جامعة دمشق

كلية الحقوق

# الحماية الجزائية للتعاقد بالوسائل الإلكترونية

رسالة أُعدت لنيل درجة الماجستير في القانون الجزائي

إعداد الطالب

**مروان جمال الدّين الطالب**

إشراف الدكتور

**حسام الدّين ساريج**

المدرّس في قسم القانون الجزائي

2017 /1438

**لا يَزَالُ الْمَرْءُ عَالِمًا مَا طَلَبَ الْعِلْمَ**

**فَإِذَا ظَنَّ أَنَّهُ عَلِمَ، فَقَدْ جَهِل**

**ابن المبارك**

# الإهداء

إلى رجالٍ صدقوا ما عاهدوا الله عليه

شهداء الحق ورجال الله الصادقين

إلى من حارَ في وصفهم اليراع وجفّت دواتي

إلى من كان دعاؤهم سر نجاحي وحنانهم بلسم جراحي

أصحاب الهيبة والوقار

أبي وأمي

إلى النجوم المضيئة في سمائي

إلى رياحين الحياة وأشقاء الروح

أخوتي وأخواتي

إلى قناديل الذكريات

إلى رفاق الأحلام والأمنيات

أصدقائي

إلى آلاء ربي وأنوار دربي

خطيبتي

# كلمة شكر

بعباراتِ شكرٍ خجولة يُغلفها الحب والاحترام والتقدير أتوجه إلى أعضاء لجنة الحكم الموقّرة، وقد ازدَدتُ فخراً بقبولهم رئاسة وعضوية هذه اللجنة رغم ضيق الوقت وثِقل المهام.....

الأستاذ الدكتور عبد الجبّار الحنيص رئيس اللجنة

الدكتور يوسف الرفاعي عضواً

الدكتور حسام الدّين ساريج عضواً مُشرفاً

وتمتد عبارات الشكر هذه إلى هامات شامخة ومدارس في علم القانون، إلى أساتذتي في كلية الحقوق عامة وقسم القانون الجزائي خاصة.

# مخطط البحث

المقدمة:

الفصل الأول: مدى صلاحية قانون العقوبات لحماية التعاقد الإلكتروني

المبحث الأول: محل الحماية

المطلب الأول: مفهوم العقد الإلكتروني

المطلب الثاني: تكوين العقد الإلكتروني

المبحث الثاني: تزوير العقد الإلكتروني

المطلب الأول: مدى تحقق أركان التزوير التقليدي في التزوير المعلوماتي

المطلب الثاني: مدى إمكانية تحقق التزوير المعلوماتي بالطرق التقليدية

الفصل الثاني: مدى كفاية التشريعات الجزائية الخاصة في حماية التعاقد الإلكتروني

المبحث الأول: مدى شمول الاعتداءات التقليدية بالتشريعات الجزائية الخاصة

المطلب الأول: مدى كفاية النص الاحتياطي في حماية العقد الإلكتروني

المطلب الثاني: مدى كفاية الحماية الخاصة بالتوقيع الإلكتروني

المبحث الثاني: مدى إحاطة المشرع بصور الاعتداءات المستحدثة

المطلب الأول: صور الاعتداءات الواقعة على وثيقة العقد الإلكتروني

المطلب الثاني: الاعتداءات المتعلقة بالتوقيع الإلكتروني

الخاتمة:

**مقدمة:**

ثورة بلا حدود، هو الوصف الحقيقي للثورة التي حدثت في قطاعي الاتصالات والمعلومات، كيف لا وقد غيّرت مسار حياتنا بشكل كبير جداً بما أفرزته من تقنيات حديثة، وسمت بالافتراضي العالم الذي نعيشه اليوم.

في هذا العالم الافتراضي أُزيلت الحدود، وقرُبت المسافات، وقُلصت الجهود، فالمعاملات التي كانت تحتاج أياماً وربما أسابيع لإنجازها أصبحت اليوم تُنجز في غضون دقائق، حتى لو كانت تفصل بين المتعاملين آلاف الكيلومترات.

ولا شك أن التعاقد الإلكتروني ثمرة من ثمار هذه الثورة، وترجمة واقعية وعملية لمفاهيم السهولة والسرعة التي أفرزتها وخاصة في المجال التجاري، والذي تتجلى فيه أهمية التعاقد الإلكتروني في كونه الوسيلة لتحقيق التجارة الدولية أهدافها، إذ ومن خلاله يمكن إنجاز المعاملات، وإبرام الصفقات التي تقتضيها فكرة التجارة الإلكترونية بكل يُسر وسهولة. ولا عجب في ذلك مادام الطابع الغالب على التعاقد الإلكتروني أنه تجاري استهلاكي، نعم استهلاكي إذ وبعد ظهور الأسواق الإلكترونية على شبكة الإنترنت أصبح بإمكان المستهلك التسوق وهو في منزله، لا يكلفه ذلك من الجهد والوقت سوى بضع دقائق ليدخل فيها ومن خلال جهازه الحاسوبي – كمبيوتر أو

غيره- إلى المتجر الإلكتروني من خلال موقع الأخير على شبكة الانترنت ويتعاقد على شراء ما يحتاج.

ولو تساءلنا عن طريقة تسليم ما تم شراؤه إلكترونياً، يمكننا القول إن التسليم يكون إلكترونياً فيما إذا كان المنتج كذلك، كأن يكون برنامجاً حاسوبياً، أو يكون التسليم تقليدياً فيما لو كان المنتج مادياً.

ولا تتوقف عند المستهلك والتجارة الإلكترونية صلات التعاقد الإلكتروني، بل تمتد أيضاً لتشمل التوقيع الإلكتروني، هذا الشكل الجديد من التوقيع الذي فرضته طبيعة التعاقد الإلكتروني، إذ عن طريقه يتم توثيق العقود والاتفاقات التجارية إلى جانب تحديد هوية المرسل والمستقبل والتأكد من صحة وصدق المعلومات العقدية.

إلا أن هذه التكنولوجيا ومهما قيل فيها تبقى سلاحاً ذا حدين. فمثلما ساهمت في إنجاز العقود وغيرها من المعاملات بشكل سريع وموثوق به أياً كان مكان المتعاملين، كانت أيضاً وسائل بالغة الخطورة والفاعلية استغلها العديد من الجناة في ارتكاب جرائمهم بطريق التزوير أو الإتلاف أو المساس بخصوصية هؤلاء المتعاملين، الأمر الذي يجعل من الضرورة بمكان تأمين الحماية الجزائية للتعاقد الإلكتروني، وذلك لترسيخ مبادئ الثقة والأمان والاستقرار في هذا الأسلوب الجديد من التعاقد.

**إشكالية البحث:**

تتبلور إشكالية البحث بتساؤلين رئيسيين: أما الأول فيتمحور حول مدى صلاحية النصوص الجزائية التقليدية في تأمين الحماية للتعاقد الإلكتروني؟ في حين يبدأ الثاني من حيث ينتهي نظيره الأول فيما لو كان جوابه بالإيجاب، فهل تحقق حينئذ النصوص التقليدية الحماية الشاملة للتعاقد الإلكتروني؟ وإن كان الجواب بالسلب، فما مدى كفاية النصوص الخاصة – إن وجدت– في تأمين هذه الحماية؟

**صعوبات البحث:**

تكمن صعوبات هذا البحث في أمرين رئيسيين هما:

١. انعدام المراجع القانونية السورية المتخصصة، وشح المراجع العربية ذات الصلة نظراً لحداثة الموضوع.

٢. موضوع البحث من المواضيع المركبة، فهو جزائي تكنولوجي لا تكفي فيه المعرفة القانونية، بل لابد أن تتوفر لدى الباحث المعرفة التكنولوجية أيضا حتى يستطيع الإحاطة بجوانب البحث كافة.

**أهداف البحث:**

تتلخص أهداف البحث في الرغبة بإيجاد نواة لتطوير النصوص القانونية المتعلقة

بالتعاقد الإلكتروني بما يكفل تأمين حماية جزائية شاملة لهذا الأسلوب الجديد من التعاقد.

**أهمية البحث:**

تتلخص أهمية هذا البحث في الرغبة بتزويد المكتبة السورية على وجه الخصوص، والعربية عموماً ببحث يبين مقومات الحماية الجزائية للتعاقد الإلكتروني في ضوء افتقار هاتين المكتبتين لمثل هكذا أبحاث متخصصة.

**منهج البحث:**

سيتم بحث هذا الموضوع وفقا للمنهجين التحليلي والتأصيلي، حيث في الأول نتناول بالتحليل النصوص القانونية ذات الصلة وإبداء الرأي حولها، فيما نرد من خلال الثاني كل رأي فقهي إلى أصحابه، وذلك عند استعراض الخلافات الفقهية حول عدد من المواضيع ذات الصلة.

**خطة البحث:**

ستتم مناقشة موضوع البحث من خلال فصلين رئيسيين:

الفصل الأول: مدى صلاحية قانون العقوبات لحماية التعاقد الإلكتروني

الفصل الثاني: مدى كفاية التشريعات الجزائية الخاصة في حماية التعاقد الإلكتروني

# الفصل الأول

## مدى صلاحية قانون العقوبات لحماية التعاقد الإلكتروني

من المعروف أن التشريع الجزائي يقوم على مبادئ أساسية عدة، يكاد مبدأ الشرعية يكون الأهم من بينها، إذ يكفل هذا المبدأ منع القاضي من تجريم فعل أو فرض عقوبة ما، لم ينص عليها القانون.

ولكن في الوقت نفسه يؤدي مبدأ الشرعية إلى خروج الكثير من الأفعال من نطاق التجريم والعقاب، مما يؤدي إلى إفلات مرتكبيها من العقاب لعدم وجود نصوص تُجّرم أفعالهم على الرغم من أنهم قد يكونون أشخاصاً على درجة عالية من الخطورة.

ولما كان التعاقد الإلكتروني واحداً من أهم ثمار ثورة الاتصالات والمعلومات، فإنه من الطبيعي أن يكون عرضة لاعتداءات قد تنال من صحته أو سلامته.

إلا أن إسباغ وصف الجريمة من عدمه على هذه الاعتداءات يعود إلى موقف المشرع خصوصاً أن هذه الاعتداءات واقعة على محل غير مادي، الأمر الذي جعلها تتميز في نواحٍ كثيرة عن نظيراتها الواقعة على محل مادي، وبالتالي نحن أمام مفاهيم عدة وجميعها يتصف بالحداثة، ولا بد لنا من إزالة الضبابية عنها وصولاً إلى تقرير الحماية الجزائية

للتعاقد الإلكتروني.

ومن الطبيعي برأينا القول إن إقرار الحماية الجزائية للتعاقد الإلكتروني لا يمكن أن يتم إلا من خلال إقرار الحماية الجزائية للعقد الإلكتروني ولرسائل الايجاب والقبول التي يتم تبادلها إلكترونياً قبيل ابرام العقد، ولهذه الغاية آثرنا تقسيم هذا الفصل إلى مبحثين نناقش في الأول منهما مفهوم العقد الإلكتروني كمحل للحماية الجزائية، ثم نستعرض في المبحث الثاني جريمة التزوير– كأبرز الاعتداءات التقليدية الواقعة على المحررات – في حال كان العقد الإلكتروني محلاً للاعتداء، في حين نُرجئ إلى جانب من الفصل الثاني البحث عن الحماية الجزائية لرسائل الإيجاب والقبول الإلكترونية.

## المبحث الأول

## محل الحماية (العقد الإلكتروني)

لما كان العقد الإلكتروني مولوداً جديداً تحيط الضبابية مفهومه لدى الكثير من الأفراد، كان لا بد لنا، كخطوة أساسية في طريق البحث عن حماية جزائية له، من توضيح مفهومه بما يكفل إزالة الضبابية عنه، وهذا ما سنعمل عليه في هذا المبحث والذي خصصنا المطلب الأول منه لبيان مفهوم العقد الإلكتروني، في حين خصصنا المطلب الثاني للبحث في إبرام العقد الإلكتروني.

## المطلب الأول

## مفهوم العقد الإلكتروني

ما إن ظهر مفهوم التجارة الإلكترونية كنتيجة طبيعية للتطور التكنولوجي الذي أحدثته الثورة المعلوماتية في قطاعي الاتصالات والمعلومات، وما نجم عنه من ظهور لشبكة الإنترنت وغيرها من وسائل الاتصال الحديثة، حتى أصبحت العقود التجارية تُبرم إلكترونياً من خلال وسائل الاتصال هذه، ما يعني أن العقد الإلكتروني هو حجر الزاوية في تكوين مفهوم التجارة الإلكترونية.

وفي سبيل توضيح مفهوم العقد الإلكتروني خصصنا الفرعين التاليين، حيث نبين في الأول منهما ماهية العقد الإلكتروني، وفي الثاني نسلط الضوء على أبرز وسائط التعاقد الإلكتروني.

**الفرع الأول: ماهية العقد الإلكتروني**

بما أن العقد الإلكتروني يختلف عن العقد التقليدي من حيث عدم توافر مجلس عقد واحد يجمع المتعاقدين، كان لا بد لنا من تعريف هذا العقد وبيان أهم خصائصه.

**أولاً: تعريف العقد الإلكتروني**

للعقد الإلكتروني تعريفات كثيرة منها ما هو قانوني ومنها ما هو فقهي وفيما يلي توضيح ذلك:

١- التعريفات القانونية للعقد الإلكتروني:

وردت في العقد الإلكتروني تعريفات قانونية عديدة، وذلك في إطار مواكبة التشريع للتطور التكنولوجي الحاصل في قطاعي الاتصالات والمعلومات، ومن هذه التعريفات نذكر ما جاء فيالمادة الثانية من قانون المعاملات الإلكترونية الأردني رقم ٨٥ لعام ٢٠٠١، وفي نصها:

"العقد الإلكتروني هو "الاتفاق الذي يتم انعقاده بوسائل إلكترونية كلياً أو جزئياً".

أما قانون المعاملات الإلكترونية السوري رقم ٣ لعام ٢٠١٤ فقد عرف العقد الإلكتروني في المادة الأولى منه بما يلي:

"العقد الالكتروني.. اتفاق بين طرفين أو أكثر يجري انعقاده أو تنفيذه كلياً أو جزئياً بوسائل إلكترونية".

وهذا التعريف يبين أن المشرع السوري أقر الصفة الإلكترونية للعقد سواء تم إبرامه أو تنفيذه إلكترونياً، وهذا محل انتقاد برأينا، لأن العقد يكون إلكترونياً بوسيلة إبرامه لا بآليه تنفيذه، وبالتالي إذا أُبرم العقد بشكل ورقي ونُفذ إلكترونياً بشكل جزئي أو كلي فإنه يبقى عقداً ورقياً.

وهذا ما يقودنا إلى القول إن وسيط التعاقد الإلكتروني هو حجر الزاوية في هذا العقد، وهو السمة الأبرز فيه والتي تميزه عن العقد الورقي.

٢- التعريفات الفقهية للعقد الإلكتروني:

جاء في العقد الإلكتروني تعريفات فقهية كثيرة، نذكر منها أن العقد الإلكتروني هو "عقد يتحقق بإيجاب وقبول مثل العقود الورقية التي تُبرم وتُوقع كتابة، غير أن الإيجاب والقبول يتحقق بوسيلة إلكترونية دون حاجة إلى مستند مكتوب "، وهناك من

---

[١] د. أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، دراسة مقارنة، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، دبي، الفترة ما بين ١٠-١٢ مايو،٢٠٠٣، المجلد الثاني، ص٥٢٠، بحث منشور على الرابط التالي:
http://slconf.uaeu.ac.ae/prev_conf/2003/2.pdf

يتبع..

يُعرّف العقد الإلكتروني بأنه " اتفاق يُبرم ويُنفذ جزئياً و كلياً عبر شبكة اتصالات دولية باستخدام التبادل الإلكتروني للبيانات، بقصد إنشاء التزامات تعاقدية، وذلك بإيجاب وقبول يمكن التعبير عنهما من خلال ذات الوسيط ".

ويُعرّف العقد الإلكتروني لدى البعض أيضاً من خلال تعريف التجارة الإلكترونية، والمقصود بالأخيرة لديهم أنها "جميع المعاملات التي تتم عبر الإنترنت حتى ولو لم تتمتع بالصفة التجارية، وإن كان الغالب أنها تتمتع بالصفة التجارية من جانب مقدم الخدمة على الأقل، والذي غالبا ما يكون تاجراً"، ولكن يؤخذ على هذا التعريف أنه يحصر العقد الإلكتروني بالمعاملات التي تتم عبر الإنترنت دون غيره من وسائل الاتصال الحديثة القائمة، أو ما يمكن أن تفرزه تكنولوجيا المعلومات مستقبلاً .

وبالتالي يمكن القول إنه وعلى الرغم من تعدد التعريفات الفقهية للعقد الإلكتروني إلا أن جميعها يتفق – حسبما يرى البعض ونحن نؤيده – في أن "العقد الإلكتروني هو

---

تاريخ الزيارة:٢٠١٤/٥/٢٥، الساعة ٤,٠٠ مساءً.

[١] أ. رحيمة الصغير ساعد نمديلي، العقد الإداري الإلكتروني، دراسة تحليلية مقارنة، دار الجامعة الجديدة، ٢٠٠٧، ص٤٥.

[٢] د. لورانس محمد عبيدات، إثبات المحرر الإلكتروني، دار الثقافة للنشر والتوزيع، ط١، عمان، ٢٠٠٥، ص٢٥

[٣] د. إيهاب فوزي السقّا، جريمة التزوير في المحررات الإلكترونية، دار الفكر العربي، ٢٠٠٨، ص٣٦.

اتفاق بين طرفين أو أكثر عبر الوسائل الإلكترونية".

وعلى هذا الأساس يمكننا تعريف العقد الإلكتروني: بأنه اتفاق يتم إبرامه باستخدام الوسائل الإلكترونية.

**ثانياً: خصائص العقد الإلكتروني:**

للعقد الإلكتروني مجموعة من الخصائص ساهمت في جعله أسلوباً متطوراً في التعاقد عن بعد، ويمكن أن نجمل هذه الخصائص بما يلي :

١- انعدام التعاصر المادي بين طرفي العقد:

لما كان العقد الإلكتروني منتمياً إلى طائفة العقود المبرمة عن بعد، كان من الطبيعي ألا يجمع طرفيه مجلس عقد واحد – على الأقل من حيث المكان –ولوقلنا بغير ذلك لما كنا أمام عقد مبرم عن بعد.

بمعنى آخر يمكننا القول إن طرفي العلاقة في العقد الإلكتروني يجمعهما مجلس عقد

---

[١] للتوسع في هذه الخصائص وغيرها راجع كل من: فراس محمد وليد عدي، إبرام العقد بالوسائط الإلكترونية، المشرف: د. أيمن أبو العيال، المشرف المشارك: د. عمار غزال، رسالة دكتوراه، جامعة دمشق، ٢٠١٠، ص٥٥، د. خالد ممدوح ابراهيم، التوقيع الإلكتروني، الدار الجامعية، ٢٠١٠، ص٣٣٧وما بعدها، د. أسامة أحمد بدر، حماية المستهلك في التعاقد الإلكتروني، دراسة مقارنة، دار النهضة العربية، ٢٠٠٥، ص٢١، أ. رحيمة الصغير ساعد نمديلي، المرجع السابق، ص٤٥.

واحد من حيث الزمان وذلك على أبعد تقدير، وقد لا يتحقق ذلك فنكون عندها أمام مجلس عقد متفرق من حيث الزمان والمكان.

٢- العقد الإلكتروني عقد غير مادي:

أي أنه لا يتمتع بكيان مادي ملموس فيما لو قُورن بالعقد التقليدي المكتوب على الورق مثلاً، ولا يُؤثر في ذلك كون العقد الإلكتروني يُحفظ على دعامة مادية لتمكين الشخص من الاطلاع على العقد من خلال الوسائل الخاصة بذلك كلما دعت الحاجة. ومثال هذا الوعاء المادي أقراص التخزين المضغوطة أو المرنة.

٣- العقد الإلكتروني عقد أسلوبي: بمعنى أنه ليس عقداً مسمى كعقد البيع أو غيره مثلاً، وإنما هو أسلوب أو طريقة للتعاقد يكون الوسيط فيها إلكترونياً، أو هو وعاء أو قالب للتعاقد يمكن أن ينصب فيه أي عقد من العقود كالبيع أو الإيجار أو غيرها.

٤- العقد الإلكتروني غالباً ذو طابع دولي: بما أن أغلب العقود الإلكترونية تتم من خلال شبكة المعلومات الدولية(الانترنت) فهي تتصف غالباً بالطابع الدولي.

٥- العقد الإلكتروني لا يبرم إلا بوسيط إلكتروني:

تكاد تكون هذه الخاصية هي أهم ما يميز العقد الإلكتروني عن العقد التقليدي، فالوسيط الإلكتروني هو الأساس في إبرام هذا العقد بحيث لا يخلو أي تعريف للعقد

الإلكتروني من التطرق لهذا الوسيط.

وهنا تجدر الإشارة إلى أن العقد الإلكتروني – وفيما عدا هذه الخصائص – لا يختلف عن العقد التقليدي سواء من حيث محله، أو أطرافه، أو خضوعه لأحكام النظرية العامة للعقد.

ونحن إذ نتحدث عن الوسيط الإلكتروني في إبرام العقد لا بد لنا أن نستعرض أهم تطبيقاته وذلك فيما يلي:

**الفرع الثاني: وسائط التعاقد الإلكتروني**

إن التطور الهائل الذي أحدثته الثورة المعلوماتية في مجال الاتصالات والمعلومات هو ما جعلنا اليوم نتواصل مع بعضنا وكأننا في مكان واحد، حتى ولو كانت تفصل بيننا آلاف الكيلومترات، ولا شك أن شبكة الإنترنت أو ما يعرف بالشبكة العنكبوتية تحتل المرتبة الأولى والأهم بين وسائل الاتصال الحديثة، والتي يكاد يكون العالم برمته مديناً لها لما تقدمه لنا من خدمات مذهلة بسرعة كبرى و بجهود أقل من صغرى .

ولا شك أيضاً أن الإنترنت يُمثل اليوم ظاهرة عالمية تركت تأثيراً كبيراً في كافة مجالات الحياة وعلى الأخص المجال التجاري، وأبرز ما يدلل على ذلك هو ازدياد حجم التعاقد باستخدام الإنترنت .[٢]

وينبغي ألا ننسى أن شبكة الإنترنت أصبحت اليوم تقدم خدمات كثيرة تعد بحد ذاتها وسائط إلكترونية يمكن استخدامها في التعاقد، والتي ما كان لها أن ترى النور لولا وجود شبكة الإنترنت، وأبرز هذه الخدمات خدمة التصفح عبر الويب، والبريد الإلكتروني، وهي ما سنستعرضها فيما يلي:

---

[١] فراس محمد وليد عدي، المرجع السابق، ص٦١

[٢] فراس محمد وليد عدي، المرجع السابق، ص٦٤

**أولاً: التعاقد عبر الويب**

على اعتبار أن العملية التجارية سواء أكانت بيعاً أم شراءً أم.. الخ لم تعد محصورة اليوم في إطار السوق التقليدية، ومن أجل السير بشكل متوازٍ مع التطور الهائل الحاصل في قطاعي الاتصالات والمعلومات، فقد أصبح الويب يمثل سوقاً تجارية إلكترونية تضم أعداداً هائلة من المحال التجارية الإلكترونية الممثلة في المواقع الإلكترونية.

ويكاد لا يخفى على أحد – خصوصاً في هذا العصر– أن هذه المواقع الإلكترونية تُنشأ عن طريق الاشتراك في خدمة إنشاء صفحة خاصة بالعميل، أو مقدم الخدمة حيث يعرض الأخير في موقعه الإلكتروني ما يشاء من السلع والخدمات مزودة بصور ثلاثية الأبعاد، وأحياناً بمقاطع فيديو تُظهر السلعة وهي تعمل للاطلاع على أدائها ومميزاتها بشكل عملي ، وإلى جانب ذلك يقوم مقدم الخدمة بإعداد عقد[١] مطبوع يتضمن كافة شروط التعاقد– التي تختلف سعةً وضيقاً حسب نوع العملية التجارية ال مقصودة — ويضع في آخر العقد أيقونة للقبول، حيث يقوم المتعاقد الآخر(القابل) بالضغط عليها في حال قبل بالشروط المنصوص عليها في العقد.

