

جامعة محمد خيضر بسكرة  
كلية الحقوق والعلوم السياسية  
قسم الحقوق

# جريمة تزوير الوثيقة الرسمية الإدارية

## ذات الطبيعة المعلوماتية

أطروحة مقدمة لنيل شهادة دكتوراه علوم تخصص قانون جنائي

إعداد الطالبة :

براهمي حنان

إشراف :

الأستاذ الدكتور عمر فرحاتي

لجنة المناقشة :

رئيسا	أستاذ التعليم العالي - جامعة بسكرة -	أ.د. عزري الزين
مشرفا	أستاذ التعليم العالي - جامعة بسكرة -	أ.د. فرحاتي عمر
ممتحنا	أستاذ التعليم العالي - جامعة المسيلة -	أ.د. فريجة حسين
ممتحنا	أستاذ محاضر أ - جامعة بسكرة -	د. حوحو رمزي
ممتحنا	أستاذ محاضر أ - جامعة ورقلة -	د. بن محمد محمد
ممتحنا	أستاذ محاضر أ - جامعة باتنة -	د. دراجي عبد القادر

السنة الجامعية 2014 / 2015

# اهداء

إلى روح زوجي الطاهرة " الطاهر "

إلى شمسي و قمري " أمي \*\*\* أبي "

إلى قرة عيني ابني " أحمد صابر "

إلى " اخوتي و أخواتي "

إلى جميع " الأساتذة " الذين أشرفوا على تكويني

إلى كل " طالب للعلم و المعرفة "

# شكر وتقدير

الشكر "لله" الذي أعانني على إتمام هذا العمل .

ثنائي على زوجي الذي زرع بذرة هذا البحث ، وسقتها الأيام والسنين .

الشكر والتقدير لأستاذ الدكتور " عمر فرحاتي " مشرفا على هذه الأطروحة، بدعمه وتحفيزه المتواصل.

شكر خاص لأخي " محمد " الذي رافقني وساعدني خلال تربيصاتي العلمية .

الشكر الجزيل لمن أشرفت على الإخراج المطبعي لهذه الأطروحة " سميرة " .

أشكر كل من ساعدني في جمع هذه المادة العلمية من مختلف الجامعات والمكتبات بالجزائر، مصر، سوريا، الإمارات العربية المتحدة .

الشكر والتقدير لكل الأساتذة الذين ساهموا في تكويني العلمي .

شكرا لكل من أعانني ولو بكلمة طيبة .

## مقدمة :

شهدت البشرية في منتصف القرن 20 بداية ثورة المعلومات والاتصالات والتكنولوجيا الرقمية المعتمدة على الحاسب الآلي ، حيث استعملت هذه التكنولوجيا في البداية في مجالات مهمة وحساسة ، مما جعل نطاقها يتسع فيما بعد في مختلف المجالات الحياتية ، مغيرة بذلك من نمط الكثير منها ، وقد زاد من اتساع هذا النطاق وسرعة التغيير التزاوج الذي حصل بين التقنية الرقمية وشبكة الاتصالات للإنترنت، مما انعكس على طبيعة أعمال المنظمات عند القيام بأنشطتها وتحقيق أهدافها، حيث بدأت تتحول نحو النموذج الإلكتروني، ثم انتقل هذا النموذج إلى الإدارة العامة عند إنجاز معاملاتها المختلفة لتتحول تدريجيا من البيئة الورقية إلى البيئة الافتراضية، لتصل في مستوى متقدم إلى إدارة عامة رقمية، تتعامل بوثائق ذات طبيعة معلوماتية تتناسب مع هذه البيئة.

إن ازدياد نسبة التعامل بهذه الوثائق كان له دورا ايجابيا في تقليص التكاليف والوقت والحد من التضخم الورقي، وتحسين أداء الخدمة للمتعامل، لكنه في نفس الوقت حمل معه مخاطر الاعتداءات على هذا النوع من الوثائق في أشكال مستحدثة استفادت من تكنولوجيا المعلومات والاتصالات في اتجاه سلبي وغير مشروع .

