# الحماية الجزائية للمستند الإلكتروني في التشريعات الأردنية والعراقية

# Penal protection for the electronic document In Jordanian and Iraqi legislation

إعداد

Pprrepared by

الباحث /عمر حسين الدليمي

Researcher / Omar Hussein Al-Dulaimi

كلية الحقوق والعلوم السياسية

Faculty of Law and Political Science

جامعة سوسة/ تونس

University of Sousse / Tunisia

oomar1502@gmail.com

2020

**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 الإلكتروني، ومن ثم المنهج التحليلي لدراسة النصوص القانونية الواردة في قانون الجرائم الإلكترونية 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 الإلكتروني، قانون الجرائم الإلكترونية.**

## 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.**

**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 . ( شنين ،2013 : 15)

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 إرتكاب جرائمهم بإستخدام وسائل إتصال يصعب إختراقها، وهو ما يعني أن التقدم التقني قد أمد المجرمين بوسائل بالغة الفاعلية في إرتكاب جرائمهم . ( الزعبي ،2017: 245)

**مشكلة الدراسة:**

تثير الدراسة التساؤل عن التشريعات الجنائية الأردنية والعراقية الخاصة بالحماية الجزائية للمستند الإلكتروني، وبيان مدى كفاية خطة التشريعات الأردنية والعراقية وبعض التشريعات المقارنة الأخرى في تجريم الأفعال التي تنال من المستند الإلكتروني وبيان مدى فاعلية خطة التجريم هذه.

1. ما هو نطاق فكرة المستند الإلكتروني؟ وكيفية تمييزها عما قد يختلط بها من حقوق ومصالح أخرى تخرج عن مدلولها؟
2. ما هي أهم الأفعال الإجرامية التي تنال من المستند الإلكتروني؟

**أهداف الدراسة**

تهدف الدراسة إلى إيضاح معالم المستند الإلكتروني 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.

**أهمية الدراسة**

تنبع أهمية الدراسة من النقاط التالية:-

1. 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.
2. 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.

**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 الإلكتروني). وهي دراسة في التشريع المصري للدكتور أشرف توفيق شمس الدين.

**منهجية الدراسة**

تتبع هذه الدراسة المنهج الوصفي المقارن في الحماية الجنائية المقررة للمستند الإلكتروني في التشريعين الأردني والعراقي.

## 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 الغرض نفسه وهو الإثبات.

## شروط المستند الالكتروني

من شروط المستند الإلكتروني نذكر مايلي:-

### أولاً: الكتابة الإلكترونية

تعد 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، وتعد الكتابة بدقة عن الواقعة التي أعدت لإثباتها، فهي تعتبر دليلاً عند حدوث نزاع بين أطراف الاتفاق وتعطي قدراً كبيراً من الاطمئنان لدى أصحاب الحقوق (براهيمي ،2015 : 107 ـ 108)

وبالتالي تعد الكتابة الشرط الأساسي والأهم في المستندات الإلكترونية .( السقا ،2002 : 28)

والتي تكون على شكل معادلات خوارزمية تنفذ 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 ( عبيدات، 2009 : 79)

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.

3. يجب أن يصعب العبث بها أو التعديل فيها دون أن يترك ذلك أثرا على المحرر الذي يحتويها. (عبد الفتاح ، 2014 : 17)

**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). (المصدر السابق : 33) وعرف أيضاً التوقيع الإلكتروني بأنه: (مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته) .(نصيرات ، 2005 : 33)

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 يمكنهم يستخدموها لإثبات ماتتضمنه من تصرفات قانونية، ولهذا السبب يطلق عليهم البعض، وكلاء الإثبات . (عبد الفتاح ، 2014 : 71)

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) . (نصيرات ، 2005 : 125 ـ 126)

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).

وتؤدي 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 مفتاح تشفير خاص يتسم بالسرية، حيث يحتفظ به الموقع، ويتم تثبيت نصفه في جهاز الكمبيوتر الخاص به، والنصف الأخر في بطاقة إلكترونية ( عبيدات، 2009: 112) أما جهة التوثيق فتحتفظ بالمفتاح العام، حيث تقوم بإرساله بالبريد الإلكتروني إلى الأشخاص الذين يتعامل معهم الموقع، وذلك لاستخدامه في فك التشفير.(براهيمي ، 2015 : 153)

**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 .( عبيدات . 2009: 112)

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.
3. الاحتفاظ بالمعلومات إن وجدت والتي تمكن من استبانة منشأ المستند الإلكتروني وجهة وصوله، وتاريخ ووقت إرساله واستلامه . (براهيمي،2015 : 164)

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).