---

[١] د. سامح عبد الواحد التهامي، التعاقد عبر الإنترنت، دار الكتب القانونية، مصر، ٢٠٠٨، ص٩١

إذاً ومن خلال خدمة الويب يستطيع مقدم الخدمة ترويج بضاعته ليتمكن من الاطلاع عليها كل من يرغب بذلك، دون أن يكلفه الأمر سوى أن يكون مشتركاً بخدمة الإنترنت، بل وأكثر من ذلك دون أن يحتاج لكلمة مرور "password"إذ أن أغلب هذه المواقع الإلكترونية ذات صفة عامة أي مباحة للجمهور، تماماً كما هو الحال في المحال التجارية التقليدية.

**ثانياً: التعاقد عبر البريد الإلكتروني**

بدايةً لا بد من القول إن البريد الإلكتروني- حسب معرفتنا- هو النسخة المحدَّثة والمطوَّرة من البريد العادي، وهو أسلوب سهل وبسيط في إرسال واستقبال الرسائل الإلكترونية سواء تضمنت نصوصاً مكتوبة أم صوراً أم مقاطع فيديو، ويتم إنشاء صندوق البريد الإلكتروني وفق خطوات معينة تكاد تكون معروفة لدى أغلب مستخدمي الإنترنت، ويكون لهذا البريد عنواناً خاصاً به يميزه عن غيره وكلمة سر لا يعرفها إلا صاحب هذا البريد، والتي من خلالها يستطيع أن يطلع على ما ورد إلى بريده من رسائل.

ومن الجدير بالذكر أن التعاقد عبر البريد الإلكتروني يتميز عن التعاقد عبر الويب بعدة نقاط، أهمها أنه يوفر للشركات وسيط اتصال خارجي تتمكن من خلاله من وضع

منتجاتها وما لديها من عروض بين أيدي الزبائن، وهذا مالا يتوافر باستخدام مواقع الويب التي تعتمد على زيارة الزبون للموقع ،كما أن البريد الإلكتروني يُمكّن الزبون من الحصول على معلومات إضافية عن المنتج أو الخدمات التي تقدمها الشركة، وذلك من خلال إرسال رسالة إلكترونية إلى البريد الإلكتروني الخاص بالتاجر أو الشركة متضمنة الاستفسار، ليقوم الأخير – التاجر أو الشركة– بالرد على استفسار الزبون وذلك برسالة إلكترونية يرسلها إلى البريد الإلكتروني الخاص بالزبون .

وإذا تلاقت ارادة الأطراف على التعاقد من خلال البريد الإلكتروني، فإن ذلك يتم من ارسال الموجب للقابل عبر بريده الإلكتروني وثيقة عقد موقعة منه، ليقوم القابل حال استلامها بطباعتها وتوقيعها ومن ثم اعادة تحميلها كصورة من خلال جهاز الماسح الضوئي وارسالها للموجب عبر بريده الإلكتروني.

وفي سياق الحديث عن الوسيط الإلكتروني في التعاقد لا بد لنا من معرفة ما إذا كان هذا الوسيط يلعب دوراً في تغيير التكوين القانوني للعقد، أو يُوجب إخضاعه لأحكام خاصة خارج النظرية العامة للعقود.

---

[1] فراس محمد وليد عدي، المرجع السابق، ص٦٥

## المطلب الثاني

## تكوين العقد الإلكتروني

لا شك أن العقد الإلكتروني لا يختلف عن العقد التقليدي من حيث تكوينه القانوني، فكلاهما يقوم على الرضا والأهلية والمحل والسبب- وهذه مقومات العقد وفق النظرية العامة للعقود – إلا أن ما يميز العقد الإلكتروني عن نظيره التقليدي[١] – كما أسلفنا- هو إبرامه باستخدام الوسائل الإلكترونية، الأمر الذي يعطي العقد الإلكتروني جانباً من الخصوصية، ولا سيما فيما يتعلق بتوثيق هذا العقد ، وهذا ما سنعمل على بيانه في الفرعين الآتيين:

### الفرع الأول: إبرام العقد الإلكتروني

قبل البحث في النصوص الخاصة عن الجوانب المتعلقة بإبرام العقد الإلكتروني، لا بد لنا أن نتعرف على مدى إمكانية إبرام العقد إلكترونياً وفق النظرية العامة للعقود.

#### أولاً: مدى إمكانية إبرام العقد إلكترونياً في إطار النظرية العامة للعقود

وفق القواعد العامة لا يبرم العقد إلا إذا توافقت إرادتان متطابقتان على إحداث أثر

---

[١] د. محمد وحيد الدين سوار، شرح القانون المدني- النظرية العامة للالتزام – ج١، جامعة دمشق، ٢٠٠٦، ص٥٥

قانوني معين .[١]

وهذا التوافق هو التطبيق العملي لمبدأ الرضائية في العقود ، هذا المبدأ الذي يعطي المتعاقد حرية التعبير عن إرادته بشكل صريح أو ضمني مالم يشترط القانون شكلاً محدداً للتعبير عن الإرادة، كما هو الحال في اشتراط الرسمية في عقد الهبة أو الكتابة في عقد الشركة .[٢]

بمعنى آخر يمكننا القول إن القواعد العامة تقضي بعدم وجود شكل أو وسيلة محددة للتعبير عن الإرادة، فالمنطق السليم يقضي بقبول التعبير عن الإرادة بوسائل إلكترونية الأمر الذي يقودنا للقول إن العقد الإلكتروني لا يخرج في إبرامه عن القواعد العامة، ولو رجعنا إلى بعض نصوص القانون المدني السوري والمصري لوجدنا أن المشرع في هذين البلدين عالج منذ القدم العقد الإلكتروني دون تسميته صراحةً بهذا الاسم،

---

[١] تنص المادة ٩٢ من القانون المدني السوري والتي تقابلها المادة ٨٩ من القانون المدني المصري على أن (يتم العقد بمجرد أن يتبادل الطرفان التعبير عن إرادتين متطابقتين، مع مراعاة ما يقرره القانون فوق ذلك من أوضاع معينة لانعقاد العقد) وتنص المادة ٨٧ من القانون المدني الأردني على أنّ (العقد هو ارتباط الإيجاب الصادر من أحد المتعاقدين بقبول الآخر وتوافقهما على وجه يثبت أثره في العقود ويترتب عليه التزام كل منهما بما وجب عليه للآخر)

[٢] المادة ١/٤٥٦ ق. م. س:"تكون الهبة بسند رسمي، وإلا وقعت باطلة مالم تتم تحت سند آخر"
المادة ١/٤٧٥ ق. م. س: "يجب أن يكون عقد الشركة مكتوباً وإلا كان باطلاً....."

ولعل أبرز ما يُدلل على ذلك في النصوص القانونية العامة ما نصت عليه المادة ٩٥ من القانون المدني السوري والتي تقابلها المادة ٩٤ من القانون المدني المصري حيث جاء في فقرتيهما الأولى(إذا صدر الإيجاب في مجلس العقد ،دون أن يعين ميعاد للقبول، فإن الموجب يتحلل من إيجابه إذا لم يصدر القبول فوراً وكذلك الحال إذا صدر الإيجاب من شخص إلى آخر **بطريق التلفون أو بأي طريق مماثل)**،وبما أن جهاز الهاتف يعد من وسائل الاتصال الحديثة وأنه بحكم النص وسيلة مقبولة في التعاقد، فمن الطبيعي أن يعد كذلك كل ما أفرزته تكنولوجيا الاتصالات والمعلومات من وسائط إلكترونية للتعبير عن الإرادة كشبكة الانترنت وما ارتبط بها من خدمات تعد بحد ذاتها وسائط للتعاقد الإلكتروني، وأبرزها كما أسلفنا سابقاً البريد الإلكتروني والتصفح عبر الويب وكل هذه الوسائل يمكن أن تندرج– حسب أحد الآراء الفقهية ونحن نؤيده– تحت عبارة "أو بأي طريق مماثل" التي جاءت في النصوص المذكورة .

والإيجاب وإن تم بوسائل إلكترونية إلا أنه لا يخرج في أحكامه ومضمونه عما نصت عليه القواعد العامة أيضاً من وجوب كونه تعبيراً جازماً عن الإرادة، يعرض فيه الموجِب على الموجَب له/لهم إبرام عقد وفق الشروط التي يحددها (أيالموجِب)، وبغير

---

[١] راجع في هذا الرأي: فراس محمد وليد عدي، المرجع السابق، ص٩٤

ذلك لا يكون هناك إيجاب وإنما دعوة للتعاقد أو التفاوض .

وأما القبول فهو التعبير الجازم والنهائي عن إرادة إبرام العقد يصدر ممن وُجّه إليه الإيجاب، والقبول لا بد أن يكون مطابقاً تماماً للإيجاب أما إذا اقترن بما يزيد أو يعدل أو يقيد في الإيجاب فإنه لا يعد قبولاً، ولا ينعقد به العقد وإنما يعد إيجاباً جديداً يحتاج لقبول من الموجِب الأول الذي أصبح مُوجَباً له .

وبما أن القبول الجازم لا يستلزم شكلاً أو وسيلة معينة، لذا فمن الممكن برأينا أن يتم بوسائل إلكترونية– مَثله في ذلك مَثل الإيجاب– ومثال ذلك أن يتم القبول الإلكتروني بالنقر على المكان الذي يخصصه الموجِب على شاشة الحاسب لإبداء القبول.

وفي معرض الحديث عن القبول يُطرح تساؤل مهم، حول ما إذا كان السكوت يُعد قبولاً أم لا؟ وهنا نقول إن السكوت مظهر سلبي من مظاهر التعبير عن الإرادة وإن كان لا يصدق على الإيجاب فهو ممكن أن يعد قبولاً ويستخلص ذلك من الظروف والملابسات، هذا إذا كان العقد تقليدياً، أما في العقد الإلكتروني فالسكوت على ما يرى البعض غير كافٍ، ولا بد من تصرف إيجابي إلكتروني يُعلن فيه الشخص الموُجِّه

---

[١] د. محمد وحيد الدين سوار، المرجع السابق، ص٧٠

[٢] د. محمد وحيد الدين سوار، المرجع السابق، ص٧٣ وما بعدها

إليه الإيجاب رغبته الحقيقية في قبوله، وبالتالي إبرام العقد إلا إذا نص القانون أو اتفق الأطراف على أن يكون السكوت دليل قبول فيما لو اقترنت به ظروف ملابسة تفيد في دلالته على الرضا .[١]

إذاً من الملاحظ أن النصوص التقليدية مكّنت ولو بشكل غير صريح من إبرام العقد بوسائل إلكترونية، إلا أن المشرع –رغبة منه في مواكبة التشريع للتطور الحاصل في وسائط التعاقد – جاء بنصوص صريحة وواضحة تجيز التعبير عن الإرادة بوسائل إلكترونية وفق ما سيتبين لنا في الأسطر القادمة.

**ثانياً: إبرام العقد الإلكتروني في إطار النصوص الخاصة**

يتجه المشرع وفي العديد من الدول إلى إصدار قوانين خاصة تنظم التعاملات الإلكترونية، فالمادة ١١ ف١ من قانون الأونسترال النموذجي الصادر عن لجنة الأمم المتحدة والخاص بالتجارة الإلكترونية رقم ٨٥ لعام ١٩٩٦نصت على أنه " في سياق تكوين العقود، وما لم يتفق الطرفان على غير ذلك، يجوز استخدام رسائل البيانات للتعبير عن العرض وقبول العرض. وعند استخدام رسالة بيانات في تكوين العقد لا

---

[١] د. خالد ممدوح إبراهيم، المرجع السابق، ص٣٦٥، وكذلك د. لورانس محمد عبيدات، المرجع السابق، ص٤٧.

يفقد ذلك العقد صحته أو قابليته للتنفيذ لمجرد استخدام رسالة بيانات لذلك الغرض" وكذلك المادة ١٣ من قانون المعاملات الإلكترونية الأردني رقم ٨٥لعام ٢٠٠١ حيث جاء فيها: " تعتبر رسالة المعلومات وسيلة من وسائل التعبير عن الإرادة المقبولة قانوناً لإبداء الإيجاب أو القبول بقصد إنشاء التزام تعاقدي".

وفي سوريا أصدر المشرع مؤخراً قانون المعاملات الإلكترونية رقم ٣ لعام ٢٠١٤، حيث عمل من خلاله على سد ما كان قائماً في التشريع من فراغ حول مفهوم العقد الإلكتروني، حيث عرّف العقد الإلكتروني في المادة الأولى منه بأنهُ: "اتفاق بين طرفين أو أكثر يجري انعقاده أو تنفيذه كلياً أو جزئياً بوسائل إلكترونية"، كما أقر بقبول الوسائل الإلكترونية كطرق للتعبير عن الارادة وذلك بصريح المادة ٤ من القانون ذاته حيث جاء فيها:"تعد الوسائل الإلكترونية طريقة مقبولة قانونا للتعبير عن الإرادة لإبداء الايجاب أو القبول بقصد إنشاء التزام أو تعديله أو نقله أو إلغائه".

ومن الملاحظ في هذا النص أن المشرع لم يستخدم مصطلح "رسالة المعلومات أو البيانات" وإنما استخدم مصطلح "الوسائل الإلكترونية" وهو مصطلح أوسع من ذاك الأول فهو من وجهة نظرنا يستوعب ما هو موجود من وسائل إلكترونية وما يمكن أن تفرزه التكنولوجيا في مراحل قادمة.

إضافةً لما سبق– وعلى غرار غالبية القوانين المقارنة ذات الصلة – فقد أفرد المشرع السوري فصلاً خاصاً لإثبات وصول الرسالة الالكترونية، وزمان ومكان العقد الالكتروني ،ليُوضح بذلك كافة الأحكام الخاصة بالعقد الإلكترونّي، والتي كان من

---

[١] من هذه القوانين نذكر قانون المعاملات الإلكترونية الأردني رقم ٨٥ لعام ٢٠٠١ في المواد (١٦-١٧-١٨) وكذلك قانون الأونسترال النموذجي بشأن التجارة الإلكترونية رقم ٨٥ لعام ١٩٩٦ في المادة (١٥).

[٢] جاء في الفصل الرابع من قانون المعاملات الإلكترونية السوري رقم ٣ لعام ٢٠١٤ ما يلي:

**الفصل الرابع**

إثبات وصول الرسالة الإلكترونية وزمان ومكان العقد الإلكتروني

المادة (٦)

أ- تعد الرسالة الإلكترونية صادرة عن المرسل ويحق للمرسل إليه أن يتصرف على أساس هذا الافتراض:

١- إذا كان المرسل هو الذي أرسلها بنفسه أو أُرسلت من شخص له صلاحية التصرف نيابة عن المرسل.

٢- إذا أرسلت من وسيط إلكتروني ينوب عن المرسل.

٣- إذا استخدم المرسل إليه نظام معلومات الكترونيا سبق أن اتفق مع المرسل على استخدامه لهذا الغرض للتحقق من أن الرسالة الالكترونية صادرة عن المرسل.

ب- لا تسري أحكام الفقرة الأولى من هذه المادة في الحالات الآتية:

١- إذا علم المرسل إليه أو كان بوسعه أن يعلم أن الرسالة الالكترونية لم تصدر عن المرسل.

٢- إذا كان هناك اتفاق بين الطرفين على غير ذلك.

المادة (٧)

أ- إذا علق المرسل أثر الرسالة الالكترونية على إبلاغه باستلامها من قبل المرسل إليه فتعامل الرسالة وكأنها لم تكن إلى حين تسلمه هذا الإبلاغ.

ب- إذا طلب المرسل من المرسل إليه بموجب الرسالة الإلكترونية إبلاغه بتسلم تلك الرسالة أو كان متفقا معه على ذلك فإن قيام المرسل إليه بإبلاغ المرسل بالوسائل الالكترونية أو بأي وسيلة أخرى أو قيامه

بأي تصرف أو إجراء يشير إلى أنه قد استلم الرسالة الالكترونية يعد استجابة لذلك الطلب أو الاتفاق هذا ما لم يتفق المرسل والمرسل اليه على كون الإبلاغ وفق شكل معين.

ج- لا يعد إبلاغ المرسل باستلام الرسالة الإلكترونية من قبل المرسل إليه دليلا على أن مضمون الرسالة التي تسلمها المرسل إليه مطابق لمضمون الرسالة الالكترونية التي أرسلها المرسل إلا إذا تضمن الإبلاغ مضمون هذه الرسالة.

المادة (٨)

أ- تعد الرسالة الالكترونية قد أُرسلت منذ وقت دخولها إلى نظام معلومات الكتروني لا يخضع لسيطرة المرسل أو من ينوب عنه.. هذا ما لم يتفق المرسل والمرسل إليه على غير ذلك.

ب- إذا كان المرسل إليه قد حدد نظام معلومات إلكترونيا لتسلم الرسائل الإلكترونية فتعد الرسالة قد تم تسلمها منذ وقت دخولها إلى ذلك النظام فإذا أُرسلت الرسالة إلى نظام غير الذي تم تحديده فيعد وقت تسلمها هو وقت اطلاع المرسل إليه عليها أول مرة.

ج- إذا لم يحدد المرسل إليه نظام معلومات إلكترونيا لتسلم الرسائل الإلكترونية فيعد وقت تسلم الرسالة هو وقت دخولها لأي نظام معلومات إلكتروني تابع للمرسل إليه حتى لو لم يطلع المرسل إليه عليها فعليا.

المادة (٩)

أ- تعد الرسالة الإلكترونية قد أُرسلت من المكان الذي يقع فيه مقر عمل المرسل وإنها استُلمت في المكان الذي يقع فيه مقر عمل المرسل إليه وإذا لم يكن لأي منهما مقر عمل فالعبرة لمكان إقامته هذا ما لم يتفق المرسل والمرسل إليه على غير ذلك.

ب- إذا كان للمرسل أو المرسل إليه أكثر من مقر عمل فيعد المقر الأكثر صلة بالمعاملة هو مكان الإرسال أو التسلم وعند تعذر الترجيح يعد مقر العمل الرئيسي هو مكان الإرسال أو التسلم وذلك مع عدم الإخلال بالأحكام الخاصة بالشخص الاعتباري.

المادة (١٠)

يعد العقد الالكتروني قد تم في المكان والزمان الذي استلم فيه القبول ما لم يتفق على غير ذلك.

المادة (١١)

ما لم يوجد اتفاق بين أطراف العقد الالكتروني على القانون الواجب التطبيق يطبق على القانون الواجب التطبيق قواعد القانون الدولي الخاص المنصوص عليها في القانون المدني.

الأفضل برأينا أن يأتي النص عليها في القانون رقم ٤ لعام ٢٠٠٩ والخاص بالتوقيع الإلكتروني وخدمات الشبكة، على اعتبار أن التوقيع الإلكتروني جزءٌ لا يتجزأ من العقد الإلكتروني، وهو أداة التوثيق فيه على ما سنرى في الفرع الآتي.

---

المادة (١٢)

تنطبق على العقود الالكترونية القواعد المتعلقة بالاختصاص الدولي العام المنصوص عليها في قانون أصول المحاكمات المدنية وتعديلاته إذا كان طرفا العقد في بلدين مختلفين اما إذا كانا في سورية فتنطبق القواعد العامة في الاختصاص.

**الفرع الثاني: توثيق العقد الإلكتروني (التوقيع الإلكتروني)**

يتمتع التوقيع التقليدي من وجهة نظرنا بأهمية كبيرة اكتسبها من قدرته على تحديد هوية الموقع ونسبة الحق أو الالتزام الموقع عليه له، إضافة إلى أنه يكسب المحرر المهور به حجية في الإثبات، ولكن مزايا التوقيع هذه لا تتبلور إلا حينما يرتبط الأخير بمحرر تقليدي.

أما اليوم و مع ظهور العقد الإلكتروني كواحد من أهم تطبيقات المحرر الإلكتروني نتيجة للتطور المذهل الذي تسير به عجلة التكنولوجيا، كان لابدّ من إيجاد وسيلة يُمكن من خلالها إعطاء العقد الإلكتروني قيمة ثبوتية من أجل حث الناس على التعامل به، و هذه القيمة في الواقع لا يمكن أن تأتي إلا من خلال التوقيع، و لكن لما كان الأخير لا يصلح من حيث طبيعته التقليدية لأن يستخدم في العقد الإلكتروني، ظهر ما يسمى بالتوقيع الإلكتروني والذي شكل إلى جانب العقد الإلكتروني كلاً متكاملاً سهّل التعامل بين الناس بطبيعته الإلكترونية، وقوته الثبوتية التي مُنحت له من قبل عدد كبير من المشرعين في العالم .[١]

ونظراً للارتباط الوثيق بين العقد الإلكتروني والتوقيع الإلكتروني، كان من الضروري

---

[١] خالد ممدوح ابراهيم، المرجع السابق، ص ١٣ وما بعدها

بمكان التعرف أكثر على التوقيع الإلكتروني من حيث تعريفه وشروطه ووظائفه وصوره وهذا ما سنبينه في الفقرات التالية:

**أولاً: تعريف التوقيع الإلكتروني**

للتوقيع الإلكتروني تعريفات كثيرة تختلف فيما بينها من حيث الأساس الذي يقوم عليه التعريف وهو إما وسيلة إعداد التوقيع أو الوظيفة التي يقوم بها، وهذه التعريفات منها ما كان قانونياً ومنها ما كان فقهياً.

١- التعريفات القانونية للتوقيع الإلكتروني:

يُعرف التوقيع الإلكتروني في م٢ف١ من قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية الصادر عام ٢٠٠١ على أنه "بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها ومرتبطة بها منطقياً، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات".

ويُعرف التوقيع الإلكتروني في م١ف(ج) من قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المصري رقم ١٥ لعام ٢٠٠٤ بأنه" ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها

ويكون له طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره".

أما قانون التوقيع الإلكتروني السوري رقم ٤ لعام ٢٠٠٩ فقد عرف التوقيع الإلكتروني في م١ بأنه:

"جملة بياناتُ تدرج بوسيلة إلكترونية على وثيقة إلكترونية وترتبط بها، وتتخذ شكل حروف أو أرقام أو رموز أو إشارات أو أي شكل آخر مشابه، ويكون لها طابع متفرّدٍ يسمح بتحديد شخص الموقِّع ويميزه عن غيره وينسب إليه وثيقة إلكترونية بعينها".

ومن خلال هذه التعريفات يمكن أن نلاحظ ما يلي:

(١) بينت هذه التعريفات بوضوح الطبيعة الإلكترونية للتوقيع الإلكتروني.

(٢) التعريفات لم تحدد صوراً حصرية للتوقيع الإلكتروني كما هو الحال في التوقيع التقليدي، وذلك لإبقاء الطريق مفتوحاً أمام صور جديدة لهذا التوقيع يمكن أن يفرزها التطور التكنولوجي.

(٣) بينت هذه التعريفات الدور الوظيفي للتوقيع الإلكتروني في تحديد هوية الموقع وتمييزه عن غيره.

٢- التعريفات الفقهية للتوقيع الإلكتروني:

من المهم بمكان القول إن الفقه وإن كان يختلف في تعريف التوقيع الإلكتروني إلا أن

خلافه هذا محصور في بيان الأسس التي يقوم عليها هذا التوقيع، والمتمثلة في تحديد وظائف التوقيع الإلكتروني وبيان كيفية إنشائه إلكترونياً، لذلك يمكن القول إن الفقه منقسم حول تعريف التوقيع الإلكتروني ضمن هذه الأسس إلى طائفتين :

**الأولى**: ركزت على إنشاء التوقيع الإلكتروني دون أي ذكر لوظائف هذا التوقيع

ونذكر من هذه التعريفات أن التوقيع الإلكتروني "كل توقيع يتم بطريقة غير تقليدية".

**الثانية**: ركزت على كيفية إنشاء التوقيع الإلكتروني كمجموعة إجراءات تقنية دون تحديد لهذه الإجراءات، مفسحةً المجال أمام ما تفرزه تكنولوجيا المعلومات من إجراءات جديدة إضافة لتركيزها على تحديد وظائف التوقيع الإلكتروني في تحديد هوية الموقِع وتأكيد التزامه بمضمون ما جاء في المحرر الموقَع، ونذكر من هذه التعريفات أن التوقيع الإلكتروني هو" مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته".

ويكاد يكون هذا التعريف من وجهة نظرنا هو الأدنى إلى المنطق والأقرب إلى الواقع العملي كونه يشمل بيان وظائف التوقيع الإلكتروني إلى جانب بيان طبيعته

---

[1] راجع في أنصار هاتين الطائفتين د. لورانس محمد عبيدات، المرجع السابق، ص١٢٧

الإلكترونية، وجديرٌ بالذكر في هذا الصدد أن تعريفات الفقه للتوقيع الإلكتروني لا تقتصر على هذين التعريفين، وإنما هناك تعريفات أخرى كثيرة، وإن كانت لا تخرج في مضمونها عما أشارت إليه التعاريف المذكورة آنفاً .

