسي، تبسة، 2019 .

03- دالي خلود، التزوير الإلكتروني، مذكرة ماستر، تخصص القانون الجنائي الأساسي و العدالة الجنائية، جامعة باجي مختار، عنابة، 2016 .

04- سارة غادري، الأدلة القولية (الإعتراف و الشهادة)ودورها في الإثبات الجنائي، مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة المسيلة، 2014 .

3- المقالات العلمية:

01- أحمد محمد حسان، " الحماية القانونية للمحادثات الهاتفية و الشخصية ضد التنصت و التسجيل الصوتي "، مجلة كلية الدراسات العليا، دون عدد، دون سنة نشر .

02- عبد الله بلقاسم، " الطبيعة الخاصة لجريمة التزوير الإلكتروني في المحررات الإلكترونية "، مجلة الدراسات القانونية المقارنة، المجلد 06، العدد 02، 2020 .

03- عبد الرحمان فرزات، " المعلوماتية و قانون العقوبات الواقع و الآفاق "، مجلة المحامون السورية، العدد 05 و 06، أيار، حزيران، 2001 .

04- فتيحة عمارة، " جريمة التزوير الإلكتروني "، مجلة القانون و المجتمع، المجلد 07، العدد 01، 2019.

05- لامية مجدوب، " إجراء التفتيش في التزوير الإلكتروني "، مجلة التواصل في الاقتصاد و الإدارة و القانون، المجلد 25، العدد 03، 2019.

الفهرس

الفهرس

العنوان	الصفحة
الآية القرآنية **شكر وعرفان** **الاهداء**	
المقدمة	**1**
الفصل الأول : الأحكام الموضوعية لجريمة التزوير الإلكتروني	
المبحث الأول : مفهوم جريمة التزوير الإلكتروني	**7**
المطلب الأول : تعريف التزوير الإلكتروني و تمييزه عن غيره من المصطلحات المشابهة	**7**
الفرع الأول : تعريف التزوير الإلكتروني	**7**
الفرع الثاني : تمييز التزوير الإلكتروني عن غيره من المصطلحات المشابهة	**10**
المطلب الثاني : خصائص جريمة التزوير الإلكتروني	**12**
الفرع الأول : ارتكاب الجريمة في أي مرحلة من مراحل نظام التشغيل	**12**
الفرع الثاني : انعدام الأثر المادي للتزوير الإلكتروني	**12**
الفرع الثالث : جريمة عابرة للحدود الوطنية	**13**
الفرع الرابع : جريمة فادحة الأضرار	**13**
الفرع الخامس : يرتكبها مجرم الكتروني	**14**
الفرع السادس : تحتاج إلى خبرات فنية عالية	**14**
المطلب الثالث : صور جريمة التزوير الإلكتروني	**14**
الفرع الأول : تزوير التوقيع الإلكتروني	**14**
الفرع الثاني : تزوير بطاقة الائتمان	**16**

الفرع الثالث : التزوير عن طريق البريد الإلكتروني	17
المبحث الثاني : أركان جريمة التزوير الإلكتروني و الجزاءات المقررة لها	19
المطلب الأول : أركان جريمة التزوير الإلكتروني	19
الفرع الأول : الركن الشرعي في جريمة التزوير الإلكتروني	19
الفرع الثاني : الركن المادي في جريمة التزوير الإلكتروني	21
الفرع الثالث : الركن المعنوي في جريمة التزوير الإلكتروني	25
المطلب الثاني : الجزاءات المقررة لجريمة التزوير الإلكتروني	26
الفرع الأول : بالنسبة للشخص الطبيعي	26
الفرع الثاني : بالنسبة للشخص المعنوي	30
الفصل الثاني : الأحكام الإجرائية لجريمة التزوير الإلكتروني	
المبحث الأول : إجراءات جمع الأدلة في جريمة التزوير الإلكتروني	37
المطلب الأول : الإجراءات التقليدية	37
الفرع الأول : الإجراءات المادية	37
الفرع الثاني : الإجراءات الشخصية	47
المطلب الثاني : الإجراءات الحديثة	50
الفرع الأول : الإجراءات المستحدثة بموجب قانون الإجراءات الجزائري	50
الفرع الثاني : الإجراءات المستحدثة بموجب القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتهما	55
المبحث الثاني : إثبات جرائم التزوير الإلكتروني	58
المطلب الأول : طرق الإثبات	58
الفرع الأول : مدى فعالية طرق الإثبات في التزوير الإلكتروني	58
الفرع الثاني : الإثبات العلمي	62

المطلب الثاني : ضوابط سلطة القاضي الجنائي في قبول وتقدير الدليل الإلكتروني	**64**
الفرع الأول : أساس قبول وتقدير الدليل الإلكتروني في إثبات جرائم التزوير الإلكتروني	**65**
الفرع الثاني : القيود الواردة على حرية القاضي الجنائي في قبول الدليل الإلكتروني	**69**
الخاتمة	**74**
قائمة المصادر و المراجع	**77**
الفهرس	
الملخص	

الملخص :

إثر التطورات العلمية في مجال التكنولوجيا ، فقد ظهرت ما يعرف بالجرائم الإلكترونية نتيجة لسوء استخدامها ، ومن بين هذه الجرائم نجد جرائم التزوير الإلكتروني و التي لها طبيعة خاصة تختلف عن جرائم التزوير التقليدية سواء في أحكامها الموضوعية المنصوص عليها في قانون العقوبات الجزائري أو الإجرائية المنصوص عليها في قانون الإجراءات الجزائية ، لذلك فقد سلطت الضوء على هذه جرائم التزوير الإلكتروني لمعرفة مدى تصدي المشرع الجزائري لمعالجة هذا النوع من الجرائم .

Summary :

Following the scientific developments in the field of technology, what is known as cybercrime has emerged as a result of its misuse, and among these crimes we find the crimes of electronic forgery, which have a special nature that differs from traditional forgery crimes, whether in its substantive provisions stipulated in the Algerian Penal Code or the procedural ones stipulated in The Code of Criminal Procedure, so it has shed light on these crimes of electronic fraud to know the extent to which the Algerian legislature has addressed this type of crime.