## 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 .(السقا،2002 : 18)

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 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 . (عبد الفتاح،2014 : 21)

**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 . (كحول ،2015 : 9)

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 الإلكتروني فهو يعالج عن طريق المكونات المادية والمعنوية لأجهزة الحوسبة والاتصالات، ويسجل على دعامة مغناطيسية تحمل الطابع الافتراضي أو المعنوي . ( بن خليفة ، 2018 : 23)

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 . ( الرومي، 2007: 106)

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 (بن خليفة،2016: 26) 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 . (كحول، 2015 : 11)

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.

## 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 . (طعباش،2013: 58)

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.

### الحماية الجزائية الموضوعية للمستند الإلكتروني

### وفقا للنصوص العقابية التقليدية

تعد 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 . (يوسف ، 2013: 43)

## 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. أركان جريمة تزوير مستند الكتروني

نرى أن المساس بمحتوى المستند الالكتروني، عن طريق تزويره يكون أشد صعوبة من تزوير المستند الورقي . (الرومي ، 2007 : 88) 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 . (براهيمي ، 2015 :184)

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. **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. ( عبد اللطيف ، 2012 : 46)

بالنسبة للمشرعين الأردني والعراقي، فقد أدرجا النصوص الخاصة بتزوير المحررات في المواد من260-272 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 1-441 من قانون العقوبات الفرنسي لتجرم التزوير الذي من شأنه أن يسبب ضررا والذي يتم بأي وسيلة كانت وفي محرر أو سند للتعبير 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 . ( الرومي ، 2007: 90)

2. **تغيير الحقيقة:** يقصد بتغيير الحقيقة هو إبدالها بما يغايرها، وبالتالي فلا يعد 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 . ( طعباش ، 2013 : 63)

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 وفقا للنص القانوني لا يتم إلا في حال حدوث التزوير في المعلومات الخارجة من النظام المعلوماتي . ( براهيمي،2015 : 205)

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 . ( الرومي ، 2007 : 94)

**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 أركان الجريمة كافة، كما قد لا يتحقق القصد الجنائي إذا كان الفعل الذي يقوم به الجاني غير واضح بصورة صريحة 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 . (عبد اللطيف ،2012 : 49)

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 . ( براهيمي ، 2015 : 266)

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 . ( يوسف ، 2013 : 120)

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 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.

## 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،

**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 . ( الشوابكة ، 2007: 220) وهنا الإتلاف يشمل مختلف الوثائق قد 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 تعد منقولات المواشي التي يعدها القانون المدني عقارات بالتخصيص، كذلك محاصيل مزرعة والتي يرد عليها الإتلاف على هذه الأشياء كمحل للجريمة . (الرومي ، 2007 : 90 ـ 91 )

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 . (المصدر السابق :92)

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 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 .(الشوابكة ، 2007: 224)

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 . ( براهيمي،2015:62)

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

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 . (الرومي ، 2007: 102)

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.

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 . ( بركات، 2009: 27)

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

**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 السرقة الإلكترونية على أنها: استخدام الوسائط الحاسوبية وشبكات الإنترنت لأخذ مال متقوم مملوك للغير، خفية، من حرز صاحبه . (الشوابكة ، 2007 : 230)

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 بناءً 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 . ( بركات ، 2009 : 34)

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 الآخر الشخصي فهو نية الجاني في تملك الشئ وحيازته، حيث عند تشغيل الحاسب الآلي والحصول على معلومات أو البيانات يكون قد اختلسها واستحوذ عليها بطريق غير مشروع . (عبد اللطيف ، 2012 : 35) 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. (الشوابكة ، 2007 : 156)

أما الرأي المعارض فقد رأى عدم وجود إمكانية وقوع جريمة السرقة المعلوماتية، لارتباط فعل الاختلاس بالمحل المادي للاختلاس في السرقة. ( الرومي ، 2007 : 103) 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 . ( بركات ، 2009 : 40)

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 . (الشوابكة ، 2007 : 158) 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 ممغنط يحتوي على برامج معلوماتية واختلسه من صاحبه، ثم قام بتشغيله لمعرفة محتواه ثم رده فإن إرادة الاختلاس، تنتفي لديه ويختلف القصد العام عنده . ( عبد اللطيف ، 2012 : 58 )

**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"[1]. وتعرف خيانة الأمانة على أنها استيلاء الأمين عمداً على الحيازة الكاملة لمال سلم إليه بمقتضى سند من سندات الأمانة التي نص عليها القانون . ( القهوجي ، 1999: 365)

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.