**ثانياً: الشروط الواجب توفرها في التوقيع الإلكتروني .**

حتى يكون للتوقيع الإلكتروني المرتبط بمحرر حجة في الإثبات لا بد من أن يستجمع عدداً من الشروط التي نصت عليها القوانين الخاصة بالمعاملات الإلكترونية ومنها قانون التوقيع الإلكتروني السوري رقم ٤ لعام ٢٠٠٩ حيث يلخص هذه الشروط في المادة الثالثة منه وقد جاء فيها:

"يعدّ التوقيع الإلكتروني المصدَّق، المدرج على وثيقة إلكترونية، مستجمعًا للشروط المطلوبة للحجيّة في الإثبات، وهي:

١. ارتباط التوقيع بالموّقع وحده دون غيره، وكفايته للتعريف بشخص الموقِّع.

٢. سيطرة الموّقع وحده دون غيره على منظومة إنشاء التوقيع الإلكتروني المستخدمة.

٣. ارتباط التوقيع الإلكتروني بالوثيقة الإلكترونية ارتباطًا لا يمكن بعده إحداث أي

---

[١] للتوسع في التعريفات الفقهية للتوقيع الإلكتروني راجع د. خالد ممدوح إبراهيم، المرجع السابق، ص ٥٧ وما بعدها.

[٢] راجع في هذه الشروط د. خالد ممدوح ابراهيم، المرجع السابق، ص ١٣٢ وما بعدها

تعديل أو تبديل على الوثيقة دون ظهور أثر قابل للتدقيق والكشف".

**ثالثاً: وظائف التوقيع الإلكتروني**

يمكن من وجهة نظرنا استنباط وظائف التوقيع الإلكتروني من خلال تعريفاته القانونية والفقهية، والتي سبق أن تطرقنا إليها، ويمكن أن نُلخص هذه الوظائف بما يلي:

١- تحديد هوية الموقِع: لابد أن يحدد التوقيع الإلكتروني هوية الموقع دون أي لبس لكي ينصرف إلى الموقع وحده الالتزام بما جاء في المحرر الموقع عليه.

٢- نسبة المستند للموقِع: للتوقيع عموماً دور هام في نسبة المحرر للشخص الذي وقع عليه، وما إن تثبت هذه الصلة حتى تترتب المسؤولية القانونية للموقع عن كل ما جاء في المحرر المؤقع إلى جانب التزامه بذلك.

٣- القبول بمضمون المستند الموقَّع: يدل التوقيع عموماً دلالة لا تقبل الشك على أن الموقِع قد وافق على ما جاء في المحرر الذي مهره بتوقيعه.

**رابعاً: صور التوقيع الإلكتروني**

للتوقيع الإلكتروني عدة صور نذكر أهمها فيما يلي:

1- التوقيع الرقمي: هذا الشكل من التوقيع الإلكتروني هو الأكثر شيوعاً وموثوقية وهو كما يدل اسمه ليس عبارة عن خطوط متعرجة أو غير ذلك، إنما هو عبارة عن

مجموعة من الأرقام تُحوِّل باستخدام عمليات حسابية معقدة رسالة البيانات المرتبطة بها من رسالة مقروءة إلى رسالة مشفَّرة، وعملية التشفير هذه تستلزم وجود مفتاحين الأول خاص ويوجد لدى المرسل ومن خلاله يتم تشفير الرسالة، والثاني عام يوجد لدى المرسل إليه و به يتم فك تشفير الرسالة لتعود لصورتها الأصلية المقروءة .

ومن الجدير بالذكر أن عملية التشفير هذه التي يقوم عليها التوقيع الرقمي تنطوي على مقدار كبير من الموثوقية وفيها ضمان للسرية والخصوصية في التعاملات الإلكترونية التي تتطلب ذلك .[٢]

إلا أن العيب الوحيد في هذا الشكل من التوقيع هو في حال سرقة هذه الأرقام أو معرفتها من قبل الغير والتصرف بها بطريقة غير مشروعة، خصوصاً مع ازدياد عمليات القرصنة الهادفة للوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني ونسخها وإعادة استخدامها .[٣]

---

١حنان مليكة، النظام القانوني للتوقيع الإلكتروني في ضوء قانون التوقيع الإلكتروني السوري رقم٤ لعام ٢٠٠٩، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٢٦، العدد الثاني، ٢٠١٠ص٥٦٢، وكذلك فراس محمد وليد عدي، المرجع السابق، ص٢٨٥ وما بعدها.

٢حنان مليكة، المرجع السابق، ص٥٦٢

٣ محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، رسالة ماجستير، جامعة القاهرة، ٢٠٠٤، ص٢٢٨

٢- التوقيع البيو ميتري (التوقيع بالخواص الذاتية) : يقوم هذا التوقيع في الأساس على الخواص البيولوجية المرتبطة بجسم الإنسان والتي تختص به دون غيره كنبرة صوته أو بصمة اصبعه أو الشبكية في عينه، مما يجعله يتمتع بدرجة عالية من الموثوقية التي تحفز المتعاملين على اعتماده في تعاملاتهم.

ويتجسد هذا التوقيع من خلال أخذ عينة من إحدى الخصائص البيولوجية الخاصة بالإنسان وحده، ويتم تخزينها على الحاسب بعد تشفيرها إلكترونياً ليتم مطابقتها بنظيراتها المستخدمة عند التوقيع.

3- التوقيع بالقلم الإلكتروني : هذا الشكل من التوقيع الإلكتروني يتم باستخدام قلم[٢] إلكتروني يُمكّن مستخدمه من التوقيع بشكل مباشر على شاشة الحاسب، وذلك من خلال برنامج حاسوبي يعمل على مقارنة التوقيع المستخدم بالتوقيع المخزن في بيانات المستخدم الخاصة للتأكد من تطابقهما.

وعلى الرغم من تعدد صور التوقيع الإلكتروني، فإن حمايته جزائياً تعد ضرورة أساسية لجعل الحماية الجزائية للتعاقد الإلكتروني شاملة لكل مفرداته بما فيها العقد الإلكتروني،

---

[١] حنان مليكة، المرجع السابق، ص٥٦٣

[٢] حنان مليكة، المرجع السابق، ص٥٦٤

وما قد يتعرض له من اعتداءات سنأتي على شرح أبرز صورها التقليدية في المبحث الآتي.

## المبحث الثاني

## تزوير العقد الإلكتروني

لا شك أن العقد الإلكتروني عرضة لجملة من الاعتداءات التي يمكن وصفها بالتقليدية كالسرقة والإتلاف والتزوير وغيرها.

ومما لا شك فيه أيضاً أن التزوير هو أهم وأخطر هذه الاعتداءات لما ينطوي عليه من تهديد لصحة العقد، وزعزعة لعوامل الثقة والأمان التي يُفترض أن تتوافر لدى المتعاقدين، الأمر الذي دفعنا في الواقع إلى تسليط الضوء على هذا الاعتداء بشكل خاص.

إلا أن البحث في مدى صلاحية النصوص التقليدية الخاصة بالتزوير في حماية العقد الإلكتروني يتطلب منّا بدايةً معرفة ما إذا كان هذا العقد يصلح محلاً للتزوير وفق المفهوم التقليدي أم لا. وهذا ما سنعمل على بيانه في المطلبين الآتيين.

المطلب الأول: مدى تحقق أركان التزوير التقليدي في التزوير المعلوماتي

المطلب الثاني: مدى امكانية تحقق التزوير المعلوماتي بالطرق التقليدية

## المطلب الأول

## مدى تحقق أركان التزوير التقليدي في التزوير المعلوماتي

لبيان مدى إمكانية وقوع التزوير في المجال المعلوماتي لا بد من توضيح مفهوم جريمة التزوير التقليدية وننطلق في ذلك من م ٤٤٣ ق.ع. س وقد جاء فيها:

**"التزوير هو تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط يُحتج بهما يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي".**

وكما هو واضح من النص المذكور فإن جريمة التزوير تقوم كأي جريمة أخرى على ركنين هما الركن المادي والركن المعنوي، وهذا ما سيتم بيانه في الفرعين الآتيين:

الفرع الأول: الركن المادي

الفرع الثاني: الركن المعنوي

**الفرع الأول: الركن المادي**

ينطوي الركن المادي في جريمة التزوير على ثلاثة عناصر هي:

**أولاً: تحريف الحقيقة**

بالمفهوم الجزائي يمكن القول إن تحريف الحقيقة هو تغيير أو تبديل الحقيقة فيما هو مسطور إما حذفاً أو إضافةً، وهذا بالطبع إن كان المحرر معداً مسبقاً، أو اختلاق محرر جديد منافٍ للحقيقة لم يكن موجوداً من قبل أو بتغيير الحقيقة المقصودة من إنشاء المحرر، وهذا حال من يُدون عقد بين طرفين على أنه عقد بيع وهو في الأصل عقد إيجار .[١]

وتحريف الحقيقة بهذا المفهوم لابد أن ينصب على ما هو مسطور في المحرر سواء أكان كلمات أو أرقام أو رموز أو علامات ذات دلالة معينة، وأن يكون من شأن هذا التغيير تبديل الحقيقة بما يخالفها، وعلى أساس ذلك لا يعد تحريفاً للحقيقة ولا تقوم جريمة التزوير فيما لو كتب مبلغ القرض إلى جانب رقمه أو إضافة بيانات لا تؤثر على مضمون المحرر وفحواه، كذلك الحال لا يُعد تزوير عندما يُقر شخص ما أمام

---

[١] القاضي عبد الوهاب بدرة، جرائم التزوير في التشريع السوري، الطبعة الجديدة، دمشق، بلا سنة نشر، ص١٦

موظف مختص بمعلومات يعتقد أنها غير صحيحة ويدونها الموظف في محرر خاص بها ثم يتبين أنها مطابقة للحقيقة ، وعلى هذا الأساس يُعرِّف بعض الفقه جريمة التزوير[١] بأنها "إظهار الكذب في محرر بمظهر الحقيقة وذلك غشاً لعقيدة الغير "

باختصار يمكن القول إن التزوير هو كذب ولكن من نوع خاص إذ ليس كل كذب جرماً يعاقب عليه القانون، وإن كان كذلك فليس من الضروري أن يكون تزويراً، وعلى هذا الأساس يمكن القول إن الكذب الذي تقوم به جريمة التزوير هو كذب مكتوب، من شأنه المساس بحقوق الغير والإضرار بهم مما يؤدي إلى زعزعة الثقة العامة بمصداقية المحررات التي يدون الناس فيها معاملاتهم .

أما عن طبيعة الحقيقة التي يقع التزوير بتغييرها فهي الحقيقة التي أُعدَّ المحرر من أجلها "لإثباتها" سواء أكانت حقيقة قانونية أو واقعية .

ويجب أن يكون المحرر الذي زُوِّرت فيه الحقيقة صالحاً لأن يتخذ أساساً للمطالبة بحق

---

[١]القاضي عبد الوهاب بدرة، المرجع السابق، ص١٧، وكذلك د. فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية،١٩٨٨، ص٢٤٥

[٢]د. رمسيس بهنام، الجرائم المضرة بالمصلحة العامة، منشأة المعارف بالإسكندرية، ١٩٨٦، ص١٦٢

[٣]د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، مصر ٢٠٠٢، ص١٣٧

[٤]القاضي عبد الوهاب بدرة، المرجع السابق، ص ٢٣.

ما أو اكتسابه، ولذلك فإن التاجر المفلس الذي يُقدِّم تقريراً مخالفاً لوضعه المالي لا يرتكب جرم التزوير، إذ ليس من شأن هذا التقرير أن يكون أساساً للمطالبة بحق أو اكتسابه .ومن الجدير بالذكر أن عنصر تغيير الحقيقة هو جوهر التزوير بشكل عام ويقوم به التزوير المعلوماتي مثلما يقوم به التزوير التقليدي، سوى أنه في الحالة الأولى لا بد أن ينصب على المعلومات والبيانات التي تشكل مضمون العقد الإلكتروني، وهذا ما يؤكده تعريف التزوير المعلوماتي لدى جانب من الفقه بأنه تغيير الحقيقة في المستندات المعالجة آلياً والمستندات المعلوماتية وذلك بنية استعمالها .

ولكن إذا كان هناك توافق ما بين التزوير المعلوماتي والتقليدي بالنسبة لعنصر تحريف الحقيقة، فإن المسألة ليست كذلك بالنسبة للمحرر الذي تُحرف فيه الحقيقة وفق ما سيتبين لنا فيما يلي.

**ثانياً: التحريف في محرر**

من المعلوم أن لكل جريمة محل لا يمكن أن تقوم بدونه، والمحرر هو محل جريمة التزوير

---

[1] القاضي عبد الوهاب بدرة، المرجع السابق، ص ٢٧.

[2] د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص١٣٩.

المنصوص عليها في م ٤٤٣ق.ع. س وقد أشار إليه المشرع في هذه المادة بقوله "**صك أو مخطوط يحتج بهما** ".

ويُعرف المحرر محل جريمة التزوير التقليدية حسب جانب من الفقه بأنه:"كل مكتوب يُفصح عن شخص من صدر عنه ويتضمن ذكراً لواقعة أو تعبيراً عن إرادة، ومن شأنه إنشاء مركز قانوني معين أو تعديله أو إنهاؤه أو إثباته سواء أعد المحرر لذلك أساسا" أو ترتب عليه هذا الأثر بقوة القانون" [١] .

وهناك من الفقه من يعرف المحرر بأنه: "كل مكتوب منسوب إلى شخص معين يتضمن إثباتا لوقائع أو إعلاناً عن إرادة" [٢] .

وهذه التعريفات تظهر بوضوح أن المحرر التقليدي ينطوي على مجموعة من العناصر لا يمكن له أن يقوم بدونها ويكون محلاً صالحاً للتزوير، وهذه العناصر يمكن توضيحها بما يلي : [٣]

١- شكل المحرر:

---

[١] د. عوض محمد، الجرائم المضرة بالمصلحة العامة، دار المطبوعات الجامعية، الإسكندرية، ١٩٨٥، ص١٧٤.

[٢] مأمون محمد سلامة، قانون العقوبات-القسم الخاص- ج١، الجرائم المضرة بالمصلحة العامة، دار الفكر العربي،١٩٨٢-١٩٨٣، ص٤٠٨.

[٣] القاضي عبد الوهاب بدرة، المرجع السابق، ص ٤٥ وما بعدها.

الكتابة هي الشكل الذي يتخذه المحرر محل التزوير سواء أكانت الكتابة باليد، أو بالآلة الكاتبة، أو حفراً، أو بآلة ما، وسواء اتخذت شكل كلمات أو رموز أو إشارات أو رسوم مادامت تحمل في طياتها معنىً مفهوماً ، ويستوي أن تُسطر الكتابة على الورق أو الحجر أو القماش أو المعدن أو أي محل يجعلها مستقرة الكيان، وعليه لا تعد الكتابة على الرمل محرراً .[١]

ويستوي أن يكون المحرر المزور عقداً أو خطاباً أو فاتورة أو عريضة أو غير ذلك .

2- مصدر المحرر:

لابد أن يكون للمحرر محل التزوير مصدر معروف أي لابد أن يكون معلوم الجهة التي أصدرته دون حاجة لوجود إمضاء أو توقيع أو بصمة إصبع، بل يكفي لمعرفة الجهة التي صدر عنها المحرر وجود عبارات أو رسوم في المحرر تشير بشكل لا يدع مجالاً للشك إلى الجهة التي أصدرته، وعليه لا يمكن القول بتزوير سند دين لا يعرف من هو المدين فيه، إذ في هذه الحالة لا يمكن أن ينصرف الضرر إلى جهة معينة وهذا ما يحول دون وقوع التزوير .[١]

---

[١] عفيفي كامل عفيفي، تقديم أ. د فتوح الشاذلي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، منشورات الحلبي الحقوقية، ٢٠٠٣، ص٢٤٢.

[٢] عفيفي كامل عفيفي، المرجع السابق، ص٢٤٢.

٣- مضمون المحرر:

لا بد أن يكون المحرر المزور معبراً عن فكرة معينة من خلال ما سُطر فيه من عبارات أو علامات أو رسوم ذات دلالة، وهذا ما يعنيه مصطلح الكتابة المعبِرة .

والكتابة المعبرة عن فحوى المحرر هي ما يجب أن يمسه التحريف حتى يقع التزوير، ومثال ذلك أن يتم التحريف في اسم أحد المتعاقدين أو في مواصفات المبيع أو ثمنه، أما إن وقع التزوير على ما هو مكتوب في المحرر دون أن يكون له علاقة بالفكرة التي يعبر عنها المحرر فلا يقع التزوير، ومثال ذلك تغيير اسم المطبعة التي طبعت وثيقة العقد .[٣]

٤- غاية المحرر:

لا يقوم التزوير إلا إذا كان المحرر صالحاً لأن يكون وثيقة يحتج بها في إثبات أمر ما أو نفيه، ولا يشترط لقيام التزوير أن يكون المحرر قد حُرر ليكون بالأصل حجة للإثبات أو النفي، وإنما يكفي أن يكون صالحاً لأن يكون مستقبلاً دليلاً يُحتج به في النفي أو

---

[١] القاضي عبد الوهاب بدرة، المرجع السابق، ص٤٨.

[٢] القاضي عبد الوهاب بدرة، المرجع السابق، ص٤٨.

[٣] القاضي عبد الوهاب بدرة، المرجع السابق، ص٤٩.

الإثبات .[١]

باختصار يمكن القول إنَّ المحرر بهذه المحددات هو العنصر الأساس في جريمة التزوير وفق م ٤٤٣ق.ع. س، وعليه نقول إن أي تحريف للحقيقة لا يكون محله محرراً لا تقوم به جريمة التزوير وإن كان من الممكن أن تقع به جرائم أخرى كالشهادة الكاذبة أو الاحتيال .[٢]

ولكن السؤال الذي يطرح نفسه هنا هل تنطبق عناصر المحرر هذه على العقد الإلكتروني، ويكون بالتالي محلاً صالحاً لجريمة التزوير وفق المادة ٤٤٣ق.ع. س؟

في الواقع لا يمكن للمنطق والعقل السليم أن يتصور وقوع تزوير يُستخدم فيه الحاسب الآلي ويكون محله محرراً تقليدياً لاختلاف الطبيعة ما بين محل الاعتداء ووسيلته، ولو كان الأمر غير ذلك لما أفرزت الثورة المعلوماتية شكلاً جديداً للمحرر يفتقد إلى الطبيعة المادية وهو المحرر المعلوماتي، والذي يُعرف عند جانب من الفقه بأنه كل جسم منفصل أو يمكن أن يتم فصله عن نظام المعالجة الآلية للمعلومات، وقد سُجلت عليه معلومات معينة سواء أكان معداً للاستخدام بواسطة نظام المعالجة الآلية

---

[١] القاضي عبد الوهاب بدرة، المرجع السابق، ص٤٩ وما بعدها.

[٢] القاضي عبد الوهاب بدرة، المرجع السابق، ص٥٠-٥١.

للمعلومات أم مشتقاً من هذا النوع .[١]

وإذا كان المحرر التقليدي لا يقوم إلا بتوافر مجموعة من العناصر فالمحرر المعلوماتي أيضا كذلك، ولكن إذا استرجعنا عناصر المحرر التقليدي نجد أن جزءاً منها ينطبق على المحرر المعلوماتي دون إشكال، وهذه تعتبر نقاط تشابه بين عناصر المحررين، فالمحرر لا بد أن يكون معلوم المصدر وأن تكون له غاية و قيمة ثبوتية حتى يمكن القول بوقوع التزوير عليه ، ويبقى الفارق الأكبر بين المحررين في عنصر الكتابة وهي الجوهر في كليهما، ويأتي هذا الخلاف من طبيعة المحرر المعلوماتي الذي يوجب أن تأخذ الكتابة فيه الطبيعة نفسها، وهذا ما أدى إلى ظهور ما يسمى بالكتابة الإلكترونية كنظير للكتابة التقليدية والتي تتصدر تعريفاتها أغلب القوانين الخاصة بالتعاملات الإلكترونية ، ونذكر منها تعريف المشرع السوري في المادة١ [٢]من قانون التوقيع الإلكتروني رقم ٤ لعام ٢٠٠٩، وقد جاء فيها :

---

[١] د. أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، دار النهضة العربية، القاهرة،٢٠٠٠، ص ٤٢٢.

[٢] من هذه التعريفات ما جاء في الفقرة /أ / من المادة الأولى من قانون التوقيع الإلكتروني المصري رقم ١٥ لعام ٢٠٠٤ وفي نصها:"الكتابة الإلكترونية: كل حروف أو أرقام أو رموز أو أي علامات أخرى تُثبت على دعامة إلكترونية أو رقمية أو ضوئية أو أي وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك".

**الكتابة الإلكترونية: حروف أو أرقام أو رموز أو أية علامات أخرى تثبت على حامل إلكتروني وتعطي دلالة قابلة للإدراك.**

والكتابة الإلكترونية وفق هذه التعريفات تستجمع مقومات الكتابة المعتبرة في تكوين المحررات، والمتمثلة في قابلية الاطلاع عليها وإن كان ذلك من خلال وسيط إلكتروني، وهذا أمر طبيعي بالنسبة لمحرر يفتقر للطبيعة المادية، إضافة إلى قابلية هذا النوع من الكتابة للثبات وهذا ما هو حاصلٌ بالفعل، إذ أثبتت الكتابة الإلكترونية قابليتها للثبات والاستمرار أكثر من نظيراتها التقليدية، وهذا ما حدا بالجهات الحكومية في سورية إلى التوجيه بحفظ المستندات الورقية في نسخ إلكترونية .

ويبقى من هذه المقومات وجوب أن تُعبر الكتابة الإلكترونية عن أفكار إنسانية مترابطة، وهذا ما تحققه الكتابة الإلكترونية برأينا، وإن لم تكن التعريفات المذكورة سابقاً تُعبر بشكل واضح عن ذلك، لأن العبرة في تحديد مدلول الكتابة ليس بقابليتها للإدراك وإنما لكونها تُعبر عن أفكار إنسانية مترابطة كون الحرف أو الرقم يتوفر فيه الإدراك ولا يتوفر فيه المعنى المفهوم المترابط، ومن هنا نرى أنه كان أولى بالمشرع السوري وكذلك المصري أن يستبدلا بالجزء الأخير من تعريفهما للكتابة الإلكترونية ما

[1] مثال ذلك نظام الأرشفة الإلكترونية المطبق لدى مصرف سورية المركزي.

يُوضح إمكانية الكتابة للتعبير عن أفكار إنسانية مفهومة ومترابطة، تماماً كما فعل المشرع الفرنسي حيث نص في المادة ١٣١٦ من القانون رقم ٢٣٠/٢٠٠٠ والصادر عام ٢٠٠٢ والخاص بالمبادلات والتجارة الإلكترونية على أن الكتابة تتضمن كل تدوين للحروف أو العلامات أو الأرقام أو أي إشارات أو رموز أخرى **ذات دلالة تعبيرية مفهومة للآخرين** أياً كان نوع الوسيط أو الدعامة التي تقع عليه وأياً كانت طريقة نقلها .[١]

وعلى ما سبق يمكننا القول إن اختلاف عنصر الكتابة ما بين المحرر محل المادة ٤٤٣ ق.ع.س والعقد الإلكتروني يؤدي بشكل لا يدع مجالاً للشك إلى خروج الأخير من تطبيقات المادة المذكورة- على اعتبار أن العقد الإلكتروني شكل من أشكال المحرر الإلكتروني- وهذا ما يشكل جوهر الإشكالية في هذا البحث.

**ثالثاً: إمكانية حصول ضرر**

من الناحية القانونية يُعد الضرر أحد عناصر الركن المادي في التزوير والمتمثل في النتيجة الجرمية المترتبة على السلوك الإجرامي فيه، أما من الناحية العملية فيعبر عن

[١] د. أيمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية،٢٠٠٧، ص ٢٣٨.

الضرر بنية استعمال المحرر المزور فيما زُوِّر من أجله بغض النظر عن الاستعمال الفعلي من عدمه، اذ لا تلازم بين التزوير والاستعمال الفعلي للمحرر المزوَّر، وإلى وقت ارتكاب الجريمة يعود تقدير توافر الضرر أو احتمال توافره، دون النظر إلى ما يمكن أن يطرأ بعد وقوع التزوير ويحول دون وقوع الضرر .

وتجدر الإشارة في معرض الحديث عن الضرر إلى أن المشرع السوري لم يشترط لوقوع التزوير أن يكون الضرر حالاً، وإنما اكتفى بأن يكون الضرر ممكن الوقوع وفق المجرى العادي للأمور، وهذا ما نجده واضحاً من عبارة المشرع" **يُمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي**" [٢] .

