جامعة الشرق الأوسط
MIDDLE EAST UNIVERSITY
Amman - Jordan

الحماية الجزائية للمستند الالكتروني

"دراسة مقارنة"

Criminal Protection of the Electronic Document

"A comparative Study "

إعداد

عمر حسين علي الدليمي

إشراف

الأستاذ الدكتور أحمد اللوزي

قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في القانون العام

قسم القانون العام

كلية الحقوق

جامعة الشرق الأوسط

حزيران، 2019

تفويــض

أنا عمر حسين علي الدليمي أفوض جامعة الشرق الأوسط بتزويد نسخ من رسالتي ورقياً وإلكترونياً للمكتبات، أو المنظمات، أو الهيئات والمؤسسات المعنية بالأبحاث والدراسات العلمية عند طلبها.

الاسم: عمر حسين علي الدليمي

التاريخ: 16 / 06 /2019.

التوقيع:

قرار لجنة المناقشة

نوقشت هذه الرسالة وعنوانها: " **الحماية الجزائية للمستند الالكتروني(دراسة مقارنة)**". وأجيزت بتاريخ: ١١/٦/2019.

أعضاء لجنة المناقشة

	جهة العمل	التوقيع
الدكتور محمد الشباطات	رئيساً جامعة الشرق الاوسط	.....
الأستاذ الدكتور احمد اللوزي	مشرفاً جامعة الشرق الاوسط	.....
الأستاذ الدكتور اكرم الفايز	عضواً خارجياً جامعة الاسراء	.....

الشكر والتقدير

بسم الله والصلاة والسلام على أشرف المرسلين وخاتم الأنبياء سيدنا محمد صلى الله عليه وسلم.

أتقدم بجزيل الشكر والعرفان الجميل الى من شملني بعلمه وفكره وتشجيعه وعطائه وسعه صدره ولم يبخل علي بوقته وارشاداته وتوجيهاته المثمرة الى الذي كان لي كألاب والاخ والمثل الاعلى الى مشرفي الدكتور أحمد اللوزي.

كما أتقدم بوافر الشكر وعظيم الامتنان لأعضاء لجنة المناقشة أساتذتي الدكتور أكرم الفايز، والدكتور محمد الشباطات.

وأتقدم بالشكر الموصول إلى أساتذتي الأفاضل في قسم القانون في جامعة الشرق الأوسط على كل ما قدموه من جهود طيلة فترة الدراسة.

الباحث

الإهداء

إلى

من كلله الله بالهيبه والوقار.....الى من علمني العطاء دون انتظار

الى من احمل اسمه بكل افتخار.....الى من حصد الاشواك عن دربي ليمهد لي طريق العلم

(والدي العزيز) الى ملاكي في الحياة... الى معنى الحب والحنان والتفاني...الى بسمه الحياة

وسر الوجود الى من كان دعائها سر نجاحي..... وحنانها بلسم جروحي (والدتي الغالية)

من تكاتفت أيدينا دوماً لنكون جسداً واحداً.... إخوتي وأخواتي

إلى من شجعني وحفزني وساندني....

الباحث

عمر حسين علي الدليمي

فهرس المحتويات

الموضوع	الصفحة
العنوان	أ
التفويض	ب
قرار لجنة المناقشة	ج
الشكر والتقدير	د
الإهداء	هـ
فهرس المحتويات	و
الملخص باللغة العربية	ح
الملخص باللغة الانجليزية	ط
الفصل الأول: خلفية الدراسة وأهميتها	
أولاً: المقدمة	1
ثانياً: مشكلة الدراسة	2
ثالثاً: اسئلة الدراسة	2
رابعاً: أهداف الدراسة	3
خامساً: أهمية الدراسة	3
سادساً: حدود الدراسة	4
سابعاً: محددات الدراسة	4
ثامناً: المصطلحات الاجرائية	4
تاسعاً: الدراسات السابقة	5
عاشراً: الإطار النظري للدراسة	5
حادي عشر: منهجية الدراسة	6
الفصل الثاني: ماهية المستند الإلكتروني	
المبحث الأول: مفهوم المستند الإلكتروني	8
المطلب الأول: تعريف المستند الإلكتروني وخصائصه	8
المطلب الثاني: صور المستند الإلكتروني	16
المبحث الثاني: نطاق المستند الإلكتروني	19
المطلب الاول: شروط المستند الإلكتروني	19
المطلب الثاني: تمييز المستند الإلكتروني عن المستند التقليدي	25

الفصل الثالث: الحماية الجزائية الموضوعية للمستند الإلكتروني

المبحث الاول: الحماية الجزائية الموضوعية للمستند الإلكتروني وفقاً للنصوص العقابية التقليدية 29
المطلب الاول: مدى خضوع المستند الالكتروني للنصوص العقابية لجريمة التزوير 29
المطلب الثاني: مدى خضوع المستند الالكتروني للنصوص العقابية لجرائم الأموال 36
المبحث الثاني: الحماية الجزائية الموضوعية للمستند الإلكتروني وفقاً للنصوص العقابية المستحدثة ... 47
المطلب الاول: جريمة الدخول أو البقاء عن طريق الغش داخل نظام المعالجة الآلية للمعطيات ... 49
المطلب الثاني: جرائم الإعتداء على سلامة المعطيات 53
المطلب الثالث: الجرائم المنصوص عليها في قانون المعاملات الالكترونية "جرائم التوقيع والتصديق الإلكترونيين" 55

الفصل الرابع: الحماية الجزائية الإجرائية للمستند الإلكتروني

المبحث الاول: إجراءات التحري والتحقيق في الجرائم الماسة بالمستند الالكتروني 59
المطلب الاول: إجراءات التحري والتحقيق التقليدية في الجرائم الماسة بالمستند الإلكتروني 60
المطلب الثاني: إجراءات التحري والتحقيق الحديثة في الجرائم الماسة بالمستند الإلكتروني 66
المبحث الثاني: إجراءات المحاكمة في الجرائم الماسة بالمستند الإلكتروني 69
المطلب الاول: تحديد المحكمة الجنائية المختصة 69
المطلب الثاني: تقييم الأدلة الرقمية المستخلصة من الجرائم الماسة بالمستند الإلكتروني 74
الفصل الخامس: الخاتمة (النتائج والتوصيات) 79
أولا: الخاتمة 79
ثانيا: النتائج 79
ثالثا: التوصيات 81
قائمة المصادر والمراجع 82

الحماية الجزائية للمستند الالكتروني

"دراسة مقارنة"

إعداد الطالب: عمر حسين الدليمي

اشراف الدكتور: أحمد اللوزي

الملخص

جاءت الدراسة لتسليط الضوء على المسؤولية الجزائية للمستند الإلكتروني والمفاهيم المرتبطة بها، اعتمدت الدراسة في الإجابة على الإشكالية المطروحة على المنهج الوصفي، الذي يساعد في وصف جزئيات متعددة في موضوع المستند الالكتروني، ومن ثم المنهج التحليلي لدراسة النصوص القانونية الواردة في قانون الجرائم الالكترونية الأردني رقم 27 لسنة 2015 وفي التشريعات العقابية العراقية، ومن ثم المنهج المقارن لدراسة النظام القانوني للحماية الجزائية للمستند الإلكتروني في كل من التشريعات الجزائية الأردنية والعراقية بالمقارنة مع بعض القوانين العربية والغربية، وذلك بهدف التوصل إلى النتائج المتوخاة من هدف الدراسة.

وقدمت الدراسة عدد من التوصيات أهمها: أن ينظم المشرع العراقي حماية جنائية موضوعية كافية للمستند الإلكتروني، من خلال النص على الجرائم الواقعة عليه، والتي تتلائم مع الطبيعة غير المادية لهذه المستندات، كالتزوير الإلكتروني، جريمة الاحتيال الإلكتروني، جريمة الاستخدام غير المشروع لأدوات الدفع الإلكتروني على غرار التشريعات العقابية الأخرى، ومنها الأردني. كما أنه على المشرعين الأردني والعراقي وضع إجراءات خاصة أكثر دقة للتحقيق والمحاكمة للجريمة المعلوماتية تختلف عن الجريمة التقليدية.

الكلمات المفتاحية: الحماية الجزائية، المستند الالكتروني، قانون الجرائم الالكترونية.

Criminal Protection of Electronic Document
"A comparative study"

Preparation by: Omar al-Dulaimi

Supervised by: Dr. Ahmed Lozi

Abstract

The study aimed at shedding light on the criminal responsibility of the electronic document and the related concepts. The study relied on the problem of descriptive approach, which helps to describe multiple aspects of the electronic document, and then the analytical approach to study the legal texts contained in the Jordanian Electronic Crimes Law No. 27 of 2015 and the draft Iraqi Crimes Act of 2012, and then the comparative approach to study the legal system for the criminal protection of the electronic document in both the Jordanian and Iraqi criminal legislation compared to some laws Arab and Western, with the aim of reaching the desired results of the study objective.

We made a number of recommendations, the most important of which is that the Iraqi legislator should regulate adequate criminal protection of the electronic document by providing for the crimes that are committed to it and which are compatible with the intangible nature of such documents, such as electronic mail, e-fraud, By means of information technology, the crime of the illegal use of electronic payment tools in line with other penal legislation, including Jordanian law. Jordanian and Iraqi legislators should also develop more specific procedures for investigating and prosecuting information crimes that differ from conventional crimes.

Keywords: Criminal Protection, Electronic Document, Jordanian Electronic Crimes Law.

الفصل الأول

خلفية الدراسة وأهميتها

أولاً: المقدمة

تتيح التكنولوجيا الحديثة القيام بالكثير من الأعمال التي كان يستحيل من قبل إنجازها، فلقد وفرت هذه التكنولوجيا في مجال الإتصالات الإلكترونية إمكانية تحقق التواصل الإنساني وإنجاز المعاملات في سهولة ويسر، وأتاح إستخدامها حسن تقديم خدمات الرعاية الصحية وتنمية الملكية الفكرية، وغيرها من مجالات.

وتعد شبكات المعلومات ونظم التبادل الإلكتروني للبيانات تطبيقا للإستخدام التكنولوجي الحديث في مجال الإتصالات ونقل المعلومات وهي تختلف بذلك كثيرا عن غيرها من الوسائل التقليدية للاتصال والإعلام، وهذا الإختلاف يؤدي إلى أمرين: الأول هو تعدد أوجه إستعمالات هذه الوسائل وإتساعها، والثاني هو الحاجة إلى تنظيم قانوني يضع الإطار لهذه الإستعمالات[1].

غير أن هذه التكنولوجيا قد يساء إستعمالها وأن يهدد إستخدامها السلامة العامة والمصلحة الوطنية، فإذا كانت وسائل الإتصال الإلكتروني الحديثة تتيح إنجاز المعاملات المالية بشكل سريع؛ فإن إستعمال هذه الوسائل لا يخلو من مخاطر، فقد يستغل بعض المجرمين هذه الوسائل في إرتكاب جرائمهم بطريق الإحتيال أو المساس بخصوصية هؤلاء المتعاملين وسرية معاملاتهم. وإذا كان التقدم التقني قد حاول مكافحة الجرائم في مجال الإتصالات ولجأ إلى تشفيرها بما يحفظ سريتها، فإن هذه الإجراءات قد أفضت إلى إستغلال الجناة لهذه الإجراءات في

([1]) شنين، صالح (2013). **الحماية الجنائية للتجارة الالكترونية، دراسة مقارنة**، أطروحة دكتوراه، جامعة أبو بكر بلقايد، تلمسان، الجزائر، ص15.

إرتكاب جرائمهم بإستخدام وسائل إتصال يصعب إختراقها، وهو ما يعني أن التقدم التقني قد أمد المجرمين بوسائل بالغة الفاعلية في إرتكاب جرائمهم[1].

ثانياً: مشكلة الدراسة:

تثير الدراسة التساؤل عن ماهية المستند الإلكتروني وعناصره وعن أهم الأفعال الإجرامية التي تنال من المستند الإلكتروني، وماهية خطة التشريعات الجنائية الأردنية والعراقية وبعض التشريعات المقارنة الأخرى في تجريم هذه الأفعال.

وفي النهاية تكمن مشكلة الدراسة في بيان مدى كفاية خطة التشريعات الأردنية والعراقية وبعض التشريعات المقارنة الأخرى في تجريم الأفعال التي تنال من المستند الإلكتروني وبيان مدى فاعلية خطة التجريم هذه.

ثالثاً: أسئلة الدراسة

1. ما هو المستند الإلكتروني؟ وما هي عناصره؟
2. ما هي الصلة التي تربطه بغيره من الحقوق والمصالح التي يحميها الشارع؟
3. ما هو نطاق فكرة المستند الإلكتروني؟ وكيفية تمييزها عما قد يختلط بها من حقوق ومصالح أخرى تخرج عن مدلولها؟
4. ما هي أهم الأفعال الإجرامية التي تنال من المستند الإلكتروني؟

([1]) الزعبي، جلال والمناعسة، أسامة (2017). **جرائم تقنية نظم المعلومات الالكترونية، دراسة مقارنة**، ط3، عمان: دار الثقافة للنشر والتوزيع، ص245.

رابعاً: أهداف الدراسة

تهدف الدراسة إلى إيضاح معالم المستند الإلكتروني من حيث تعريفه وعناصره وطبيعته القانونية، ونطاق حمايته من خلال بيان الافعال الإجرامية التي تنال منه، وبيان خطة التشريعين الأردني والعراقي وبعض التشريعات المقارنة العربية والغربية في كفالة الحماية الجنائية له.

خامساً: أهمية الدراسة

تنبع أهمية الدراسة من النقاط التالية:-

1. من شأن كفالة الحماية الجنائية للمستند الإلكتروني أن يفضي إلى سهولة المعاملات التجارية وسرعة إنجازها وإلى توفير النفقات.
2. للمستند الإلكتروني صلة وثيقة بالحق في السرية والخصوصية.
3. للمستند الإلكتروني صلة بحماية حقوق المستهلك، فهذا المستند يتبلور فيه حقوق طرفي التعاقد، فهو المرجع للوقوف على ما أتفق عليه الطرفان وتحديد التزاماتهما القانونية، والحماية المقررة للمستند الإلكتروني تضمن في الوقت ذاته حماية للمستهلك.
4. حماية المستند الإلكترونية تؤدي إلى تحقيق الإستقرار والأمان القانوني، فحماية المستند الإلكتروني سواء من حيث الشكل أو التوقيع، وصيانته من المساس بسريته وكشف محتواه يكفل للافراد الطمأنينة وإستقرار المعاملات، كما يؤدي إلى أن يصبح هذا المستند دليلا في الإثبات يقف على قدم المساواة مع المستند الورقي، وهو ما يؤدي في النهاية إلى استقرار النظام القانوني وقله المنازعات.

سادساً: حدود الدراسة

- **الحدود الزمانية:** الحد الزماني لهذه الدراسة ينصب على قانون الجرائم الالكترونية الأردني رقم 27 لسنة 2015 وتعديلاته ومشروع قانون الجرائم المعلوماتية العراقي لعام 2012، وبعض التشريعات العربية والغربية الأخرى.
- **الحدود المكانية:** الحدود المكانية للدراسة محددة بالأردن والعراق.
- **الحدود الموضوعية:** تتحدد الحدود الموضوعية في دراسة الحماية الجنائية للمستند الالكتروني من حيث مفهومه والأفعال الإجرامية التي يتعرض لها وأوجه حمايته.

سابعاً: محددات الدراسة

تعد هذه الدراسة من الدراسات التي تتناول موضوع الحماية الجنائية للمستند الالكتروني في التشريعين الأردني والعراقي، دراسة مقارنة ببعض التشريعات العربية والغربية الأخرى، من حيث ماهية السند الالكتروني وعناصره والاعتداءات التي تقع عليه وأوجه الحماية الجنائية لها.

ثامناً: المصطلحات الإجرائية

- **المستند الالكتروني:** يعرف بأنه: (المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل الكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر، تبادل البيانات الإلكترونية أو التلكس أو النسخ البرقي) [1].
- **التوقيع الالكتروني:** يعرف بأنه: (البيانات التي تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، وتكون مدرجة بشكل الكتروني أو أي وسيلة أخرى مماثلة في السجل

([1]) المادة 22/2 من قانون الاونسترال للتجارة الالكترونية لعام 1996.

الإلكتروني أو تكون مضافة علية أو مرتبطة به، بهدف تحديد هوية صاحب التوقيع وانفراده باستخدامه وتميزه عن غيره)[1].

تاسعاً: الدراسات السابقة

بالرغم من البحث والتحري من قبل الباحث، إلا أنه لم يجد في المكتبة القانونية العربية إلا دراسة سابقة واحدة، تناولت موضوع دراسته (الحماية الجنائية للمستند الالكتروني). وهي دراسة في التشريع المصري للدكتور أشرف توفيق شمس الدين.

عاشراً: الإطار النظري للدراسة

تتضمن الدراسة وعنوانها " **الحماية الجنائية للمستند الالكتروني** "**دراسة مقارنة**" عدة فصول، منها ما يتضمن **الفصل الأول، مقدمة عامة للدراسة** تعالج خلفية الدراسة وأهميتها ومشكلتها وأهدافها وأسئلتها ومصطلحات الدراسة، انتهاءً بمنهجية الدراسة وأدواتها. وستتناول هذه الدراسة في **الفصل الثاني، ماهية المستند الالكتروني** من خلال توضيح مفهوم المستند الإلكتروني، ومن ثم تناول نطاق المستند الالكتروني، **أما الفصل الثالث فقد وضح الحماية الجزائية الموضوعية للمستند الإلكتروني،** من خلال توضيح الحماية الجزائية الموضوعية للمستند الإلكتروني وفقاً للنصوص العقابية التقليدية، والحماية الجزائية الموضوعية للمستند الإلكتروني وفقاً للنصوص العقابية المستحدثة. وتناولت هذه الدراسة في **الفصل الرابع موضوع الحماية الجزائية الإجرائية للمستند الالكتروني.** تناولت إجراءات التحري والتحقيق في الجرائم الماسة بالمستند الالكتروني، ثم إجراءات المحاكمة في الجرائم الماسة بالمستند الإلكتروني، انتهاءً **بالفصل الخامس وتضمن الخاتمة والنتائج والتوصيات.**

([1]) المادة 9/2 من قانون المعاملات الالكترونية الأردني رقم 15 لسنة 2015 وتعديلاته.

حادي عشر: منهجية الدراسة

المنهجية المتبعة في هذه الدراسة، تتمثل في اتباع عدة مناهج هي:-

- **المنهج الوصفي:** تقتضي مراحل الدراسة الاستعانة بالوصف، لأن المنهج الوصفي يساعد في وصف جزئيات متعددة في موضوع المستند الالكتروني، وربط أحكامه بالقواعد الفقهية والقانونية من حيث التعريف والطبيعة القانونية والأفعال الإجرامية التي تناله والحماية المقررة له.
- **المنهج التحليلي:** حيث يجب دراسة النصوص القانونية الواردة في قانون الجرائم الالكترونية الأردني رقم 27 لسنة 2015 ومشروع قانون الجرائم المعلوماتية العراقي لعام 2012 ومن ثم الوقوف على مدى الحماية الجنائية المقررة للمستند الالكتروني في التشريعين الأردني والعراقي.
- **المنهج المقارن:** دراسة النظام القانوني للحماية الجنائية للمستند الإلكتروني في كل من التشريعات الجنائية الأردنية والعراقية بالمقارنة مع بعض القوانين العربية والغربية، لمعرفة أوجه الاختلاف والاتفاق في هذه الأنظمة المقارنة، ومحاولة وضع مقترحات في نهاية الدراسة لذلك.

ثاني عشر: أدوات الدراسة

قانون الجرائم الالكترونية الأردني رقم 27 لسنة 2015

مشروع قانون الجرائم المعلوماتية العراقي لسنة 2012.