لقد أصبحت هذه الاعتداءات تشكل هاجسا كبيرا يهدد مكاسب الثورة الرقمية ليس فقط بالنسبة للأفراد، أو في إطار محلي محدود ، بل على مستوى واسع وفي فضاء دولي مفتوح، بسبب تطورها وازدياد حجمها بعلاقة طردية مع تطور المعلوماتية جعلها تأخذ طابعا جرميا لمساسها بمصالح محمية جنائيا ، ومن المصالح المحمية جنائيا بنصوص القوانين الجنائية تلك المصلحة المرتبطة بالثقة العامة في الوثائق الرسمية من خلال تجريم الإعتداء عليها بالتزوير ، لكن الطبيعة المستجدة للوثيقة لا سيما الوثيقة الرسمية الإدارية حملت تحديات في مواجهة النص الجنائي التقليدي - النص المتعلق بتزوير الوثيقة الرسمية الورقية - من حيث مبدأ الشرعية وحظر القياس ، مما جعل الجهود

التشريعية تتكاثف وتتعاون دوليا في مواجهة هذا النوع من الجرائم التي تعتبر من أخطر الجرائم المرتكبة عن طريق الحاسب الآلي .

## 1- أهمية البحث :

أصبحت الإدارة العامة تعتمد على الوثيقة المعلوماتية في إنجاز وتسيير أعمالها في مختلف المستويات، أو عند أداء الخدمات للمتعاملين معها ، وذلك نتيجة التوجه نحو نظام الحكومة الإلكترونية التي تعتمد على أجهزة الحواسيب المرتبطة بشبكة داخلية، كما تعتمد على شبكة الإنترنت لربط هذه الشبكة بغيرها من الشبكات .

إن الإ اعتماد على هذه البيئة الإلكترونية يعني أن المعلومات ستكون معالجة آليا، فإذا كانت هذه المعلومات تثبت حقا أو مركزا قانونيا، أو لها أثر قانوني معين فإن التلاعب فيها إضرارا بالغير يثير مسألة مدى اعتبار هذا الفعل تزويرا ، وفيما إذا كانت الوثيقة المعلوماتية تعتبر محررا في إطار النص الجنائي التقليدي، باعتبار أن التزوير هو تغيير للحقيقة في محرر بقصد استعماله فيما أعد له مما يولد ضررا للغير ، ولما كانت العلة في تجريم التزوير هي حماية الثقة في المحرر عند تداوله بين الأفراد، فإن مسألة حماية الثقة عند التعامل بالوثيقة المعلوماتية تصبح أكثر أهمية إذا كانت هذه الوثيقة تخص إدارة عامة أو موقعة من موثق أو من هو مكلف بذلك قانونا .

إن هذه الثقة ناتجة مما يتمتع به المحرر من قيمة ثبوتية خاصة إذا كان محررا رسميا، لذا اتجهت الجهود التشريعية والفقهية إلى مناقشة قيمة الوثيقة المعلوماتية في الإثبات مقارنة بالمحرر الورقي ، حيث يرتبط تجريم تزوير هذه الوثيقة بمدى اعتبارها دليلا للإثبات في إطار التشريع المتعلق بالإثبات ، ولذلك أصبحت أغلب النظم التشريعية الحديثة في الإثبات تتناول مسألة الإثبات في المعاملات الإلكترونية لكنها تختلف في اتجاهاتها، وهو ما انعكس على التشريعات الجنائية في تجريم تزوير الوثيقة المعلوماتية بصفة عامة .

## 2- أسباب اختيار موضوع البحث :

يمكن حصر أسباب اختيار موضوع البحث فيما يلي :

1. انعكاسات ثورة المعلوماتية على طبيعة الوثائق المتداولة إداريا ، وارتفاع نسبة المعاملات المعتمدة على الحاسب الآلي لدى الجهات الإدارية العامة.
2. ارتفاع نسبة الغش المعلوماتي بتنامي دور المعلوماتية ، ومن أخطر صوره التزوير باعتباره يمس بوثيقة ذات قيمة قانونية، خاصة إذا كانت صادرة عن جهة إدارية عامة .
3. تأثير المعلوماتية على النظم القانونية المتعلقة بالإثبات من حيث تحديدها لمفهوم الوثيقة وكيفية انشائها وتداولها، وطريقة حفظها ، وتحديد قيمتها القانونية .
4. الجدل التشريعي والفقهى حول القيمة القانونية للوثيقة المعلوماتية في الإثبات .
5. امتداد الجدل التشريعي والفقهى حول القيمة القانونية للوثيقة المعلوماتية في الإثبات إلى مناقشة إمكانية وقوع التزوير فيها ، نظرا للإرتباط بين قانون الإثبات والنص الجنائي المجرم للتزوير .
6. اختلاف الصيغ التشريعية في تجريم تزوير الوثيقة المعلوماتية .