وجديرٌ بالذكر أن فكرة الضرر لا تختلف في التزوير التقليدي عنها في التزوير المعلوماتي، فالضرر الاجتماعي واحد في حال تزوير محرر رسمي سواء أكان الأخير تقليدياً أم معلوماتياً، وكذلك الحال بالنسبة للضرر المادي والمعنوي ، وفي هذا الصدد يقول الدكتور عبد الفتاح بيومي حجازي "إن الضرر في التزوير المعلوماتي، مع التسليم

---

[١] د. عبد الجبار الحنيص، الحماية الجزائية لبطاقات الائتمان الممغنطة من التزوير، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٢٤، العدد الثاني، ٢٠٠٨، ص١٥٦-١٦٢

[٢] القاضي عبد الوهاب بدرة، المرجع السابق، ص٧٧.

[٣] راجع في أنواع الضرر، د. فوزية عبد الستار، المرجع السابق، ص٢٧٧.

به، لا يمكن مناقشته بعيداً عن الضرر في النظرية العامة للتزوير في الجريمة التقليدية ".

وفي إطار استكمال دراسة جريمة التزوير لابد لنا من دراسة ركنها المعنوي وهو موضوع الفرع التالي.

[١] د. عبد الفتاح بيومي حجازي، المرجع السابق، ص٢٥٩.

**الفرع الثاني: الركن المعنوي**

إن جريمة التزوير من الجرائم المقصودة التي لا يُتصور فيها الخطأ وذلك بدليل كلمة "**مفتعل**" الواردة في المادة ٤٤٣ ق.ع.س، ولا يكفي وجود القصد العام لدى الجاني لقيام التزوير بل لابد من وجود قصد خاص يتمثل في نية الجاني استعمال المحرر المزور فيما زُور من أجله .[١]

وعليه فإن جريمة التزوير لا تقوم إلا إذا كان الجاني عالما بأنه يُحرف حقيقة ما في محرر، وأن تتجه إرادته إلى ذلك وهذا هو القصد العام، وأن تتجه نيته إلى استعمال المحرر المزور فيما زُوِّر من أجله وهذا هو القصد الخاص .

ولا يختلف الركن المعنوي من وجهة نظرنا في التزوير المعلوماتي عنه في التزوير التقليدي، حالهُ في ذلك حال كافة عناصر التزوير التقليدية والتي تبين بنتيجة البحث إمكان تحققها في التزوير المعلوماتي باستثناء شكل المحرر، وقد تبين أنه يتمتع في التزوير التقليدي بالطبيعة المادية في حين أنه يفتقر إلى هذه الطبيعة في التزوير المعلوماتي.

---

[١] د. محمود نجيب حسني، شرح قانون العقوبات–القسم الخاص–دار النهضة العربية،١٩٩٢، ص٢٧١.

[٢] د. محمود نجيب حسني، المرجع السابق، ص٢٧٢، وأيضاَ د. إيهاب فوزي السقّا، المرجع السابق، ص٥٨.

ولكن إذا كانت مسألة تحقق أركان التزوير التقليدي في التزوير المعلوماتي بالشكل الذي تقدم بيانه، فما هو الحال بالنسبة للطرائق التي يقع بها التزوير، بمعنى آخر ما إمكانية تحقق التزوير المعلوماتي بالطرائق التقليدية؟

## المطلب الثاني

## مدى إمكانية تحقق التزوير المعلوماتي بالطرائق التقليدية

لا شك أن المشرع السوري قد أشار–ومن خلال نصوص المواد ٤٤٥ و٤٤٦ ق.ع.س– إلى نوعين من التزوير يتم التمييز بينهما من خلال الطرائق التي يقع بها التزوير وهما التزوير المادي والمعنوي.

### الفرع الأول: التزوير المادي

يمكن تعريف التزوير المادي بأنه تحريف الحقيقة في محرر تحريفاً يترك أثراً يمكن إدراكه بالحواس ، وقد نص المشرع السوري صراحة على هذا النوع من التزوير مبينا طرائق ارتكابه وذلك في م ٤٤٥ق.ع.س وقد جاء فيها:

**"١–يعاقب بالأشغال الشاقة المؤقتة خمس سنوات على الأقل الموظف الذي يرتكب تزويراً مادياً في أثناء قيامه بالوظيفة:**

**إما بإساءته استعمال إمضاء أو خاتم أو بصمة إصبع، وإجمالاً بتوقيعه إمضاء مزور، وإما بصنع صك أو مخطوط.**

---

[1] د. إيهاب فوزي السقّا، المرجع السابق، ص٦١

**وإما بما يرتكبه من حذف أو إضافة أو تغيير في مضمون صك أو مخطوط.**

**٢- ولا تنقص العقوبة عن سبع سنوات إذا كان السند المزور من السندات التي يعمل بها إلى أن يدعى تزويرها.**

**٣- تطبق أحكام هذه المادة في حال إتلاف السند إتلافا كليا أو جزئيا".**

وهذا النص يشير بشكل واضح إلى مجموعة من النقاط نوردها فيما يلي:

- لا بد أن يكون المحرر المزور محرراً رسمياً.
- لا بد أن يكون الجاني موظفاً وأن يرتكب التزوير أثناء قيامه بالوظيفة أيأن يكون من اختصاصه تنظيم المحرر الذي قام بتزويره.
- بين المشرع طرق التزوير المادية على سبيل الحصر، والتي سنذكرها تباعا فيما يلي:

أولاً: إساءة استعمال إمضاء أو خاتم أو بصمة إصبع

ويُقصد بذلك وضع التوقيع سواء أكان إمضاءً أو خاتماً أو بصمة إصبع في غير المكان الذي يجب أن يوضع فيه، ولما كان التوقيع - بأي شكل من أشكاله - يعبر عن إرادة صاحبه، فإن تزوير التوقيع بهذه الطريقة معناه أن المزور قد نَسب إلى صاحب التوقيع مُحرراً لم يصدر عنه، ولا يُعبر عن إرادته، ويستوي أن يكون المحرر المزور بهذه الطريقة محرراً تقليدياً أو معلوماتياً، ولا سيما أن الثورة المعلوماتية قد رفدت

التقدم التكنولوجي الذي نعيشه اليوم بالكثير من الأجهزة المساعدة لجهاز الحاسب الآلي _ كجهاز الماسح الضوئي (scanner) _ والتي استغلها الجناة لتسهيل ارتكاب جرائمهم، إذ أصبح معلوماً لدى الجميع إمكان سحب توقيع ما من خلال جهاز الماسح الضوئي ووضعه بواسطة الحاسب الآلي على وثيقة معلوماتية مزورة وما يصدق على الإمضاء يصدق على الخاتم وبصمة الإصبع .

ثانياً: صنع صك أو مخطوط: يسمى التزوير إذا ما وقع بهذه الطريقة تزويراً بالاصطناع لأن الجاني في هذه الحالة يخلق محرراً كاملاً _لا وجود له من قبل_ وينسبه إلى غير مُحرِرِه .[٢]

ولا شك بأن التقدم التكنولوجي جعل وقوع التزوير المعلوماتي بهذه الطريقة أمراً ممكناً ويسيراً، إذ بإمكان الجاني أن يُدخل إلى جهاز الحاسب الآلي ما يريد من بيانات ومعلومات سواء من خلال لوحة المفاتيح أو الماسح الضوئي أو حتى عن طريق شبكة الإنترنت وصياغتها في محرر، ثم طبعه بواسطة الطابعة، واستعماله فيما بعد في الغاية التي اصطنع المحرر من أجلها .[٣]

---

[١] د. عبد الفتاح بيومي حجازي، المرجع السابق، ص١٨٢.

[٢] القاضي عبد الوهاب بدرة، المرجع السابق، ص٩١.

[٣] د. عبد الفتاح بيومي حجازي، المرجع السابق، ص٢٠٢.

ثالثاً: التحريف بالحذف: يقع التزوير بهذه الطريقة عندما يعمد الجاني إلى محو عبارات أو أرقام أو إشارات يتغير مع محوها مضمون المحرر، ولا يهُم الطريقة التي يقع بها المحو فقد تكون حكاً أو شطباً أو وضع مادة كيميائية، إنما المهم أن يتغير مضمون المحرر بعد عملية الحذف وبهذا يقع التزوير .[١]

رابعاً: التحريف بالإضافة: التزوير بهذه الطريقة معاكس تماما للطريقة السابقة حيث يعمد الجاني إلى إضافة كلمة، أو عبارة، أو رقم، أو أي إشارة تؤدي إلى تغيير مضمون المحرر، ومثال ذلك أن يضيف الجاني في عقد البيع نقطة إلى يمين الرقم الذي يمثل ثمن المبيع فيزيده عشرة أضعاف، أما لو وضع النقطة عن يساره فلا يؤثر ذلك في شيء ولا يقع التزوير .[٢]

إذاً إنَّ كل إضافة أو حذف في محرر رسمي يترتب عليها تغيير في مضمون المحرر يعتبر تزويراً، وهنا لا بد من الإشارة إلى أن المحرر في حال التزوير بالحذف أو الإضافة يكون موجوداً مسبقاً، ويتم تغيير مضمونه حذفاً أو إضافةً، أما في حال التزوير بالاصطناع

---

[١] القاضي عبد الوهاب بدرة، المرجع السابق، ص٩٠-٩١.

[٢] القاضي عبد الوهاب بدرة، المرجع السابق، ص٨٣.

فالمحرر لا وجود له، وإنما يتم اختلاقه وعملية الاختلاق هذه هي التزوير بالاصطناع .

والتزوير المعلوماتي بالحذف أو الإضافة أمر ممكن الحدوث، حيث بات من المعروف أن جهاز الحاسب الآلي يقوم بمعالجة البيانات والمعلومات التي يتلقاها، وتتم المعالجة هنا بناء على الأوامر الصادرة عن المزوِّر، وخلال عملية المعالجة يتم الحذف، أو الإضافة، أو التعديل، ثم يُتوج ذلك بطباعة المحرر ليتم استعماله فيما زُوِّر من أجله .

خامساً: التحريف بالإتلاف: يميز قانون العقوبات السوري بين الإتلاف والتزوير كجرمين مستقلين عن بعضهما، ولا سيما إذا كان محل التجريم محرراً، وذلك استناداً للغاية المرجوة من كل منهما حيث أن غاية الإتلاف جعل المحرر المتلف غير صالح للاستعمال فيما أعد له، في حين أن غاية التزوير هي تغيير الحقيقة في محرر بغية استعماله فيما زُوِّر من أجله .[٣]

بمعنى آخر يمكننا القول إن التزوير بالإتلاف هو الإتلاف الذي لا يعدم المحرر قيمته ولا يحول دون استخدامه فيما أُعد له.

---

[١] القاضي عبد الوهاب بدرة، المرجع السابق، ص٩١.

[٢] د. عبد الفتاح بيومي حجازي، المرجع السابق، ص١٨٨.

[٣] القاضي عبد الوهاب بدرة، المرجع السابق، ص٩٥.

والتزوير المعلوماتي عن طريق التحريف بالإتلاف لا يختلف عنه في باقي أشكال التحريف السالف ذكرها من حيث إمكانية وقوعه، وعليه يمكن القول إن التزوير المعلوماتي ممكن الوقوع بأي طريقة من الطرق المادية المذكورة في المادة ٤٤٥ ق.ع.س، ويبقى السؤال عن مدى إمكانية وقوع التزوير المعلوماتي بالطرق المعنوية، وهذا هو موضوع بحثنا في الفرع الآتي:

**الفرع الثاني: التزوير المعنوي**

جاء في نص المادة ٤٤٦ ق.ع.س ما يلي:

**"يُعاقب بالعقوبة المنصوص عليها في المادة السابقة مع ما اشتملت عليه من فوارق، الموظف الذي ينظم سنداً من اختصاصه فيحدث تشويهاً في موضوعه أو ظروفه:**

**إما بإساءته استعمال إمضاء على بياض اؤتمن عليه، أو بتدوينه مقاولات أو أقوال غير التي صدرت عن المتعاقدين أو التي أملوها، أو بإثباته وقائع كاذبة على أنها صحيحة أو وقائع غير معترف بها على أنها وقائع معترف بها، أو بتحريفه أية واقعة أخرى بإغفاله أمراً أو إيراده على وجه غير صحيح".**

ومن خلال هذه المادة يمكن القول إن التزوير المعنوي هو تحريف الحقيقة في مضمون المحرر وأثناء إنشائه دون ترك أي أثر يمكن إدراكه بالعين .

وطرائق التزوير المعنوي حسب النص المذكور هي:

**أولاً:** إساءة استعمال إمضاء على بياض.

---

[1] القاضي عبد الوهاب بدرة، المرجع السابق، ص١٠٠

في هذه الطريقة من التزوير يُوقع صاحب العلاقة بإمضائه على محرر خالٍ من الكتابة، ويسلمه إلى شخص آخر _الجاني_ ليستعمله في الغرض الذي تم الاتفاق عليه، إلا أن الأخير لا يُلقي بالاً لذلك ويستعمل الإمضاء على بياض في غير ما تم الاتفاق عليه .[١]

**ثانياً**: تدوين مقاولات أو أقوال غير التي صدرت عن المتعاقدين أو التي أملوها.

يقع التزوير بهذه الطريقة عندما يقوم كاتب المحرر وأثناء تدوينه بتحريف المعلومات التي صدرت عن أولي الشأن، وذلك كأن ينسب الجاني بعض بيانات المحرر المزور للغير، أو يدونها بصورة مشوهة ومخالفة لإرادة من صدرت عنه .

**ثالثاً**: إثبات وقائع كاذبة على أنها صحيحة أو وقائع غير معترف بها على أنها وقائع معترف بها.

١- إثبات وقائع كاذبة على أنها صحيحة: في هذه الطريقة من التزوير لا يكون للواقعة الكاذبة أي وجود في الأصل، وإنما يقوم من دوَّن المحرر بإثبات حدوثها كذباً، ومثال ذلك كاتب المحكمة الذي يثبت في محضره أن الشاهد قد حلف اليمين وهو في

---

[١] القاضي عبد الوهاب بدرة، المرجع السابق، ص١٠٢ وما بعدها.

[٢] د. عبد الفتاح بيومي حجازي، المرجع السابق، ص٢٠٤

الواقع لم يحلف .[١]

٢-إثبات وقائع غير معترف بها على أنها وقائع معترف بها: في هذه الطريقة من التزوير ينسب كاتب المحرر إلى أولي الشأن وقائع لم يعترفوا بها، وبالأحرى لم يدلوا بها كما لو دوَّن كاتب المحكمة اعتراف المتهم بارتكاب فعل كان القاضي قد سأله عنه وهو في الأصل لم يُقر بارتكابه.

**رابعاً**: تحريف أي واقعة أخرى بإغفال أمر أو إيراده على وجه غير صحيح: في هذه الطريقة من التزوير يعمَد كاتب المحرر إلى تجاهل إثبات واقعة ما كانت قد دونت على لسان أولي الشأن، أو يعمَد إلى تدوينها بشكل مخالف لما أقر به أولي الشأن .

وإذا كان وقوع التزوير المعلوماتي بالطرائق المادية لا يثير أي إشكال، فالأمر برأينا كذلك أيضاً بالنسبة للتزوير المعلوماتي بالطرائق المعنوية، إذ يمكن وقوع هذا النوع من التزوير بأي طريقة من طرائق التزوير المعنوي المشار إليها سابقاً، لا بل إن التزوير المعلوماتي بالطرائق المعنوية أكثر وقوعاً منه بالطرق المادية، لأن التزوير بالطرائق المعنوية لا يقع إلا عند إنشاء المحرر، إضافةً لكونه لا يترك آثاراً مادية تُظهر بوضوح ما جرى

---

[١] القاضي عبد الوهاب بدرة، المرجع السابق، ص١١٢-١١٣

[٢] القاضي عبد الوهاب بدرة، المرجع السابق، ص١١٤

من تحريف للحقيقة في مضمون المحرر.

وجديرٌ بالقول إن الفقه الجزائي لم يكن متفق الرأي حول عدم انطباق نصوص التزوير التقليدية في حال التزوير المعلوماتي بل كان منقسماً في ذلك إلى اتجاهين رئيسيين:

**الاتجاه الأول:**

يرفض أنصار هذا الاتجاه القول بانطباق النصوص التقليدية على التزوير المعلوماتي، ويدعمون رأيهم بمجموعة من الحجج نذكر أبرزها فيما يلي:

١-يتمتع المحرر بمفهومه التقليدي بالطبيعة المادية وهو غالباً ما يكون من الورق المكتوب [١].

٢-تعريف الفقه للمحرر بأنه كل مسطور يتضمن علامات تعطي معنى مترابطاً وينتقل بها الفكر الإنساني من شخص لآخر بمجرد النظر إليه، وهذا يعني أن حاسة البصر هي الوسيط الوحيد الذي يؤدي إلى اكتشاف الفكرة التي يعبر عنها المحرر لتصل إلى ذهن الإنسان، في حين أن الفكرة في المحرر المعلوماتي لا تنتقل إلى الذهن بمجرد النظر إليها وإنما لا بد قبل ذلك من استخدام وسيط إلكتروني

[١] عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، بدون ناشر، ١٩٩٥، ص٧٨وما بعدها.

يسمح بعرض المحرر على شاشة الحاسب الآلي، حتى تتمكن العين المجردة من الاطلاع على ما يتضمنه المحرر من أفكار .[١]

٣-المعلومات مهما بلغت أهميتها القانونية لا يمكن أن تعد محرراً بالمفهوم التقليدي، ولا يمكن أن ينطبق على تغييرها وصف التزوير المنطبق على تحريف الحقيقة في البيانات المكتوبة على الورق .[٢]

٤-فكرة التوقيع في المحرر التقليدي مرتبطة بصور حصرية له هي الإمضاء والخاتم وبصمة الإصبع، وهذه الصور لا تتوافر في التوقيع الإلكتروني والذي له عدة صور تتناسب وطبيعته الإلكترونية .[٣]

٥-المحررات التقليدية المزورة تصلح للاستعمال كوسيلة إثبات أما التسجيلات المعلوماتية فلا تصلح لذلك .[٤]

**الاتجاه الثاني:**

يرى أنصار هذا الاتجاه أن النصوص التقليدية الخاصة بالتزوير تنطبق على التزوير

---

[١] د. أيمن عبد الله فكري، المرجع السابق، ص٣٦٦.

[٢] د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول – الجرائم الناشئة عن استخدام الحاسب الآلي، ط١، دار النهضة العربية، القاهرة،١٩٩٢، ص١١٦ وما بعدها.

[٣] محمد السعيد رشدي، حجية وسائل الاتصال الحديثة في الإثبات، بدون تاريخ، ص٧٧.

[٤] راجع في أنصار هذا الاتجاه، عفيفي كامل عفيفي، المرجع السابق، ص ٢٢٥ وما بعدها.

المعلوماتي، ويدعمون رأيهم بمجموعة من الحجج نذكر أبرزها فيما يلي :

١- لم يحدد المشرع مفهوم التزوير وهذا ما يُزيل العَقَبَة أمام عدم انطباقه على التزوير المعلوماتي.

٢- إن ضرورة الاستعانة بأجهزة خاصة لعرض مضمون المحرر المعلوماتي حتى تتمكن العين المجردة من الاطلاع عليه لا ينفي عنه وصف المحرر.

٣- بما أن المشرع لم يحدد مفهوم المحرر فهذا يعني الأخذ بمفهومه الواسع، والذي يشمل المحررات التقليدية والمعلوماتية على السواء.

٤- عندما تتوافر في المحرر المعلوماتي الشروط نفسها التي يتطلبها القانون في المحرر التقليدي، ويؤدي الوظائف نفسها، فإنه يجب أن يُمنح الأول ذات الحماية المقررة للثاني.

٥- لا يوجد تلازم بين فكرة الكتابة والورق، إذ مثلما يمكن أن تَرِد الكتابة على الخشب أو الجلد يمكن أن ترد على دعامة معلوماتية، أي أن المشرع لم يشترط طبيعة معينة للدعامة التي يُكتب عليها، وإنما اشترط أن تحقق الكتابة وظائف معينة مهما كانت طبيعة المادة المدونة عليها.

---

[١] راجع في أنصار هذا الاتجاه، د. أيمن عبد الله فكري، المرجع السابق، ص ٣٦٩ وما بعدها.

باختصار يمكننا القول إن الطبيعة غير المادية للمحرر المعلوماتي هي ما جعلت الفقه منقسماًحول إمكانية انطباق النصوص التقليدية ولا سيما الخاصة بالتزوير على حالة تزوير العقد الإلكتروني – موضوع بحثنا- ونحن وعلى الرغم من وجاهة كلا الرأيين إلا أننا نؤيد الاتجاه القائل بعدم انطباق النصوص التقليدية على تزوير العقد الإلكتروني، **ولنا في تدعيم هذا الرأي اعتبارات عدة نذكر من أهمها:**

١– القول بانطباق نص المادة ٤٤٣ ق.ع.س في حال كان العقد الإلكتروني محلاً للتزوير ما هو إلا توسع في تفسير هذا النص وهذا ما يُعارض وبوضوح أحد المبادئ الأساسية في القانون الجزائي وهو التفسير الضيق للنصوص الجزائية.

٢–القول بانطباق نص المادة ٤٤٣ ق.ع.س في حال كان العقد الإلكتروني محلاً للتزوير يمكن اعتباره من قبيل القياس، وهذا ما يُخالف أيضاً أحد المبادئ الأساسية في القانون الجزائي وهو حظر القياس في النصوص الجزائية.

ولا شك أن خرق مبادئ التفسير الضيق للنصوص الجزائية وحظر القياس فيها هو في الوقت نفسه خرق لمبدأ شرعية الجرائم والعقوبات – وهو المبدأ الرئيس وحجر الزاوية في القانون الجزائي– لأنه في حال التوسع بالتفسير أوالأخذبالقياس سنكون أمام واقعة جُرِّمت وفُرضت بحق مرتكبها العقوبة دون وجود نص صريح في ذلك، وهو ما يُعد

خروجاً صريحاً على مبدأ الشرعية السالف ذكره.

٣–إن ما يدعم وجهة نظرنا في عدم انطباق نص المادة ٤٤٣ ق.ع.س في حال كان العقد الإلكتروني محلاً للتزوير هو موقف المشرع بحد ذاته، إذ قد بدأ الأخير وفي العديد من الدول – ومنها سوريا– بإصدار قوانين خاصة تجرم الاعتداء على البرامج والبيانات وغيرها مما يدخل في نطاق الكيان المنطقي للحاسب الآلي ومنها المحرر الإلكتروني، وهذا الأمر بحد ذاته هو اعتراف من المشرع بقصور النصوص التقليدية عن تأمين الحماية الجزائية للمعلومات والبرامج والبيانات وعلى وجه الخصوص المحرر الإلكتروني ( ومنه العقد الإلكتروني موضوع بحثنا)،ولو كان الأمر خلاف ذلك لما عزم المشرع على إصدار مثل هذه القوانين الخاصة والتي ستكون موضوع بحثنا في الفصل الآتي.

**خلاصة الفصل الأول:**

تم في هذا الفصل توضيح مفهوم كل من العقد الإلكتروني والتوقيع الإلكتروني من خلال استعراض الأحكام الخاصة بهما في إطار القانون السوري، والمنصوص عليها في قانون تنظيم المعاملات الإلكترونية رقم ٣ لعام ٢٠١٤، وكذلك قانون التوقيع الإلكتروني وخدمات الشابكة رقم ٤ لعام ٢٠٠٩، كما تم دراسة إمكانية تطبيق الأحكام التقليدية الخاصة بالتزوير والمنصوص عليها في قانون العقوبات السوري الصادر عام ١٩٤٨، حيث تبين بالنتيجة عدم إمكانية تطبيق هذه الأحكام فيما لو كان العقد الإلكتروني محلاً للاعتداء وذلك لكون هذه الأحكام تخص المحررات ذات الطبيعة المادية(الورقية) وهي التي يفتقر إليها العقد الإلكتروني.

وبالتالي كان لزاماً علينا التوجه شطر النصوص الخاصة في القانون السوري لمعرفة ما إذا كانت مظلة التجريم والعقاب قد امتدت لتشمل هذه الاعتداءات وغيرها أم لا، وهذا ما سيكون موضوع بحثنا في الفصل الآتي.

## الفصل الثاني

## مدى كفاية التشريعات الجزائية الخاصة في حماية التعاقد الإلكتروني

أصبح من الثابت القول إن الاعتداءات التي يمكن أن تتعرض لها وثيقة العقد الإلكتروني – بما فيها التوقيع الإلكتروني- لا تخرج عن إحدى طائفتين، الأولى اعتداءات تقليدية تُرتكب بوسائل إلكترونية، والثانية اعتداءات مستحدثة ارتبط ظهورها بظهور المحرر الإلكتروني عموماً، ومنه العقد الإلكتروني وأداة التوثيق فيه وهي التوقيع الإلكتروني.