قانون المعاملات الالكترونية الأردني رقم 15 لسنة 2015.

قانون التوقيع الالكتروني والمعاملات الإلكترونية العراقي رقم 78 لسنة 2012.

الفصل الثاني

ماهية المستند الإلكتروني

تتعدد التعاملات الإلكترونية وتختلف فيما بينها إختلافاً كبيراً، فمن ناحية قد تكون هذه التعاملات على شبكات اتصال مفتوحة للكافة دون تمييز كشبكة الإنترنت، أو شبكات مغلقة يقتصر التعامل من خلالها على عدد محدود من الأفراد أو الهيئات، ومثالها الشبكات الخاصة بالشركات والمؤسسات الحكومية والهيئات التي تقدم خدمات مثل الرعاية الصحية والتأمينية.

وقد أسهمت نظم جديدة في الإتصالات في زيادة أهمية وكفاءة المعاملات الإلكترونية ومثالها الشبكات الخاصة للمعاملات (سويفت) التي بمقدورها إتمام التصرف في لحظات معدودة، وكذلك وسائل الإتصال عن بعد ونظم التبادل الإلكتروني للبيانات[1].

فتبرز الحاجة هنا إلى تحديد مدلول محدد للمستند الإلكتروني، وذلك حتى يتسنى تحديد نطاقه ومعالمه واستظهار الأفعال الماسة به. وتبدو أهمية تحديد هذا المدلول من اختلاف خطة التشريعات في النص على المستند الإلكتروني وفي مدى الحماية المقررة له في التشريعات. فغالبية التشريعات لا تفرد نظرية عامة للمستند الإلكتروني، ولا تحدد قواعد عامة تسري على أي مستند تتوافر له الصفة الإلكترونية؛ وإنما تقتصر هذه التشريعات – كما سنرى – على النص على أهم تطبيقات فكرة المستند الإلكتروني مثل التوقيع والسجلات الإلكترونية.

---

[1] لطفي، محمد حسام الدين (2002). **الإطار القانوني للمعاملات الإلكترونية، دراسة في قواعد الإثبات في المواد المدنية والتجارية مع إشارة خاصة لبعض قوانين البلدان العربية**، القاهرة: دار النهضة العربية، ص28.

وللوقوف على ماهية المستند الإلكتروني نتناول هذ الفصل في المبحثين الآتيين:-

المبحث الأول: مفهوم المستند الإلكتروني

المبحث الثاني: نطاق المستند الالكتروني

المبحث الأول

مفهوم المستند الإلكتروني

إن تعاملاتنا اليومية تتسم بالوضوح والتحديد من حيث مضمونها، إلى جانب توافر قدر من الأمان والثقة تجاهها، ويرجع ذلك إلى كتابة هذه التعاملات في مستندات يمكن الرجوع إليها في أي وقت إذا استدعى الأمر ذلك، أما الآن وعلى الرغم من التطور الكبير الذي تشهده التقنيات الإلكترونية والأمان الذي توفره هذه التقنيات، إلا أنها تقف عاجزة أحيانا أمام بعض التجاوزات التي قد يقوم بها بعض الأشخاص باستخدامهم وسائل احتيالية.

ولبيان مفهوم المستند الإلكتروني لا بد من تناول تعريف المستند الإلكتروني وخصائصه (المطلب الأول)، وصور المستند الإلكتروني (المطلب الثاني)، وذلك وفق المطلبين الآتيين:-

المطلب الأول

تعريف المستند الإلكتروني وخصائصه

عرفت بعض التشريعات الحديثة المهتمة بسن قوانين خاصة بعمليات التعامل عبر أجهزة وشبكات الحاسب الآلي، المستند الإلكتروني من زوايا مختلفة، مع استخدامها مصطلحات

مترادفة مثل: السند الإلكتروني، المحرر الإلكتروني، الكتابة الإلكترونية، الوثيقة الملعلوماتية، السجل الإلكتروني، رسالة البيانات، وعلى الرغم من الاختلاف، إلا أنها تحمل معنى واحد[1].

ولتحديد هذه الاختلافات نتناول هذا المطلب من خلال تعريف المستند الالكتروني، ومن ثم بيان خصائصه، وذلك في الفرعين الآتيين:-

الفرع الأول: تعريف المستند الإلكتروني

قبل التطرق إلى تعريف المستند الإلكتروني لا بد أن نعرف المستند أو المحرر في شكله التقليدي، والذي هو عبارة عن مجموعة من العلامات والرموز تعبر إصطلاحاً عن مجموعة مترابطة من الأفكار والمعاني الصادرة عن شخص أو أشخاص معينين ومنه نستنتج أنّ المحرر في شكله التقليدي هو عبارة عن سند يحمل كتابة ذات أثر قانوني، قد تكون يدوية أو آلية يمكن فهمها وإدراكها بمجرد النظر إليها[2].

وبالعودة إلى تعريف المستند الإلكتروني، سوف نتناوله من خلال النقاط الآتية:-

أولاً: التعريف الفقهي للمستند الإلكتروني

لقد عرف الفقه المستند الإلكتروني بأنه كل جسم منفصل أو يمكن فصله عن نظام المعالجة الآلية للمعلومات أو يكون مشتقاً من هذا النوع، كما ذهب بعض من الفقه إلى تعريف

---

[1] السقا، إيهاب فوزي (2002). **جريمة التزوير في المحررات الإلكترونية**، الإسكندرية: دار الجامعة الجديدة ص14.

[2] بن خليفة، إلهام (2016). **الحماية الجنائية للمحررات الإلكترونية من التزوير**، أطروحة دكتوراه، جامعة الحاج لخضر، باتنة، الجزائر، ص24-ص25.

المحرر الإلكتروني بأنه كل جسم منفصل ، وقد سجلت عليه معلومات معينة ، سواء كانت معدة للاستخدام بواسطة نظام المعالجة الآلية للمعلومات أو يكون مشتقاً من هذا النوع[1].

كما عرف أحدهم المستند الالكتروني بأنه عبارة عن معلومات تم إنشاؤها أو إرسالها أو تخزينها أو استلامها بوسيلة الكترونية أو ضوئية أو رقمية أو صوتية ما دامت تتضمن إثبات واقعة أو تصرف قانوني محدد وتتضمن توقيع الكتروني ينصب هذه الواقعة أو التصرف لشخص محدد[2].

ويختلف المستند المعالج آلياً عن المستند الغير معالج آلياً، وتعتبر مستندات معلوماتية الأوراق: المعدة لتسطير المعلومات عليها والأقراص الممغنطة التي لم يسجل عليها أي شئ بعد والملاحظات التي تكون على شكل كتب أو نشرة متعلقة بطريقة استخدام البرامج[3].

كذلك يقصد بالمستند المعالج آلياً: كل دعامة مادية يمكن أن يدون عليها شيءٌ معنوي، ويقصد بالمستند في مجال المعلوماتية كل شيء مادي متميز (قرص أو شريط ممغنط أو خلافه)، يصلح لأن يكون دعامة أو محلاً لتسجيل المعلومات المعالجة، ويستوي بعد ذلك أن يكون هذا الشيء قد خرج من الآلة وتم تصنيفه أو تخزينه أو أنه مازال بداخلها انتظارا لاستخراجه أو تعديله[4].

---

[1] السقا، إيهاب فوزي (2002). مرجع سابق، ص16.

[2] الرومي، محمد أمين (2007). **المستند الإلكتروني**، ط1، الإسكندرية: دار الفكر الجامعي، ص55.

[3] بن خليفة، إلهام (2016). مرجع سابق، ص27.

[4] لطفي، محمد حسام الدين (2002). مرجع سابق، ص31.

ثانياً: التعريف القانوني للمستند الإلكتروني

عرف المشرع الأردني في قانون المعاملات الإلكترونية رقم 15 لسنة 2015، السند الإلكتروني في المادة الثانية منه بقوله: (السند الذي يتم إنشاؤه والتوقيع عليه وتداوله إلكترونياً)، كما عرفّ السجل الإلكتروني بأنه: (رسالة المعلومات التي تحتوي على قيد أو عقد أو أي مستند أو وثيقة من نوعٍ آخر يتم إنشاء أي منها أو تخزينها أو استخدامها أو نسخها أو إرسالها أو تبليغها أو تسلمها باستخدام الوسيط الإلكتروني).

بالمقابل عرفّ قانون الاونسيترال النموذجي المستند الإلكتروني برسالة البيانات طبقاً للمادة (2/ج) منه على أنه: (يعني المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل الكترونية أو ضوئية أو بوسائل مشابهة بما في ذلك، على سبيل المثال لا على سبيل الحصر، تبادل البيانات الإلكتروني أو بيانات البريد الإلكتروني أو البرق أو التلكس أو النسخ البرقي) [1].

وقد عرفّ أيضاً قانون التجارة الأمريكي المستند الإلكتروني في المادة (7/2) منه على أنه: (سجل يتم إنشاؤه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية على وسيط ملموس أو على أي وسيط إلكتروني آخر، ويكون قابلاً للاسترجاع بشكلٍ يمكن فهمه) [2].

يقصد أيضاً بتعبير المستندات المعالجة آلياً وفقاً للقانون الفرنسي الصادر سنة 1988 والمتعلق ببعض جرائم المعلوماتية، أنها مستندات تم بالفعل خضوعها لمعالجة آلية، بمعنى آخر تمّ بالفعل صياغتها في صورة إحدى لغات الحاسب الآلي, وبالتالي فلفظ المحررات المعلوماتية

---

[1] براهمي، حنان (2012). **المحررات الإلكترونية كدليل إثبات**، مجلة الفكر، كلية الحقوق والعلوم السياسية، جامعة بسكرة، الجزائر، العدد 9، ص138.

[2] شنين، صالح (2013). **الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة**، أطروحة دكتوراه، جامعة تلمسان، الجزائر، ص45.

هو خطوة أولى لكي يتم فيها بعده في خطوة تالية، المعالجة الآلية وعلى هذه المستندات المعالجة آلياً يقع التزوير، وهذا هو مقصد المشرع[1]، وهنا نجد أنها تكمن حداثة استخدام المشرع الفرنسي للتعبير الجديد، وهي نقطة تحسب له في تفتحه على المصطلحات التكنيكية الجديدة.

كذلك عرفّ القانون العربي النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات في المادة الأولى منه الفقرة 18، الكتابة الإلكترونية بأنها: عملية تسجيل البيانات على وسيط الكتروني لتخزينها[2].

كذلك عرف المشرع المصري المستند الإلكتروني في القانون رقم 15 لسنة 2004، والخاص بالتوقيع الإلكتروني في مادته الأولى في الفقرة (ب) بأنه: (رسالة تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل كلياً أو جزئياً بوسيلة إلكترونية أو رقمية أو ضوئية أو بأية وسيلة أخرى مشابهة).

ويتضح للباحث من التعاريف السابقة، أنّ المشرع قصد بالمحرر الإلكتروني، أنّه رسالة إلكترونية مدون فيها بيانات ومعلومات يكون منشؤها أو تخزينها إلكترونياً، كما أنها ترسل وتستقبل عبر وسيلة إلكترونية أو ما شابه.

كما تعرضت بعض التشريعات الأخرى لمفهوم المحرر الإلكتروني بمصطلحات مترادفة مثل المستند الإلكتروني أو الوثيقة الإلكترونية، ففي التشريع الإماراتي، عرفّ المحرر الإلكتروني في قانون التجارة الإلكتروني الخاص بإمارة دبي رقم 2 لسنة 2002 بأنه: (سجل أو مستند

---

[1] قشقوش، هدى حامد (2011). **جرائم الحاسب الإلكتروني في التشريع المقارن**، القاهرة: دار النهضة العربية، ص120.

[2] حجازي، عبد الفتاح بيومي (2009). **مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي**، ط1، القاهرة: دار النهضة العربية، ص743.

الكتروني يتم إنشاؤه أو تخزينة أو استخراجه أو نسخة أو أرساله أو إبلاغه أو استلامه بوسيلة إلكترونية على وسيط ملموس أو على أي وسيط الكتروني آخر، ويكون قابلاً للاسترجاع بشكل يمكن فهمه).

وعلى أي حال، وسنداً لما تقدم يستطيع الباحث تعريف المستند الإلكتروني بأنه: " عبارة عن وسيط الكتروني، والذي هو كل شيء مادي متميز لقرص صلب أو مظغوط أو شريط ممغنط أو خلافه، يصلح لأن يكون محلاً لتسجيل أو تخزين معلومات فيه، معالجة بواسطة نظام المعالجة الآلية للمعطيات، بمعنى أنّ المعلومات أو الكتابة الإلكترونية تنشأ عن طريق المكونات المادية والمعنوية للحاسب الآلي بواسطة هذا النظام ثم تفصل عنه".

الفرع الثاني: خصائص المستند الإلكتروني

الخصائص المميزة التي يختص بها المستند الإلكتروني عديدة، وسوف نعرض لأهمها فيما يلي:-

أولاً: الصفة الإلكترونية.

يحمل هذا المستند أو المحرر الصفة الإلكترونية، بما يعني أن العمليات التي يمر بها هذا المحرر، مثل ضغطه أو تخزينه أو استرجاعه أو نقله أو نسخه، متصلة بتقنية تكنولوجية إلكترونية، ولا يمكن استخدامه خارج هدا الوسيط الإلكتروني، بالإضافة إلى أنه يمكن أن يتم تحميل هذا المحرر ونقله من جهاز إلكتروني لأخر عن طريق دعامة إلكترونية[1].

---

[1] السقا، إيهاب فوزي (2002). مرجع سابق، ص17.

وبالتالي تعتمد هذه الخاصية للمستند الإلكتروني على عدم وجود أي دعامة ورقية على عكس السند التقليدي المودع على دعامة ورقية، ومن هذا الصدد نلاحظ أنه يوجد دائما ارتباط وثيق الصلة بين المضمون في السند التقليدي والدعامة، ويرجع ذلك إلى أن للمضمون أن لا يكون منفصلا عن هذا الوسيط ، بينما يفترض في السند الإلكتروني أن يسجل على دعامة محددة قرص صلب أو مرن ، قرص ضوئي،.... إلخ[1].

ثانياً: القيمة القانونية.

يحتوي المحرر الإلكتروني على كتابة لها قيمة قانونية، أي تصلح للتمسك أو للاحتجاج بها، وهي لا تكون كذلك إلا إذا كانت تقرر حق سواءً بإنشائه أم بتعديله أو بإلغائه أو تثبيته[2]. بالإضافة إلى أن المحرر الإلكتروني يتضمن تعبيراً عن المعاني والأفكار الإنسانية المترابطة، وهو ما يعني أن يكون هذا المحرر أداة للتفاهم وتبادل الأفكار بين الأفراد، وأن يكون له قيمة قانونية، يمكن التعويل عليه عند المعاملات بين الأفراد والمؤسسات والحكومات، مما يخضعهم للمسائلة القانونية عند المساس به أو تغيير ما يحمله من حقائق[3].

ثالثاً: السرعة والائتمان في إبرام المعاملات.

تتميز المستندات الإلكترونية بالسرعة في إبرام التعاقد، إذ يستطيع الشخص الذي ينوي التعاقد عن طريق وسائل الاتصال الفوري، بتأمين وصول إيجابه إلى شخص الأخر الذي ينوي

---

[1] كحول، سماح (2015). **حجية الوسائل الإلكترونية في إثبات العقود التجارية**، رسالة ماجستير، جامعة قاصدي مرباح، ورقلة، الجزائر، ص5.

[2] القهوجي، علي عبد القادر (2010). **الحماية الجنائية لبرامج الحاسب الآلي**، الإسكندرية: دار الجامعة الجديدة للنشر، ص144.

[3] السقا، إيهاب فوزي (2002). مرجع سابق، ص17.

التعاقد معه في أي مكان كان والحصول على إجابة في ثواني معدودة، وهكذا يسمح بتوفير الوقت واختصاره بشكل كبير لاسيما في التجارة الإلكترونية[1].

كذلك مكنت المستندات الإلكترونية من تسليم بعض الأشياء وأداء بعض الخدمات فوراً في البيئة الافتراضية، كالحصول على خدمات معينة، وتسمح أيضاً بالوفاء فوراً، أي يمكن دفع الثمن إلكترونيا بأحد الأساليب المعروفة للوفاء على شبكة الانترنت، سواءً عن طريق بطاقات الائتمان أم النقود الرقمية أم البطاقات الذكية، وغيرها من وسائل الدفع الإلكتروني[2].

رابعاً: السرية.

تتميز المستندات الإلكترونية بالسرية، حيث لا يمكن لأحد ما الإطلاع عليها، إلا المرسل أو المرسل إليه، لأنها مستخرجة من تقنيات متطورة توفر الأمن لها، كما أن تشريعات المعاملات الإلكترونية أضفت عليها حماية لضمان الثقة فيها، وذلك بأن نصت على استخدام وسائل تقنية تحفظها وتحول دون أن تمتد إليها يد العابثين عليها تتمثل في أنظمة التشفير وتسليم شهادة تصديق من طرف جهات موثوقة من الدولة، تثبت أن ما على المحررات من حقوق يعود لصاحب التوقيع الإلكتروني عليها[3].

---

[1] العبودي، عباس (2010). **تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها**، ط1، بيروت: منشورات الحلبي الحقوقية، ص40.

[2] شنين، صالح (2013). مرجع سابق، ص52.

[3] بن خليفة، إلهام (2016). مرجع سابق، ص23–ص24.

المطلب الثاني

صور المستند الإلكتروني

المستندات الورقية إما أن تكون مستندات رسمية وهي التي يقوم بتحريرها موظف عام مختص وفقاً للأوضاع المقررة قانوناً، وإما أن تكون مستندات عرفية وهي التي يقوم بتحريرها الأفراد فيما ينهم وذلك لإثبات تصرف أو واقعة قانونية[1].

هذا بالنسبة للمستندات الورقية، أما المستندات الإلكترونية فصورها متعدد نذكر منها على سبيل المثال:

- **العقود الإلكترونية:** والتي تعني :العقد الذي يتم انعقادة بوسيلة الإلكترونية كلياً أو جزئياً، وسواء تمثلت الوسيلة الإلكترونية في وسيلة كهربائية أو مغناطيسية أو ضوئية أو إلكترومغناطيسة أو أي وسيلة أخرى مشابهة صالحة لتبادل المعلومات بين المتعاقدين[2].
- ومن بين صور المستند الإلكتروني أيضا نجد **الشيك الإلكتروني:** والذي هو عبارة عن رسالة تحتوي على جميع البيانات التي يمكن أن نجدها بالشيك الورقي العادي، بحيث يقوم المشتري بتحرير شيك الكتروني للبائع وإرساله له إلكترونياً عبر أي وسيلة إلكترونية كالفاكس أو البريد الإلكتروني في أغلب الأحيان، وتكون جميع التوقيعات التي يتضمنها هذا الشيك توقيعات الكترونية أو رقمية[3].

---

[1] المادة 6 وما بعدها من قانون البينات الأردني رقم 30 لسنة 1952 والمعدل بالقانون رقم 22 لسنة 2017.

[2] الرومي، محمد أمين (2007). مرجع سابق، ص38.

[3] كحول، سماح (2015). مرجع سابق، ص24.