## 3- الخلفية النظرية للبحث :

لقد تناولت مجموعة من الدراسات والبحوث العلمية جريمة تزوير الوثيقة ذات الطبيعة المعلوماتية ضمن أطر مختلفة قد تتسع أو تضيق أحيانا ، حيث تطرق البعض منها لهذه الجريمة ضمن " نظرية عامة للجرائم المعلوماتية"، بينما تناولها البعض الآخر ضمن " الحماية الجنائية للمستند الإلكتروني"، فيما ركزت بعض الدراسات القليلة على البحث في " جريمة تزوير المحرر الإلكتروني ضمن نظرية عامة "، والبعض الآخر تناول بعض أصناف التزوير المعلوماتي " كتزوير التوقيع الإلكتروني " .

ولذلك سنتناول الدراسات السابقة ضمن الترتيب المذكور أعلاه وهي كالتالي :

أ- " الحماية الجنائية للبيانات المعالجة الكترونيا " للدكتور " علي عبد القادر القهوجي " وهو عبارة عن بحث مقدم لمؤتمر " القانون والكمبيوتر والإنترنت " لجامعة الإمارات

العربية المتحدة في "مايو 2000" حيث تطرق لجريمة التزوير المعلوماتي معتمدا التشريع الفرنسي نموذجا، منطلقا من اعتبار تلك العمليات ذات الآثار القانونية الهامة والخطيرة التي يقوم بها الحاسب الآلي لا يصدق عليها وصف المستند في القانونين المدني والجنائي، مما أثار شكا حول دلالتها في الإثبات وإمكانية وقوع جريمة التزوير العادية عليها، وهو ما خلق وضعاً تشريعياً صعباً ، ولذلك كان التدخل التشريعي الفرنسي ذو أهمية بالغة من خلال توسيع صيغة النص المجرم للتزوير .

ب- " جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون " للمؤلفين " فتوح الشاذلي " ، " عفيفي كامل عفيفي " عام "2003"، حيث تناول في الفصل الرابع " الحماية الجنائية للبيانات في إطار جرائم التزوير "، وقد إنطلقا من اصطدام تطبيق النص التجريمي المتعلق بالتزوير على التلاعب في البيانات لعدم وجود محرر، مما أدى اختلاف التشريعات المقارنة بشأن التغلب على هذه الصعوبة، وقد سلما بأن نص التزوير التقليدي لا ينطبق على تغيير الحقيقة في المعلومات المعالجة آلياً ، ولذلك لابد من تحديد عناصر التزوير المعلوماتي.

ج- " الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت " للدكتور " عبد الفتاح بيومي حجازي " عام "2005"، حيث تناول في الفصل الثاني من هذه الدراسة " جريمة التزوير المعلوماتية " مناقشا الإتجاهات التشريعية المختلفة في تجريم التزوير المعلوماتي، والجدل الفقهي حول مفهوم الوثيقة المعلوماتية محل التزوير، والإتجاهات المتعلقة بتحديد القيمة الثبوتية للوثيقة المعلوماتية لربطها بمدى وقوع التزوير من عدمه ، كما حاول حصر جوانب نظرية التزوير سواء كانت الوثيقة رسمية أو عرفية بمناقشة طرق تزويرها والضرر المترتب على ذلك.

د- " جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن " للمؤلف " بلال أمين زين الدين " عام "2008" ، حيث تناول في المبحث الثاني من هذه الدراسة " جريمة التزوير المعلوماتي " من خلال عرض الإتجاهات الفقهية في تحديد مفهوم الوثيقة المعلوماتية

محل جريمة التزوير ، وكذا القيمة الثبوتية لها باعتبارها سبب تجريم التزوير فيها ، محاولا بيان أركان هذه الجريمة .