وحتى تكون الحماية الجزائية للتعاقد الإلكتروني شاملة لا بد أن تشمل بالتجريم والعقاب كافة الاعتداءات المنضوية تحت هاتين الطائفتين.

ولما كان الفصل الأول من هذه الرسالة قد بين عدم صلاحية قانون العقوبات لتطبيق نصوصه على الاعتداءات التقليدية الواقعة على العقد الإلكتروني ولا سيما لجهة التزوير، كان لا بد لنا من البحث في طيات النصوص الخاصة عن الحماية الجزائية للعقد الإلكتروني من أي اعتداء يمكن أن ينضوي تحت أي من الطائفتين السالف ذكرهما.

وهنا نسأل هل كان للمشرع السوري خطة لتأمين هذه الحماية وإن كان كذلك فما مدى شموليتها؟

في الإجابة عن هذا السؤال سيكون لدينا المبحثان الآتيان:

المبحث الأول: مدى شمول الاعتداءات التقليدية بالتشريعات الجزائية الخاصة

المبحث الثاني: مدى إحاطة المشرع بصور الاعتداءات المستحدثة

## المبحث الأول

## مدى شمول الاعتداءات التقليدية بالتشريعات الجزائية الخاصة

إذا كنّا قد قصرنا في البحث في الفصل السابق على مدى انطباق نص المادة ٤٤٣ ق.ع.س في حال كان العقد الإلكتروني محلاً للتزوير، فنحن لا نعني بذلك عدم إمكانية تعرض العقد الإلكتروني لغير هذا الاعتداء، وإنما لكونه من أبرز الاعتداءات التي يمكن أن تقع على المحررات.

وإذا ما بحثنا في القوانين السورية الخاصة بالتعاملات الإلكترونية عن تجريم الاعتداءات التقليدية التي يمكن أن يتعرض لها العقد الإلكتروني، لعثرنا على نصين أساسيين في تجريم هذه الاعتداءات، الأول منهما احتياطي عام وهو المنصوص عليه في المادة ٢٨ من قانون تنظيم التواصل على الانترنت ومكافحة الجريمة المعلوماتية رقم ١٧ لعام ٢٠١٢، والثاني خاص بالاعتداءات الواقعة على التوقيع الإلكتروني وهو ما جاء النص عليه في المادة ٣١ من قانون التوقيع الإلكتروني وخدمات الشابكة رقم ٤ لعام ٢٠٠٩، وعلى هذا الأساس آثرنا تقسيم هذا المبحث إلى مطلبين:

المطلب الأول: مدى كفاية النص الاحتياطي في حماية العقد الإلكتروني

المطلب الثاني: مدى كفاية الحماية الخاصة بالتوقيع الإلكتروني

## المطلب الأول

## مدى كفاية النص الاحتياطي في حماية العقد الإلكتروني

رغبةً من المشرع السوري في عدم إفلات أي مجرم من العقاب ، وانسجاماً مع خطته في مواكبة القانون للتطور التكنولوجي،فقد سنّ مجموعة من القواعد المتعلقة بالجرائم التقليدية و الشابكة وبكيفية تطبيق القوانين الجزائية، وذلك وفق ما جاء في المادة٢٨ من قانون تنظيم التواصل على الانترنت ومكافحة الجريمة المعلوماتية الصادر بالمرسوم التشريعي رقم ١٧ لعام ٢٠١٢،وفي نصها:

المادة (٢٨)

"تطبيق القوانين الجزائيّة

/أ/ إذا انطبق نصّ في القوانين الجزائيّة النّافذة على إحدى الجرائم المنصوص عليها في هذا القانون تُطبَّق العقوبة التي هي أشد.

/ب/ يضاعف الحدّ الأدنى للعقوبة المقرّرة لأيّ من الجرائم المنصوص عليها في القوانين الجزائيّة النّافذة الأخرى في إحدى الحالتين التّاليتين:

١) إذا ارتُكبت الجريمة باستخدام الشابكة أو وقعت على الشابكة.

---

[1] القاضي د. محمد طارق الخن، الجريمة المعلوماتية، الجامعة الافتراضية السورية، ٢٠١٢، ص٨٨

**٢)** إذا وقعت الجريمة على جهاز حاسوبي أو منظومة معلوماتيّة بقصد التّأثير على عملها أو على **المعلومات أو البيانات المخزّنة عليها**."

وما يهمنا من هذا النص في واقع الأمر هو معرفة ما إذا كان يؤمن الحماية الجزائية للعقد الإلكتروني مما قد يقع عليه من اعتداءات تقليدية أم لا؟ وفي سبيل ذلك سيكون لدينا الفرعين التاليين حيث نسلط الضوء في الأول منهما على كيفية معالجة المشرع للجرائم التقليدية الواقعة في الإطار التكنولوجي، ثم نبين في الثاني مواطن القصور في النص.

**الفرع الأول: كيفية معالجة الجرائم التقليدية الواقعة في الإطار التكنولوجي**

يتضح من خلال نص المادة ٢٨ المذكورة آنفاً أن المشرع عالج الجرائم التقليدية الواقعة في إطار التكنولوجيا من خلال إقرار قاعدتين أساسيتين، الأولى خاصة بوجوب فرض العقوبة الأشد عند انطباق نص في قانون جزائي نافذ على جريمة منصوص عليها في قانون مكافحة الجريمة المعلوماتية، والثانية خاصة بالجرائم التقليدية المرتكبة في الوسط التكنولوجي.

**أولاً: وجوب فرض العقوبة الأشد**

تشير الفقرة (أ) من المادة ٢٨ المذكورة أنفاً إلى أنه إذا انطبق نص في القوانين الجزائية النافذة على جريمة ما منصوص عليها في قانون مكافحة الجريمة المعلوماتية، فهنا يجب تطبيق النص ذي العقوبة الأشد، والغاية من هذا النص واضحة وهي رغبة المشرع في تطبيق العقوبة الأشد في حال انطباق نصين على واقعة جرمية معلوماتية .

---

[1] القاضي د. محمد طارق الخن، الجريمة المعلوماتية، الجامعة الافتراضية السورية، ٢٠١٢، ص٨٥-٨٦ ونضرب مثالاً على هذه الحالة من المادة ٢٩ من قانون مكافحة الجريمة المعلوماتية، والتي تعاقب بالحبس من ستة أشهر إلى ثلاث سنوات والغرامة من ١٠٠ألف إلى ٥٠٠ ألف ليرة سورية كل من يقوم بالترويج لأي جريمة باستخدام الشابكة، في حين جاءت المادة ٨ من قانون مكافحة الإرهاب رقم ١٩لعام ٢٠١٢، لتعاقب بالأشغال الشاقة المؤقتة على جريمة ترويج الأعمال الإرهابية المرتكبة على موقع

ولما كان الهدف من دراسة أي نص قانوني في هذا البحث هو بيان مدى تأمينه الحماية الجزائية للعقد الإلكتروني، لا بد لنا من القول إن هذا النص- فقرة أ/٢٨- لا يمكن أن يؤمن في الواقع أي حماية جزائية للعقد الإلكتروني، لعدم وجود نصوص جزائية تجرم الاعتداءات الواقعة على وثيقة العقد الإلكتروني سواء أكانت هذه الاعتداءات تقليدية أم مستحدثة، باستثناء ما جاء في قانون مكافحة الجريمة المعلوماتية ذاته والتي سنأتي على بيانها تباعاً كل في مكانه المناسب من هذا البحث وبداية ذلك الفقرة الآتية:

**ثانياً: شمول التجريم للجرائم التقليدية المرتكبة في الوسط التكنولوجي**

إن من أبرز ما يشير إليه نص الفقرة (ب) من المادة (٢٨) من قانون مكافحة الجريمة المعلوماتية هو أن المشرع السوري جاء بنص وحيد مدّ من خلاله مظلة التجريم والعقاب لتشمل كافة الجرائم التقليدية الواقعة باستخدام الشابكة أو عليها دون أن يفرد لكل جريمة نصاً خاصاً بها.

وهذا ما يمكن اعتباره برأينا خطوة إيجابية في سياسة المشرع السوري، إلا أنه وعلى

---

إلكتروني، حيث يجب على المحكمة في هذه الحال أن تطبق النص ذو العقوبة الأشد وهو المادة ٨ من قانون مكافحة الإرهاب.

الرغم من وضوح رغبة الأخير من صياغة هذا النص في إيجاد نص احتياطي يطال مختلف الجرائم التقليدية التي تقع باستخدام الشابكة، أو التي تكون الشابكة محلاً لها بالإضافة إلى الجرائم الواقعة على الأجهزة الحاسوبية والمنظومات المعلوماتية بقصد التأثير على عملها أو على المعلومات أو البيانات المخزنة عليها، لم يخلُ البند٢ من الفقرة/ب/- من وجهة نظرنا- من اللبس وعدم الوضوح، إذ لم يبين حقيقة موقف المشرع فيما إذا كان يقصد من هذا البند تجريم الاعتداء المادي الواقع على الجهاز الحاسوبي أو المنظومة المعلوماتية، كالحرق أو التحطيم للتأثير على عملها أو التأثير على المعلومات أو البيانات المخزنة عليها، أم أنه كان يقصد الاعتداء على الكيان المنطقي للحاسب الآلي أو المنظومة المعلوماتية، وتوضيح هذا الغموض نراه أمراً غاية في الأهمية لأن مثل هكذا اعتداء مادي مجرّم بالنصوص العامة. وما نبحث عنه حقيقة الأمر هو حماية العقد الإلكتروني بما يتضمنه من معلومات وتواقيع إلكترونية، وهو ما يعتبر جزءاً من الكيان المنطقي للحاسب الآلي أو المنظومة المعلوماتية.

ولكن لو سلمنا جدلاً أن المقصود من النص هو تجريم الاعتداء الواقع على الكيان المنطقي للحاسب الآلي، فإن هناك مغالطة تقنية كبيرة وقع بها المشرع بالنسبة لمفهومي البيانات والمعلومات، **وهي ما تعتبر برأينا الإشكالية الكبرى في هذا النص و موطن**

**القصور فيه**، لأن ما نبحث عنه من حماية جزائية للعقد الإلكتروني يمكن استخلاصها من الحماية المقررة في هذا النص للمعلومات والتي تشكل مضمون الرسالة الإلكترونية التي تتضمن التعبير عن الإيجاب والقبول .وبيان هذه المغالطة التقنية يتطلب منا بداية [١] بيان حقيقة مفهومي البيانات والمعلومات، ومن ثم بيان موقف المشرع السوري حيال ذلك، وصولاً في النهاية إلى بيان أوجه القصور في النص، وهذا ما سنبينه فيما يلي:

**١ – مفهوم البيانات والمعلومات**

في الواقع تختلف الآراء حول تفسير معنى البيانات والمعلومات، حيث أن هناك من يفرق بين هذين المفهومين، وهناك من لا يرى لهذا الفرق أي ضرورة .

أما الفريق الأول فيعرف أنصاره البيانات بأنها "مجموعة من الأرقام والكلمات والرموز أو الحقائق أو الإحصاءات الخام التي لا علاقة بينها ولم تخضع بعد للتفسير أو التجهيز للاستخدام، والتي تخلو من المعنى الظاهر في أغلب الأحيان "، في حين أن المعلومات هي "المعنى المستخلص من هذه البيانات".

---

[١] المادة (١) من القانون (٣) لعام ٢٠١٤ الناظم للتعاملات الإلكترونية

"الرسالة الإلكترونية: معلومات ترسل أو تستلم بوسائل إلكترونية"

[٢] راجع في أطراف هذا الخلاف، نائلة محمد فريد قوره، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بلا سنة نشر، ص٩٧ وما بعدها

في حين أن الفريق الآخر لا يرى أي ضرورة لهذه التفرقة، ويفضل استخدام البيانات والمعلومات كمترادفين.

ومن الناحية التقنية هناك فرق بين البيانات والمعلومات ، حيث تُعرف البيانات أو المعطيات بأنها :

"١- المعلومات المميّزة لحالة أو لموضوع معيّن. وتكون المعطيات عبارة عن ثوابت أبجد عددية ورقميّة.

٢- قيم عددية أو رقميّة ناتجة عن تجارب واختبارات علمية.

٣- مجموعة الاستعلامات التي تصف حالة معينة أو كائن معين ".

وهناك من يُعرف البيانات بأنها: المواد الخام التي تُستخرج منها المعلومات ، وتُعرف البيانات أيضاً بأنها: مجموعة الحقائق الأولية (المجردة) .

---

[1]Joyrup Bhattacharya، Rudiments of Computer Science ، Academic Publishers ،no published date ،P-1-2-1

[٢]د. عبد الحسن الحسيني، القاموس الموسوعي في المعلوماتية والاتصالات والمعلوماتية القانونية، ط١، مكتبة صادر، بيروت، ٢٠٠٤، ص٢٦٠

في حين تُعرف المعلومات بأنها: معطيات واستعلامات يتم تسجيلها أو تصنيفها و تنظيمها وتفسيرها ووضعها في إطار عمل معين لإظهار معانيها ، ويمكن تعريف المعلومات بأنها: النتائج المقروءة بعد معالجة البيانات .

أما نحن فنتفق مع الجانب التقني الذي يقول بأن المعلومات تختلف عن البيانات، فالبيانات برأينا هي المعلومات في مرحلة المعالجة الآلية، وهي في هذه المرحلة تُعتبر مواداً خام ولا تعبر عن أي معنى، كما أنها في هذه المرحلة لا تقبل التخزين لأن نظام معالجة البيانات ليس من وحدات التخزين في الأجهزة الحاسوبية، في حين أن المعلومات هي الحقائق المعبرة عن معنى معين، وتُستخرج بنتيجة معالجة البيانات.

---

[1]Martha Henderson Hurley –Dena Hanley, Correctional Administration and Change Management, Taylor & Francis Group, an **informa** business, no published date Page 56.

[3] Ralph M. Stair and George W. Reynolds, fundamentals of information systems, Eighth Edition, no published date Page 5.

[4]د. عبد الحسن الحسيني، المرجع السابق، ص٤٢٩

[5]Martha Henderson Hurley –Dena Hanley, The previous reference, no published date، Page 56.

## ٢- موقف المشرع السوري

لم يكن موقف المشرع السوري واضحاً تجاه مفهومي البيانات والمعلومات، حيث يبدو وكأنه لا يتبنى أي تفريق بينهما حينما اقتصر على تعريف المعلومات دون البيانات في المادة الأولى من قانون مكافحة الجريمة المعلوماتية ، في حين ينتقض هذا الفرض عندما يأتي المشرع في القانون ذاته على استخدام عبارة "البيانات أو المعلومات " في أغلب المواضع التي يتحدث فيها عن المعلومات وكأنه بهذا يشير إلى وجود فرق بينهما، وهذا التناقض برأينا يخلق إشكالية هامة تؤدي إلى خروج بعض الاعتداءات من دائرة التجريم والعقاب، الأمر الذي يجعل النص قاصراً وغير قادر على تأمين الحماية المطلوبة للعقد الإلكتروني مما قد يقع عليه من اعتداءات تقليدية، وبيان مواطن القصور في النص سيكون موضوع الفرع الآتي.

---

[١] المادة (١) ...تعاريف ...

**المعلومات**: العلامات أو الإشارات أو النّصوص أو الرّسائل أو الأصوات أو الصّور الثّابتة أو المتحركة التي تحمل معنى قابلاً للإدراك، مرتبطاً بسياق محدَّد.

**الفرع الثاني: مواطن القصور في النص**

ينحصر موطن قصور النص برأينا في أمرين أساسيين:

**أولاً: عدم وضوح موقف المشرع حيال مفهومي البيانات والمعلومات**

إن عدم الوضوح في موقف المشرع حيال مفهومي البيانات والمعلومات محل الجريمة في المادة ٢٨/ب/٢المذكورةآنفاً، والتي اشترط المشرع أن تكون مخزّنة على الجهاز الحاسوبي أو المنظومة المعلوماتية ما هو إلا تناقض في موقفه يؤدي إلى خروج طائفة من الاعتداءات من مظلة هذا النص، لأن هذا التناقض لا يخرج عن أحد احتمالين:

أ- إذا كان المشرع قد تبنى فكرة التمييز بين المعلومات والبيانات فمعنى ذلك أن الفقرة ب/٢ من المادة ٢٨ المذكورة آنفاً تتضمن خللاً في المفهوم التقني حيث يتجسد هذا الخلل في اشتراط المشرع أن تكون البيانات مخزنة كالمعلومات، والبيانات في مرحلة المعالجة الآلية لا تقبل التخزين كما أسلفنا.

ب- أما إذا كان المشرع لم يميز بين البيانات والمعلومات وكان استخدامه لهذين المصطلحين كمترادفين بنفس معنى المعلومات المشار إليه في المادة الأولى من القانون المذكور، فمعنى ذلك أن الاعتداء على البيانات في مرحلة المعالجة الآلية يخرج عن مظلة التجريم والعقاب في المادة ٢٨ فقرة /ب/٢.

والأكثر من ذلك أننا نرى إمكانية وقوع اعتداءات معينة على المعلومات لا يمكن أن تقع على البيانات فعلى سبيل المثال سرقة وثيقة العقد الإلكتروني أو أي وثيقة إلكترونية أخرى لا يمكن أن تتم إلا بعد الانتهاء من معالجة بيانات هذا العقد وتحولها إلى معلومات، والسبب في ذلك أنه وخلال قيام نظام المعالجة الآلي بمعالجة البيانات لا يمكن إجراء عمليات القص واللصق أو النسخ واللصق –كما هو الحال في جريمة نسخ المعلومات– في حين من المتصور وقوع التزوير على البيانات بحيث تتم معالجتها وهي مزورة وتتبلور بهذا الوصف كمعلومات، ويتم تخزينها في ذاكرة الجهاز الحاسوبي (hard disk ) على هذ الأساس ، أي أننا أصبحنا أمام معلومات تم[١] تزويرها قبل وصولها إلى وحدة التخزين.

والمثال على تزوير البيانات هو قيام الوكيل عن أحد أطراف التعاقد بتحريف بيانات العقد أثناء كتابتها على الحاسب الآلي كأن يغير ثمن المبيع المتفق عليه، أو يغير أسلوب الدفع نقداً أو بالتقسيط، وفي هذه الحالة يقوم نظام المعالجة الآلية للبيانات بمعالجة هذه البيانات وهي مزورة، وتتحول بهذا الوصف إلى معلومات، وبالتالي تكون

---

[١] hard disk (قرص صلب) وهو" قرص مغناطيسي بسعة خزن كبيرة" راجع د. عبد الحسن الحسيني، المرجع السابق، ص ٣٩٣

المعلومات قد زُوِّرت قبل مرحلة التخزين، وهذا مالم ينص عليه المشرع السوري في الفقرة ب/٢ من المادة ٢٨ من القانون المذكور.

**ثانياً: إمكانية تعرض المعلومات للاعتداء قبل مرحلة التخزين**

يُضاف إلى أوجه القصور التي نراها في النص أن المشرع اشترط في المعلومات محل الاعتداء أن تكون مخزنة، وبالتالي فإن المعلومات غير المخزنة تخرج عن تطبيقات النص المذكور، وبالتالي فإن المعلومات التي تشكل مضمون وثيقة العقد الإلكتروني قد تتعرض للاعتداء قبل مرحلة التخزين، لأن المعلومات عندما تتم معالجتها في نظام المعالجة الآلية باسم البيانات تنتقل بالدرجة الأولى إلى الذاكرة العشوائية في الجهاز الحاسوبي والمعروفة باسم (RAM[١])، وفي هذه المرحلة لا يمكن القول إن المعلومات مخزنة في الجهاز الحاسوبي بدليل فقدانها فيما لو انقطع التيار الكهربائي، ومن هذه الذاكرة يقوم المستخدم بإجراء عملية حفظ المعلومات فتنتقل حينها إلى ذاكرة الجهاز الحاسوبي hard disk لتخزن فيها، حيث يستطيع المستخدم في هذه الحالة الرجوع إليها في هذه الذاكرة متى شاء.

وبناء على ما سبق يمكننا القول إن خطة المشرع السوري في حماية البيانات والمعلومات

---

[١] د. عبد الحسن الحسيني، المرجع السابق، ص ٦٧٥

– سواء أشكلت مضمون وثيقة العقد الإلكتروني أو أي وثيقة إلكترونية أخرى –لم تكن كافية، وعلى المشرع تحديد موقفه من مفهوم البيانات والمعلومات، وإعادة صياغة نص الفقرة السابقة في ضوء ذلك بحيث يشمل التجريم الاعتداء على المعلومات سواء أكانت مخزنة أم لا، بالإضافة إلى شموله الاعتداء على البيانات بمفهومها كمواد خام للمعلومات لا تقبل التخزين.

ولكن إذا كانت خطة المشرع السوري المشار إليها آنفاً غير كافية، فإن المطلب الآتي سيبين كفايتها من عدمه فيما لو كان موضوع الحماية التوقيع الإلكتروني.

## المطلب الثاني

## مدى كفاية الحماية الخاصة بالتوقيع الإلكتروني

بعد أن بات التوقيع الإلكتروني عاملاً مهماً في إتمام التعاملات الإلكترونية، أصبح هدفاً للاعتداءات ذاتها التي يتعرض لها نظيره التقليدي.

ولما كان لهذه الاعتداءات تأثير سلبي على الثقة الواجب توفرها في التعاملات الإلكترونية من جهة، وكون التوقيع الإلكتروني من وجهة نظرنا لا يختلف عن العقد الإلكتروني من حيث عدم انطباق النصوص التقليدية عليه طالما كانت الطبيعة الإلكترونية هي القاسم المشترك بينهما. كان لا بد من مواجهة هذا التأثير السلبي وإدخال هذه الاعتداءات ضمن دائرة التجريم والعقاب.

وهنا نسأل: إذا كان النص الاحتياطي – المذكور آنفاً– قاصراً ولم يُوفر الحماية الكافية للعقد الإلكتروني من الاعتداءات التقليدية التي قد يتعرض لها، فهل يختلف الحال حينما يكون التوقيع الإلكتروني محلاً لهذه الاعتداءات، وهل من نصوص خاصة في القانون السوري تؤمن الحماية المرجوة للتوقيع الإلكتروني من الاعتداءات التقليدية؟

في الواقع وبنتيجة البحث في قانون التوقيع الإلكتروني وخدمات الشابكة نجد المشرع

السوري قد اقتصر على تجريم تزوير وإتلاف بيانات أو منظومة إنشاء التوقيع الإلكتروني دون غيرها من الاعتداءات التقليدية حسبما سيتبين في الفرعيين الآتيين:

**الفرع الأول :المساس بموثوقية التوقيع الإلكتروني**

نتناول في هذا الفرع خطة المشرع السوري في حماية التوقيع الإلكتروني من التزوير والإتلاف وفق الآتي.

**أولاً: تزوير التوقيع الإلكتروني:**

لم يكن التوقيع الإلكتروني أفضل حالاً من العقد الإلكتروني، حيث كان كالأخير عرضة لجريمة التزوير أيضاً.

إلا أن هذه الجريمة وفيما يخص التوقيع الإلكتروني تتميز عن باقي جرائم التزوير الأخرى بأنها جريمة مركبة، أي أنها تتكون من جريمتين، الأولى سرقة منظومة التوقيع الإلكتروني لشخص ما، والثانية استخدام هذه المنظومة دون إذن مالكها .

وأمام خطورة هذه الجريمة لم يقف المشرع السوري مكتوف الأيدي بل جرم صراحةً التزوير الواقع ليس فقط على التوقيع الإلكتروني وإنما أيضاً الواقع على بيانات أو منظومة إنشاء هذا التوقيع إضافة إلى تجريمه تزوير شهادة التصديق الإلكتروني، وذلك في الفقرتين ٢-٥ من المادة ٣١ من قانون التوقيع الإلكتروني وفي نصها:

---

[1] خالد العبيدي، الحماية الجنائية للتعاملات الالكترونية في نظام المملكة العربية السعودية، رسالة ماجستير، جامعة نايف للعلوم الأمنية، ٢٠٠٩، ص١٧٣

مادة ٣١ – مع عدم الإخلال بأية عقوبة أشد منصوص عليها في أي قانون آخر نافذ:

" يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من خمسمائة ألف ليرة إلى مليوني ليرة سورية، كل من قام قصداً بارتكاب أحد الأفعال التالية:

٢- تزوير أو تحريف توقيع إلكتروني أو بيانات أو منظومة إنشاء توقيع إلكتروني بأي طريق كان.

٥- تقديم أوراق أو معلومات مزورة أو غير صحيحة بقصد الحصول على شهادة تصديق إلكتروني أو تعليق العمل فيها أو إلغائها".