- كذلك من بين الصور نجد **البطاقات الإلكترونية:** والتي تتخذ أشكالاً متعددة ووظائف مختلفة، كما أنها قد تصدر عن جهات حكومية، أو عن مؤسسات مالية خاصة من أجل المبادلات التجارية أو الاستفادة من بعض الخدمات، ومن بينها البطاقات البنكية أو المصرفية، ومن بين الأنواع الشائعة للبطاقة الإلكترونية،بطاقة التعريف الوطنية، جواز السفر الإلكتروني، بطاقة الضمان الاجتماعي، رخصة القيادة الإلكترونية، بالإضافة إلى بطاقة الوفاء والتي هي عبارة عن آداة وفاء تصطبغ بصبغة مصرفية وتسمح لحاملها باتخاذ الإجراءات اللازمة لخصم وتحويل مبلغ محدد من المال من حسابه لدى البنك المصدر للبطاقة لمصلحة وحساب شخص آخر[1].

كذلك من بين الصور نجد بطاقة الائتمان وهي بطاقة خاصة يصدرها المصرف لعميله كي تمكنه من الحصول على السلع والخدمات من محلات وأماكن معينة عند تقديمه هذه البطاقة. أيضا نجد بطاقة الصراف الآلي وهي بطاقة مخصصة للقيام بالعمليات المصرفية عبر الصراف الآلي، كعمليات السحب وكشف الحساب، والعمليات الممكنة بواسطة هذا الجهاز، إذ يمكن سحب مبالغ نقدية بسقف محدد متفق عليه، بإدخال البطاقة في الفتحة الخاصة بالجهاز، وادخال الرقم السري ليتم صرف المبلغ آليا وتسجيل المبلغ في الجانب المدين من حساب الحامل[2].

وتتكون البطاقات الإلكترونية من مكونات مادية تتمثل في جسم البطاقة الذي يتميز بأبعاد معينة من حيث الطول والعرض والسمك، بالإضافة إلى تموضع كل مكونات البطاقة من حيث المسافات الرأسية والأفقية بين الحروف والأرقام والصورة وشريط التوقيع والشريط الممغنط،

---

[1] الرومي، محمد أمين (2007). مرجع سابق، ص44–ص45.

[2] كحول، سماح (2015). مرجع سابق، ص26.

وتستخدم في صناعة هذه البطاقات طبقة بلاستيكية خاصة تغطيها لحماية المعلومات والبيانات من العوامل البيئية المحيطة والحرارة. أما المكونات المعلوماتية للبطاقة فإن الشريط الممغنط أو الشريحة الإلكترونية يحتوي على بيانات معالجة إلكترونية تتعلق بصاحب البطاقة، حيث لايمكن إدراك هذه البيانات بصرياً، إلا أنه من الممكن قراءتها وفقا للأصول الفنية الخاصة بها[1].

وبالتالي يجد الباحث أن البطاقة الإلكترونية تحمل مجموعة من المعلومات والبيانات التي ترتبط بمركز مالي أو قانوني معين لصاحبها، سواء كانت ظاهرة أو كانت الكترونية، أما المعلومات الإلكترونية الموجودة على الشريط الممغنط فهي جزء من المستند الإلكتروني.

---

[1] الرومي، محمد أمين (2007). مرجع سابق، ص47.

المبحث الثاني

نطاق المستند الالكتروني

ارتبط ظهور المحرر الإلكتروني وانتشاره، بعدة مصطلحات الكترونية أخرى، تستخدم عند التعامل به، واعتبارها كثيراً من الفقه شروطاً لكي يكون للمستند الإلكتروني الحجية الكاملة في الإثبات، وامكانية مساواته بالسندات الرسمية والعرفية، ومن أهم هذه المصطلحات، الكتابة الإلكترونية والتوقيع والتوثيق وهي نفسها الموجودة في المستند التقليدي، إلا أنّ هذا لا يعني أنهما متماثلان رغم أنهما يؤديان إلى نفس الغرض وهو الإثبات.

وعلى أساس ذلك؛ سيتم تناول نطاق المستند الإلكتروني من خلال المطلبين الآتيين:-

المطلب الأول: شروط المستند الالكتروني

المطلب الثاني: تمييز المستند الإلكتروني عن المستند التقليدي

المطلب الأول

شروط المستند الالكتروني

من شروط المستند الإلكتروني نذكر مايلي:-

أولاً: الكتابة الإلكترونية

تعتبر الكتابة من أول طرق الإثبات المختلفة في إثبات التصرفات القانونية، ويرجع ذلك لطبيعتها من حيث تحديدها ووضوحها وامكانية بقائها واستمرارها، دون الارتباط بكاتبها أو موقعها، ونظراً لانتشار الكتابة وشيوعه، نجد المشرع، في القوانين الحديثة، أضفى عليها حجية

مطلقة، مادام الخصم لم ينكرها أو يدعِ تزويرها، ولذلك فهي لا تخضع لتقدير القاضي، وتعبر الكتابة بدقة عن الواقعة التي أعدت لإثباتها، فهي تعتبر دليلاً عند حدوث نزاع بين أطراف الاتفاق وتعطي قدراً كبيراً من الاطمئنان لدى أصحاب الحقوق[1].

وبالتالي تعتبر الكتابة الشرط الأساسي والأهم في المستندات الإلكترونية[2].

والتي تكون على شكل معادلات خوارزمية تنفذّ من خلال عمليات إدخال البيانات واخراجها من خلال شاشة الحاسب الآلي، والتي تتم من خلال تغذية الجهاز بهذه المعلومات عن طريق وحدات الإدخال والتي تتبلور في لوحة المفاتيح أو استرجاع المعلومات المخزنة في وحدة المعالجة المركزية، وبعد الفراغ من معالجة البيانات يتم كتابتها على أجهزة الإخراج التي تتمثل في شاشة الحاسب الآلي، أو طباعة هذه المحررات على الطابعة أو الأقراص الممغنطة أو أي وسيلة من وسائل تخزين البيانات[3].

ويجب توافر مجموعة من الشروط التي توصف بالفنية أو التقنية حتى يعتد بالكتابة في المجالات القانونية نذكر منها:

1. يجب أن تكون الكتابة مقروءة ومستبينة حتى يمكن الاعتداد بها، ولهذا تأثيرات قانونية خطيرة، حيث أنه في حالة تخلف هذا الشرط يمكن أن يبطل التصرف القانوني.
2. يجب أن تكون الكتابة دائمة، أي يجب حفظها في شروط تضمن بقائها مدة معقولة.

---

[1] براهمي، حنان (2015). **جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية**، أطروحة دكتوراه، جامعة محمد خيضر، بسكرة، الجزائر، ص107–ص108.

[2] السقا، إيهاب فوزي (2002). مرجع سابق، ص28.

[3] عبيدات، لورنس محمد (2009). **إثبات المحرر الإلكتروني**، ط1، عمان: دار الثقافة للنشر والتوزيع، ص79.

3. يجب أن يصعب العبث بها أو التعديل فيها دون أن يترك ذلك أثرا على المحرر الذي يحتويها[1].

ثانياً: التوقيع الإلكتروني

عرفّ قانون الأونسترال النموذجي في المادة (2) منه،التوقيع الإلكتروني بأنه: (بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقياً، يجوز أن تستخدم لتقييم هوية الموقع بالنسبة إلى رسالة البيانات ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات). كما عرفت المادة الثانية من قانون المعاملات الإلكترونية الأردني رقم 15 لسنة 2015، التوقيع الإلكتروني بأنه: (البيانات التي تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها وتكون مدرجة بشكل الكتروني أو أي وسيلة أخرى مماثلة في السجل الإلكتروني، أو تكون مضافة عليه أو مرتبطة به بهدف تحديد هوية صاحب التوقيع وانفراده باستخدامة وتمييزه عن غيره).

كما يعرف التوقيع الإلكتروني بأنه: (جزء صغير مشفر من بيانات يضاف إلى رسالة الكترونية، فهو جزء من الرسالة ذاتها، يشفر ويرسل مع الرسالة، ليتم التوثق من صحة الرسالة، بفك التشفير وانطباق محتواه على الرسالة) [2]. وعرف أيضاً التوقيع الإلكتروني بأنه: (مجموعة

---

[1] عبد الفتاح، عابد (2014). **الكتابة الإلكترونية في القانون المدني بين التطور القانوني والأمن التقني**، الإسكندرية: دار الجامعة الجديدة، ص17.

[2] عبد الفتاح، عابد (2014). مرجع سابق، ص33.

من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته) [1].

وقد نصت المادة (3/13) من قانون البينات الأردني رقم 30 لسنة 1952 والمعدل بالقانون رقم 22 لسنة 2017 على: (

أ. وتكون لرسائل الفاكس والتلكس والبريد الإلكتروني قوة الأسناد العادية في الإثبات ما لم يثبت من نسب إليه إرسالها أنه لم يقم بذلك أو لم يكلف أحد بإرسالها.

ب. وتكون رسائل التلكس بالرقم السري المتفق عليه بين المرسل والمرسل إليه حجة على كل منهما.

ج. وتكون لمخرجات الحاسوب أو الموقعة قوة الأسناد العادية من حيث الإثبات ما لم يثبت من نسبت إليه أنه لم يستخرجها أو لم يكلف أحد باستخراجها).

ثالثاً: التوثيق الإلكتروني (التصديق).

يقصد به اللجوء إلى طرف ثالث محايد ومستقل عن الأطراف سواءً كان فرداً عادياً أو شركة أو جهة من الجهات، من أجل توثيق المعاملات الإلكترونية لأشخاص، وبهذا يتحدد وضع الموثق أو المصدقّ بأنه وسيط بين المتعاملين، يلجأ إليه بغرض منح الثقة في محرراتهم حتى

---

[1] نصيرات، علاء محمد (2005). **حجية التوقيع الإلكتروني في الإثبات، دراسة مقارنة**، ط1، عمان: دار الثقافة للنشر والتوزيع، ص33.

يمكنهم يستخدموها لإثبات ماتتضمنه من تصرفات قانونية، ولهذا السبب يطلق عليهم البعض، وكلاء الإثبات[1].

كما يعرف التوثيق بأنه: (مجموعة من الإجراءات المعتمدة أو المقبولة تجارياً أو المتفق عليها بين الأطراف بهدف التحقق من أن قيداً الكترونياً "توقيع الكتروني" لم يتعرض إلى أي تعديل من تاريخ التحقق منه وفق إجراءات التوثيق) [2].

وأيضاً عرفت المادة الثانية من قانون المعاملات الإلكترونية الأردني رقم 15 لسنة 2015 التوثيق الإلكتروني بأنه: (التحقق من هوية مستخدم شهادة التوثيق الإلكتروني وصحتها وصلاحيتها)، أما شهادة التوثيق الالكتروني فعرفتها المادة المذكورة بأنها: (الشهادة الصادرة عن جهة التوثيق الإلكتروني لإثبات نسبة توقيع الكتروني إلى شخص معين استناداً إلى إجراءات توثيق معتمدة).

أما جهة التوثيق الالكتروني فعرفتها المادة المذكورة بأنها: (الجهة المرخصة أو المعتمدة من هيئة تنظيم قطاع الاتصالات أو المخولة قانوناً بإصدار شهادات التوثيق وتقديم أي خدمات متعلقة بهذه الشهادات وفقاً لأحكام هذا القانون والأنظمة والتعليمات الصادرة بموجبه).

وتلعب شهادة التوثيق الإلكتروني دوراً مهماً في عملية التوقيع الرقمي، حيث تؤكد صحة المفتاحين العام والخاص المستخدمين في ذلك، حسب المعلومة الواردة بهذه الشهادة الخاصة بصاحبها، والمنشئة من جهة محايدة، ذلك أن منح هذه الشهادة من جهة التوثيق الإلكتروني يتطلب تقديم المعلومات الخاصة بطالب التوقيع والتأكد من صحتها، ليتم منح هذا الشخص

---

[1] عبد الفتاح، عابد (2014). مرجع سابق، ص71.

[2] نصيرات، علاء محمد (2005). مرجع سابق، ص125-ص126.

مفتاح تشفير خاص يتسم بالسرية، حيث يحتفظ به الموقع، ويتم تثبيت نصفه في جهاز الكمبيوتر الخاص به، والنصف الأخر في بطاقة إلكترونية[1]، أما جهة التوثيق فتحتفظ بالمفتاح العام، حيث تقوم بإرساله بالبريد الإلكتروني إلى الأشخاص الذين يتعامل معهم الموقع، وذلك لاستخدامه في فك التشفير[2].

رابعاً: حفظ المعلومات (سلامة المحتوى)

إن بقاء محتوى المستند كما هو عند إنشائه هو ما نعنيه بحفظ المعلومات طوال مدة التقادم التي يخضع لها التصرف المحفوظ، ولذلك يلاحظ أن عملية الحفظ لها دور هام في مجال الإثبات، ولذلك يجب حفظ المعلومات والمعطيات على دعامة إلكترونية ضد التلف والتعديل أو أي صورة من صور الهلاك[3].

وقد أشار قانون الأونسترال النموذجي في المادة (10) إلى الشروط التي يجب توافرها عند حفظ المستند الإلكتروني وهي:

1. تيسير الإطلاع على المعلومات الواردة به على نحو يتيح استخدامها بالرجوع إليها لاحقاً.
2. الاحتفاظ بالشكل الذي أنشئ أو استلم به أو بشكل يمكن إثبات أنه يمثل بدقة المعلومات التي أنشأت أو استلمت.

---

[1] عبيدات، لورنس محمد (2009). مرجع سابق، ص112.

[2] براهمي، حنان (2015). مرجع سابق، ص153.

[3] عبيدات، لورنس محمد (2009). مرجع سابق، ص132.

3. الاحتفاظ بالمعلومات إن وجدت والتي تمكن من استبانة منشأ المستند الإلكتروني وجهة وصوله، وتاريخ ووقت إرساله واستلامه[1].

وقد بينت المادة (2) من قانون المعاملات الإلكترونية الأردني مفهوم المعلومات الإلكترونية بأنها: (البيانات أو النصوص أو الصور أو الرسومات أو الأشكال أو الأصوات أو الرموز أو قواعد البيانات وما شابه ذلك). أما رسالة المعلومات الإلكترونية فعرفتها المادة المذكورة بأنها: (الملعومات التي يتم إنشاؤها أو ارسالها أو تسلمها أو تخزينها بأي وسيلة الكترونية ومنها البريد الإلكتروني أو الرسائل القصيرة أو أي تبادل للمعلومات الكترونياً).

المطلب الثاني

تمييز المستند الإلكتروني عن المستند التقليدي

يتماثل المحرر الالكتروني مع المحرر التقليدي في عدة أمور، ويختلف في أمور أخرى، حيث أنّ كلاً منهما يحمل ملامح وخصائص يتميز بها عن الآخر، وفيما يلي نوضح نقاط الاتفاق والاختلاف بين كل منهما:-

أولاً: أوجه الاتفاق.

يتشابه المحرر الإلكتروني والمحرر التقليدي (الورقي) في أن كلاهما يحتوي على مجموعة من الرموز التي تعبر عن مجموعة مترابطة من الأفكار والمعاني الإنسانية، يدعو المشرع لحمايتها[2].

كما يرتب الاعتداء على كلاهما وقوع ضرر يمس مصلحة عامة في المجتمع تتمثل في المساس بالثقة العامة، التي تضفيها الدولة عليهما، كما يتشابه المحرر الإلكتروني والتقليدي

---

[1] براهمي، حنان (2015). مرجع سابق، ص164.

[2] السقا، إيهاب فوزي (2002). مرجع سابق، ص18.

أيضا أن كلهما قد يحمل صفة المحرر الرسمي أو المحرر العرفي، وحتى يمكن استيعاب مفهوم المحرر الإلكتروني والذي له حجية الإثبات يتعين بيان مفهوم المحرر في صورته التقليدية، فالمحرر في صورته الورقية قد يكون ورقة رسمية أو عرفية، فيعتبر المحرر رسميا إذا أثبت فيه موظف عام أو شخص مكلف بخدمة عامة أمر ما، نظمه على يده أو تلقاه من ذوي الشأن، طبقاً للأوضاع القانونية وفي حدود سلطته واختصاصه[1].

ثانياً: أوجه الاختلاف

المستند الإلكتروني مجرد، أي ليس له كيان ملموس، بعكس السند الورقي، فالمتعامل يرى الدعامة الورقية والكتابة عليها مباشرة دون اللجوء إلى أي وسيط تقني أو واقعي، في حين أنه بالنسبة للمستند الإلكتروني، لا يجد أمامه سوى الدعامة الإلكترونية (مثل قرص مدمج أو غيره)، ولا يستطيع الوصول إلى الكتابة المفهومة إلا عن طريق وسيط أو أجهزة إلكترونية (كجهاز كمبيوتر)، قادر على ترجمة البيانات التقنية المحفوظة إلى كتابة مفهومة للإنسان، تظهر على شاشة الكمبيوتر أو تطبع على الورق[2].

وبالتالي يجد الباحث أن السند الورقي قابل للقراءة مباشرة أما السند الإلكتروني فليس كذلك.

ويختلف المحرر الإلكتروني عن المحرر في شكله التقليدي، أن المحرر التقليدي يكتب بطريقة يدوية أو آلية في كيان مادي ملموس، ومن ثم يسهل قراءته بالعين المجردة ،أما المحرر

---

[1] عبد الفتاح، عابد (2014). مرجع سابق، ص21.

[2] كحول، سماح (2015). مرجع سابق، ص9.

الإلكتروني فهو يعالج عن طريق المكونات المادية والمعنوية لأجهزة الحوسبة والاتصالات، ويسجل على دعامة مغناطيسية تحمل الطابع الافتراضي أو المعنوي[1].

كما تحقق المستندات الإلكترونية عنصر الثقة والأمان، حيث يصعب العبث فيها أو تغيير محتواها، وذلك لأنها تعتمد على تكنولوجيا التأمين والتشفير، فهناك شفرة سرية تستخدم في حفظ السندات بحيث لا يمكن الإطلاع عليها إلا في حالة قرصنة الشيفرة، على عكس السندات التقليدية التي قد تتعرض للتغيير أو السرقة وبالتالي تفتقد عنصر السرية والأمان والثقة[2].

المحرر الورقي له أصل ورقي، حتى وإن تم إرساله عبر أجهزة شبكات الحاسب الآلي، مثل الفاكس والبريد الإلكتروني بعد إجراء عملية المسح الضوئي له، بينما المحرر الإلكتروني مخزن ومحفوظ إلكترونياً[3]. كما يتميز المحرر الورقي بصفة الدوام والثبات، فهو يكون بطريقة نهائية ومن ثم يسهل كشف أي تلاعب أو تزوير فيه بينما لا يتمتع المحرر الإلكتروني بهذه الصفة، لأنه قابل للمحو أو التعديل أو التلف دون ترك أثر ملحوظ يكشف التلاعب به، وخاصة إذا قام بذلك خبير أو مهني متخصص في الحاسب والمعلوماتية، ويمكن أن يتم ذلك أيضا بسبب الخلل الفني أو التقني في الأجهزة المستعملة سواء أتم ذلك تلقائيا أو بفعل فاعل مثل إطلاق الفيروس على البرامج لتدميره [4].

غير أن الباحث يرى أن هذا الكلام مبالغ، فيه لأن التكنولوجيا الحديثة أوجدت أنظمة تقنية وقائية على درجة عالية من الثقة تحفظ وتؤمن المحررات الإلكترونية من أي تلاعب أو أي اعتداء يقع عليها.

---

[1] بن خليفة، إلهام (2016). مرجع سابق، ص23.

[2] الرومي، محمد أمين (2007). مرجع سابق، ص106.

[3] بن خليفة، إلهام (2016). مرجع سابق، ص26.

[4] كحول، سماح (2015). مرجع سابق، ص11.

الفصل الثالث

الحماية الجزائية الموضوعية للمستند الإلكتروني

صاحب ظهور شبكة الانترنت تطورات كبيرة في شتى المجالات، حيث أصبحت معظم المعاملات التجارية تتم من خلال هذه الشبكة، مثل البيع والشراء، وغيرها. فتطورت المستندات الالكترونية وأضحت جزء لا يتجزأ من هذه المعاملات، وفي إطار ذلك قام بعض المجرمين بالاعتداء على هذه المستندات، حيث استخدموا طرق من أجل ذلك، على غرار الإتلاف والتزوير المعلوماتي، والسرقة الالكترونية بالإضافة إلى المساس بسرية المستند الالكتروني[1].