هـ- "الحماية الجنائية للمستند الإلكتروني" للدكتور أشرف توفيق شمس الدين عام "2006"، حيث تناول في هذه الدراسة مدلول المستند الإلكتروني وعناصره ، وكذا القيمة القانونية له في التشريعات المقارنة ، وبعض صور هذا المستند ، مبينا في الفصل الأول الأفعال الماسة بمحتوى المستند الإلكتروني ومن بينها تزوير هذا المستند من خلال تأصيل خطة التشريعات المقارنة في تجريم تزوير المستند الإلكتروني من حيث النص على الركن المادي، وكيفية تحديد عناصره، ونوع القصد الجنائي المطلوب.

و- " جريمة التزوير في المحررات الإلكترونية " للدكتور " إيهاب فوزي السقا" عام "2008" ، حيث بين مفهوم المحررات الإلكترونية انطلاقا من تعريفات الفقه والقانون المقارن ، مبينا خصائصها واختلافها عن المحررات الورقية ، محددًا الشروط الواجب توافرها لإعتبارها حجة في الإثبات ، كما تناولت الدراسة طبيعة جريمة التزوير في المحررات الإلكترونية بالتركيز على التشريع المصري من خلال بيان أركان الجريمة .

ر- "تزوير التوقيع الإلكتروني" للمؤلفين "منير محمد الجنبهي" و "ممدوح محمد الجنبهي عام "2006"، حيث تناولوا شروط تمتع التوقيع الإلكتروني بالحماية الجنائية في التشريعات المقارنة، وبيننا طبيعة التزوير في التوقيع الإلكتروني وأضرار هذه الجريمة .

#### 4- إشكالية البحث :

هل يعد تغيير الحقيقة في المعلومات المعالجة آليا تزويرا في وثيقة في إطار المعاملات الإدارية الحكومية، إذا تعلقَت هذه المعلومات بإثبات حقوق أو مراكز قانونية معينة؟  
- ويتفرع عن هذه الإشكالية التساؤلات التالية :

هل ينطبق النص المجرم للتزوير في قانون العقوبات على فعل تغيير الحقيقة في الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية؟ .



هل تجريم تزوير الوثيقة المعلوماتية بصفة عامة يحتاج إلى نص جنائي خاص؟.  
ماهي الإتجاهات التشريعية والفقهية في تجريم تزوير الوثيقة المعلوماتية ؟ .

#### 5- فرضيات البحث :

سنحاول الإجابة عن الأسئلة المطروحة من خلال الفرضيات التالية :

**فرضية 1 :** يشكل تغيير الحقيقة في الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية جريمة تزوير .

**فرضية 2 :** ينطبق نص التزوير في قانون العقوبات على فعل تغيير الحقيقة في الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية .

**فرضية 3 :** يحتاج تجريم فعل تغيير الحقيقة في الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية إلى نص جنائي خاص.

#### 6- محددات البحث :

إن البحث في الإشكالية السابقة والفرضيات المطروحة محدد موضوعيا من خلال نماذج قوانين دولية ووطنية ، عربية وغربية تناولت هذا الموضوع من حيث تنظيم المعاملات المعتمدة على الوثيقة المعلوماتية وبيان قيمتها الثبوتية، وكذا من حيث كيفية وضع النص المجرم للتزوير، حيث إن إختيار هذه النماذج كان على أساس سبقها في تنظيم التعامل في بالوثيقة المعلوماتية ، وكذا خصوصية منهجها في التجريم .

بناء على ما سبق كانت الدراسة محددة موضوعيا من خلال تشريع الأونسترال والتوجيه الأوربي على المستوى الدولي ، وكذا التشريع الأردني ، الإماراتي ، والمصري على المستوى الوطني كنماذج تشريعية عربية ، والتشريع الفرنسي كنموذج تشريعي غربي.