وهنا لا بد من الاشارة بدايةً إلى أن المشرع السوري لم يعرف التزوير في القانون الخاص بالتوقيع الإلكتروني والذي يمكن تسميته بالتزوير المعلوماتي، ولكن هذا لا يؤثر برأينا، لطالما أنه سبق للمشرع تعريف التزوير في المادة ٤٤٣ ق.ع، وإن كان هذا التعريف خاصاً بالتزوير التقليدي، إلا أن جوهر التزوير واحد – سواء في التزوير المعلوماتي أو التقليدي- وهو التحريف المقصود للحقيقة، ويبقى الخلاف بينهما في طبيعة محل التزوير، وما يؤكد حقيقة ذلك هو موقف المشرع الفرنسي حيث عمل على توسيع نطاق التزوير ليشمل المحررات الورقية والإلكترونية معاً وذلك من خلال تعديل م

١/٤٤١ من قانون العقوبات الفرنسي الجديد والتي عرفت التزوير بأنه: "كل تغيير بطريق الغش في الحقيقة ويكون من شأنه إحداث ضرر ، ويُرتكب بأية طريقة، سواء أكان ذلك بالكتابة أم بأي إفصاح آخر للتعبير عن الفكر الذي يكون الغرض منه أو كنتيجة له شأناً في إثبات حق أو واقعة لها آثار قانونية" .

ومن هنا تأتي أهمية النص السوري المذكور آنفاً أنه مدّ مظلة التجريم والعقاب لتشمل التزوير الواقع على التوقيع الإلكتروني وذلك تطبيقاً لمبدأ الشرعية، ولا تتوقف أهمية النص عند هذا الحد، بل تمتد برأينا إلى مضمونه الذي يشير صراحة إلى خروج المشرع عن خطته التقليدية في حصر الوسائل التي يُرتكب بها التزوير، ليجعل التزوير المعلوماتي ممكن الوقوع بأي وسيلة، وذلك من خلال استخدامه عبارة " بأي طريق كان" وهذا في الواقع أمر إيجابي كونه يضفي على النص مرونة تجعله يستوعب أي وسيلة جديدة يمكن أن تفرزها تكنلوجيا المعلومات، ويمكن استخدامها في تزوير التوقيع الإلكتروني .

ولهذا النص جانب إيجابي أيضاً يتمثل في قيام المشرع بتجريم استعمال التوقيع

---

[١] د. أيمن عبد الله فكري، المرجع السابق، ص٤٠٨ وما بعدها

الإلكتروني المزور بشكل مستقل عن تجريمه تزوير التوقيع الإلكتروني حيث يُبنى على هذا التوجه أمران : [١]

الأول: أن المشرع يُعاقب على التزوير وإن لم يعقبه استعمال للتوقيع المزور، لا بل إن عدول المزور عن استعمال التوقيع المزور بعد تزويره لا يعفيه من العقاب على جريمة التزوير ذاتها.

الثاني: أن استقلالية تجريم استعمال التوقيع المزور تعني أن الجاني يُعاقب سواء أكان هو المزور أم لا.

ولكن في حال تم استعمال التوقيع المزور من قبل الغير يجب أن يعلم هذا الأخير بأن التوقيع الذي يستعمله مزور . [٢]

كما وتجدر الاشارة إلى أن مُستعمل التوقيع الإلكتروني المزور يُعاقب وإن لم يُعاقب مُزور التوقيع ذاته لانتفاء القصد الجرمي أو انقضاء الدعوى بالوفاة أو التقادم أو انعدام مسؤولية الفاعل الجزائية لقيام أحد موانع المسؤولية الجزائية .

---

[١] خالد العبيدي، المرجع السابق، ص١٩٧

[٢] د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، دار الكتب القانونية، ٢٠٠٧، ص ١٣٦

٣خالد العبيدي، المرجع السابق، ص١٩٧

كذلك تبدو إيجابية التشريع السوري في النص على تجريم الحصول غير المشروع على شهادة التصديق الإلكتروني كما هو منصوص عليه في الفقرة الخامسة المذكورة آنفاً. وبالتالي يمكن القول إن خطة المشرع السوري في حماية التوقيع الإلكتروني من التزوير متكاملة إلى حد كبير، وهنا نسأل هل كانت خطته كذلك بالنسبة لجريمة الإتلاف؟

**ثانياً: إتلاف بيانات أو منظومة إنشاء التوقيع الإلكتروني**

في الواقع لم يرد مصطلح الإتلاف في أي فقرة من فقرات المادة ٣١ من قانون التوقيع الإلكتروني السوري، ولكن هذا لا يعني برأينا عدم تجريم فعل الإتلاف، إذ نص المشرع في الفقرة ٤ من المادة المذكورة على تجريم تعطيل بيانات أو منظومة إنشاء التوقيع الإلكتروني عن أداء وظيفتها ، ومصطلح التعطيل في الواقع لا يعدو أن يكون صورة من صور الاتلاف وقد استخدمه المشرع الفرنسي إلى جانب مصطلحات الإفساد والمحو والتعديل والإدخال وذلك في معرض تجريمه إتلاف نظام المعالجة الآلية (المادة

---

[1] مادة ٣١- مع عدم الاخلال بأي عقوبة أشد منصوص عليها في أي قانون آخر نافذ:
يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من خمسمئة ألف ليرة إلى مليوني ليرة سورية، كل من قام قصداً بارتكاب أحد الأفعال التالية:
٤- التوصل بأي وسيلة كانت إلى الحصول بغير حق على بيانات انشاء توقيع الكتروني أو منظومة انشاء توقيع الكتروني أو وثيقة الكترونية، أو اختراق أي منها أو اعتراضها أو **تعطيلها عن أداء وظيفتها**.

٢،٣/٣٢٣ من قانون العقوبات الفرنسي الجديد ).

والتعطيل يعني توقف الشيء عن القيام بوظيفته لفترة مؤقتة قد تكون طويلة وقد تكون قصيرة ، وبالتالي فإن تعطيل بيانات أو منظومة إنشاء التوقيع الإلكتروني يعني إيقافها عن العمل وجعلها غير صالحة للاستعمال فيما أُعدت له وهذا هو جوهر الإتلاف . وبالتالي يمكن أن نصف بالنجاعة خطة المشرع السوري في حماية التوقيع الإلكتروني من التزوير والإتلاف، ولكن السؤال الذي يطرح نفسه هنا هل كانت خطته كذلك

---

[١] المادة ٢/٣٢٣ (يُعاقب بالحبس لمدة تتراوح ما بين ثلاثة أشهر وثلاث سنوات وبالغرامة التي تتراوح ما بين عشرة ألاف ومائة ألف فرنك أو بإحدى هاتين العقوبتين كل من عطل أو أفسد متعمداً – ودون مراعاة لحقوق الغير- تشغيل نظام المعالجة الآلية للمعطيات)

المادة ٣/٣٢٣(كل من أدخل عمداً ودون مراعاة لحقوق الغير – مباشرة أو بصورة غير مباشرة- معطيات في نظام المعالجة الآلية أو محى أو عدل في المعطيات التي يحويها النظام أو في طرق معالجتها أو نقلها يُعاقب بالحبس مدة تتراوح ما بين ثلاثة شهور إلى ثلاث سنوات وبغرامة تتراوح ما بين ٢٠٠٠- ٥٠٠٠٠٠ فرنك أو بإحدى هاتين العقوبتين)

وكذلك استخدم المشرع العراقي في المادة ٤٧٧ ق.ع المصطلحات (هدم- خرب- أتلف- عطل- شوه- جعله غير صالح للاستعمال) وذلك في معرض تجريمه الاتلاف.

[٢] محمد حمّاد مرهج الهيتي، جرائم الحاسوب، دار المناهج للنشر والتوزيع، ط١، ٢٠٠٦، ص٢٠٦

[٣] أسامة بن غانم العبيدي، جريمة الإتلاف المعلوماتي، ص٩٥وما بعدها على الموقع التالي:

http://informationstudies.net/issue_list.php?action=getbody&titleid=56

تاريخ الزيارة: ٢٠١٥/٧/٣، الساعة ١١,١٥ صباحاً.

بالنسبة لسائر الاعتداءات التقليدية ولا سيما السرقة؟ إجابتنا على هذا التساؤل ستكون في الفرع الاتي.

**الفرع الثاني: اعتداءات لم يجرمها المشرع**

إذا كان المشرع السوري قد أرسى أُسساً واضحة لحماية التوقيع الإلكتروني من التزوير والإتلاف، فإن الحال لم يكن كذلك بالنسبة لسرقة بيانات أو منظومة إنشاء التوقيع الإلكتروني وإتلاف التوقيع الإلكتروني وهذا ما سيتم بيانه في فيما يلي:

**أولاً: سرقة بيانات أو منظومة إنشاء التوقيع الإلكتروني**

اذا ما أمعنا النظر في قانون التوقيع الإلكتروني السوري نجده خالياً من أي نص يجرم سرقة بيانات أو منظومة إنشاء التوقيع الإلكتروني على الرغم مما تنطوي عليه هذه الجريمة من خطورة كبيرة، ولعل المشرع السوري تأثر في ذلك بالقانون النموذجي الصادر عن لجنة الأمم المتحدة للقانون التجاري الدولي حيث أن الأخير لم يُجرم سرقة منظومة التوقيع الإلكتروني أو بيانات انشائه [١].

ويبرر أنصار هذا الاتجاه التشريعي المتبني فكرة عدم التجريم هذه بأن سرقة منظومة التوقيع الإلكتروني لا تظهر ولا يمكن اكتشافها إلا بعد استخدامها [٢].

وعليه بحسب أنصار هذا الاتجاه فإن تجريم سرقة منظومة التوقيع الإلكتروني يغدو أمراً

---

[١] خالد العبيدي، المرجع السابق، ص١٧٤

[٢] راجع في هذا الاتجاه، خالد العبيدي، المرجع السابق، ص١٧٤

لا قيمة له إذ لا إمكانية لاكتشاف السرقة إلا بعد استخدام المنظومة المسروقة، وفي هذه الحالة نُصبح أمام جريمة أخرى مختلفة تماماً عن السرقة وهي جريمة تزوير التوقيع الإلكتروني، والتي سبق القول إنها جريمة مركبة تنطوي على سرقة منظومة التوقيع الإلكتروني واستخدامها.

ولكن تجريم تزوير التوقيع الإلكتروني على النحو السابق لا يمكن اعتباره برأينا تجريماً لسرقة منظومة هذا التوقيع أو بيانات إنشائه وذلك استناداً لمبدأ الشرعية.

والأكثر من ذلك أن عدم استخدام المنظومة المسروقة يعني عدم قيام جريمة التزوير مع بقاء فعل السرقة خارج مظلة التجريم والعقاب، لأن السرقة حسب المادة ٦٢١/١ق.ع.س هي "أخذ مال الغير المنقول دون رضاه"، ولكن هذا النص لا يمكن تطبيقه من وجهة نظرنا في حال سرقة منظومة التوقيع الإلكتروني، لأن هذا النص يُعنى فقط بالسرقة التي يكون محلها مالاً مادياً والمنظومة المعلوماتية ليست مالاً مادياً وبالتالي فإن تجريم سرقتها يحتاج لنص خاص كما فعل مشرعنا بالنسبة للاحتيال حيث جرم وبنص خاص الاحتيال الواقع عبر الشابكة في المادة ٢١ من قانون مكافحة الجريمة المعلوماتية ، وفيه وسع المشرع مفهوم المال محل الاحتيال ليشمل إلى جانب

---

[1] م ٢١ /الاحتيال عن طريق الشابكة

يتبع...

المال المادي المعلومات والبرامج ذات القيمة المالية، وفي هذا التزام واضح بمبدأ الشرعية والذي يحتم على المشرع السوري أن يبقى ملتزماً به في مجال سرقة منظومة التوقيع الإلكتروني أو بيانات إنشائه من خلال إضافة نص خاص بذلك إلى قانون التوقيع الإلكتروني ليسد نقصاً في التشريع ما كان يجب على المشرع أن يغفل عنه.

**ثانياً: إتلاف التوقيع الإلكتروني**

إن البحث في قانون التوقيع الإلكتروني السوري يؤدي بنا إلى النتيجة نفسها التي وصلنا إليها عند البحث عن نص يُجرم سرقة بيانات أو منظومة إنشاء التوقيع الإلكتروني وهي عدم وجود نص خاص بذلك، إلا أن الحال يختلف بالنسبة لإتلاف

---

"/أ/ يعاقب بالحبس من ثلاث إلى خمس سنوات والغرامة من خمسمئة ألف إلى مليونين ونصف المليون ليرة سورية كل من استولى باستخدام الأجهزة الحاسوبية أو الشابكة على مال منقول أو عقار أو معلومات أو برامج ذات قيمة مالية أو سند يتضمن تعهداً أو إبراءاً أو أي امتياز مالي آخر وذلك عن طريق خداع المجني عليه أو خداع منظومة معلوماتية خاضعة لسيطرة المجني عليه بأية وسيلة كانت.

/ب/ وتكون العقوبة الاعتقال المؤقت والغرامة من خمسمئة ألف إلى مليونين ونصف المليون ليرة سورية في الحالات التالية:

١- إذا وقعت الجريمة على ثلاثة أشخاص فأكثر

٢- إذا تجاوز مبلغ الضرر مليون ليرة سورية

٣- إذا وقع الاحتيال على مصرف أو مؤسسة مالية

/ج/ ولا تطبق الأسباب المخففة التقديرية إلا إذا أسقط المضرور حقه الشخصي".

التوقيع الإلكتروني ذاته بغض النظر عن بياناته أو منظومة إنشائه، لأنه أمر غير متصور برأينا والسبب في ذلك أن آلية إتلاف التوقيع الإلكتروني تقتضي فنياً تعطيل الوسيلة الإلكترونية- المنظومة المعلوماتية- المستخدمة لإنشاء التوقيع الإلكتروني، وبالتالي فإن تعطيل منظومة انشاء التوقيع الإلكتروني ما هو إلا إتلاف للتوقيع الإلكتروني، وهذا ما أشار إليه المشرع صراحة في المادة ٤/٣١ من قانون التوقيع الإلكتروني.

خلاصة القول إن النقص الحاصل في خطة المشرع السوري في حماية التوقيع الإلكتروني – لجهة السرقة- إلى جانب الغموض الذي اكتنف خطته في حماية المعلومات – وفق النص الاحتياطي- يجعل الخطة التشريعية في حماية وثيقة العقد الإلكتروني ككل من **الاعتداءات التقليدية** خطة غير كافية، وغير موحدة ومنقوصة إلى حد كبير جداً، ولا تؤمن الحماية اللازمة لترسيخ الثقة في التعاقد الإلكتروني، وعلى المشرع إعادة النظر في هذه الخطة وذلك بتوضيح ما شابه الغموض وملء ما اعتراه النقص.

ولكن لو تساءلنا عن حال خطة مشرعنا في حماية التعاقد الإلكتروني من الاعتداءات المستحدثة وليس التقليدية، فسوف نجد الإجابة على ذلك في المبحث الآتي.

## المبحث الثاني

## مدى إحاطة المشرع بصور الاعتداءات المستحدثة

مما لا شك فيه أن الطابع التكنولوجي في العقد الإلكتروني أدى إلى ظهور أشكال جديدة من الاعتداء على هذا العقد لا يمكن تصورها في زمن العقد التقليدي، والحال نفسه ينطبق على التوقيع الإلكتروني.

وهذه الاعتداءات لم تكن في خطورتها أقل من تلك التقليدية المرتكبة بوسيلة إلكترونية، الأمر الذي أوجب على المشرع توسيع دائرة التجريم والعقاب ليشمل هذا الصنف المستحدث من الاعتداء، وهذا ما فعله المشرع السوري حيث جرّم صراحة مجموعة من هذه الاعتداءات والتي تكون المعلومات محلاً لبعضها في حين يكون التوقيع الإلكتروني محلاً للبعض الآخر، وفيما يلي بيان لهذه الاعتداءات وما إذا كان تجريمها يؤمن الحماية الكافية للعقد الإلكتروني أم لا.

ولتحقيق هذه الغاية تم تقسيم هذا المبحث إلى مطلبين:

المطلب الأول: صور الاعتداءات الواقعة على وثيقة العقد الإلكتروني

المطلب الثاني: الاعتداءات المتعلقة بالتوقيع الإلكتروني

## المطلب الأول

## صور الاعتداءات الواقعة على وثيقة العقد الإلكتروني

لعل أكثر ما يهدد وثيقة العقد الإلكتروني من اعتداءات مستحدثة هو اعتراض ما تتضمنه هذه الوثيقة من معلومات أثناء تداولها، إضافة إلى فك شفرة هذه المعلومات، وهذا ما سنناقشه بالتفصيل في الفرعين الآتيين.

### الفرع الأول: اعتراض الرسائل الخاصة بالتعاقد الإلكتروني

قد تتعرض الرسالة الإلكترونية المتضمنة الإيجاب أو القبول إلى الاعتراض أثناء إرسالها من الموجِب إلى الموجَب له أو بالعكس، واعتراض هذه الرسالة برأينا ما هو إلا اعتراض للمعلومات التي تتضمنها.

ورغبةً من المشرع السوري في حماية المعلومات أثناء تداولها نصَّ على تجريم اعتراض المعلومات صراحةً في المادة ١٨/فقرة أ/ من قانون تنظيم التواصل على الانترنت ومكافحة الجريمة المعلوماتية رقم ١٧ لعام ٢٠١٢ حيث جاء في نصها:

"المادة (١٨) اعتراض المعلومات..

/أ/ يعاقب بالحبس من ثلاثة أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة ألف

ليرة سورية كل من اعترض أو التقط قصداً بوجه غير مشروع المعلومات المتداولة على منظومة معلوماتية أو الشابكة أو تنصت عليها".

وهذه الفقرة توضح أركان جريمة اعتراض المعلومات، والتي نبينها فيما يلي، ثم ننتقل لدراسة اعتراض المعلومات المشفرة.

**أولاً: أركان جريمة اعتراض المعلومات**

يتمثل النشاط الجرمي في هذه الجريمة بفعل الاعتراض أو الالتقاط أو التنصت، وهناك من يرى أنه لا خلاف في المفهوم بين هذه الأفعال مادامت النتيجة الجرمية التي تؤدي إليها أي منها واحدة ألا وهي الوصول بوجه غير مشروع إلى المعلومات المتداولة على منظومة معلوماتية أو على الشابكة .[١]

ولكن حسب ما يتضح لنا فإن هناك فروقات بين صور النشاط الجرمي الثلاث، ولا سيما الاعتراض والتنصت، أما الاعتراض فنرى أنه يؤدي إلى عدم وصول المعلومات المرسلة إلى المرسل إليه أو قد يؤدي إلى تعديلها من قبل المعترض وإرسالها مُعدلة إلى المرسل إليه الأساسي دون علمه بالتعديل، وذلك ضمن ما يسمى في علم التقانة

---

[١] القاضي د. محمد طارق الخن، المرجع السابق، ص٤١

والشبكات (Man in the middle attack) ، أما التنصت فمعناه مراقبة المعلومات المتداولة ومعرفة مضمونها دون إجراء أي تعديل عليها .

وعدم مشروعية الوصول تعني أن الفاعل شخص غير مصرح له بالوصول إلى هذه المعلومات . [٣]

كما يُلاحظ من النص أن المشرع لم يحدد وسيلة الاعتراض وحسناً فعل حيث يمتلئ عالم التكنولوجيا بالبرامج التي تسمح باعتراض المعلومات، فهناك على سبيل المثال وسيلة تستخدم في اعتراض المعلومات وتُعرف بالتقاط الموجات الكهربائية وهي جمع للمعلومات عن بعد، إذ من الممكن جمع معلومات يتم إرسالها من أحد الحواسيب داخل مبنى وذلك باستعمال شاشة عرض يتم توصيلها بجهاز تسجيل خارج المبنى حيث يتم التقاط الموجات الكهربائية المحيطة بالحاسوب ليتم تحويلها إلى معلومات مقروءة على الشاشة . [٤]

---

[1]William Stallings- Cryptography and Network Security- Principles and Practice (6 the Edition) Pearson (2014) pdf, p 15-16.

[2]William Stallings, The previous reference, p 15-16.

[٣] القاضي د. محمد طارق الخن، المرجع السابق، ص٤١

[٤] نائلة عادل محمد فريد قورة، المرجع السابق، ص ٣٥٠

كما يُشير هذا النص بوضوح إلى أن الشرط الأساسي في اعتراض المعلومات هو أن تكون هذه المعلومات متداولة وليست مخزنة أي أثناء عملية إرسالها أو استقبالها .

ومن الجدير بالذكر في هذا السياق أن جريمة اعتراض المعلومات جريمة مقصودة تتطلب توافر القصد العام بعنصريه العلم والإرادة، أي يجب أن يعلم الفاعل أنه يعترض بغير حق معلومات الغير وأن تتجه إرادته إلى ذلك .

وهنا نسأل هل تقوم جريمة اعتراض المعلومات فيما لو كانت الأخيرة مشفرة؟

**ثانياً: اعتراض المعلومات المشفرة**

في الواقع تعد جريمة اعتراض المعلومات من الجرائم ذات النتيجة، والأخيرة مضمونها الوصول إلى المعلومات المتداولة، والوصول برأينا يعني الاطلاع على المعلومات وفهم معناها من خلال قراءتها على شاشة الحاسب – حسب المثال المذكور آنفاً- وبما أن المعلومات المشفرة معلومات غير مقروءة فمعنى ذلك أن الاطلاع على فحواها كنتيجة للاعتراض لم يتحقق، واذا ما انتفت النتيجة انتفى الركن المادي وانتفت الجريمة برمتها،

---

[١] القاضي د. محمد طارق الخن، المرجع السابق، ص٤١

[٢] القاضي د. محمد طارق الخن، المرجع السابق، ص٤٢

ولا يمكن أن يُسأل الفاعل في مثل هذه الحالة عن الشروع، والسبب في ذلك أن جريمة اعتراض المعلومات المنصوص عليها في الفقرة/أ/م ٢٨ من قانون تنظيم التواصل على الانترنت إنما هي جريمة ذات وصف جنحوي، والشروع في الجنح غير معاقب عليه من حيث المبدأ إلا اذا نص القانون صراحة على ذلك .

ولكن السؤال المطروح في حال اعتراض المعلومات المشفرة هو ما الحل فيما لو نجح الفاعل في فك الشفرة والاطلاع فعلاً على محتوى المعلومات؟

هل نطبق نص المادة ١٨/فقرة أ/ الخاص باعتراض المعلومات في ظل عدم وجود نص خاص يُجرم فك شفرة المعلومات؟

من وجهة نظرنا لا يمكن العودة لنص المادة ١٨/فقرة أ/ وتطبيقه في حال تمكن الفاعل من فك شفرة المعلومات المعترضة، لأنه وبعدم تمكن الفاعل من الاطلاع على المعلومات حال اعتراضها لكونها مُشفَّرة فإنه لا تقوم بحقه جريمة اعتراض المعلومات لتخلف أحد عناصر الركن المادي وهو النتيجة، وإذا ما قام بفك شفرة المعلومات

---

[1] تنص المادة ٢٠١ /فقرة ١/ من قانون العقوبات السوري على ما يلي:
"لا يعاقب على الشروع في الجنحة وعلى الجنحة الناقصة إلا في الحالات التي ينص عليها القانون صراحة".

المعتَرضة فمعنى ذلك أنه يقوم بنشاط ايجابي "**جديد**" يريد من خلاله الاطلاع على فحوى المعلومات المعترَضة ، وبالتالي نكون أمام اعتداء جديد يمكن أن تتعرض له المعلومات، الأمر الذي يُحتم علينا معرفة ما إذا كان هذا الاعتداء قد دخل مظلة التجريم والعقاب أم لا، وهو موضوع الفرع الثاني.

**الفرع الثاني: فك شفرة المعلومات**

يُعتبر التشفير اليوم من أفضل التقنيات التي أفرزتها التكنولوجيا لحماية المعلومات من الاطلاع عليها أو اجراء تعديل غير مرغوب به من قبل شخص لا يملك الصلاحية .

ولعل السؤال عن مفهوم التشفير هو ما يمكن أن يطرح بدايةً عند الحديث عن فك شفرة المعلومات، وتماشياً مع ذلك سنتعرض في هذا الفرع لتعريف التشفير أولاً ثم نبين موقف المشرع السوري من هذا الاعتداء.

**أولاً: تعريف التشفير**

التشفير هو "تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو اشارات لحماية هذه البيانات من اطلاع الغير عليها أو من تعديلها أو تغييرها" .