ولقد اختلف الفقهاء ورجال القانون في تكييف الجرائم الواقعة على المستند الإلكتروني، باعتبارها جرائم معلوماتية، فمنها من أخضعها إلى النصوص العقابية التقليدية باعتبارها جرائم عادية مثلها مثل جرائم التزوير، السرقة، الاحتيال، إساءة الائتمان... ، ومنها من سن لها نصوص عقابية خاصة ومستحدثة نظرا للطابع الرقمي للأدلة الناتجة عن ارتكابها. لذلك سنتناول في هذا الفصل من خلال مبحثين متتالين هما:

المبحث الأول: الحماية الجزائية الموضوعية للمستند الإلكتروني وفقاً للنصوص العقابية التقليدية

المبحث الثاني: الحماية الجزائية الموضوعية للمستند الإلكتروني وفقاً للنصوص العقابية المستحدثة

---

[1] طعباش، أمين (2013). **الحماية الجنائية للمعاملات الإلكترونية**، رسالة ماجستير، جامعة باتنة، ص58.

المبحث الأول

الحماية الجزائية الموضوعية للمستند الإلكتروني

وفقا للنصوص العقابية التقليدية

تعتبر الجرائم المعلوماتية من الجرائم المستحدثة، وهي تستهدف قطاعات كثيرة، مما جعل الفقه، فيما يخص تحديدها وتصنيفه، يتميز بالصعوبة، على عكس الجرائم التقليدية التي يمكن تصنيفها بسهولة فائقة، وبالتالي لم يستقر الفقهاء على معيار واحد لتصنيف الجرائم المعلوماتى، وذلك راجع إلى تشعب هذه الجرائم، وسرعة تطورها[1].

وسنحاول في هذا المبحث الوقوف عن مدى كفاية النصوص العقابية التقليدية في توفير حماية جزائية فعالة للمستند الإلكتروني، وذلك من خلال التطرق إلى مدى خضوع المستند الإلكتروني للنصوص العقابية لجريمة التزوير (المطلب الأول)، ثم مدى خضوع المستند الإلكتروني للنصوص العقابية لبعض جرائم الأموال (المطلب الثاني)، وذلك في المطلبين الآتيين:-

المطلب الأول

مدى خضوع المستند الالكتروني للنصوص العقابية لجريمة التزوير

نرى أن المساس بمحتوى المستند الإلكتروني، وذلك عن طريق تزويره يكون أشد صعوبة من تزوير المستند الورقي، لذا سنتناول هذا المطلب وفق الفروع الآتية:-

---

[1] يوسف، صغير (2013). **الجريمة المرتكبة عبر الانترنت**، رسالة ماجستير، جامعة مولود معمري، تيزي وزو، الجزائر، ص43.

الفرع الأول: تعريف جريمة التزوير

سوف نتعرض إلى تعريف التزوير التقليدي ثم التزوير المعلوماتي، وكما يلي:-

أولا: تعريف التزوير التقليدي: يعرف التزوير بأنه: " تغيير الحقيقة في المحرر بإحدى الطرق التي حددها القانون تغييراً من شأنه أن يترتب عنه ضرراً للغير وبنية استعمال هذا المحرر فيما أعد له"[1]. كما يعرف أيضا بأنه:" تحريف مفتعل للحقيقة في الواقع والبيانات التي يراد إثباتها بصك أو مخطوط يحتج به يمكن أن ينتج عنه ضرراً أدبياً أو مادياً أو اجتماعياً"[2].

المشرعين الأردني والعراقي قد أعطى كل منهما تعريفا له في نص المادة (260) من قانون العقوبات الأردني وفي المادة (286) من قانون العقوبات العراقي، وكذلك فعل القانون اللبناني في مادته (453) والمشرع السوري في نص المادة (440)[3].

ومما يؤخذ على المشرع المصري وبعض التشريعات العربية أنها لم تعط تعريفا للتزوير وانما يستخلص ذلك من نصوص تلك التشريعات.

ثانيا: تعريف التزوير المعلوماتي: التزوير في وثيقة معلوماتية هو:" تغيير للحقيقة في المستندات المعالجة آلياً والمستندات المعلوماتية، وذلك بنية استعمالها"[4]. كما عرف بأنه: "تغيير

---

[1] عبد الستار، فوزية (1990). **شرح قانون العقوبات، القسم الخاص**، القاهرة: دار النهضة العربية، ص244.

[2] براهمي، حنان (2015). **جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية**، أطروحة دكتوراه، جامعة محمد خيضر بسكرة، الجزائر، ص184.

[3] طعباش، أمين (2013). مرجع سابق، ص61.

[4] براهمي، حنان (2015). مرجع سابق، ص184.

للحقيقة بأي وسيلة كانت سواء كان ذلك في محرر أو دعامة طالما أن هذه الدعامة ذات أثر في إنشاء حق، أو لها شأن في إحداث نتيجة معينة"[1].

إذن يتضح للباحث أن التزوير المعلوماتي يتخذ مفهومين، الأول مفهوم تقليدي يبرز انطلاقا من كون النظام المعلوماتي وسيلة لارتكاب جريمة التزوير، أما الثاني فهو مفهوم حديث يتجسد انطلاقا من فكرة كون تغيير الحقيقة ينصب على معطيات موجودة ومخزنة داخل النظام المعلوماتي أي المحرر الالكتروني.

الفرع الثاني: أركان جريمة تزوير مستند الكتروني

نرى أن المساس بمحتوى المستند الالكتروني، عن طريق تزويره يكون أشد صعوبة من تزوير المستند الورقي[2]. وسنتناول بيان أركان جريمة تزوير المستند الالكتروني في النقاط التالية:-

أولا: الركن المادي في التزوير: يتمثل في جريمة تزوير مستند معلوماتي في بتغيير الحقيقة في محرر معلوماتي بإحدى الطرق التي نص عليها القانون تغييرا من شأنه أن يسبب ضررا[3].

ومن هنا ولقيام هذه الجريمة، يجد الباحث أنه لابد من توافر ثلاثة عناصر أساسية: **1.** وجود محرر. **2.** تغيير الحقيقة بإحدى الطرق المنصوص عليها قانونا. **3.** أن يترتب على ذلك ضرر عام أو خاص في الحاضر أو في المستقبل.

وسنبين كل عنصر من هذه العناصر:-

---

[1] طعباش، أمين (2013). مرجع سابق، ص63.

[2] الرومي، محمد أمين (2007). مرجع سابق، ص88.

[3] براهمي، حنان (2015). مرجع سابق، ص184.

1. **وجود محرر**: اشترط المشرع في جريمة التزوير التقليدية أن يقع فعل تغيير الحقيقة على محرر من المحررات العمومية أو الرسمية أو في المحررات العرفية أو التجارية أو المصرفية أو في بعض الوثائق الإدارية والشهادات، كما اشترط في المحرر أن يكون في شكل "كتابة" أو عبارات خطية، في حين أنه في جريمة التزوير المعلوماتي فإن المستند المعلوماتي هو الدعامة المادية التي تم تحويل المعطيات المعالجة عليها فيكون إما قرص مضغوط أو شريط ممغنط[1].

بالنسبة للمشرعين الأردني والعراقي، فقد أدرجا النصوص الخاصة بتزوير المحررات في المواد من 260-272 من قانون العقوبات الأردني والمواد 286-298 من قانون العقوبات العراقي التي تشترط المحرر لتطبيق جريمة التزوير، وعليه فإنه لا يمكن إخضاع أفعال التزوير المعلوماتي للنصوص العامة للتزوير وهذا ما يستدعي حقا تدخلا تشريعيا، إما بتعديل نصوص التزوير التقليدي على غرار المشرع الفرنسي عند إضافته لعبارة" أي سند للتعبير عن الرأي " لتعوض فكرة المحرر التقليدية، أو بإدراج نص خاص بالتزوير المعلوماتي.

والمستند المعلوماتي الذي يقع عليه فعل التزوير هو كل جسم منفصل أو يمكن فصله عن نظام المعالجة الآلية للمعطيات التي نظمها المشرع الفرنسي في الباب الثالث من القسم الثاني من الكتاب الثاني من قانون العقوبات الفرنسي في المواد من 1-323 إلى 7-232 وتجريم المشرع الفرنسي لتزوير الوثائق المعلوماتية جاء بسبب ارتباط هذه الوثائق أو المستندات المعلوماتية بقانون الإثبات، لذلك جاءت المادة 441-1 من قانون العقوبات الفرنسي لتجرم التزوير الذي من شأنه أن يسبب ضررا والذي يتم بأي وسيلة كانت وفي محرر أو سند للتعبير

---

[1] عبد اللطيف، معتوق (2012). **الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن**، رسالة ماجستير، جامعة الحاج لخضر، باتنة، الجزائر، ص46.

عن الرأي، ويشمل ذلك الأقراص الممغنطة والأسطوانات المدمجة، وأي بطاقة مغناطيسية أو وسيط يصلح لممارسة حق أو تصرف، أي أن المشرع الفرنسي اشترط أن يكون للمستند المعلوماتي قيمة في الإثبات لأي حق من الحقوق[1].

2. **تغيير الحقيقة:** يقصد بتغيير الحقيقة هو إبدالها بما يغايرها، وبالتالي فلا يعتبر تغييرا للحقيقة أي إضافة لمضمون المحرر أو حذف منه طالما ظل مضمون المحرر في حالته قبل الإضافة أو الحذف، ويقوم ذلك بصدد المستندات المعلوماتية في حالة حذفها أو إضافتها أو التلاعب فيها بأي صورة سواء كانت هذه البيانات مخزنة في ذاكرة الآلة أم كانت تمثل جزء من برنامج التشغيل أو برامج التطبيق، ويجب في هذه الحالة أن يكون محلا للتجريم[2].

ولذلك فإن تغيير الحقيقة في المعلومات المعالجة آلياً، قد يظهر على كيان مادي سواء كان ورقي أو دعامة الكترونية كالشرائط الممغنطة والأقراص الالكترونية وغيرها من الدعامات المماثلة، وفي هذا الغرض يفرق بعض الفقهاء بين تغيير المعلومات المخزنة في الجهاز، وبين إثبات هذه المعلومات في المستندات الصادرة عن النظام المعلوماتي والتي يتحقق فيها وصف المحرر، وبالتالي تتمتع بحماية القانون لها حسب نصوص التزوير باعتبارها معدة للتداول بين الأفراد، حيث يعتبر التزوير المعلوماتي منصب على مخرجات الحاسب الآلي، أي البيانات والمعلومات الخارجة منه، بشرط أن تطبع على دعامة مكتوبة أو مسجلة، أي يكون لها كيان مادي يمكن إدراكه، ولو تم تغيير الحقيقة دون طباعة فلا يمكن أن يطلق عليه تزويرا، فالتجريم

---

[1] الرومي، محمد أمين (2007). مرجع سابق، ص90.

[2] طعباش، أمين (2013). مرجع سابق، ص63.

وفقا للنص القانوني لا يتم إلا في حال حدوث التزوير في المعلومات الخارجة من النظام المعلوماتي[1].

3. **الضرر**: هو عنصر جوهري في جريمة التزوير، الضرر عنصر جوهري من عناصر جريمة التزوير، لا تقوم لها قائمة بدونه فإذا تخلف الضرر انتفى التزوير حتما ولو توافرت سائر أركانه، ذلك لأن التزوير في القانون لا عقاب عليه إلا إذا كان ضاراً، بحيث لا يكفي لقيام الركن المادي لهذه الجريمة أن يقع تغيير الحقيقة في محرر بإحدى الطرق التي بينها القانون وإنما يلزم فوق ذلك أن يكون من شأن هذا التغيير أن يسبب ضرراً[2].

ثانيا: الركن المعنوي في التزوير: يتمثل الركن المعنوي في جريمة تزوير المستندات المعلوماتية في القصد الجنائي، على اعتبار أن هذه الجريمة من الجرائم العمدية، وبالتالي يتخذ القصد الجنائي فيها صورة القصد العام والمتمثل في علم الجاني بفعل تغيير الحقيقة في المستند، مع إرادة إلحاق ضرر بشخص ما. أما إذا كان الجاني جاهلا بأن الفعل الذي يرتكبه غير مشروع فلا يتحقق لديه القصد الجرمي، وكذلك الحال إذا انتفى علم الجاني بأي ركن من أركان الجريمة، فلا يترتب عليه توافر القصد الجنائي لأنه يفترض بالفاعل أن يكون عالما بكافة أركان الجريمة، كما قد لا يتحقق القصد الجنائي إذا كان الفعل الذي يقوم به الجاني غير واضح بصورة صريحة

---

[1] براهمي، حنان (2015). مرجع سابق، ص205.

[2] الرومي، محمد أمين (2007). مرجع سابق، ص94.

كما هو الحال بالنسبة لانتحال صفة الغير أو الاتصاف بصفه غير صحيحة فقد يقوم مبرمج بيانات بتغيير الحقيقة في المحررات ولكنه غير عالما بهذا التغيير[1].

كما لا يكفي لقيام الركن المعنوي توافر القصد العام، إذ لا يكفي توافر الإرادة والعلم بمكونات الجريمة، بل لا بد أن تكون نية الجاني قد اتجهت وقت ارتكاب هذا الفعل إلى استعمال المحرر المزور فيما زور من أجله، أي إلى الاحتجاج به على اعتبار أنه صحيح[2].

حيث أن المشرع الفرنسي في جريمة التزوير في المستندات المعلوماتية يتطلب قصدا جنائيا خاصا يتمثل في نية الجاني إلى إحداث ضرر– سواء حقيقي أو احتمالي – للغير[3].

ويخلص الباحث إلى أن الركن المعنوي لجريمة التزوير في نطاق المعاملات الالكترونية هو اتجاه إرادة الجاني إلى تزوير مستندات معلوماتية مع نية مسبقة في استعمال المستندات المزورة فيا لغرض الذي تم تزويرها من أجله، وأن يؤدي هذا الفعل إلى حصول ضرر فعلي أو احتمالي لمن ارتكب ضده فمتى توافر الركن المادي والمعنوي قامت جريمة التزوير واستحق مرتكبها العقوبة.

وتعقيبا على ما تطرقنا إليه فيما يخص التزوير المعلوماتي، فإن الباحث يؤكد على ضرورة تدخل المشرع العراقي لتجريم التزوير المعلوماتي الذي يقع على مستند معلوماتي كالبطاقات الالكترونية وذلك إما بتعديله للنصوص المجرمة للتزوير في المحررات في قانون العقوبات، مثلما فعل المشرع الفرنسي بإضافة لعبارة: "أي سند التعبير عن فكرة "في المادة 441–1 من

---

[1] عبد اللطيف، معتوق (2012). مرجع سابق، ص49.

[2] براهمي، حنان (2015). مرجع سابق، ص266.

[3] يوسف، صغير (2013). مرجع سابق، ص120.

قانون العقوبات الفرنسي، مما أمكن معه متابعة أعمال التزوير التي تقع على بطاقات الائتمان وغيرها من البطاقات المغناطيسية، لأن هناك فراغ تشريعي في القانون العراقي في هذا المجال ولا يمكن تطبيق نصوص الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بالنظر إلى أن المستند المعلوماتي المتمثل في مخرجات الحاسب الآلي كبيانات أو معلومات مسجلة على بطاقات الكترونية أو أقراص مضغوطة هو جسم منفصل عن نظام المعالجة الآلية للمعطيات ولم تنص المواد 286-298 من قانون العقوبات العراقي عن حالة تغيير أو حذف معطيات منفصلة عن نظام المعالجة الآلية.

المطلب الثاني

مدى خضوع المستند الإلكتروني للنصوص العقابية لجرائم الأموال

إذا كان الكيان المادي للمعلوماتية يخضع للنشاط الإجرامي لجرائم الأموال دون أي إشكال، إذن سنحاول في هذا المطلب دراسة مدى إمكانية خضوع المستند الإلكتروني للنشاط الإجرامي ومدى تحقق الحماية الجزائية له وفقا للقواعد العامة المقررة لجرائم الإتلاف، السرقة، النصب وخيانة الأمانة، وفي الفروع الآتية:-

الفرع الأول: مدى خضوع المستند الالكتروني للنشاط الإجرامي في جريمة الإتلاف

عند تحقيق المجرم المعلوماتي لغايته باختراق النظام المعلوماتي أو البقاء فيه دون إذن يدفعه ذلك البقاء في غالب الأحيان إلى الإطلاع على المعطيات أو البيانات الموجودة داخل النظام، مما قد يدفعه في النهاية لإتلاف تلك البيانات أو المكونات المعنوية لنظام المعالجة الآلية للمعطيات،

وسنتطرق في هذا الفرع إلى تعريف جريمة الإتلاف التقليدية ثم جريمة اتلاف المستند الإلكتروني للتعرف على مدى انطباق النصوص المنظمة لها على إتلاف المستندات الإلكترونية.

أولا: تعريف جريمة الإتلاف التقليدي: تعني تخريب الشيء أو التقليل من قيمته بجعله غير صالح للاستعمال أو تعطيله، وقد يقصد بالإتلاف إفناء مادة الشيء أو هلاكه كليا أو جزئيا، أما التخريب فهو توقف الشيء تماما عن أداء منفعته كليا أو جزئيا دون إتلاف مادته [1]. ويقصد به أيضا تلك الأفعال المادية التي يأتيها الجاني بغرض التخريب وهنا تخريب الوثيقة أي إزالتها أو محو آثارها عمدا بوسائل مختلفة قد تكون التمزيق، الحذف ..... إلخ[2].

فالإتلاف إذن برأي الباحث يرد على كل المال أو على جزء منه بشرط أن يكون الإتلاف في الحالة الأخيرة من شأنه أن يجعل المال غير صالح للإستعمال، كما أنه لا يشترط أن يتم بوسيلة معينة، بشرط ألا تكون هذه الوسيلة مما يخضع لنص عقابي آخر.

ثانيا: تعريف جريمة إتلاف مستند الكتروني: نصت العديد من التشريعات على جريمة إتلاف المستند الالكتروني أو إتلاف البرامج والمعلومات المخزنة على الحاسب الآلي[3]. ويكون الإتلاف العمدي للبرامج والبيانات بمحوها كلية أو تدميرها إلكترونيا، أو تشويهها على نحو يقع فيه الإتلاف بما يجعلها غير صالحة للاستعمال[4]. وقد يتحقق الإتلاف أو التخريب بوسائل مختلفة

---

[1] براهمي، حنان (2015). مرجع سابق، ص52.

[2] الرومي، محمد أمين (2007). مرجع سابق، ص81.

[3] الرومي، محمد أمين (2007). مرجع سابق، ص89.

[4] الشوابكة، محمد أمين (2007). **جرائم الحاسوب والانترنت (الجريمة المعلوماتية)**، ط1، عمان: دار الثقافة للنشر و التوزيع، الأردن، ص216.

مادية أو معنوية سواء بالاعتداء على المعطيات والدعامة الموجودة عليها، أو محو المعطيات دون إصابة الدعامة، أو تعطيل البرامج أو محوها باستخدام أداة لهذا الغرض[1].

وبالتالي يجد الباحث أن محل جريمة الإتلاف في نطاق السندات الإلكترونية هو كل من المكونات المادية والمتمثلة في الأجهزة كشاشات العرض وأجهزة الإدخال والإخراج والقرص الصلب...إلخ. إضافة إلى المكونات المعنوية والمتمثلة في البرامج والبيانات والتي تحقق المعالجة الآلية للمعطيات شرط أن تكون ملك للغير.