## 7- مناهج البحث :

لمعالجة إشكالية البحث ومناقشة فرضياته ، تم استخدام مجموعة من المناهج العلمية وهي :

أ- **المنهج الإستدلالي** : استخدم هذا المنهج في التعريف بالوثيقة المعلوماتية وتحديد عناصرها، وتحديد مدلول جريمة التزوير المعلوماتي وبيان أركانها ، كما استخدم في تحليل الصيغ التشريعية في تجريم تزوير الوثيقة المعلوماتية ، والاتجاهات الفقهية في المسألة .

ب- **المنهج الجدلي** : استخدم هذا المنهج لبيان الجدل التشريعي والفقهي في تحديد القيمة الثبوتية للوثيقة المعلوماتية ، ومن ثم تحديد مدى وقوع التزوير فيها .

ج- **المنهج المقارن** : استخدم هذا المنهج في المقارنة بين منهج بعض التشريعات العربية والغربية في تحديد القيمة الثبوتية للوثيقة المعلوماتية وتجريم التزوير فيها .

## 8- صعوبات البحث :

إن موضوع هذه الرسالة العلمية يجمع بين جانبيين على نفس القدر من الأهمية وهما القانون والمعلوماتية ، حيث لا يمكن دراسة هذا الموضوع من الناحية القانونية فقط بمعزل عن الناحية التقنية، وهو ما خلق صعوبات في هذا البحث من حيث عدم التخصص في مجال المعلوماتية، وعدم الإلمام بالمصطلحات التقنية ذات العلاقة بالموضوع لفهم أعمق للجوانب القانونية فيه ، مما قد يؤثر على محاولات الربط العلمي السليم بين عناصره من الناحية التقنية، أو محاولة تفسير العلاقات القائمة، أو تحديد طبائع بعض العناصر استنادا إلى هذا التخصص الدقيق، وما له من انعكاسات على الجانب القانوني .

## 9- ضبط مصطلحات البحث :

باعتبار موضوع البحث له علاقة بتكنولوجيا المعلومات ، فلا بد من ضبط المصطلحات المتعلقة بذلك والتي لها علاقة بالموضوع وهي :

1. المعلوماتية : "هي تكنولوجيا المعلومات أي المعلومة الخاضعة للمعالجة الآلية " .

2. وثيقة معلوماتية : " وثيقة تحوي معلومات مرتبطة بنظام معلوماتي ، وقد خضعت للمعالجة الآلية " .

3. الوثيقة الرسمية الإدارية المعلوماتية : " الوثيقة التي يتم إنشاؤها أو إرسالها أو تداولها بين المؤسسات الحكومية الإدارية ، أو بينها وبين الأشخاص بوسائل معلوماتية " .

4. نظام المعالجة الآلية : " مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تكون كل من الذاكرة والبرامج والبيانات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي تربط بينها مجموعة من العلاقات التي عن طريقها تحقق نتيجة معينة وهي معالجة البيانات " .

5. المعاملة الإلكترونية: "كل معاملة تتم باستخدام كتابة الكترونية لإحداث أثر قانوني معين".

6. المعاملة الرسمية الإدارية : "المعاملة التي تتم بين الإدارات العامة، أو بين الإدارة العامة والأشخاص" .

## 10- تقسيم البحث :

لمعالجة الإشكالية تم تقسيم البحث إلى بابين وفصل تمهيدي ، حيث خصص الفصل التمهيدي لبيان تأثير المعلوماتية على الأنظمة القانونية من حيث تحديد أسباب ظهور المعاملات الإلكترونية، وأصناف الجرائم المرتبطة بالمعلوماتية.

أما الباب الأول فقد خصص للوثيقة المعلوماتية محل التزوير من خلال فصلين تعلق الفصل الأول منهما بتحديد مفهوم الوثيقة المعلوماتية تشريعا وفقها ، بينما ارتبط الفصل الثاني ببيان القيمة القانونية لها، فيما خصص الباب الثاني لبيان الصيغ التشريعية في تجريم تزوير الوثيقة المعلوماتية من خلال ثلاثة فصول ، تضمن الفصل الأول منها تحديد مفهوم تزوير الوثيقة المعلوماتية في التشريعات المقارنة، من خلال تشريع الأونسترال على المستوى الدولي، أما على المستوى الوطني فمن خلال التشريع الأردني، الإماراتي، والمصري (نموذجاً للتشريعات العربية)، والتشريع الفرنسي (نموذجاً للتشريعات

الغربية)، أما الفصل الثاني فقد خصص لتحديد أركان جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، والعقوبات المقررة لها ، بينما تعلق الفصل الثالث ببيان الصور الخاصة لجريمة التزوير المعلوماتي من خلال جريمة تزوير التوقيع الإلكتروني، وجريمة تزوير البطاقة الإئتمانية .