---

[١] د. خالد ممدوح ابراهيم، المرجع السابق، ص١٤٧

بمعنى آخر يمكننا القول إن التشفير هو عملية تحويل المعلومات والبيانات من الشكل المفهوم إلى الشكل غير المفهوم(المشفّر).

وتتم هذه العملية من خلال طريقة حسابية معقدة تستند إلى صيغ رياضية معقدة تسمى الخوارزميات، وتعتمد قوة وفاعلية التشفير على عاملين رئيسيين هما الخوارزمية وطول المفتاح مقدراً بالبت(Bits) [٢] .

وبالتالي فإن التشفير هو العلم الذي يستخدم الرياضيات للتشفير وفك التشفير ، وله نوعان أساسيان هما التشفير المتماثل والتشفير اللامتماثل.

١- التشفير المتماثل : [٤]

في هذا النوع من التشفير يستخدم كل من المرسل والمستقبل ذات المفتاح السري في تشفير وفك تشفير رسالة المعلومات، حيث يتفق الطرفان مسبقاً على كلمة المرور التي

---

[١] د. هدى قشقوش، الحماية الجنائية للتوقيع الإلكتروني، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، دبي، الفترة ما بين ١٠-١٢ مايو، المجلد الثاني، ٢٠٠٣، ص٥٩٠، بحث منشور على الرابط التالي:
http://slconf.uaeu.ac.ae/prev_conf/2003/2.pdf
تاريخ الزيارة: ٢٠١٤/٥/٢٥ الساعة ٤,٠٠ مساءً

[٢] د. خالد ممدوح ابراهيم، المرجع السابق، ص١٥١

[٣] د. خالد ممدوح ابراهيم، المرجع السابق، ص١٥٢

[٤] د. خالد ممدوح ابراهيم، المرجع السابق، ص١٥٧

ستستخدم بينهما. اذ وعندما يقوم المرسل بإرسال الرسالة يقوم بإدخال كلمة المرور إلى برنامج التشفير حيث يعمل الأخير على تحويلها إلى عدد ثنائي، وهذا العدد هو مفتاح تشفير الرسالة، وعند وصول رسالة المعلومات إلى المستقبل يستخدم الأخير كلمة المرور نفسها لفك شفرة الرسالة، حيث تقوم حينئذ البرمجيات بترجمة كلمة المرور مرة أخرى ليتشكل المفتاح الثنائي الذي يتولى إعادة النص المشفر إلى شكله المفهوم.

٢- التشفير اللامتماثل:

في هذا النوع من التشفير يستخدم المرسل والمستقبل مفتاحين أحدهما عام والآخر خاص، حيث يكون الأخير معروفاً لدى شخص واحد هو المرسل ويستخدمه الأخير لتشفير وفك تشفير رسالة المعلومات، أما المفتاح العام فيوجد لدى أكثر من شخص ويستخدم لفك شفرة رسالة المعلومات التي شفرها المفتاح الخاص، ويتم تأمين نظام التشفير اللامتماثل عن طريق بروتوكول الطبقات الأمنية (SSL) - هو اختصار ل Secure Socket Layers حيث يساعد هذا الأخير على التحقق من المفتاح العام، والتأكد من سلامة رسالة المعلومات وأنها لم تُحرّف أثناء إرسالها عبر الشابكة .

وفي هذا النوع من التشفير يتمتع المفتاحان الخاص والعام بخاصية هامة وهي أنه لو

---

[١] د. خالد ممدوح ابراهيم، المرجع السابق، ص١٥٨

عُرف أحد هذين المفتاحين لا يمكن معرفة المفتاح الآخر .

ولزيادة درجة أمان هذا النوع من التشفير فقد تم تطويره بنظام الخصوصية المتفوقة (PGP ) والذي لا يزال منيعاً حتى هذا اليوم، حيث يستخدم[٢] مفتاح بطول ١٢٨ بت بالإضافة إلى البصمة الإلكترونية لرسالة المعلومات .

وكما ذكرنا سابقاً فإن درجة الأمان والموثوقية في أي مفتاح تشفير تزداد كلما زاد طول هذا المفتاح، حيث أن الحد الأدنى لطول هذا المفتاح هو ٢٥٦ بت، كما وينصح باستخدام مفتاح بطول ٣٨٤ أو ٥١٢ أو ١٠٢٤ بت، بيد أن المصابين بهوس التشكك وحتى مقدمي خدمة التشفير يفضلون استخدام المفاتيح التي طولها ٢٠٥٦ بت، وهو الطول الذي يستنزف مجموع القوى الحسابية في العالم لآلاف السنين من البحث المستمر للوصول إلى التخمين الصحيح للمفتاح .

وبسبب أهمية التشفير في مجال عقود التجارة الإلكترونية فقد جاء النص عليه في العديد من القوانين منها ما جاء في المادة ٢٨ من القانون الفرنسي رقم

---

[١] د. هدى قشقوش، الحماية الجنائية للتوقيع الإلكتروني، المرجع السابق، ص٥٩٢

[٢] PGP هو اختصار ل Pretty Good Privacy

[٣] د. خالد ممدوح ابراهيم، المرجع السابق، ص١٥٨-١٥٩

[٤] د. خالد ممدوح ابراهيم، المرجع السابق، ص١٦١

١٩٩٠/١١٧٠و الخاص بتنظيم الاتصالات عن بعد والتي عرفت التشفير بأنه "كل الأعمال التي تهدف إلى تحويل معلومات أو إشارات واضحة عبر اتفاقات سرية، إلى معلومات أو إشارات غامضة للغير، أو إلى إجراء العملية العكسية عبر وسائل مادية أو معلوماتية مخصصة لهذا الغرض" [١].

وكذلك ما جاء في الفصل الثاني من الباب الأول من القانون التونسي رقم ٨٣ لعام ٢٠٠٠ بشأن المبادلات والتجارة الالكترونية والذي حدد التشفير بأنه: "إما استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول الى المعلومة بدونها ".

أما القوانين السورية الخاصة بالمعاملات الإلكترونية، وتنظيم التواصل على الانترنت، والتوقيع الإلكتروني فقد خلت من أي ذكر لبرامج التشفير، ما يعني أن اهتمام المشرع حتى الآن لم ينصرف إلى هذه البرامج والتي تعتبر شكلاً من أشكال الحماية التكنولوجية وإلى ما قد يقع عليها من اعتداءات تستوجب تشميلها بالتجريم والعقاب.

---

[١] د. خالد ممدوح ابراهيم، المرجع السابق، ص١٥٣

**ثانياً: عدم تجريم فك شفرة المعلومات في القانون السوري**

كنا ولا نزال نردد القول إن التطور التكنولوجي سلاحٌ ذو حدين، فمثلما أتاح التطور التكنولوجي إمكانية تشفير المعلومات وجعل سلطة فك هذا التشفير من صلاحية شخص معين، أتاح في الوقت نفسه العديد من الوسائل والأساليب التي تمكن من فك شفرة المعلومات من قبل أشخاص لا يملكون صلاحية ذلك.

ولكن المشكلة ليست في التطور التكنولوجي وإنما في بطء عجلة التشريع عن مواكبة هذا التطور، وما يؤكد حقيقة ذلك خلو القوانين السورية الخاصة بالمعاملات الإلكترونية، ومكافحة الجريمة المعلوماتية، والتوقيع الإلكتروني من أي نص يُعرف التشفير أو يجرم فك شفرة المعلومات، وهذا نقص تشريعي واضح وخطير كان أولى بالمشرع عدم الوقوع به، خصوصاً أن هذا الاعتداء يحمل في طياته تهديداً ومساساً بأمن وسرية المعلومات ويُعبر عن خطورة أكبر في شخصية فاعله، وبالتالي يجب على المشرع الإسراع في سد هذا النقص التشريعي وذلك من خلال تضمين قانون مكافحة الجريمة المعلوماتية تعريفاً واضحاً للتشفير ونصاً يُجرم فك شفرة المعلومات، سواء أكانت مُعترضة أم تم التوصل إليها من خلال الدخول غير المشروع إلى جهاز حاسوبي أو منظومة معلوماتية أو بأي طريق آخر، وذلك حتى تكتمل خطته في حماية المعلومات

مما قد يقع عليها من اعتداءات مستحدثة، و التي لم يكن التوقيع الإلكتروني بمنأى عنها حسب ما سنرى في المطلب الآتي.

## المطلب الثاني

## الاعتداءات المتعلقة بالتوقيع الإلكتروني

جرّم المشرع السوري مجموعة من الاعتداءات المستحدثة التي تنال من التوقيع الإلكتروني، وفي الفرعين التاليين بيانها إلى جانب بيان مدى كفايتها في حماية التوقيع الإلكتروني كأداة لتوثيق العقد الإلكتروني.

### الفرع الأول: الاعتداءات المتعلقة بشهادة التصديق وبيانات التوقيع الإلكتروني

نتناول في هذا الفرع مجموعة من الاعتداءات المستحدثة والتي عمل المشرع السوري على ادخالها ضمن مظلة التجريم والعقاب وهي على الشكل التالي.

**أولاً: إصدار شهادات تصديق إلكتروني دون ترخيص**

حصر المشرع السوري بالهيئة الوطنية لخدمات الشابكة مهمة الترخيص للجهات الراغبة في مزاولة أعمال إصدار شهادة التصديق الإلكتروني، وحظر في الوقت نفسه إصدار هذه الشهادة دون الحصول على هذا الترخيص .

---

[1] مادة٢٣

"أ . الهيئة هي الجهة المخولة حصراً بمنح التراخيص للجهات التي ترغب في مزاولة أعمال إصدار شهادات التصديق الإلكتروني أو أعمال تسجيل أسماء النطاقات تحت النطاق العلوي السوري .

ب . الهيئة هي الجهة المخولة بإصدار شهادات التصديق الإلكتروني للعاملين في الجهات العامة بصفاتهم

واعتبر الخروج على هذا الحظر جريمة معاقب عليها بصريح المادة ٣١ ف ١ حيث جاء فيها:

"مادة ٣١- مع عدم الاخلال بأي عقوبة أشد منصوص عليها في أي قانون آخر نافذ:

يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من خمسمئة ألف ليرة إلى مليوني ليرة سورية، كل من قام قصداً بارتكاب أحد الأفعال التالية:

١- إصدار شهادات تصديق الكتروني أو تقديم أية خدمات تتعلق بالتوقيع الالكتروني للعموم دون الحصول على الترخيص اللازم لذلك من الهيئة".

---

الوظيفية، ويحق لها العهدة بذلك لجهات أخرى مرخص لها وفق النواظم والضوابط التي يصدرها الوزير، بناء على قرار من مجلس إدارة الهيئة .

ج ـ يحق للهيئة ان تباشر بنفسها أعمال تسجيل أسماء النطاقات تحت النطاق العلوي السوري ".

مادة ٢٤ .

"لا يجوز مزاولة أي عمل في مجال إصدار شهادات التصديق الالكتروني في الجمهورية العربية السورية أو في مجال تسجيل أسماء النطاقات تحت النطاق العلوي السوري إلا بترخيص من الهيئة، وذلك لقاء بدل دوري يحدده مجلس إدارتها، ووفقاً لأحكام هذا القانون، وللإجراءات والنواظم والضوابط والضمانات التي يصدرها الوزير، بناء على قرار من مجلس إدارة الهيئة، وذلك مع مراعاة ما يلي :

1. أن يجري اختيار المرخص له في إطار من العلانية وتكافؤ الفرص .
2. أن يحدد مجلس إدارة الهيئة مدة الترخيص .
3. أن تحدد وسائل الإشراف والمتابعة التقنية"

وفي هذه الصورة من التجريم يتجلى السلوك الإجرامي بانتحال الجاني صفة مزود خدمات التصديق وذلك من خلال تقديمه الخدمات التي يقدمها مزود الخدمة، وتتمثل في إصدار شهادات تصديق إلكتروني وخدمات أخرى تتعلق أيضاَ بالتوقيع الإلكتروني، وكل ذلك دون الحصول على ترخيص من الهيئة الوطنية لخدمات الشابكة ، ولا شك أن هذه الجريمة القصدية تنطوي على جانب كبير من الخطورة كونها تمس الثقة الواجب توفرها في التوقيع الإلكتروني، ومنه إلى الوثائق الإلكترونية عامة والعقود الإلكترونية خاصة. ونظراً لخطورة هذه الجريمة تكاد لا تخلو القوانين الخاصة بالمعاملات الإلكترونية من النص عليها إذ قد سبق المشرع السوري إلى هذا النص المشرع المصري في م ٢٣/أ من قانون التوقيع الالكتروني المصري رقم ١٥ لعام ٢٠٠٤ ، وكذلك المشرع التونسي في الفصل ٤٦ من القانون الخاص بالمبادلات والتجارة الالكترونية رقم ٨٣ لعام ٢٠٠٠ .[١]

---

[١] د. عبد الفتاح بيومي حجازي، التجارة الالكترونية في القانون العربي النموذجي، المرجع السابق، ص ١٢٩

[٢] "مادة ٢٣ – مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من:

(أ) أصدر شهادة تصديق الكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة".

**ثانياً: الوصول غير المشروع إلى بيانات أو منظومة إنشاء توقيع إلكتروني**

جاء النص على هذه الجريمة في المادة ٣١ ف ٤ من قانون التوقيع الإلكتروني السوري وفيها:

"مادة ٣١- يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من خمسمئة ألف ليرة إلى مليوني ليرة سورية، كل من قام قصداً بارتكاب أحد الأفعال التالية:

٤- التوصل بأية وسيلة كانت إلى الحصول بغير حق على بيانات إنشاء توقيع إلكتروني أو منظومة إنشاء توقيع إلكتروني أو وثيقة إلكترونية، أو اختراق أي منها أو اعتراضها أو تعطيلها عن أداء وظيفتها".

والواضح من هذا النص أنه يتضمن أربع صور للتجريم سنعمل على بيانها فيما يلي باستثناء الصورة الرابعة وقد تناولناها مسبقاً بالشرح في البند المخصص لإتلاف التوقيع الإلكتروني.

---

[١] الفصل ٤٦

" يعاقب كل من يمارس نشاط مزود خدمات المصادقة الالكترونية بدون الحصول على ترخيص مسبق طبقا للفصل ١١ من هذا القانون بالسجن لمدة تتراوح بين شهرين و٣ سنوات وبخطية تتراوح بين ١,٠٠٠ و١٠,٠٠٠ دينار أو بإحدى هاتين العقوبتين".

*١ – الحصول بدون حق وبأية وسيلة على بيانات أو منظومة إنشاء توقيع إلكتروني:*

لا شك أن الحصول على بيانات أو منظومة إنشاء توقيع إلكتروني عندما يكون بدون حق فهو حصول غير مشروع، وعدم المشروعية هنا ممكن أن يتخذ صوراً عديدة منها ما يتم من خلال إساءة الائتمان شريطة أن يكون المال المعلوماتي " بيانات أو منظومة إنشاء التوقيع الإلكتروني " قد سلمت من المجني عليه إلى الجاني وفق أحد العقود الخمسة المحددة في المادة ٦٥٦ من قانون العقوبات السوري، وهي الوديعة والوكالة والاجازة والعارية والرهن، وعلى أساس ذلك يمكن أن يرتكب مزود خدمات التصديق جُرم الحصول غير المشروع على بيانات أو منظومة إنشاء توقيع إلكتروني عندما يختلف شخصه عن شخص من أنشأ منظومة التوقيع للمُوقع نفسه، ويقوم الأخير بتسليم هذه المنظومة بناء على عقد الوديعة مثلاً لمزود خدمات التصديق ويقوم الأخير بتغيير نيته ويستولي على المنظومة لنفسه .[١]

*٢ – اختراق بيانات أو منظومة إنشاء توقيع إلكتروني*

في الواقع تبدو لنا هذه الصورة من السلوك الإجرامي هي ذاتها التي نص عليها المشرع

---

[١] د. عبد الفتاح بيومي حجازي، التجارة الالكترونية في القانون العربي النموذجي، المرجع السابق، ص١٤٤ومابعدها.

السوري في المادة ١٥ من قانون تنظيم التواصل على الانترنت تحت اسم جريمة الدخول غير المشروع، وإن اقتصر محل الدخول هنا على بيانات أو منظومة إنشاء التوقيع الإلكتروني أو الوثيقة الإلكترونية.

وهذا الدخول يمكن أن يتم بأي وسيلة تقنية إذ ليس متصوراً الدخول المادي إلى أي من ذلك، وعليه يمكن أن يتم الاختراق من خلال استخدام كلمة السر إذا كان الجاني غير مخول باستخدامها أو من خلال كسر نظام الحماية الخاص بتلك البيانات أو المنظومة إن وجد .[١]

ويتضح من النص أيضاً أن المشرع عاقب على الاختراق المجرد وإن لم يترتب عليه أي نتيجة، مما يعني أن جريمة الاختراق موضوع البحث هي جريمة شكلية.

٣ – *اعتراض بيانات أو منظومة إنشاء التوقيع الإلكتروني*

تتحقق هذه الصورة من السلوك الإجرامي بأي عمل من شأنه ارباك نظام معالجة البيانات أو الوسيط المستخدم في إنشاء التوقيع الإلكتروني– منظومة إنشاء التوقيع

[١] راجع في معنى الاختراق، د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، المرجع السابق، ص ١٤٥ وما بعدها

الإلكتروني- على نحو يفسد وظيفته أو يمنعه من القيام بها .

ويبقى السؤال الأهم بعد هذا العرض عن موقف المشرع السوري من سرية بيانات المتعاقدين، ومدى صونه لها، وهو ما سيتجلى واضحاً في الفرع الآتي.

---

[1] د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، المرجع السابق، ص ١٤٧ وما بعدها.

**الفرع الثاني: إفشاء سرية بيانات المتعاقدين**

تقتضي طبيعة التعاملات الإلكترونية احترام الحق في سرية البيانات الخاصة بالعملاء ، وهذا ما كان محل اهتمام العديد من المشرعين في القوانين الخاصة بالتعاملات الإلكترونية، وما يهمنا من ذلك هو موقف المشرع السوري وخطته في حماية سرية البيانات الخاصة بالعملاء، وهذا ما سيتم بيانه من خلال الفقرتين الآتيتين:

**أولاً: المبدأ العام**

في إطار خطته الرامية لتأمين حماية متكاملة للتوقيع الإلكتروني اعتبر المشرع السوري البيانات الخاصة بإنشاء التوقيع الإلكتروني سرية، ولا يجوز لمن قُدمت إليه بحكم عمله إفشاؤها أو استخدامها في غير الغرض الذي خصصت من أجله، وهذا ما يشير إليه صراحة نص المادة ٤/ب من قانون التوقيع الإلكتروني السوري وقد جاء فيها:

"مادة ٤-

ب – تعد بيانات إنشاء التوقيع الإلكتروني والمعلومات التي تقدم إلى مزود خدمات التصديق الإلكتروني المرخص له بإصدار شهادات التصديق الإلكتروني سرية، ولا يجوز لمن قدمت إليه أو اتصل بها بحكم عمله إفشاؤها للغير أو استخدامها في غير الغرض

---

[١] د. هدى قشقوش، المرجع السابق، ص٥٨٠ وما بعدها.

الذي قدمت من أجله".

ولصون سرية هذه البيانات جرّم المشرع السوري إفشاء سريتها أو استخدامها في غير الغرض الذي قدمت من أجله، وهذا ما نصت عله المادة ٣١ ف ٦ من القانون ذاته حيث جاء فيها:

"مادة ٣١ – مع عدم الإخلال بأية عقوبة أشد منصوص عليها في أي قانون آخر نافذ:

يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من خمسمئة ألف ليرة إلى مليوني ليرة سورية، كل من قام قصداً بارتكاب أحد الأفعال التالية:

٦ – إفشاء أية بيانات تتعلق باستخدام التوقيع الإلكتروني أو التحقق من عائديته، أو استخدامها في غير الغرض الذي قدمت من أجله من قبل أحد العاملين لدى مزود خدمات التصديق الإلكتروني. ويكون المزود في هذه الحالة مسؤولاً بالتضامن عن الوفاء بما يحكم به العامل من غرامات إذا ثبت أن إخلال المسؤول عن الإدارة الفعلية للمزود بواجباته قد أسهم في وقوع هذه الجريمة".

وبموجب هذا النص فإن الجاني شخص له حق الاطلاع على هذه البيانات أو له صلة مشروعة بها كونه أحد العاملين لدى مزود خدمات التصديق الإلكتروني، والذي تُقدم

إليه هذه البيانات من قبل أصحابها للحصول على شهادة التصديق الإلكتروني .

وإفشاء السرية هنا معناه إخراج هذه البيانات من حيز الكتمان وإطلاع الغير عليها ممن ليس لهم الحق بذلك، وتختلف الدوافع وراء جريمة الإفشاء هذه إذ قد يكون الدافع لذلك الحصول على المال من خلال بيع هذه البيانات أو استخدامها في غرض غير مشروع كتهديد أصحابها أو ابتزازهم أو الضغط عليهم للقيام أو الامتناع عن القيام بعمل ما .[٢]

إلا أن بعض هذه القوانين يتيح الاطلاع على المعلومات السرية على سبيل الاستثناء، وفي حالات محددة منصوص عليها قانوناً، وهذا ما سنبينه في الفقرة الأتية:

**ثانياً: الاستثناء**

إذا كانت السرية في البيانات الخاصة بالمتعاقدين مبدأ عاماً جاء النص عليه في أغلب القوانين المتعلقة بالتوقيع الإلكتروني والمعاملات الإلكترونية، فإن الاستثناء على هذا المبدأ اقتصر على بعض هذه القوانين دون البعض الآخر، وما يهمنا من هذه القوانين

---

[١] د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت، المرجع السابق، ص ١٤٠ وما بعدها.

[٢] د. عبد الفتاح بيومي حجازي، التجارة الالكترونية في القانون العربي النموذجي، المرجع السابق، ص١٤٠

هو موقف المشرع السوري الذي يُشير الى خلو قانون التوقيع الإلكتروني من أي استثناء على مبدأ السرية في حين جاءت هذه الاستثناءات في قوانين أخرى نذكر منها المادة ٣١ من قانون إمارة دبي الخاص بالمعاملات والتجارة الالكترونية رقم ٢ لعام ٢٠٠٢ حيث جاء فيها:

"المادة ٣١

١- يُعاقب كل شخص تمكن بموجب أي سلطات ممنوحة له في هذا القانون من الاطلاع على معلومات في سجلات أو مستندات أو مراسلات إلكترونية، وأفشى متعمداً أياً من هذه المعلومات، بالحبس وبغرامة لا تجاوز 100.000 درهم، او بإحدى هاتين العقوبتين .وتكون العقوبة الغرامة التي لا تجاوز 100.000درهم في حالة تسببه بإهماله في إفشاء هذه المعلومات.

٢- يستثنى من أحكام الفقرة (١) من هذه المادة حالات التصريح التي تتم لأغراض هذا القانون، أو أي إجراءات جزائية حول جرم ارتكب بالمخالفة لأي قانون، أو لأغراض الأوامر الصادرة عن أية سلطة قضائية".

والحقيقة أنه لا ضير برأينا فيما لو اتبع المشرع السوري منهج المشرع الإماراتي في ذلك إذ أنه عندما يصدر إذن من السلطات القضائية بالاطلاع على هذه المعلومات فهو

أمر مبرر ما دام ذلك في خدمة وحماية المصلحة العامة.

ولكن لو تساءلنا هل كانت خطة المشرع السوري في حماية التوقيع الإلكتروني من خلال تجريم هذه الاعتداءات كافية أم لا؟

في الواقع وبالنظر إلى ما يمكن أن يتعرض له التوقيع الإلكتروني من اعتداءات نجد أن خطة المشرع السوري لم تكن متكاملة إذ كان يشوبها النقص لجهة عدم النص على بعض أهم أشكال الاعتداءات التي تنال من التوقيع الإلكتروني مما يجعل هذه الحماية غير قادرة على تأمين الثقة اللازمة بالتوقيع الإلكتروني.

فعلى سبيل المثال لم ينص المشرع السوري على تجريم مواصلة مزود الخدمة نشاطه بعد انتهاء مدة الترخيص أو إلغائه أو تعليق العمل به، كذلك لم ينص على تجريم استعمال شهادة التصديق الإلكتروني من قبل صاحبها بعد انتهاء صلاحيتها أو إلغائها، وأيضاً لم ينص على تجريم صناعة برنامج أو نظام معلوماتي لإعداد التوقيع الإلكتروني، تماماً كما لم ينص على جريمة فض مفاتيح التشفير.

وبالتالي لا بد للمشرع السوري أن يُوسع من نطاق حمايته للتوقيع الإلكتروني ليشمل هذه الأفعال – مستعيناً بالتجارب التشريعية المقارنة – وذلك بالتوازي مع ضرورة سنه

نصاً خاصاً يُجرم فك شفرة المعلومات وذلك كله في سبيل تأمين حماية متكاملة لوثيقة العقد الإلكتروني مما قد تتعرض له من اعتداءات مستحدثة.