ثالثا: أركان جريمة إتلاف سندات

1. **الركن الشرعي:** جاء في نص المادة 3/262 من قانون العقوبات الأردني أنه: "تطبق أحكام هذه المادة في حال إتلاف السند إتلافاً كلياً أو جزئياً". بينما نصت المادتين (300-301) من قانون العقوبات العراقي على جريمة اتلاف المحررات، حيث نصت المادة (1/300) على: "يعاقب بالسجن مدة لا تزيد على سبع سنوات أو بالحبس كل من أتلف أو أفسد أو عيب أو أبطل بسوء نية محرراً موجداً أو مثبتاً لدين أو تصرف في مال أو إبراء أو مخالصة أو أي محرر يمكن استعماله لإثبات حقوق الملكية". (والمقابلة للمادة 371 مكرر من قانون العقوبات المصري والمادة 1/322 من قانون العقوبات الفرنسي).
2. **الركن المادي لجريمة الإتلاف: السلوك الإجرامي فيها هو:** الإتلاف الإزالة بطريق الغش لوثيقة أو سند أو عقود أو أموال منقول[2]. وهنا الإتلاف يشمل مختلف الوثائق قد

---

[1] براهمي، حنان (2015). مرجع سابق، ص54.

[2] الشوابكة، محمد أمين (2007). مرجع سابق، ص220.

تكون المستندات أو عقود والتي تكون في حوزة الموظف كما تشمل أموال منقولة كانت في عهدته، فالمال المنقول يقصد به ذلك المال الذي يمكن تغيير موقعه نتيجة للفعل المادي، وهنا الإتلاف المعدي الذي يتم بواسطة الغش فمدلول المنقول في القانون الجنائي واسع عن القانون المدني بحيث تعبر منقولات المواشي التي يعتبرها القانون المدني عقارات بالتخصيص، كذلك محاصيل مزرعة والتي يرد عليها الإتلاف على هذه الأشياء كمحل للجريمة[1].

وما يلاحظ الباحث، أن فعل الإتلاف بصفة عامة له عدة صور، ومن الطبيعي أن يختلف مضمون وصور الإتلاف في قانون العقوبات عن إتلاف البرامج والمعلومات، ويرجع ذلك الاختلاف إلى محل الجريمة، حيث يشترط أن يقع الإتلاف أو التعييب على مال منقول أو عقار، مملوك للغير.

3. **الركن المعنوي:** جريمة الإتلاف بصفة عامة هي من الجرائم العمدية، تتطلب توفر القصد الجنائي العام بعنصريه العلم والإرادة أي توجيه إرادة الجاني وهو مدرك كامل الإدراك إلى قيامه بالفعل أي إلى الإزالة أو إتلاف الوثائق الموضوعة بحوزته أو تغيير مجرى الأموال المنقولة بغرض الإضرار به، او يشترط أن يعلم الجاني أن المال الذي يقوم بإتلافه أو تعيبه مملوك للغير[2].

وعموما فلقد اختلف الفقه بين مؤيد ومعارض لوقوع جريمة الإتلاف على المعلومات والبرامج المعلوماتية، لذلك فإن الإشكالية في هذا المقام تتمثل في مدى إمكانية تطبيق النصوص

---

(1) الرومي، محمد أمين (2007). مرجع سابق، ص90-ص91.

(2) الرومي، محمد أمين (2007). مرجع سابق، ص92.

التقليدية، التي تعاقب على أفعال الهدم والتخريب الواقعة على أملاك الدولة والأفراد، على إتلاف المعلومات والبرامج المعلوماتية ؟

وللإجابة على هذه الإشكالية لابد من التطرق إلى الآراء المختلفة حول ذلك:-

- **الرأي المؤيد لإمكانية تطبيق النصوص التقليدية لجريمة الإتلاف على جرائم المستند الإلكتروني:** إن المشكلة تكمن في وصف المال بأنه منقول، وليس في الطبيعة المادية وغير المادية للنظام المعلوماتي بما يحتوي من معلومات وقواعد بيانات ونظم التشغيل اللازمة لها، وهذه الطبيعة المادية تمثل الجانب الأكبر من قيمة النظام كله، لذلك، فإن جوهر الإتلاف هو إفقاد صلاحية المال المتلف من الغرض المعد له، وهو مايفقده قيمته الحقيقية[1].

وإن البرامج والبيانات المنطقية هي مجموعة من المعلومات والأوامر لا يمكن الاستفادة منها إلا إذا وضعت في شيء مادي يمكن تعامله مع الجهاز، ومن هذا المنطلق، ذهب البعض إلى اعتبار البرنامج شيء مادي، وبالتالي إمكانية تطبيق النصوص التقليدية، كون الأسطوانة التي يوضع فيها، لها وجود مادي ملموس[2].

وقد استندت هذه الآراء لتأكيد إمكانية تطبيق النصوص التقليدية، إلى العديد من الحجج:-

---

[1] الشوابكة، محمد أمين (2007). مرجع سابق، ص224.

[2] براهمي، حنان (2015). مرجع سابق، ص62.

أ. إن البرنامج المعد والمعلومات المذكورة التي تشمل بطبيعتها العنصرين المادي والمعنوي، لايمكن فصل أحدهما عن الآخر، فلا يتصور أن يوجد برنامج دون وسيط مادي.

ب. إن التطور الهائل في عالم التكنولوجيا جعل المعلومات تحتل مركزا مهما، يمكن أن تكون معها محلا للملكية، وعلى هذا الأساس يمكن اعتبارها في حكم الشيء المادي ذات القيمة الإقتصادية على ضوء ماتقدم، يمكن القول أن البرنامج هو عبارة عن أوامر موضوعية بشكل منطقي، فلا يمكن الإستفادة منه إلا إذا وضع في شيء مادي، إلا أنه يجب الفصل بينه وبين الوسيط المادي، لأنه يمكن الدخول إلى البرنامج واتلاف المعلومات الموجودة بداخله دون المساس بالوسيط المادي.

- **الرأي المعارض لإمكانية تطبيق النصوص التقليدية لجريمة الإتلاف على جرائم المستند الإلكتروني:** اعتبر هذا الرأي أن المعلومات المبرمجة آليا كالنبضات الكهربائية، تفتقر إلى الطبيعة المادية، وان هذه المعلومات ذات طبيعة معنوية، وهي تستقل من ناحية الأصل عن الوعاء المفرغة فيه من ناحية الشكل الخارجي، ولها ذات القيمة الاقتصادية للمال المادي، وبالتالي يتعين أن تخضع لأحكامه وتعامل تماما كما يعامل، فيعطيها الحماية والحقوق ذاتها، المقررة للمال المادي[1].

ويمكن للباحث القول أن الرأي المعارض قد ميز بشكل واضح بين المعلومات كمنقول معنوي، وبين أدوات الكومبيوتر وآلاته التي تخضع للنصوص التقليدية، كونها شيئا ماديا بحتا، ومن هنا تظهر صعوبة تطبيق النصوص التقليدية.

---

[1] الرومي، محمد أمين (2007). مرجع سابق، ص102.

بالإضافة إلى ذلك، فإن العقوبات التي تفرض لا توازي قيمة الضرر، فأضرار الشركات تقدر بالملاين، بل بالمليارات وبالتالي، فإن النصوص التقليدية عاجزة عن المساواة بين الضرر وبين العقوبة، من هنا كانت الحاجة إلى تدخل المشرع لسد هذه الثغرات[1].

إلا أن الرأي الراجع في الفقه يتجه إلى وقوع جريمة الإتلاف على البرامج والمعلومات وبالتالي وقوعها على المستند الإلكتروني.

الفرع الثاني: مدى خضوع المستند الإلكتروني للنشاط الإجرامي في جريمة السرقة وخيانة الأمانة

إذا كان الكيان المادي للمعلوماتية يخضع للنشاط الإجرامي لجرائم الأموال دون أي إشكال، إذن سنحاول في هذا الفرع دراسة مدى إمكانية خضوع المستند الإلكتروني للنشاط الإجرامي لجرائم السرقة والنصب وخيانة الأمانة ومدى تحقق الحماية الجزائية له وفقا لنصوص هذه الجرائم.

أولا: جريمة السرقة: تتفق السرقة عبر الانترنت مع السرقة التقليدية في أوجه كثيرة إلا أن اختلافهما يكون في محل السرقة ذاته، فمحل السرقة التقليدية مال منقول مملوك للغير، أما محل السرقة عبر الانترنت فهي المعلومات والبيانات المعالجة إلكترونيا. ويمكن تعريف جريمة

---

[1] بركات، ميساء مصطفى (2009)، **جرائم التعدي على المعلوماتية (الإتلاف والتزوير)**، رسالة ماجستير، جامعة بيروت، لبنان، 2009، ص27.

السرقة الإلكترونية على أنها: استخدام الوسائط الحاسوبية وشبكات الإنترنت لأخذ مال متقوم مملوك للغير، خفية، من حرز صاحبه [1].

ويفهم الباحث من هذا التعريف أن السرقة في مجال المعاملات الإلكترونية لا تستهدف الشريط الممغنط أو الأسطوانة، لأن السارق لا يستهدف سرقتها للحصول على القيمة المادية بل يسرق ماهو مسجل عليها، أي يسرق المعلومات والبيانات المعالجة الكترونياً.

1. **الركن المادي لجريمة السرقة في نطاق المعاملات الإلكترونية:** إن البحث في مدى تحقق الركن المادي لجريمة السرقة في نطاق المعاملات الإلكترونية هو مراعاة لمدى تحقق فعل الأخذ أو الاختلاس في هذه الجريمة، ويستوي فعل الاختلاس في أن يكون الجاني قد استولى على المال خلسة أو عنوة أو تسلمه بناءا على يد عارضة فغير نيته واستولى عليه، ومن ثم فإن فعل الاختلاس يقتضي نقل حيازة المال موضوع الاختلاس أو السرقة من حيازة المجني عليه إلى الجاني، بمعنى أن يظهر الجاني بوصفه صاحب السلطة والسيطرة الفعلية[2].

ولقد أختلف الفقهاء بخصوص فكرة السرقة المعلوماتية، فالرأي المؤيد لفكرة السرقة المعلوماتية يرى أن الركن المادي للسرقة المعلوماتية وهو فعل الاختلاس يتكون من عنصرين هما العنصر الموضوعي وهو النشاط أو السلوك الإرادي المؤدي إلى النتيجة مع وجود علاقة سببية بينهما، أما العنصر الأخر الشخصي فهو نية الجاني في تملك الشئ وحيازته، حيث عند تشغيل الحاسب الآلي والحصول على معلومات أو البيانات يكون قد اختلسها واستحوذ عليها

---

[1] الشوابكة، محمد أمين (2007). مرجع سابق، ص230.

[2] بركات، ميساء مصطفى (2009). مرجع سابق، ص34.

بطريق غير مشروع[1]. لذلك أدانت محكمة (Grenoble) الفرنسية، دائرة الجنح– المستأنفة في 1995/02/15، عامل بتهمة السرقة، كان قد أخرج من المؤسسة التي يعمل بها أوراقا سرية كان سيقوم بتصويرها ثم يعيدها للمؤسسة[2].

أما الرأي المعارض فقد رأى عدم وجود إمكانية وقوع جريمة السرقة المعلوماتية، لارتباط فعل الاختلاس بالمحل المادي للاختلاس في السرقة[3]. ويترتب على ذلك أن التوقيع الإلكتروني والمستند الإلكتروني، والرسالة الإلكترونية، والكتابة الإلكترونية كل هذه عبارة عن قيم منقولة أو اعتبارية ليست أشياء، وبالتالي لا يمكن أن يخضع الاستيلاء عليها بدون و جه حق لجريمة السرقة[4].

2. **الركن المعنوي لجريمة السرقة في نطاق المعاملات الإلكترونية:** يتخذ الركن المعنوي في جريمة السرقة في نطاق المعلوماتية صورة القصد الجنائي العام والخاص، ويتحقق القصد الجنائي العام، بتوافر العلم والإرادة[5]. فيجب أن تتجه إرادة الجاني إلى الاستيلاء على المعلومات المسجلة إلكترونيا سواء المعلومات المخزنة داخل النظام المعلوماتي أو المعلومات المسجلة إلكترونيا، والمخزنة على دعامة خارجية مثل الأسطوانات والشرائط الممغنطة، مع علمه بأن المعلومات محل السرقة ملكا له، فإذا قام شخص بأخذ قرص

---

(1) عبد اللطيف، معتوق (2012). مرجع سابق، ص35.

(2) الشوابكة، محمد أمين (2007). مرجع سابق، ص156.

(3) الرومي، محمد أمين (2007). مرجع سابق، ص103.

(4) بركات، ميساء مصطفى (2009). مرجع سابق، ص40.

(5) الشوابكة، محمد أمين (2007). مرجع سابق، ص158.

ممغنط يحتوي على برامج معلوماتية واختلسه من صاحبه، ثم قام بتشغيله لمعرفة محتواه ثم رده فإن إرادة الاختلاس، تنتفي لديه ويختلف القصد العام عنده[1].

ثانياً: مدى تحقق الحماية الجنائية للمستند الالكتروني وفقا للقواعد العامة لجريمة خيانة الأمانة

تنص المادة (453) من قانون العقوبات العراقي على: "كل من أؤتمن على مال منقول مملوك للغير أو عهد به إليه بأية كيفية كانت أو سلم له لأي غرضٍ كان، فاستعمله بسوء قصد لنفسه أو لفائدته أو لفائدة شخص آخر، أو تصرف به بسوء قصد خلافاً للغرض الذي عهد به إليه أو سلم له من أجله حسب ما هو مقرر قانوناً أو حسب التعليمات الصريحة أو الضمنية الصادرة ممن سلمه إياه أو عهد به إليه يعاقب بالحبس أو الغرامة،....إلخ"[2].

وتعرف خيانة الأمانة على أنها استيلاء الأمين عمداً على الحيازة الكاملة لمال سلم إليه بمقتضى سند من سندات الأمانة التي نص عليها القانون[3].

والملاحظ أن كلا المشرعين الأردني والعراقي لم يتطرقا لجريمة خيانة الأمانة في المجال المعلوماتي، بالرغم من استحداث الأول لنصوص تعالج المساس بالأنظمة المعالجة الآلية للمعطيات وتعالج الغش المعلوماتي بشكل مباشر وتعالج التزوير مثلاً، إلا أنه أغفل ذلك فيما يتعلق بجريمة خيانة الأمانة.

---

[1] عبد اللطيف، معتوق (2012). مرجع سابق، ص58.

[2] تقابلها المادة (422) من قانون العقوبات الأردني.

[3] القهوجي، علي عبد القادر (1999). **شرح قانون العقوبات، القسم العام**، الإسكندرية: دار المطبوعات الجامعية، ص365.

والسؤال المطروح: هل يمكن القول بخضوع المكونات المعنوية للأنظمة المعلوماتية ومنها المستند الالكتروني للقواعد العامة التي تحكم جريمة خيانة الأمانة ؟

في هذا الصدد يرى جانب من الفقه أن الطبيعة المعنوية أو الغير مادية للقيم " المعلومات " في المجال المعلوماتي تثير بعض الصعوبات، وعلى الرغم من ذلك فان هذه القيم المعنوية مثل المعلومات والبرامج تصلح لأن تكون من ذلك محلا لجريمة خيانة الأمان، إما لأنها تعتبر بمثابة بضائع، وإما لأنها تدخل في مفهوم المكاتيب التي ترتب إلتزاما أو تحوي مخالصة[1].

وبالتالي يستنتج الباحث أن المعلومات التي يتم تداولها في مجال المعاملات الالكترونية تصلح لأن تكون محلا لجريمة خيانة الأمانة، ومتى تجسدت تلك المعلومات في شكل مرئي سواء على الشاشة الحاسب الآلي أو على دعامات خارجية كالأوراق والأقراص، فهي تعد من قبيل الأموال التي لها قيمة اقتصادية.

ويتمثل الركن المادي لهذه الجريمة في الأفعال الاختلاس والاستعمال والتبديد، أما الركن المعنوي فيتطلب في هذه الجريمة، القصد العام وهو أن يعلم الجاني أن ما يستولي عليه هو مال منقول مملوك للغير. وان تتجه إرادته إلى الاستيلاء على الحيازة الكاملة للشيء والظهور عليه بمظهر المالك أو صاحب الحق عليه. أما القصد الخاص فيتمثل في نية التملك أو الإتلاف أو غير ذلك[2].

---

[1] بركات، ميساء مصطفى (2009). مرجع سابق، ص45.

[2] القهوجي، علي عبد القادر (1999). مرجع سابق، ص391.

المبحث الثاني

الحماية الجزائية الموضوعية للمستند الإلكتروني

وفقا للنصوص العقابية المستحدثة

نظرا لقصور الحماية الجزائرية الموضوعية للمستند الالكتروني بواسطة النصوص العامة التقليدية وبصفة خاصة نصوص جرائم الأموال وجرائم التزوير، ظهرت الحاجة إلى ضرورة سن نصوص عقابية موضوعية خاصة حديثة لمكافحة الجرائم الماسة بالمستند الالكتروني.

وفي هذا الشأن تدارك المشرع الأردني خلال السنوات الأخيرة الفراغ القانوني في مجال الإجرام المعلوماتي عموماً، فلقد جرم المشرع الأردني الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات والتي تعاقب على الاختراقات الغير مصرح بها داخل نظم المعالجة الآلية للمعطيات، وذلك من خلال إصداره قانون الجرائم الالكترونية رقم 27 لسنة 2015 وقانون المعاملات الالكترونية رقم 15 لسنة 2015. أما التشريع العراقي، فإنه لم يخطو كثيراً في هذا المجال، فلديه مشروع قانون جرائم المعلوماتية لسنة 2010 والذي لم يرى النور حتى الآن ولم يتم إقراره بعد من قبل المشرع العراقي.

وقبل التطرق إلى هذه الجرائم، يجب أولاً التعريف بأنظمة المعالجة الآلية للمعطيات، حيث لم يقم المشرع الأردني بتعريفيها وهذا على غرار المشرع الفرنسي، إلا أن مشروع قانون جرائم المعلوماتية العراقي لسنة 2010 قد عرفها في المادة الأولى منه بقوله: " المعالجة الآلية للبيانات هي: العمليات والمهام التي تخضع لبيانات الحاسوب، بما في ذلك انشاؤها أو إرسالها أو استقبالها أو تخزينها أو تجهيزها بأي وجه آخر".

أما الفقه الفرنسي فقد عرفها كما يلي:" هي كل مركب يتكون من وحدة أو مجموعة وحدات المعالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط والتي يربط بينها مجموعة من العلاقات التي عن طريقها تتحقق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية"[1]. وإن الشرط الأول الذي يلزم لتحقق الجرائم الماسة بالنظم المعلوماتية، هو وجود نظام معالجة البيانات أو نظام المعالجة الآلية للمعطيات، ونظرا لقيمة نظم المعلومات فقد جرم المشرع الأردني التعدي عليها، سواء كان ذلك بالتعييب أو التدمير، أو إعاقة عملها أو الدخول إليها على وجه غير مشروع[2].

وسنتناول في هذا المبحث جرائم المساس بأنظمة المعالجة الآلية للمعطيات من خلال التطرق لجريمة الدخول أو البقاء عن طريق الغش داخل نظام المعالجة الآلية للمعطيات (المطلب الأول)، جرائم الإعتداء على سلامة المعطيات (المطلب الثاني)، الجرائم المنصوص عليها في قانون المعاملات الالكترونية "جرائم التوقيع والتصديق الإلكترونيين" (المطلب الثالث)، وذلك في المطالب الثلاث الآتية:-

---

([1]) قشقوش، هدى حامد (2012). **جرائم الحاسب الالكتروني في التشريع المقارن**، القاهرة: دار المهضة العربية، ص88.