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 غير المادية 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 . ( بركات ، 2009: 45)

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.( القهوجي ، 1999: 391)

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

---

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

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 العقوبتين.

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 اليسيرة 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 غير المشروع، إما محو أو تغير في المعطيات الموجودة في النظام أو التخريب لنظام اشتغال المنظومة.( قشقوش ، 2012 : 92) وسنتناول بيان ذلك في الفرعين الآتيين:-

## 1. الركن المادي للجريمة الدخول أو البقاء الغير مشروع في النظام.

عالج المشرع الأردني جريمة الدخول والبقاء غير المشروع 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 غير المشروع متى كان مسموحا للجاني بالدخول لجزء معين في البرنامج حيث تجاوزه إلى جزء آخر غير مسموح له بالدخول فيه . ( حجازي ، 2007 : 31)

ويلاحظ الباحث أن المشرع الأردني يعاقب بمجرد الدخول أو البقاء غير المشروع 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.

**ثانيا: فعل البقاء:** يعرف البقاء غير المشروع بأنه التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له لحق في السيطرة على هذا النظام . ( قشقوش، 2012: 92) 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 . (طعباش ، 2013: 78)

## 2. الركن المعنوي لجريمة الدخول أو البقاء غير المشروع داخل النظام

المقصود بالركن المعنوي أن يكون المتهم على علم بالدخول أو البقاء غير القانوني 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 .(قشقوش، 2013 : 109)

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

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 . ( حجازي ، 2007: 110)

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.

## 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:-

### 1. 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 . (عبد الغني ،2015: 7)

## 2. 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 .( الشوابكة ، 2007 : 91)

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 .( قشقوش، 2012 : 111)

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 .

## الجرائم المنصوص عليها في قانون المعاملات الإلكترونية

## "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 .

### جرائم التوقيع الالكتروني

نصت عليها المواد (24-26) من قانون المعاملات الإلكترونية 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".

## 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 الإلكترونية وغيرها، وإنما تتم الملاحقة والعقاب على وفق القواعد العامة، وذلك على عكس ما ورد في التشريعات الأخرى كالأردني، الذي تناول هذه الجرائم الماسة بالمستند الالكتروني في قانون الجرائم الإلكترونية 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 الإلكترونية الأردني رقم 15 لسنة 2015، المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

4. إن البعد الإجرائي للجرائم المعلوماتية، ينطوي على تحديات ومشكلات جمة، عناوينها الرئيسة الحاجة إلى سرعة الكشف خشية ضياع الدليل، وقانونية وحجية الأدلة المستقاة من بيئة معلوماتية، وهذه المشكلات كانت وما 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 توافر 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.

## ثالثاً: التوصيات

1. نتمنى أن ينظم المشرع العراقي حماية جنائية موضوعية كافية للمستند الإلكتروني، من خلال النص على الجرائم الواقعة عليه والتي تتلاءم مع الطبيعة غير المادية 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.

**المراجع:**

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

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

3 . بن خليفة، إلهام (2016). **الحماية الجنائية للمحررات الإلكترونية من التزوير**، أطروحة دكتوراه، جامعة الحاج لخضر، باتنة، الجزائر.

4. الرومي، محمد أمين (2007). **المستند الإلكتروني**، ط1، الإسكندرية: دار الفكر الجامعي.

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

6 .السقا، إيهاب فوزي (2002). **جريمة التزوير في المحررات الإلكترونية**، الإسكندرية: دار الجامعة الجديدة.

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

8 . الشوابكة، محمد أمين (2007). **جرائم الحاسوب والانترنت (الجريمة المعلوماتية)**، ط1، عمان: دار الثقافة للنشر والتوزيع.

9. طعباش، أمين (2013). **الحماية الجنائية للمعاملات الإلكترونية**، رسالة ماجستير، جامعة باتنة.

10. طعباش، أمين (2013). **الحماية الجنائية للمعاملات الإلكترونية**، رسالة ماجستير، جامعة باتنة، الجزائر.

11. 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.

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

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

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

15. عبيدات، لورنس محمد (2009). **إثبات المحرر الإلكتروني**، ط1، عمان: دار الثقافة للنشر والتوزيع.

16. قشقوش، هدى حامد (2012). **جرائم الحاسب الإلكتروني في التشريع المقارن**، القاهرة: دار النهضة العربية.

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

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

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

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