**خلاصة الفصل الثاني:**

استعرضنا في هذا الفصل بيان مدى كفاية خطة المشرع السوري في حماية كل من العقد الإلكتروني والتوقيع الإلكتروني من الاعتداءات التقليدية، وكذلك المستحدثة التي يمكن أن يتعرضا لها، وذلك من خلال تحليل النصوص القانونية الخاصة ذات الصلة والمنصوص عليها في قانون التوقيع الإلكتروني وخدمات الشابكة رقم ٤ لعام ٢٠٠٩، وكذلك قانون تنظيم التواصل على الانترنت ومكافحة الجريمة المعلوماتية رقم ١٧ لعام ٢٠١٢، حيث تبين لنا بنتيجة هذا التحليل أن خطة المشرع غير كافية ومنقوصة إلى حد كبير جداً، فضلاً عن كونها غير موحدة، و بالتالي لا تؤمن الحماية اللازمة لترسيخ عوامل الأمان والثقة في التعاقد الإلكتروني ، وعلى المشرع إعادة النظر فيها وذلك بتوضيح ما شابه الغموض وملء ما اعتراه النقص، وذلك في ضوء المقترحات المقدمة في خاتمة هذا البحث.

**الخاتمة**

في نهاية هذا البحث لا بد لنا من استعراض النتائج التي توصلنا إليها إلى جانب بيان ما في جعبتنا من مقترحات.

**أولاً: النتائج**

١- بيّن هذا البحث إمكانية وقوع التزوير في المجال المعلوماتي وذلك من خلال عملية إسقاط أركان التزوير التقليدي على التزوير المعلوماتي.

٢- أظهر هذا البحث أن الحد الفاصل بين التزوير التقليدي ونظيره المعلوماتي إنما هو طبيعة المحرر محل التزوير فهو في الأول ذو طبيعة مادية يفتقر إليها في الثاني.

٣- أظهر هذا البحث عدم إمكانية انطباق نص المادة ٤٤٣ ق.ع.س والخاص بالتزوير فيما لو كان العقد الإلكتروني محلاً للاعتداء نظراً لكون هذا النص يتعامل مع عناصر الكتابة والمحرر والتوقيع ذوات المفهوم المادي (التقليدي).

٤- نتيجة عدم انطباق النصوص التقليدية وبعد التوجه إلى النصوص الخاصة تبين لنا أن المشرع السوري لم يأتِ بحماية صريحة للتعاقد الالكتروني وإنما جاءت الحماية من خلال نصوص متفرقة في عدة قوانين، منها ما كان خاصاً بحماية المعلومات بشكل

عام ومنها ما كان خاصاً بحماية التوقيع الالكتروني.

٥- تناول هذا البحث بالتحليل نص المادة ٢٨ من قانون مكافحة الجريمة المعلوماتية، حيث تبين أنه نص احتياطي عام وضعه المشرع ليشمل بالتجريم والعقاب كافة الاعتداءات التقليدية الواقعة على جهاز حاسوبي أو منظومة معلوماتية بقصد التأثير على عملها أو على المعلومات أو البيانات المخزنة عليها، كما تبين لنا من خلال هذا البحث أن هذا النص المذكور آنفاً مشوبٌ إما بالغموض أو النقص وذلك بسبب عدم وضوح موقف المشرع تجاه مفهوم البيانات والمعلومات وفيما إذا كان يستخدم مفهوم البيانات كمرادف لمفهوم المعلومات أم لا.

٦- على الرغم من تجريمه، وعلى وجه حسن، تزوير التوقيع الإلكتروني وكذلك إتلاف بيانات ومنظومة إنشاء التوقيع الإلكتروني تبين لنا بنتيجة البحث أن المشرع لم يُجرم مثلاً سرقة التوقيع الإلكتروني أو منظومة أو بيانات إنشائه.

٧- على الرغم من تجريمه اعتراض المعلومات، فإن المشرع لم ينص صراحة على حالة ما إذا كانت المعلومات المعترضة مشفرة، وفيما لو نجح الفاعل في فك شفرة الأخيرة فهل تقوم هنا جريمة جديدة أم تتحقق جريمة الاعتراض؟

٨- على الرغم من تجريمه مجموعة واسعة من الاعتداءات المستحدثة التي يمكن أن تنال من التوقيع الالكتروني، لم يُجرم المشرع صوراً من الاعتداءات لا تقل أهمية عن تلك التي جرمها ومنها جريمة صنع أو حيازة برنامج لإعداد توقيع الكتروني وكذلك جريمة فك مفاتيح التشفير وغيرها من الاعتداءات التي أتينا على ذكرها في البحث والتي كانت موضع التجريم والعقاب في عدد من القوانين المقارنة.

**ثانياً: المقترحات**

استناداً للنتائج السابقة وحتى يُؤتي هذا البحث ثماره في وضع خطة تشريعية مُتكاملة تُؤمن الحماية الكافية للعقد الإلكتروني، وانطلاقاً من كون التوقيع الإلكتروني جزءاً لا يتجزأ من العقد الإلكتروني، فإننا نوصي بإعادة صياغة قانون التوقيع الإلكتروني رقم /٤/ لعام ٢٠٠٩ متضمناً المقترحات التالية:

**١-** إضافة كافة الأحكام المتعلقة بالعقد الإلكتروني- والمنصوص عليها في القانون رقم ٣ لعام ٢٠١٤ والناظم للمعاملات الإلكترونية- إلى قانون التوقيع الإلكتروني رقم ٤ لعام ٢٠٠٩، ولا سيما من هذه الأحكام تعريف العقد الإلكتروني الوارد في المادة الأولى من قانون المعاملات الالكترونية والذي نقترح إعادة صياغته وفق التالي:

**العقد الإلكتروني: هو كل اتفاق يتم إبرامه بالوسائل الإلكترونية.**

**٢-** يجب على المشرع تضمين قانون التوقيع الإلكتروني تعريفاً للتشفير على غرار التعريفات الواردة في عدد من القوانين العربية ذات الصلة، ونقترح في هذا الصدد التعريف الوارد في القانون التونسي الخاص بالمبادلات والتجارية الإلكترونية رقم ٨٣ لعام ٢٠٠٠، وهو ذاته الوارد في المادة الثانية من قانون المعاملات الإلكترونية السوداني لعام ٢٠٠٧، وفيه:

**( التشفير: استعمال رموز أو إشارات غير متداولة تُصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها).**

**٣-** تعديل نص المادة ٣١ من قانون التوقيع الإلكتروني لتصبح على الشكل التالي:

مادة٣١—مع عدم الإخلال بأية عقوبة أشدّ منصوص عليها في أي قانون آخر

نافذ:

أ – يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من خمسمئة ألف ليرة سورية إلى مليوني ليرة سورية، كل من قام قصداً بارتكاب أحد الأفعال التالية:

(١) إصدار شهادات تصديق إلكتروني أو تقديم أية خدمات تتعلق بالتوقيع الإلكتروني للعموم دون الحصول على الترخيص اللازم لذلك من الهيئة.

**(٢) مواصلة مزود الخدمة نشاطه بعد انتهاء مدة الترخيص أو إلغائه أو تعليق العمل به.**

**(٣) استعمال شهادة التصديق الإلكتروني من قبل صاحبها بعد انتهاء صلاحيتها أو إلغائها.**

(٤) تزوير توقيع إلكتروني أو بيانات أو منظومة إنشاء توقيع إلكتروني، **وكذلك تزوير عقد إلكتروني أو أية وثيقة إلكترونية أخرى**، بأي طريق كان.

(٥) استعمال توقيع إلكتروني مزور أو منظومة إنشاء توقيع إلكتروني مزورة أو شهادة تصديق إلكتروني مزوّرة **أو عقد إلكتروني مزور أو أية وثيقة إلكترونية مزورة**، مع علمه بذلك.

(٦) التوصل بأية وسيلة كانت إلى الحصول بغير حق على بيانات إنشاء توقيع إلكتروني أو منظومة إنشاء توقيع إلكتروني أو وثيقة إلكترونية، أو اختراق أي منها أو اعتراضها أو تعطيلها عن أداء وظيفتها.

(٧) تقديم أوراق أو معلومات مزوّرة أو غير صحيحة بقصد الحصول على شهادة تصديق إلكتروني أو تعليق العمل فيها أو إلغائها.

**(٨) صناعة أو حيازة أو الحصول على برنامج أو نظام معلوماتي لإعداد التوقيع الإلكتروني دون موافقة صاحب الشأن.**

**(٩) فك مفاتيح تشفير التوقيع الإلكتروني.**

**(١٠) سرقة بيانات أو منظومة إنشاء التوقيع الإلكتروني، وكذلك سرقة وثيقة العقد الإلكتروني أو أية وثيقة إلكترونية أخرى.**

**(١١) اعتراض الرسائل الإلكترونية المتضمنة الإيجاب أو القبول أو المتضمنة وثيقة العقد الإلكتروني ذاتها.**

**(١٢) فك شفرة وثيقة العقد الإلكتروني أو الرسائل الإلكترونية المتضمنة الإيجاب أو القبول سواء أكانت متداولة أم مخزنة.**

**(١٣)** إفشاء أي بيانات تتعلق باستخدام التوقيع الإلكتروني أو التحقق من عائديته، أو استخدامها في غير الغرض الذي قُدِّمت من أجله من قبل أحد العاملين لدى مزوّد خدمات التصديق الإلكتروني .ويكون المزوّد في هذه الحالة مسؤولاً بالتضامن

عن الوفاء بما يُحكم به العامل من غرامات إذا ثبت أن إخلال المسؤول عن الإدارة الفعلية للمزوّد بواجباته قد أسهم في وقوع هذه الجريمة.

**يستثنى من أحكام هذه المادة (٤) حالات التصريح التي تتم لأغراض هذا القانون، أو أي إجراءات جزائية حول جرم ارتكب بالمخالفة لأي قانون، أو لأغراض الأوامر الصادرة عن أية سلطة قضائية.**

ب – وتكون العقوبة الأشغال الشاقة المؤقتة إضافة إلى الغرامة المذكورة في الفقرة السابقة إذا ارتُكب تزوير التوقيع الإلكتروني أو استُعمل التوقيع المزور على وثيقة رسمية.

ج – وفى جميع الأحوال، يُحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الانتشار على الأقل، وعلى شبكات المعلومات الإلكترونية المفتوحة، وذلك على نفقة المحكوم عليه.

**٤–**لا بد من وضع تعريف خاص للبيانات في قانون مكافحة الجريمة المعلوماتية وفي هذا الصدد نقترح التعريف التالي:

**البيانات: هي المواد الخام للمعلومات، أو هي المعلومات في مرحلة المعالجة**

**الآلية.**

**٥-**ينبغي تعديل نص المادة ٢٨/ب/٢ من القانون المذكور آنفاً ليشمل الاعتداءات الواقعة على البيانات والمعلومات على حد السواء، وفي سبيل ذلك نقترح النص التالي:

/ب/ يضاعف الحدّ الأدنى للعقوبة المقرّرة لأيّ من الجرائم المنصوص عليها في القوانين الجزائيّة النّافذة الأخرى في الحالات التالية:

١) إذا ارتُكبت الجريمة باستخدام الشابكة أو وقعت عليها.

٢) إذا وقعت الجريمة على الكيان المنطقي للجهاز الحاسوبي أو المنظومة المعلوماتيّة بقصد التّأثير على عملها.

**٣) إذا وقعت الجريمة على البيانات أو المعلومات سواء أكانت الأخيرة مخزنة بشكل نهائي أو مؤقت.**

**٦-**يجب على المشرع النص على تجريم فك شفرة المعلومات سواء أكانت الأخيرة مخزنة أم متداولة عبر الشابكة، وذلك في القانون الخاص بمكافحة الجريمة المعلوماتية، وفي سبيل ذلك نقترح النص التالي:

**فك شفرة المعلومات..**

**يُعاقب بالحبس من ستة أشهر إلى ثلاث سنوات كل من قام دون حق بفك**

**شفرة المعلومات سواء أكانت الأخيرة متداولة أم مخزنة.**

**٧-** بما أن صور الاعتداءات المستحدثة التي تنال من استقرار التعاقد الإلكتروني في تزايد مستمر بسبب التطور التكنولوجي، فإنه يجب على المشرع أن يراعي المرونة في صياغة النصوص الجزائية ذات الصلة بموضوع بحثنا حتى تستوعب هذه الصور مستقبلاً بما لا يتعارض مع مبدأ الشرعية.

وفي الختام

هذا خالص جهدي

فإن أصبت فبتوفيق من الله

وإن أخطأت فمني ومن الشيطان

وما العصمة عن الخطأ إلا من شأن الأنبياء

## قائمة المراجع

### أولاً: المراجع باللغة العربية

**١– الكتب:**

**أ– الكتب العامة:**

– د. رمسيس بهنام، الجرائم المضرة بالمصلحة العامة، منشأة المعارف بالإسكندرية، ١٩٨٦

– القاضي عبد الوهاب بدرة، جرائم التزوير في التشريع السوري، الطبعة الجديدة، دمشق، بلا تاريخ نشر.

– د. علي عبد القادر قهوجي، قانون العقوبات، القسم الخاص، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠٠١

– د. عوض محمد، الجرائم المضرة بالمصلحة العامة، دار المطبوعات الجامعية، الإسكندرية ،١٩٨٥

– د. فوزية عبد الستار، شرح قانون العقوبات –القسم الخاص– دار النهضة العربية،١٩٨٨

- د. مأمون محمد سلامة، قانون العقوبات-القسم الخاص- ج١، الجرائم المضرة بالمصلحة العامة، دار الفكر العربي،١٩٨٣.

- د. محمد وحيد الدين سوار، شرح القانون المدني- النظرية العامة للالتزام - ج١، جامعة دمشق، ٢٠٠٦

- د. محمود نجيب حسني، شرح قانون العقوبات-القسم الخاص- دار النهضة العربية، ١٩٩٢.

**ب- الكتب المتخصصة:**

- د. أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، دار النهضة العربية، القاهرة،٢٠٠٠

- د. أسامة أحمد بدر، حماية المستهلك في التعاقد الإلكتروني، دراسة مقارنة، دار النهضة العربية، ٢٠٠٥

- د. إيمان مأمون أحمد سليمان، إبرام العقد الإلكتروني وإثباته، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٨

- د. أيمن عبد الله فكري، جرائم نظم المعلومات، دار الجامعة الجديدة، الإسكندرية،٢٠٠٧

– د. ايهاب فوزي السقّا، جريمة التزوير في المحررات الإلكترونية، دار الفكر العربي، ٢٠٠٨

– د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول – الجرائم الناشئة عن استخدام الحاسب الآلي، ط١، دار النهضة العربية، القاهرة،١٩٩٢

– د. خالد ممدوح إبراهيم، التوقيع الإلكتروني، الدار الجامعية، ٢٠١٠

– د. خالد بن سليمان الغثبر و د. المهندس محمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، جامعة الملك سعود، ط١، ٢٠٠٩

– أ. رحيمة الصغير ساعد نمديلي، العقد الإداري الإلكتروني، دراسة تحليلية مقارنة، دار الجامعة الجديدة، ٢٠٠٧

– د. سامح عبد الواحد التهامي، التعاقد عبر الإنترنت، دار الكتب القانونية، مصر، ٢٠٠٨

– د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر ٢٠٠٢

– د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي

لمكافحة جرائم الكمبيوتر والانترنت، دار الكتب القانونية، ٢٠٠٧

– عفيفي كامل عفيفي، تقديم أ. د فتوح الشاذلي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، منشورات الحلبي الحقوقية، ٢٠٠٣

– د. عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، بدون ناشر، ١٩٩٥

– د. عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، ٢٠٠٢

– د. لورانس محمد عبيدات، إثبات المحرر الإلكتروني، دار الثقافة للنشر والتوزيع، ط١، عمان، ٢٠٠٥

– د. ماجد عمار، المسؤولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية، ١٩٨٩

– د. محمد حمّاد مرهج الهيتي، جرائم الحاسوب، دار المناهج للنشر والتوزيع، ط١، ٢٠٠٦

– محمد السعيد رشدي، حجية وسائل الاتصال الحديثة في الإثبات، بدون تاريخ نشر.

– القاضي الدكتور محمد طارق الخن، الجريمة المعلوماتية، الجامعة الافتراضية السورية، ٢٠١٢ (ملف pdf).

– د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بلا سنة نشر.

**٢– الرسائل العلمية:**

–خالد بن عبد الله بن معيض العبيدي، الحماية الجنائية للتعاملات الإلكترونية في نظام المملكة العربية السعودية (دراسة تحليلية مقارنة)، رسالة ماجستير، جامعة نايف للعلوم الأمنية، ٢٠٠٩.

– فراس محمد وليد عدي، إبرام العقد بالوسائط الإلكترونية، رسالة دكتوراه، جامعة دمشق ،٢٠١٠.

– محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، رسالة ماجستير، جامعة القاهرة، ٢٠٠٤.

**٣– الأبحاث والمقالات:**

– حنان مليكة (طالبة دكتوراه)، النظام القانوني للتوقيع الإلكتروني في ضوء قانون التوقيع الإلكتروني السوري رقم٤ لعام ٢٠٠٩، مجلة جامعة دمشق للعلوم الاقتصادية

والقانونية، المجلد ٢٦، العدد الثاني، ٢٠١٠، ص٥٦٢-٥٦٤.

- د. عبد الجبار الحنيص، الحماية الجزائية لبطاقات الائتمان الممغنطة من التزوير، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية – المجلد ٢٤- العدد الثاني- ٢٠٠٨، ص١٥٦-١٦٢.

**٤- الأبحاث المنشورة على الشابكة:**

- أسامة بن غانم العبيدي، جريمة الإتلاف المعلوماتي، بحث منشور على الموقع الإلكتروني التالي:

http://informationstudies.net/issue_list.php?action=getbody&titleid=56

تاريخ الزيارة:٢٠١٥/٧/٣، الساعة ١١,١٥صباحاً

- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، دراسة مقارنة، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، دبي، الفترة ما بين ١٠-١٢ مايو، المجلد الثاني، ٢٠٠٣، بحث منشور على الموقع الإلكتروني التالي:

http://slconf.uaeu.ac.ae/prev_conf/2003/2.pdf

تاريخ الزيارة:٢٠١٤/٥/٢٥، الساعة ٤,٠٠ مساءً

- د. هدى قشقوش، الحماية الجنائية للتوقيع الإلكتروني، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، دبي، الفترة ما بين ١٠-١٢ مايو، المجلد الثاني، ٢٠٠٣، بحث منشور على الموقع التالي:

http://slconf.uaeu.ac.ae/prev_conf/2003/2.pdf

تاريخ الزيارة:٢٠١٤/٥/٢٥، الساعة ٤,٠٠ مساءً

**٥- القواميس التكنولوجية:**

- د. عبد الحسن الحسيني، القاموس الموسوعي في المعلوماتية والاتصالات والمعلوماتية القانونية، ط١، مكتبة صادر، بيروت، ٢٠٠٤

**ثانياً: المراجع باللغة الإنكليزية**

- Joyrup Bhattacharya, Rudiments of Computer Science, Academic Publishers, (pdf).

- Martha Henderson Hurley –Dena Hanley, Correctional Administration and Change Management, Taylor & Francis Group, an inform business, (pdf).

- Ralph M. Stair and George W. Reynolds, Fundamentals of information systems, Eighth Edition, (pdf).

William Stallings- Cryptography and Network Security- Principles and Practice (6 the Edition) Pearson (2014), (pdf).

.....

**الفهرس**

**المقدمة**.....**1**

**الفصل الأول: مدى صلاحية قانون العقوبات لحماية التعاقد الإلكتروني**....**5**

المبحث الأول: محل الحماية.....7

المطلب الأول: مفهوم العقد الإلكتروني.....8

الفرع الأول: ماهية العقد الإلكتروني.....9

أولاً: تعريف العقد الإلكتروني.....9

١- التعريفات القانونية.....9

٢- التعريفات الفقهية.....10

ثانياً: خصائص العقد الإلكتروني.....12

الفرع الثاني: وسائط التعاقد الإلكتروني.....15

أولاً: التعاقد عبر الويب.....16

ثانياً: التعاقد عبر البريد الإلكتروني.....17

المطلب الثاني: تكوين العقد الإلكتروني.....19

الفرع الأول: ابرام العقد الإلكتروني.....19

أولاً: مدى امكانية ابرام العقد إلكترونياً في إطار النظرية العامة للعقود.....19

ثانياً: ابرام العقد الإلكتروني في إطار النصوص الخاصة.....23

الفرع الثاني: توثيق العقد الإلكتروني (التوقيع الإلكتروني) .....28

أولاً: تعريف التوقيع الإلكتروني.....29

١- التعريفات القانونية.....29

٢- التعريفات الفقهية.....31

ثانياً: الشروط الواجب توفرها في التوقيع الإلكتروني .....32

ثالثاً: وظائف التوقيع الإلكتروني.....33

رابعاً: صور التوقيع الإلكتروني.....33

١- التوقيع الرقمي.....34

٢- التوقيع البيو ميتري.....35

٣- التوقيع بالقلم الإلكتروني.....35

المبحث الثاني: تزوير العقد الإلكتروني.....37

المطلب الأول: مدى تحقق أركان التزوير التقليدي في التزوير المعلوماتي.....38

الفرع الأول: الركن المادي.....39

أولاً: تحريف الحقيقة.....39

ثانياً: التحريف في محرر.....41

ثالثاً: إمكانية حصول ضرر.....48

الفرع الثاني: الركن المعنوي.....51

المطلب الثاني: مدى إمكانية تحقق التزوير المعلوماتي بالطرق التقليدية.....53

الفرع الأول: التزوير المادي.....53

الفرع الثاني: التزوير المعنوي.....59

**الفصل الثاني: مدى كفاية التشريعات الجزائية الخاصة في حماية التعاقد الإلكتروني..... 68**

المبحث الأول: مدى شمول الاعتداءات التقليدية بالنصوص الخاصة .....70

المطلب الأول: مدى كفاية النص الاحتياطي في حماية العقد الإلكتروني.....71

الفرع الأول: كيفية معالجة الجرائم التقليدية الواقعة في الإطار التكنولوجي.....73

أولاً: وجوب فرض العقوبة الأشد.....73

ثانياً: شمول التجريم للجرائم التقليدية المرتكبة في الوسط التكنولوجي.....74

١- مفهوم البيانات والمعلومات.....76

٢- موقف المشرع السوري.....79

الفرع الثاني: مواطن القصور في النص.....80

أولاً: عدم وضوح موقف المشرع حيال مفهومي البيانات والمعلومات.....80

ثانياً: إمكانية تعرض المعلومات للاعتداء قبل مرحلة التخزين.....82

المطلب الثاني: مدى كفاية الحماية الخاصة بالتوقيع الإلكتروني.....84

الفرع الأول: المساس بموثوقية التوقيع الإلكتروني.....86

أولاً: تزوير التوقيع الإلكتروني.....86

ثانياً: إتلاف بيانات أو منظومة إنشاء التوقيع الإلكتروني.....90

الفرع الثاني: اعتداءات لم يجرمها المشرع.....93

أولاً: سرقة بيانات أو منظومة إنشاء التوقيع الإلكتروني.....93

ثانياً: إتلاف التوقيع الإلكتروني.....95

المبحث الثاني: مدى إحاطة المشرع بصور الاعتداءات المستحدثة.....97

المطلب الأول: صور الاعتداءات الواقعة على وثيقة العقد.....98

الفرع الأول: اعتراض الرسائل الخاصة بالتعاقد الإلكتروني.....98

أولاً: أركان جريمة اعتراض المعلومات.....99

ثانياً: اعتراض المعلومات المشفرة.....101

الفرع الثاني: فك شفرة المعلومات.....103

أولاً: تعريف التشفير.....103

ثانياً: عدم تجريم فك شفرة المعلومات.....108

المطلب الثاني: الاعتداءات المتعلقة بالتوقيع الإلكتروني.....110

الفرع الأول: الاعتداءات المتعلقة بشهادة التصديق وبيانات التوقيع.....110

أولاً: إصدار شهادات تصديق إلكتروني دون ترخيص.....110

ثانياً: الوصول غير المشروع إلى بيانات أو منظومة إنشاء التوقيع الإلكتروني..113

الفرع الثاني: إفشاء سرية بيانات المتعاقدين.....117

أولاً: المبدأ العام.....117

ثانياً: الاستثناء.....119

الخاتمة.....124

قائمة المراجع.....134

الفهرس.....142