([2]) حجازي، عبد الفتاح بيومي (2007). **التجارة الإلكترونية وحمايتها القانونية**، الإسكندرية: دار الكتب القانونية، ص22.

المطلب الأول

جريمة الدخول أو البقاء عن طريق الغش داخل نظام المعالجة الآلية للمعطيات

تنص المادة الثالثة من قانون الجرائم الإلكترونية الأردني على أنه: "

أ. يعاقب كل من دخل قصداً إلى الشبكة المعلوماتية أو نظم معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح، بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر وبغرامة لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار أو بكلتا هاتين العقوبتبن.

ب. إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء أو حذف أو إضافة أو تدمير أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات الشبكة المعلوماتية، فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار.

ج. يعاقب كل من دخل قصداً إلى موقع الكتروني لتغييره أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) دينار".

بالتالي الصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير مشروع بينما الصورة المشددة تتحقق بتوافر الظرف المشدد لها، ويكون في الحالة التي ينتج فيها عن الدخول

أو البقاء الغير مشروع، إما محو أو تغير في المعطيات الموجودة في النظام أو التخريب لنظام اشتغال المنظومة[1]. وسنتناول بيان ذلك في الفرعين الآتيين:-

الفرع الأول: الركن المادي للجريمة الدخول أو البقاء الغير مشروع في النظام.

عالج المشرع الأردني جريمة الدخول والبقاء الغير مشروع في المادة (3) من قانون الجرائم الإلكترونية، وعليه سوف نتطرق لفعل الدخول أولا ثم فعل البقاء.

أولا: فعل الدخول: فعل الدخول الذي يشكل الركن المادي في هذه الجريمة لا يقصد به الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه بل يقصد به الدخول باستخدام الوسائل الفنية والتقنية إلى النظام المعلومات أي الدخول المعنوي أو الالكتروني، ويتحقق فعل الدخول إلى النظام متى دخل الجاني إلى النظام كله أو جزء منه كالدخول إلى شبكة الاتصال أو البرنامج، وكذالك يتحقق الدخول الغير مشروع متى كان مسموحا للجاني بالدخول لجزء معين في البرنامج حيث تجاوزه إلى جزء آخر غير مسموح له بالدخول فيه[2].

ويلاحظ الباحث أن المشرع الأردني يعاقب بمجرد الدخول أو البقاء الغير مشروع لمدة طالت أو قصرت. وبما أن المشرع الأردني لم يحدد وسيلة الدخول إلى النظام المعلومات، فإننا نرى أنه يمكن الدخول بأي وسيلة كانت، وذلك عن طريق كلمة السر الحقيقية متى كان الجاني غير مخول في استخدامها، أو باستخدام برنامج أو شفرة خاصة، أو عن طريق استخدام الرقم الكودي لشخص أخر أو الدخول من خلال شخص مسموح له بالدخول.

([1]) قشقوش، هدى حامد (2012). مرجع سابق، ص92.

([2]) حجازي، عبد الفتاح بيومي (2007). مرجع سابق، ص31.

ثانيا: فعل البقاء: يعرف البقاء الغير المشروع بأنه التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له لحق في السيطرة على هذا النظام[1]، ويتحقق الركن المادي لجريمة البقاء غير المصرح به داخل النظام المعلوماتي في الحالة التي يجد فيها الشخص نفسه داخل النظام عن طريق الخطأ أو الصدفة إلا انه يقرر البقاء داخل النظام وعدم قطع الاتصال، والبقاء المعاقب عليه قد يتحقق مستقلا عن الدخول إلى النظام وقد يجتمعان ويكون البقاء معاقب عليه استقلالا، حين يكون الدخول إلى النظام المعلوماتي مشروعاً[2].

الفرع الثاني: الركن المعنوي لجريمة الدخول أو البقاء الغير مشروع داخل النظام١

المقصود بالركن المعنوي أن يكون المتهم على علم بالدخول أو البقاء الغير قانوني وبدون وجه حق في النظام. والدخول والبقاء يشكلان جريمة عندما يرتكبان عن طريق الغش فمصطلح"عن طريق الغش" يفترض أن الدخول أو البقاء كان بإرادة الفاعل وان هذا الأخير كان على علم بارتكابه النشاط المجرم ولكن لا يهم أن يكون الفاعل أراد الإضرار أو لا بالنظام المخترق، وبالتالي الركن المعنوي في هذه الجريمة هو القصد العام. وتعد جريمتي، الدخول والبقاء في منظومة المعالجة الآلية للمعطيات من الخطر، فالجريمتين تقعن بمجرد ارتكاب فعلي الدخول أو البقاء دون أن يتطلب المشرع في ذلك نتيجة إجرامية لهذا السلوك[3].

والإشكالية التي تثور في هذا الصدد، متى تنتهي جريمة الدخول ومتى تبدأ جريمة البقاء؟

---

[1] الشوابكة، محمد أمين (2007). مرجع سابق، ص88.

[2] طعباش، أمين (2013). مرجع سابق، ص78.

[3] قشقوش، هدى حامد (2012). مرجع سابق، ص108.

يذهب رأي راجح من الفقه إلى أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي يبدأ فيها الجاني التجول داخل النظام أو يستمر في التجول داخله بعد انتهاء الوقت المحدد، أي منذ علم الجاني أنه ليس له الحق الدخول، فإذا دخل وظل ساكنا تظل الجريمة، جريمة الدخول إلى النظام، أما إذا بدأ في التجول فإن جريمة البقاء داخل النظام تبدأ من تلك اللحظة لأنه يتجول في نظام يعلم مسبقا أن مبدأ دخوله واستمراره فيه غير مشروع، ومنذ تلك اللحظة تبدأ جريمة البقاء داخل النظام[1].

ويرى الباحث أنه إذا كانت تلك الجريمة على هذه الصورة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، إلا أنها تحقق أيضا وبصورة غير مباشرة، حماية المعطيات أو المعلومات بذاتها بل يمكن من خلالها تجريم سرقة الآلة، كما يمكن أن تطبق على الاستخدام غير مشروع للبطاقات الممغنطة، إما لسرقتها أو التزوير ثم استخدامها.

([1]) حجازي، عبد الفتاح بيومي (2007). مرجع سابق، ص31.- قشقوش، هدى حامد (2012). مرجع سابق، ص110.

المطلب الثاني

جرائم الاعتداء على سلامة المعطيات

الاعتداء العمدي على سلامة المعطيات يتخذ صورتين: جريمة التلاعب بالمعطيات وجريمة التعامل بمعطيات غير مشروعة. وسنتناول بيانها في الفرعين الآتيين:-

الفرع الأول: الركن المادي لجريمة الاعتداء على سلامة المعطيات

نصت على الجريمة المادة (4) من قانون الجرائم الإلكترونية الأردني على: "يعاقب كل من أدخل أو نشر أو استخدم قصداً برنامجاً عن طريق الشبكة المعلوماتية أو باستخدام نظم معلومات لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الآخرين من الإطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول إليه أو تغيير موقع الكتروني أو الغائه أو اتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) دينار".

ما يستخلص من نص المادة أن هذه الجريمة تتم بركنها المادي عن طريق التلاعب في المعطيات الموجهة للنظام المعلوماتي عن طريق عمليات الإدخال والتعديل والإزالة لمعطيات في إطار هذا النظام المعلوماتي، حيث ينصب في هذه المرحلة نشاط الجاني على تلاعب في المعلومات المدخلة للنظام المعلوماتي دون أن يحدث تلاعب في البرامج، ولكن البرنامج يقوم

بعمله وفقا لنظامه، وهو الأمر الذي يؤدي في النهاية إلى إخراج معلومات مزورة وغير مطابقة لحقيقة المعلومات الواجب تخزينها في النظام المعلوماتي[1].

الفرع الثاني: الركن المعنوي لجريمة الاعتداء على سلامة المعطيات

يتمثل الركن المعنوي لهذه الجريمة في القصد الجنائي العام ولا يشترط توافر القصد الجنائي الخاص، إذ يكفي إن تتجه إرادة الجاني إلى الاعتداء على المعطيات والإدخال أو التعديل أو المحو، وان يعلم الجاني بأن نشاطه ذلك يترتب عليه التلاعب في المعطيات[2].

وتجدر الإشارة إلى إن الحماية الجنائية تشمل المعطيات طالما أنها تدخل في نظام المعالجة الآلية أي طالما كان يحتويها ذلك النظام وكانت تكون وحدة واحدة مع عناصر، ويترتب على ذلك أن الجريمة لا تتحقق إذا وقع النشاط الإجرامي على المعطيات خارج النظام سواء قبل دخولها أم بعد خروجها وحتى ولو لفترة قصيرة كما لو كانت مفرغة على قرص أو شريط ممغنط خارج النظام، وتقع أفعال الإدخال والمحو والتعديل المعطيات بطريق مباشرة أو غير مباشرة[3].

وبالتالي يلاحظ الباحث أن المشرع الأردني يحمي المستند الالكتروني سواء أكان داخل النظام المعلوماتي أو خارجه، فالمشرع يقصد بالمعطيات المخزنة تلك التي تكون على دعامة خارجية كالأقراص أو تكون مخزنة داخل النظام ذاته في الذاكرة، أما المعطيات المعالجة هي التي أصبحت من النظام أي أصبحت عبارة عن إشارة أو رموز تمثل معلومات معالجة آليا .

---

[1] عبد الغني، حسونة (2015). **جريمة التزوير المعلوماتي بين الأحكام التقليدية والنصوص المستحدثة**، بحث مقدم لأعمال الملتقى الوطني حول الجريمة المعلوماتية، بين الوقاية والمكافحة –كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، ما بين 16 و17، نوفمبر، 2015، ص7.

[2] الشوابكة، محمد أمين (2007). مرجع سابق، ص91.

[3] قشقوش، هدى حامد (2012). مرجع سابق، ص111.

المطلب الثالث

الجرائم المنصوص عليها في قانون المعاملات الالكترونية

"جرائم التوقيع والتصديق الالكتروني"

سعى المشرع الأردني إلى توفير حماية جزائية موضوعية للمستند الإلكتروني من خلال العديد من النصوص العقابية المتفرقة التقليدية منها والمستحدثة كما سبق وأن عرضنا في دراستنا، ولقد عمل أيضا على توفير حماية جزائية موضوعية للمستند الإلكتروني من خلال إصدار قانون المعاملات الإلكترونية الخاص بالتوقيع والتصديق الإلكتروني، والذي بدوره نص من خلاله على أحكام جزائية خاصة بالجرائم الماسة بالتوقيع والتصديق الإلكترونيين . وسنتناول في هذا المطلب تعريف التوقيع الإلكتروني (الفرع الأول)، جرائم التوقيع الإلكتروني (الفرع الثاني) .

الفرع الأول: تعريف التوقيع الالكتروني

عرفه أحدهم بأنه : "كل إشارات أو رموز أو حروف مرخص بها من الجهة المختصة باعتماد التوقيع ومرتبطا ارتباطا وثيقا بالتصرف القانوني، ويسمح بتمييز صاحبها وتحديد هويته، وينم دون غموض عن رضائه بهذا التصرف"[1].

كذلك عرفت المادة (2) كما عرفت المادة الأولى من قانون المعاملات الالكترونية الأردني رقم 15 لسنة 2015، التوقيع الالكتروني بأنه: "البيانات التي تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها وتكون مدرجة بشكل إلكتروني أو أي وسيلة أخرى مماثلة في

---

[1] طعباش، أمين (2013). مرجع سابق، ص45.

السجل الالكتروني، أو تكون مضافة عليه أو مرتبطة بو بهدف تحديد هوية صاحب التوقيع وانفراده باستخدامه وتمييزه عن غيره".

كذلك عرف قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي رقم 78 لسنة 2012، التوقيع الإلكتروني بأنه: "علامة شخصية تتخذ شكل حروف أو أرقام أو رموز أو إشارات او اصوات أو غيرها وله طابع متفرد يدل على نسبته الى الموقع ويكون معتمداً من جهة التصديق".

الفرع الثاني: جرائم التوقيع الالكتروني

نصت عليها المواد (24-26) من قانون المعاملات الالكترونية الأردني.

حيث نصت المادة (24) على ما يلي: "يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على ثلاث سنوات أو بغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار أو بكلتا هاتين العقوبتين كل من:-

أ. أنشأ أو نشر أو قدم شهادة توثيق الكتروني بغرض احتيالي أو لأي غرض غير مشروع.
ب. قدم إلى جهة التوثيق الإلكتروني معلومات غير صحيحة بقصد إصدار شهادة توثيق أو وقف سريانها أو إلغائها.

كما نصت المادة (25) من ذات القانون على: "تعاقب أي من جهات التوثيق الالكتروني المرخصة أو المعتمدة بغرامة لا تقل عن (50000) خمسين ألف دينار ولا تزيد على (100000) مائة الف دينار، بالإضافة إلى إلغاء ترخيصها أو اعتمادها إذا قدمت معلومات غير صحيحة في طلب الترخيص أو الاعتماد أو أفشت أسرار أحد عملائها أو استغلت

المعلومات المتوافرة لديها عن طالب شهادة التوثيق الالكتروني لأغراض أخرى غير أنشطة التوثيق الالكتروني دون الحصول على موافقة طالب الشهادة الخطية المسبقة".

كذلك نصت المادة (27) على ما يلي: "يعاقب كل من يمارس نشاط جهات التوثيق الإلكتروني داخل المملكة، دون الحصول على ترخيص أو اعتماد وفقاً لأحكام هذا القانون والأنظمة الصادرة بمقتضاه بغرامة لا تقل عن (50000) خمسين ألف دينار ولا تزيد على (100000) مائة ألف دينار".

الفصل الرابع

الحماية الجزائية الإجرائية للمستند الإلكتروني

تعد متابعة الجريمة المعلوماتية بصفة عامة ومتابعة جرائم المستند الإلكتروني بصفة خاصة، من أهم التحديات التي تواجه رجال الضابطة العدلية بالنظر إلى طبيعة الجريمة المعلوماتية، وهذا من حيث أنها تتعلق بمحل غير مادي بالإضافة إلى صعوبة دور الشرطة ومختلف الأجهزة الأمنية في مراقبتها ومنع حدوثها وكذلك التحري عن مرتكبيها.

كما أن المجرم المعلوماتي، عادة ما يكون ذا خبرة ودهاء خارق لا يستطيع المحقق الجنائي العادي التعامل معه، كما أن الأدلة المتحصل عليها من مسرح الجريمة تختلف عن الأدلة التقليدية.

وعليه سنتطرق في هذا الفصل إلى أهم القواعد الإجرائية التي جاء بها المشرعين الأردني والعراقي لمواجهة هذه الأنماط المستجدة من الجرائم. حيث سوف نتحدث عن إجراءات التحري والتحقق في الجرائم الماسة بالمستند الإلكتروني (المبحث الأول)، ثم عن إجراءات المحاكمة في الجرائم الماسة بالمستند الإلكتروني (المبحث الثاني).

وذلك من خلال التقسيم الآتي:-

المبحث الأول: إجراءات التحري والتحقيق في الجرائم الماسة بالمستند الالكتروني

المبحث الثاني: إجراءات المحاكمة في الجرائم الماسة بالمستند الإلكتروني

المبحث الأول

إجراءات التحري والتحقيق في الجرائم الماسة بالمستند الالكتروني

لقد عمل المشرع الأردني على تطوير أساليب التحري والتحقيق فيما يخص الجرائم المعلوماتية لتتلائم مع خصوصية هذه الجرائم، وذلك من خلال تعديل قانون أصول المحاكمات الجزائية رقم 9 لسنة 1961 بموجب القانون المعدل رقم 27 لسنة 2017، والمتضمن بعض القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. وعلى العكس من ذلك لا زال قانون أصول المحاكمات الجزائية العراقي بنصوصه التقليدية هو ما ينطبق على هذا النوع من الجرائم.

إن التحقيق والتحري وجمع الأدلة في الجريمة المعلوماتية له طابع خاص، مما يتوجب على السلطة المختصة بالتحري والتحقيق، الإلمام الواسع بمعطيات الحاسوب وطبيعته، ويتعين على المحقق في هذا المجال أن تتوفر فيه شروطا خاصة حتى يتمكن من التحقق على أكمل وجه، لذا وجب أن تتم هذه الإجراءات بصورة صحيحة وقانونية لأن اللجوء إلى الطرق الغير مشروعة يؤدي إلى بطلان هذه الإجراءات.

لذلك سنخصص هذا المبحث للحديث عن إجراءات التحري والتحقيق التقليدية في الجرائم الماسة بالمستند الإلكتروني (المطلب الاول)، وأخيرا نتطرق إلى إجراءات التحري والتحقيق الحديثة في الجرائم الماسة بالمستند الإلكتروني (المطلب الثاني).

المطلب الأول

إجراءات التحري والتحقيق التقليدية في الجرائم الماسة بالمستند الالكتروني

من خلال هذا المطلب سنتطرق إلى أهم القواعد الإجرائية التقليدية المستنبطة من الوقائع أو الأشياء (الفرع الأول)، والمستنبطة من تصريحات الأشخاص (الفرع الثاني)، والتي نص عليها المشرع الأردني في قانون الجرائم الالكترونية وقانون أصول المحاكامت الجزائية المخصصة للبحث والتحقيق عن الجرائم الماسة بالمستند الإلكتروني، وذلك وفقاً للتقسيم الآتي:-

الفرع الأول: إجراءات التحري والتحقيق التقليدية المستنبطة من الوقائع أو الأشياء

سوف نعرج في هذا الفرع الأول على أسلوب الانتقال والمعاينة، ونبحث في خصوصيات التفتيش في البيئة الرقمية، ونبحث في خصوصيات الحجز والضبط.

أولا :الانتقال للمعاينة: عرفها أحدهم بأنها: "إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة"[1]. هذا بالنسبة الانتقال للمعاينة في الحالة الجرائم في صورته التقليدية، أما الانتقال والمعاينة في الجريمة المعلوماتية فيجب التمييز دائما بين حالتين أساسيتين:

- **الحالة الأولى:** المعاينة في حالة الجرائم الواقعة على المكونات المادية للحاسب الآلي كجرائم الاعتداء على أشرطة الحاسب وكابلاته وشاشة العرض الخاصة به ومفاتيح التشغيل الأقراص وغيرها من مكونات الكومبيوتر ذات طابع المادي الملموس .

---

[1] وردة، أشرف الدين (2017). **الإثبات الجنائي بالأدلة الإلكترونية (دراسة مقارنة)**، أطروحة دكتوراه، جامعة محمد خيضر بسكرة، الجزائر، ص182.

- **الحالة الثانية:** المعاينة في الحالة الجرائم الواقعة على مكونات الغير مادية أو بواسطته، او تتمثل في تلك الجرائم الواقعة على البرامج الكمبيوتر وبياناته أو بواسطتها، وهنا تثور الصعوبات التي تحول دون فعالية المعاينة ومنها:-

أ. قلة الآثار المادية المتخلفة من الجرائم التي تقع على برامج الحاسوب والشبكات

ب. إمكانية حدوث تغيير أو تلف أو تلفيق أو عبث بالآثار المادية أو زوال بعضها.

ج. نقص الدراية ومعرفة المحقق بالجوانب الفنية والتقنية لاستخدام شبكة الانترنت والحاسوب[1].

وإذا تمت المعاينة بعد وقوع الجريمة في المجال الإلكتروني، فيجب مراعاة مايلي:

1. تصوير الحاسب والأجهزة الظرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان الصورة.
2. العناية بملاحظة الطريقة التي تم بها إعداد النظام .
3. ملاحظة واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر، فيما بعد على المحكمة .
4. عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجل.

---

[1] السقا، إيهاب فوزي (2002). مرجع سابق، ص154.

5. التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة، وفحصها، ويرفع من عليها من البصمات ذات الصلة بالجريمة.
6. التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع ومضاهاة ما قد يوجد عليها من بصمات.
7. قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر لهم الكفاءة العالية والخبرة الفنية في مجال الحاسبات[1].

وكذلك يختلف الانتقال والمعاينة في العالم الافتراضي عن الكيفية المتبعة لمعاينة مسرح الجريمة التقليدية. حيث يمكن لرجل الضبطية العدلية الانتقال إلى مسرح الجريمة في العالم الافتراضي، من خلال الحاسوب الموجود في مكتبه، أو عبر مقهى الانترنت، أو اللجوء إلى مقر مزود الخدمة ، الذي يعتبر أحسن الأماكن الإمكانية إجراء المعاينة[2].

ثانيا: التفتيش: يعرف التفتيش على انه:" إجراء من إجراءات التحقيق، بهدف إلى جمع الأدلة، وإزالة الغموض عن الجريمة ونسبتها إلى متهم معين"[3]، ويمكن تعريف تفتيش نظم الحاسوب والانترنت بأنه: "البحث في مستودع جهاز المتهم أو الضحية عن الأشياء مادية أو معنوية تفيد كشف الحقيقة ونسبتها إلية"[4].

---

[1] عقيدة، محمد أبو العلا (2003). **التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية**، بحث مقدم لأعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، في 26 نيسان 2003، كلية الحقوق، جامعة الإمارات، ص11.

[2] وردة، أشرف الدين (2017). مرجع سابق، ص186.

[3] عقيدة، محمد أبو العلا (2003). مرجع سابق، ص12.

[4] السقا، إيهاب فوزي (2002). مرجع سابق، ص154.

ثالثا: الضبط: يعرف الضبط في البيئة الالكترونية على أنه: "وضع اليد على الدعائم المادية المخزنة فيها البيانات الكترونية أو المعلومات التي تتصل بالجريمة المعلوماتية التي وقعت وتفيد في كشف الحقيقة عنها وعن مركبتها"[1].

ونظرا لكون الضبط محله في مجال الجرائم الالكترونية هو البيانات المعالجة الكترونياً، فقد ثار التساؤل حول : هل يصلح هذا النوع من البيانات لأن يكون محلا للضبط الذي يعني كما رأينا وضع اليد على شيء مادي ملموس؟

انقسم القفة إلى اتجاهين عند الإجابة عن هذا التساؤل: فيرى البعض أن بيانات الحاسب لا تصلح لأن تكون محلاً للضبط، لانتفاء الكيان المادي عنها، ولا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس[2]. ويرى الاتجاه الثاني أن البيانات المعالجة الكترونيا ماهي إلا ذبذبات الكترونية أو موجات كهرومغناطيسية تقبل التسجيل والحفظ وتخزين على وسائط مادية[3].

رابعاً: إجراءات التفتيش والضبط في الجرائم الماسة بالمستند الإلكتروني وفقا للتشريع الأردني

بالإضافة إلى إجراءات التفتيش والضبط الواردة في قانون أصول المحاكمات الجزائية الأردني، ورد في قانون الجرائم الالكترونية الأردني في المادة (13) منه بأنه: "

أ. مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية، يجوز لموظفي الضابطة العدلية، بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة، الدخول إلى أي مكان تشير الدلائل إلى استخدامه

---

[1] وردة، أشرف الدين (2017). مرجع سابق، ص189.

[2] السقا، إيهاب فوزي (2002). مرجع سابق، ص161.

[3] عقيدة، محمد أبو العلا (2003). مرجع سابق، ص16.

لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضراً بذلك ويقدمه إلى المدعي العام المختص.

ب. مع مراعاة الفقرة (أ) من هذه المادة ومراعاة حقوق الآخرين ذوي النية الحسنة، وباستثناء المرخص لهم وفق أحكام قانون الاتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون، يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون والأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها".

الفرع الثاني: إجراءات التحري والتحقيق التقليدية المستنبطة من تصريحات الأشخاص.

أولا: الشهادة:

1. **تعريف الشهادة:** هي ما يقوله أحد الأشخاص عما شاهده أو سمعه أو أدركه بحواسه عن واقعة بطريقة مباشرة، فهي تحضى باهتمام القاضي إلا أنه غالبا ما يحتاج في مقام وزن الأدلة إلى من رأى الواقعة أو سمع عنها أو أدركها بحواسه[1]. ويختلف الشاهد التقليدي عن الشاهد المعلوماتي ذلك أن الآخير هو: "الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي، والذي تكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات متى كانت مصلحة التحقيق تتطلب التنقيب

---

[1] وردة، أشرف الدين (2017). مرجع سابق، ص135.

عن المعلومات الداخلية"[1]. وتنحصر طوائف الشاهد المعلوماتي في: مشغلو الحساب الآلي وخبراء البرمجة والمحللون ومهندسو الصيانة والاتصالات ومديري النظام[2].

2. **إجراءات الشهادة في الجرائم الماسة بالمستند الإلكتروني:** اهتم المشرع الأردني بدور الشاهد المعلوماتي في مساعدة السلطات العامة في مكافحة الجرائم المعلوماتية، وهذا عن طريق إلزامه بالإعلام عن المعلومات الجوهرية التي تسمح بالدخول إلى الحاسوب وجمع الأدلة المخزنة به، كما نصت المادة 19 من اتفاقية بودابست لمكافحة جرائم الكمبيوتر لعام 2001 على إمكانية الاستعانة بالشاهد المعلوماتي، بقولها يجب على كل طرف أن يتبين الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من اجل تحويل سلطاته المختصة سلطة إصدار الأمر لأي شخص لديه معلومات عن تشغيل النظام أو الإجراءات المطبقة من اجل حماية البيانات المعلوماتية التي تضمن تقديم كل المعلومات على نحو يسمح بتطبيق الإجراءات المشار إليها في الفقرتين 1و2[3].

ثانياً: الاستجواب: هو مساءلة المتهم ومناقشته عن وقائع القضية المنسوبة إليه عن الجريمة التي ارتكبها ومجابهته بالأدلة وسماع ما لديه من دفوع التهمة المنسوبة إليه، والاستجواب في الجريمة المعلوماتية تحكمه ذات القواعد العامة لاستجواب المتهم في الجريمة لتقليدية ومن بين حقوق المتهم أثناء الاستجواب، حق المتهم في الاستعانة بمحامي وحق المحامي في الاطلاع على التحقيق[4].

---

[1] السقا، إيهاب فوزي (2002). مرجع سابق، ص166.

[2] عقيدة، محمد أبو العلا (2003). مرجع سابق، ص18.

[3] وردة، أشرف الدين (2017). مرجع سابق، ص260.

[4] السقا، إيهاب فوزي (2002). مرجع سابق، ص171.

المطلب الثاني

إجراءات التحري والتحقيق الحديثة في الجرائم الماسة بالمستند الالكتروني

إن الأنظمة المعلوماتية وفي ظل المعطيات الحديثة للمجتمعات المعاصرة تشهد انفتاحاً غير مسبوق ومحدود واتاحة للمعلومة غير مشروط وهو ما جعلها مجالا مفتوحا تهدده أخطار الاعتداءات المعلوماتية بكل أشكالها. مما جعل العديد من الدول تقوم بتطوير سياستها الجنائية تبعا لهذه الخصوصية وتمكن رجال الشرطة القضائية، من الكشف عن الجرائم، من خلال سن إجراءات حديثة للتحري والتحقيق عن الجرائم المعلوماتية ومنها جرائم الماسة بالمستند الإلكتروني، ومنه سنتطرق في هذا المطلب إلى أهم الإجراءات التحري والتحقيق الحديثة المستنبطة من الوقائع أو الأشياء (الفرع الأول)، والإجراءات المستنبطة من تصريحات الأشخاص (الفرع الثاني).

الفرع الأول: الإجراءات الحديثة المستنبطة من الوقائع أو الأشياء

تتمثل هذه الإجراءات في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بالإضافة إلى إجراء المراقبة الالكترونية.

أولا: اعتراض المراسلات السلكية واللاسلكية وتسجيل الأصوات والتقاط الصور

1. **تعريفه:** قد تضطر الشرطة القضائية لاستعمال كاميرات خفية أو أجهزة تصنت لكن يجب ان يكون ذلك في إطار احترام الشرعية الإجرائية حفاظا على كرامة الحياة الخاصة للإنسان، كما يمكن لضابط الشرطة القضائية تصوير جسم ومكان الجريمة بشكلها العام في إطار ممارسة مهامه، لكنه يمنع من الاطلاع أو تسجيل المكالمات أو الأحاديث

الخاصة إلا بإذن مسبق من طرف السلطات القضائية[1]، والمقصود بالمراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ،كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطيسية[2]. أما تسجيل الأصوات والتقاط الصور فيقصد به تسجيل المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية أو خاصة في مكان عام أو خاص، وكذالك التقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان واحد خاص[3].

2. **إجراءات إعتراض المراسلات وتسجيل الأصوات والتقاط الصور وفقا للتشريع الأردني:**

نظم قانون أصول المحاكمات الجزائية الأردني موضوع اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، يجوز لرجال الشرطة القضائية إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي[4]، والقيام باعتراض المراسلات، تسجيل الأصوات والتقاط الصور لكنه قيدهم بجملة من الشروط لتكون إجراءاتهم صحيحة ومنتجة لآثارها.

---

[1] وردة، أشرف الدين (2017). مرجع سابق، ص264.

[2] السقا، إيهاب فوزي (2002). مرجع سابق، ص178.

[3] السقا، إيهاب فوزي (2002). مرجع سابق، ص179.

[4] المقصود بالتحقيق الابتدائي، هو التحريات الأولية للضابطة العدلية.

الفرع الثاني: إجراءات التحري والتحقيق الحديثة المستنبطة من تصريحات الأشخاص

أولاً: التحفظ العاجل على البيانات المعلوماتية المخزنة: تحدث المشرع الأردني في المادة (13/ب) من قانون الجرائم الالكترونية عن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق[1].

ثالثاً: الأمر بإنتاج بيانات معلوماتية: هو إجراء جديد للتحري والتحقيق على الجرائم المعلوماتية، لم تنص عليه معظم الدول منها الأردن، لكن تم النص عليه ضمن اتفاقية بودابست لمكافحة جرائم المعلوماتية لسنة 2001 وهذا في نص المادة 18 من الاتفاقية. كما تم النص عليه ضمن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة سنة 2010 ، وهذا في نص المادة 25 من الاتفاقية[2].

---

[1] وردة، أشرف الدين (2017). مرجع سابق، ص266.

[2] السقا، إيهاب فوزي (2002). مرجع سابق، ص188.

المبحث الثاني

إجراءات المحاكمة في الجرائم الماسة بالمستند الالكتروني

تواجه الجريمة المعلوماتية بصفة عامة العديد من المشكلات المتمثلة في تحديد القانون الواجب التطبيق والمحكمة المختصة بالنظر في تلك الجرائم. وتبرز أهمية هذا التحديد في مجال الجرائم المعلوماتية جراء البعد الوطني الذي تتميز به هذه الجريمة، لأن غالبية الأفعال ترتكب من خارج الحدود أو أنها تمر عبر شبكة الانترنت، وهو ما يبرز مدى ملائمة قواعد الاختصاص والقانون الواجب التطبيق[1].

وسنتطرق في هذا المبحث إلى: تحديد المحكمة الجنائية المختصة (المطلب الأول)، ثم تقييم الأدلة الرقمية المستخلصة من الجرائم الماسة بالمستند الإلكتروني (المطلب الثاني).

المطلب الأول

تحديد المحكمة الجنائية المختصة

ثار خلاف فقهي كبير حول تحديد المحكمة الجنائية المختصة في الجرائم المعلوماتية بما فيها جرائم الاعتداء على المستند الالكتروني. وسنبين في هذا المطلب إلى موقف الفقه (الفرع الأول) من تحديد المحكمة المختصة، وتحديد القانون الواجب التطبيق (الفرع الثاني)، ثم موقف المشرعين الأردني والعراقي (الفرع الثالث).

---

[1] يوسف، صغير (2013). مرجع سابق، ص140.

الفرع الأول: موقف الفقه

حاول الفقه حل مشكلة تنتزع الاختصاص، وانقسم إلى ثلاثة اتجاهات وهي: معيار الاختصاص المكاني، معيار القانون أكثر ملائمة، ومعيار الضرر المرتقب.

أولا: معيار الاختصاص المكاني: تعتمد أغلب التشريعات في تحديد الاختصاص المكاني، إتباع ثلاثة ضوابط، وهي مكان وقوع الجريمة أو محل إقامة المتهم أو مكان ضبط إلقاء القبض عليه، وفي حالة اجتماع أكثر من ضابط، تكون المحكمة التي ترفع إليها الدعوى أولا هي المختصة بنظر الدعوى. وبالتالي ينعقد الاختصاص وفقا لهذا المعيار، للمحكمة التي يقع في نطاقها النشاط الإجرامي، وليس مكان حصول النتيجة أو الآثار المترتبة عليه، بدعوى أن اتخاذ آثار الفعل كمناط لتحديد مكان وقوع الجريمة تكنفه بعض الصعوبات. حيث يمثل السلوك الإجرامي والنتيجة الإجرامية شطري الجريمة المعلوماتية، ومن ثم فإن سلطات ومحاكم مكان النشاط الإجرامي ومكان النتيجة تكون مختصة، وعلى ذلك فإذا تم بث الفيروس المعلوماتي (السلوك الإجرامي) في مكان، وتحققت النتيجة (تدمير المعلومات) في مكان آخر وألقي القبض على الجاني في مكان ثالث، فإن الاختصاص ينعقد لمحاكم إحدى هذه الأماكن[1].

ثانيا: معيار القانون الأكثر ملائمة: يرى أصحاب هذا الاتجاه، بأنه نظرا للطبيعة الخاصة لجرائم المعلوماتية والأضرار الناجمة عنها التي تمتد ليشمل أكثر من دولة واحدة، وأحيانا قد تتفاوت نسبة الضرر بين دولة وأخرى إلى القول بأنه يجب التوسع في تفسير قاعدة اختصاص محكمة وقوع الفعل (حصول الضرر)، ليجعل الاختصاص لمحكمة الدولة الأكثر تعرضا للضرر

---

[1] حجازي، عبد الفتاح بيومي (2006). **مبادئ الإجراءات الجنائية، في جرائم الكومبيوتر**، ط1، الإسكندرية: دار الفكر الجامعي، ص51-ص52.

بشكل فعلي، مع التركيز على مبدأ التخلي أو التنازل عن الاختصاص بخلاف ذلك وان جعل الاختصاص لقانون دولة ما لمجرد إمكانية الوصول إلى المعلومة من هذه الدولة أو تلك، أصبح أمرا غير كافي من الناحية القانونية لإعلان اختصاص هذه الدولة أو تلك[1].

ثالثا: معيار الضرر المرتقب: صاحب ظهور شبكة الانترنت وجود عالم افتراضي، حيث تسري فيه مختلف المواد المعلوماتية دون إمكانية تحديد وجهتها، وهذا العالم الافتراضي لا يخضع لأي سلطة إقليمية، وبالتالي يترتب على هذه الحالة، الضرر الذي تسببه الجريمة المعلوماتية يمكن أن يحدث في أي دولة تكون متصلة بالانترنت، وهذا هو معيار الضرر المرتقب أو الافتراضي[2].

الفرع الثاني: تحديد القانون الواجب التطبيق

وفقا لمبدأ الإقليمية فإن المحاكم الجزائية تختص في الدولة بالنظر في الجرائم التي تقع كلها أو جزء منها على إقليمها أيا كانت صفة الشخص المتهم وبغض النظر عن جنسيته. فإذا ما ارتكب شخص ما جريمة معلوماتية بداخل الدولة، وتحققت نتيجتها بذات الدولة، فالقانون الواجب التطبيق بلا منازع هو قانون هذه الدولة بغض النظر عن جنسية الجاني أو المجني عليه[3].

---

[1] يوسف، صغير (2013). مرجع سابق، ص144.

[2] يوسف، صغير (2013). مرجع سابق، ص142.

[3] حجازي، عبد الفتاح بيومي (2006). مرجع سابق، ص59-ص60.

وعملا بمبدأ العينية فإن الاختصاص يكون للمحاكم إذا وقعت جريمة من جرائم الانترنت أو المستند الالكتروني بصفة خاصة تمس بمصالح الدولة الأساسية والجوهرية وان وقعت خارج الدولة وبغض النظر عن جنسية مرتكبيها[1].

ووفقاً لمبدأ شخصية القوانين فإن الفقهاء يرون أن لهذا المبدأ وجهان أحدهما إيجابي والآخر سلبي، أما الوجه الإيجابي، فيعني بتطبيق النص الجنائي على كل من يحمل جنسية الدولة، ولو ارتكبت جريمته خارج إقليمها. أما الوجه السلبي للمبدأ، فيعني بتطبيق النص الجنائي على كل جريمة يكون المجني عليه فيها منتمية إلى جنسية الدولة ولو كان مرتكب هذه الجريمة أجنبيا وارتكبها خارج إقليم الدولة[2].

الفرع الثالث: موقف المشرعين الأردني والعراقي

بالنسبة للاختصاص الجنائي الوطني، فإنه يتحدد وفقا للاختصاص المحلي للجهات القضائية بمكان وقوع الجريمة ومحل إقامة الأشخاص المشتبه في مساهمتهم في الجريمة أو بالمكان الذي تم في دائرته القبض على هؤلاء الأشخاص.

وإن أهم الإشكاليات المطروحة والمتعلقة بالاختصاص القضائي في الجرائم المتصلة بتكنولوجيا المعلوماتية تتمثل أساسا في إشكالية الاختصاص المحلي في الجرائم الواقعة خارج الإقليم الوطني وكذا إشكالية الإجراءات أمام الأقطاب القضائية المختصة.

---

[1] حجازي، عبد الفتاح بيومي (2006). مرجع سابق، ص62.

[2] يوسف، صغير (2013). مرجع سابق، ص145.

إن قواعد القانون الجنائي (بشقيه الموضوعي والإجرائي) تخضع في تطبيقها من حيث المكان لمبدأ مستقر ومعروف، ألا وهو مبدأ الإقليمية، والأصل أن عناصر الركن المادي للجريمة تكتمل في مكان واحد، وعلى ضوء ذلك يتحدد القانون الواجب التطبيق، وبالتبعية للمحكمة المختصة بنظر الدعوى. بيد أن الجرائم المعلوماتية يتجاوز مداها أحيانا حدود الدولة، حينما يتجزأ ركنها المادي أو يتوزع على أكثر من مكان بحيث يمكن وقوع السلوك في مكان، في حين تتحقق النتيجة الإجرامية الضارة في نطاق إقليم دولة أخرى[1].

وتثار مشكلة الاختصاص القضائي المحلي بالنسبة للجرائم المعلوماتية في حالة ما إذا ارتكبت الجريمة في أكثر من نطاق اختصاص محلي داخل الإقليم الوطني للدولة، بسبب طبيعة الجريمة وشبكة المعلوماتية، فالجريمة في هذه الحالة سواء تمثلت بجريمة الدخول أو إتلاف المستند الالكتروني قد وقعت بكامل أركانها في نطاق اختصاص المحاكم الجزائرية والحل المناسب لهذه المشكلة هو تمديد الاختصاص القضائي داخل إقليم الدولة بما يتناسب وطبيعة الجريمة المرتكبة إذ يمكن تطبيق أي قاعدة من قواعد الاختصاص سواء اقترفت بمكان القبض عليه، فينعقد الاختصاص للمحكمة التي دخلت الدعوى الجزائية حوزتها قبل غيرها. فإذا نظرت محكمة محل إقامة المتهم في قضية فتكون مختصة بالنظر فيها دون غيرها ولها أن تمدد الاختصاص بشأن اتخاذ أي إجراء من إجراءات المحاكمة، بشرط أن يكون التمديد بموجب نص قانوني[2].

---

[1] حجازي، عبد الفتاح بيومي (2006). مرجع سابق، ص66.

[2] حجازي، عبد الفتاح بيومي (2006). مرجع سابق، ص66-ص67..

المطلب الثاني

تقييم الأدلة الرقمية المستخلصة من الجرائم الماسة بالمستند الالكتروني

نظراً للطابع الخاص الذي تمتاز به الجريمة المعلوماتية، فقد تبين أن إثباتها تحيط به الكثير من الصعاب، ومما لا شك فيه أن إثبات هذا النوع من الجرائم يحتاج إلى أدلة ذات طبيعة خاصة، تختلف عن الأدلة التقليدية[1].

وسنتطرق في هذا المطلب إلى مفهوم الدليل الرقمي (الفرع الأول)، ثم تقدير الدليل الرقمي المستخلص من الجرائم الماسة بالمستند الإلكتروني أمام القضاء الجزائي (الفرع الثاني).

الفرع الأول: مفهوم الدليل الرقمي

أولا: تعريف الدليل الرقمي: يعرف الدليل الالكتروني المستخرج من المستند الالكتروني بأنه : "تلك الأدلة التي يمكن الحصول عليها من الحاسوب بإحدى وسائل الإخراج"[2]. أو هو ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية، وأجهزة ومعدات وأدوات الحاسب الآلي أو شبكات الاتصالات من خلال إجراءات قانونية وفنية، لتقديمها للقضاء بعد تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة، أو رسومات أو صور و أشكال و أصوات، لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها[3]. كما عرفته المنظمة العالمية لدليل

---

[1] مصطفى، عائشة بن قارة (2010). **حجية الدليل الإلكتروني في مجال الإثبات الجنائي**، الإسكندرية: دار الجامعة الجديدة، ص49.

[2] وردة، أشرف الدين (2017). مرجع سابق، ص281.

[3] مصطفى، عائشة بن قارة (2010). مرجع سابق، ص51.

الكمبيوتر IOCE في أكتوبر 2001 بأنه (المعلومات) ذات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية[1].

ومن خلال هذه التعاريف، يمكن للباحث تحديد خاصيتين للدليل الرقمي هما:

- **الخاصية الأولى:** إن الدليل الالكتروني هو عبارة عن معلومات أو بيانات الكترونية مخزنة في الحاسوب أو المنقولة بواسطته، أيا كان شكل هذا الحاسوب، سواء كان حاسوب شخصي، أو مخدم الإنترنت، أو أن يكون ضمن الهاتف الجوال، أو ساعة اليد، أو الكاميرات الرقمية وغيرها.
- **الخاصية الثانية:** القيمة الاستدلالية أو البرهانية لهذه المعلومات في إثبات أو نفي الجرائم.

ثانيا: أنواع الدليل الرقمي

هي الأدلة الإلكترونية الخاصة بأجهزة الحاسوب وشبكاته[2]: وهي تلك الأدلة المتحصل عليها بواسطة الأقراص الممغنطة و الأشرطة المغناطيسية أو غيرها من الوسائط الإلكترونية ومنها وحدات الإدخال ووحدات الإخراج، المعالجة المركزية، والبطاقات PCMIA Cardas التخزين بالإضافة إلى أجهزة المودم و الكروت أو البطاقات الممغنطة[3].

---

[1] وردة، أشرف الدين (2017). مرجع سابق، ص282.

[2] الحلبي، خالد عباد الحلبي (2014). **إجراءات التحري والتحقيق وجمع الأدلة في جرائم الحاسوب والانترنت**، ط1، عمان: دار الثقافة للنشر والتوزيع ، ص233.

[3] وردة، أشرف الدين (2017). مرجع سابق، ص285.

الفرع الثاني: تقدير الدليل الرقمي المستخلص من الجرائم الماسة بالمستند الإلكتروني أمام القضاء الجزائي

تعد مرحلة المحاكمة من أهم إجراءات الدعوى باعتبارها مرحلة حاسمة، إذ تعتبر عملية تقدير الأدلة جوهر الحكم وليس باستطاعة القاضي إدراك الدليل والوصول إليه إلا بعد ممارسة سلطته التقديرية للأدلة محل الوقائع فتتوقف سلامة الحكم على سلامة تقدير الأدلة، ويعتبر الدليل الرقمي كباقي الأدلة يتم تقديره من طرف القاضي الجنائي، غير أنه لا يستطيع هذا الأخير أن يقوم بتقدير هذا الدليل إلا إذا كانت المحكمة المرفوع أمامها الدعوى صاحبة الاختصاص بالفصل في الجريمة المعلوماتية[1].

أولا: شروط قبول الدليل الرقمي

حتى يتحقق الدليل اللازم للإثبات فإنه لابد من أن تتوفر فيه شروط تجعل له حجية وقيمة يثبت بها الحق وهي:

1. **شرط مشروعية الدليل الرقمي::** يشترط في الدليل الرقمي الجنائي عموما لقبوله كدليل إثبات أن يتم الحصول عليه بطريقة مشروعة[2]. ووفقا للأمانة والنزاهة أنه يستلزم على القاضي الجنائي تطبيق الدليل تطبيقا سليما وأن يستمد اقتناعه من دليل رقمي مقبول، لأن محل الحرية التي يتمتع بها القاضي الجنائي هو الأدلة المقبولة، وأن لا يتحصل

---

[1] الحلبي، خالد عباد الحلبي (2014). مرجع سابق، ص241.

[2] مصطفى، عائشة بن قارة (2010). مرجع سابق، ص248.

عليه من أدلة غير مشروعة كالإكراه المادي أو المعنوي أو الغش ضد الجاني في الجرائم المعلوماتية من أجل فك الشيفرة [1].

2. **شرط مناقشة الدليل الرقمي المستخرج من المستند الإلكتروني:** يستوي الأمر بالنسبة للأدلة الرقمية سواء كانت في شكل مخرجات ورقية أو الكترونية أو معروضة بواسطة الكمبيوتر على الشاشة الخاصة به، فيجب أن تعرض للمناقشة أثناء المحاكمة بوصفها أدلة إثبات، وللقاضي الجزائي الحرية في أن يستمد قناعته منها طالما أن لها ووقعت عليها المرافعات وناقشها أطراف الدعوى، ويترتب على هذه القاعدة شرطان أساسين هما:

أ. وجوب مناقشة الدليل الالكتروني بين أطراف الدعوى.

ب. الضوابط المتعلقة بالاقتناع القضائي: إذ أن سلطة القاضي الجزائي في تقديم الأدلة الرقمية وموازنتها وفقا لما يمليه وجدانه لا يخضع في ذلك لرقابة المحكمة العليا إلا أنه مع ذلك مقيد بضرورة تأسيس اقتناعه على الجزم واليقين من غير أن يكون هذا الاقتناع مخالفا لمقتضيات العقل والمنطق السليم[2].

3. **شرط يقينية الأدلة الإلكترونية:** يشترط في الأدلة المستخرجة من المستند الالكتروني أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة، ذلك أنه لا يمكن دحض قرينة البراءة وافتراض عكسها إلا عندما يصل القاضي الجزائري لحد الجزم واليقين[3].

---

[1] عبد اللطيف، معتوق (2012). مرجع سابق، ص49.

[2] الحلبي، خالد عباد الحلبي (2014). مرجع سابق، ص246.

[3] مصطفى، عائشة بن قارة (2010). مرجع سابق، ص255.

فشرط اليقين في أحكام الإدانة هو شرط عام، حيث أنه سواء كانت الأدلة التي يستنتج منها تقليدية أو مستحدثة كالدليل الرقمي، لذلك أن يكون الدليل الرقمي غير قابل للشك، إذ أن هذا الأخير يفسر لصالح المتهم استنادا إلى قاعدة أن الأصل في الإنسان البراءة، فيكفي أن يشكك القاضي من صحة إسناد التهمة إلى المتهم حتى يقضي بالبراءة[1].

ومنه يجد الباحث أنه تبقى مسألة تقييم الدليل الجنائي في إثبات الواقعة الجرمية هي مسألة موضوعية محضة، ولهذا يترك للقاضي الجنائي حرية تقدير الأدلة الجنائية وتكوين قناعته، ويبني حكمه على أي دليل متى أطمأن إليه ولو كان مستمد من محاضر الاستدلالات.

---

[1] الحلبي، خالد عباد الحلبي (2014). مرجع سابق، ص251.

الفصل الخامس

الخاتمة

(النتائج والتوصيات)

أولاً: الخاتمة

تبين معنا أن موضوع الحماية الجنائية للمستند الالكتروني من المواضيع الحديثة والتي تتعلق بالإطار القانوني للتعاملات الالكترونية، فلقد ساهمن المعلوماتية في تحويل المستندات الورقية إلى مستندات الكترونية، حيث أصبح المستند الالكتروني الأداة الأساسية لتنفيذ فكرة الحكومة الإلكترونية والتجارة الالكترونية.

كما وجدنا أن المستند الإلكتروني هو كل شيء مادي متميز لقرص صلبٍ أو مضغوط أو شريط ممغنط أو خلافه، يتضمن معلومات، معالجة الكترونياً، ومكتوب وموقع عليها بطريقة الكترونية، تكون قابلة للحفظ دون تلفها أو أحداث تغييرات عليها، ويمكن الرجوع إليها في أي وقت مع إمكانية تحويله لمستندٍ ورقي عن طريق إخراجه من مخرجاته الكمبيوترية.

ثانياً: النتائج

1. تبين معنا أن المشرع العراقي لم يسن أي قانون يعالج جرائم أنظمة المعلومات بما فيها الجرائم الواقعة على المستند الإلكتروني مثل التزوير الالكتروني والاحتيال الالكتروني والسرقة الالكترونية وغيرها، وإنما تتم الملاحقة والعقاب وفق القواعد العامة، وذلك على عكس ما ورد في التشريعات الأخرى كالأردني، الذي تناول هذه الجرائم الماسة بالمستند الالكتروني في قانون الجرائم الالكترونية رقم 27 لسنة 2015.

2. تطبق في العراق على الجرائم الواقعة على المعاملات الإلكترونية بما فيها المستندات الإلكترونية، النصوص العقابية لقانون العقوبات والقوانين المكملة له، بالرغم من الثبوت فقهيا وقانونيا عدم كفاءة وملائمة النصوص التقليدية لمكافحة هذا النوع المستحدث من الجرائم التي جاءت لمكافحة الجرائم العادية ذات الطبيعة المادية وليست الجرائم ذات الطبيعة غير المادية.

3. خص المشرع الأردني، التوقيع الالكتروني والمستند الالكتروني، بحماية جنائية خاصة، من خلال قانون المعاملات الالكترونية الأردني رقم 15 لسنة 2015، المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

4. إن البعد الإجرائي للجرائم المعلوماتية، ينطوي على تحديات ومشكلات جمة، عناوينها الرئيسية الحاجة إلى سرعة الكشف خشية ضياع الدليل، وقانونية وحجية الأدلة المستقاة من بيئة معلوماتية، وهذه المشكلات كانت ولا تزال محل اهتمام الصعيدين الوطني والدولي.

5. المستند الإلكتروني يمثل محرر له قوة إثبات قانونية والاعتراف بتلك الحجية يؤدي إلى استمرار المعاملات الإلكترونية وزيادة الثقة فيها، وحتى يتمتع المستند الإلكتروني بتلك الحجية لا بد من توفر شرط مشروعية إجراءات التحري والتحقيق في الحصول على الدليل الرقمي، ضرورة مناقشة الأدلة الرقمية المتحصل عليها من ارتكاب جرائم الماسة بالمستند الإلكتروني بالجلسة، وأن يخضع تقييم ذلك الدليل الرقمي إلى تقدير القاضي الجزائي بأن يصل في تقديره واقتناعه به إلى درجة اليقينية.

6. بالرغم من علمية الوسائل المستعملة في التحري والتحقيق للحصول على الدليل الرقمي المثبت لقيام جرائم ماسة بالمستند الإلكتروني، والتي تقترب إلى درجة الدقة العلمية القطعية، إلا أن تقدير هذا الدليل يخضع لاقتناع الشخصي للقاضي الجنائي مثله مثل كل الأدلة المادة المثبتة لقيام جريمة واقعة على المحررات الرسمية أو العرفية.

ثالثاً: التوصيات

1. نتمنى أن ينظم المشرع العراقي حماية جنائية موضوعية كافية للمستند الإلكتروني، من خلال النص على الجرائم الواقعة عليه والتي تتلائم مع الطبيعة غير المادي لهذه المستندات، كالتزوير الإلكتروني، جريمة الاحتيال الإلكتروني، الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة المرتكبة بواسطة تقنية المعلومات، جريمة الاستخدام غير المشروع لأدوات الدفع الإلكتروني... على غرار التشريعات العقابية الأخرى، ومنها الأردني.
2. نتمنى على المشرعين الأردني والعراقي ضع إجراءات خاصة أكثر دقة للتحقيق والمحاكمة للجريمة المعلوماتية تختلف عن الجريمة التقليدية.
3. ضرورة التعاون الدولي لمواجهة صور السلوك المنحرف في البيئة المعلوماتية، وذلك لان نظرا لخطورة هذه الجرائم العابرة للحدود الوطنية، ونظرا لن الدليل الرقمي قد يتواجد بإقليم دولة أخرى مما يصعب الحصول عليه وبالتالي ضياعه وافلات المجرمين من العقاب.

قائمة المصادر والمراجع

أولاً: الكتب القانونية.

- حجازي، عبد الفتاح بيومي (2009). **مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي**، ط1، القاهرة: دار النهضة العربية.
- حجازي، عبد الفتاح بيومي (2007). **التجارة الإلكترونية وحمايتها القانونية**، الإسكندرية: دار الكتب القانونية.
- حجازي، عبد الفتاح بيومي (2006). **مبادئ الإجراءات الجنائية، في جرائم الكومبيوتر**، ط1، الإسكندرية: دار الفكر الجامعي.
- الحلبي، خالد عباد الحلبي (2014). **إجراءات التحري والتحقيق وجمع الأدلة في جرائم الحاسوب والانترنت**، ط1، عمان: دار الثقافة للنشر والتوزيع.
- الرومي، محمد أمين (2007). **المستند الإلكتروني**، ط1، الإسكندرية: دار الفكر الجامعي.
- الزعبي، جلال والمناعسة، أسامة (2017). **جرائم تقنية نظم المعلومات الالكترونية، دراسة مقارنة**، ط3، عمان: دار الثقافة للنشر والتوزيع.
- السقا، إيهاب فوزي (2002). **جريمة التزوير في المحررات الإلكترونية**، الإسكندرية: دار الجامعة الجديدة.
- الشوابكة، محمد أمين (2007). **جرائم الحاسوب والانترنت (الجريمة المعلوماتية)**، ط1، عمان: دار الثقافة للنشر والتوزيع.

- عبد الفتاح، عابد (2014). **الكتابة الإلكترونية في القانون المدني بين التطور القانوني والأمن التقني**، الإسكندرية: دار الجامعة الجديدة.
- عبد الستار، فوزية (1990). **شرح قانون العقوبات، القسم الخاص**، القاهرة: دار النهضة العربية.
- عبيدات، لورنس محمد (2009). **إثبات المحرر الإلكتروني**، ط1، عمان: دار الثقافة للنشر والتوزيع.
- العبودي، عباس (2010). **تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها**، ط1، بيروت: منشورات الحلبي الحقوقية.
- قشقوش، هدى حامد (2012). **جرائم الحاسب الإلكتروني في التشريع المقارن**، القاهرة: دار النهضة العربية.
- القهوجي، علي عبد القادر (1999). **شرح قانون العقوبات، القسم العام**، الإسكندرية: دار المطبوعات الجامعية.
- القهوجي، علي عبد القادر (2010). **الحماية الجنائية لبرامج الحاسب الآلي**، الإسكندرية: دار الجامعة الجديدة للنشر.
- لطفي، محمد حسام الدين (2002). **الإطار القانوني للمعاملات الإلكترونية، دراسة في قواعد الإثبات في المواد المدنية والتجارية مع إشارة خاصة لبعض قوانين البلدان العربية**، القاهرة: دار النهضة العربية.
- مصطفى، عائشة بن قارة (2010). **حجية الدليل الإلكتروني في مجال الإثبات الجنائي**، الإسكندرية: دار الجامعة الجديدة.

- نصيرات، علاء محمد (2005). **حجية التوقيع الإلكتروني في الإثبات، دراسة مقارنة،** ط1، عمان: دار الثقافة للنشر والتوزيع.

ثانياً: الرسائل والأطروحات الجامعية.

- براهمي، حنان (2015). **جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية،** أطروحة دكتوراه، جامعة محمد خيضر بسكرة، الجزائر.
- بركات، ميساء مصطفى (2009)، **جرائم التعدي على المعلوماتية (الإتلاف والتزوير)،** رسالة ماجستير، جامعة بيروت، لبنان.
- بن خليفة، إلهام (2016). **الحماية الجنائية للمحررات الإلكترونية من التزوير،** أطروحة دكتوراه، جامعة الحاج لخضر، باتنة، الجزائر.
- شنين، صالح (2013). **الحماية الجنائية للتجارة الالكترونية، دراسة مقارنة،** أطروحة دكتوراه، جامعة أبو بكر بلقايد، تلمسان، الجزائر.
- طعباش، أمين (2013). **الحماية الجنائية للمعاملات الإلكترونية،** رسالة ماجستير، جامعة باتنة، الجزائر.
- عبد اللطيف، معتوق (2012). **الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن،** رسالة ماجستير، جامعة الحاج لخضر، باتنة، الجزائر.
- كحول، سماح (2015). **حجية الوسائل الإلكترونية في إثبات العقود التجارية،** رسالة ماجستير، جامعة قاصدي مرباح، ورقلة، الجزائر.
- وردة، أشرف الدين (2017). **الإثبات الجنائي بالأدلة الإلكترونية (دراسة مقارنة)،** أطروحة دكتوراه، جامعة محمد خيضر بسكرة، الجزائر.

- يوسف، صغير (2013). **الجريمة المرتكبة عبر الانترنت**، رسالة ماجستير، جامعة مولود معمري، تيزي وزو، الجزائر.

ثالثاً: أبحاث في دوريات ومؤتمرات

- براهمي، حنان (2012). **المحررات الإلكترونية كدليل إثبات**، مجلة الفكر، كلية الحقوق والعلوم السياسية، جامعة بسكرة، الجزائر، العدد 9.
- عبد الغني، حسونة (2015). **جريمة التزوير المعلوماتي بين الأحكام التقليدية والنصوص المستحدثة**، بحث مقدم لأعمال الملتقى الوطني حول الجريمة المعلوماتية، بين الوقاية والمكافحة –كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، ما بين 16 و17، نوفمبر، 2015.
- عقيدة، محمد أبو العلا (2003). **التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية**، بحث مقدم لأعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، في 26 نيسان 2003، كلية الحقوق، جامعة الإمارات.

رابعاً: القوانين الوطنية.

- قانون المعاملات الالكترونية الأردني رقم 15 لسنة 2015.
- قانون الجرائم الالكترونية رقم 27 لسنة 2015.
- قانون التوقيع الالكتروني والمعاملات الالكتروينة العراقي رقم 78 لعام 2012.
- مشروع القانون العراقي لجرائم أنظمة المعلومات لعام 2010.