## فصل تمهيدي

### تأثير المعلوماتية على الأنظمة القانونية

كان للمعلوماتية تأثيرا بارزا على الأنظمة القانونية المختلفة نتيجة البيئة الافتراضية للمعلومة، التي أصبحت بهذه الخصوصية محل للحماية سواء من خلال القوانين الخاصة أو العامة.

لقد أثرت المعلوماتية على القوانين الخاصة بالإثبات والمعاملات المدنية والتجارية، كما أثرت أيضا على التشريعات الخاصة بالمعاملات الإدارية والحكومية ، وقد انعكس ذلك على مفهوم الوثيقة باعتبارها الوسيلة الغالبة في إنجاز هذه المعاملات، مما يستوجب الرجوع إلى خلفيات التحول إلى البيئة اللاورقية ومجالات هذا التحول، ثم بيان الأنماط الإجرامية المستحدثة المرتبطة بالبيئة الإلكترونية والتي قد تتداخل مع التزوير المعلوماتي.

## المبحث الأول : التحول من المعاملات الورقية إلى المعاملات الإلكترونية

إن الوجه البارز لتأثير المعلوماتية على المعاملات بين الأفراد، أو بين الأفراد والحكومة، أو في مجال المشروعات هو التحول إلى العالم اللامورقي أي تلك البيئة الافتراضية التي تعتمد على اللغة الرقمية، وتستند على الوسائط الإلكترونية .

إن هذا التأثير على طبيعة المعاملات كان نتيجة عدة أسباب منها ما تعلق بظهور التجارة الإلكترونية، ومنها ما ارتبط بالإدارة الإلكترونية ، وكذا بالدخول إلى الحكومة الإلكترونية، وقد لعبت الإنترنت في كل ذلك دورا مهما.

### المطلب الأول: أسباب ظهور المعاملات الإلكترونية

لقد كانت التجارة الإلكترونية البيئة الأولى لظهور المعاملات الإلكترونية نتيجة الاعتماد على الوسائل الإلكترونية في المبادلات التجارية بمختلف أنواعها، ثم ازداد حجم المعاملات الإلكترونية وزاد انتشارها بالاستفادة من مزايا الإنترنت، التي سهلت على الدول تحويل حكوماتها إلى حكومات الكترونية، والاعتماد على الإدارة الرقمية في تسير شؤونها .

### الفرع الأول : التجارة الإلكترونية

كان أول ظهور لهذا النوع من التجارة في أوائل السبعينات من القرن الماضي، عندما استخدمت شركات أمريكية شبكات خاصة لربطها ببعضها وكذا بعملائها ، ثم بدأ تطبيق التحويل الإلكتروني للأموال، كما انتشر البريد الإلكتروني حيث استخدمه رجال الأعمال

والمؤسسات باعتباره إحدى أهم الوسائل لإتمام المبادلات التجارية وذلك بدل البريد العادي والفاكس .

ولما انتشرت شبكة الإنترنت في التسعينات تطورت التجارة الإلكترونية أكثر، حيث تم إنشاء مواقع لعرض المنتجات والخدمات، وللاّصال بالمستهلكين، إذ أن هذه المواقع تعطي للمؤسسات الإقتصادية حيز افتراضي لعرض بياناتها، مما يسمح للزبائن بالدخول إلى مختلف العروض مهما كان محل إقامتهم مع إمكانية استكمال الشراء، وإجراء الطلب واستقبال المنتج دون التنقل<sup>1</sup> .

### أولا : تعريف التجارة الإلكترونية

تعتبر التجارة الإلكترونية عملية تبادل للمعلومات الخاصة بالعمليات التجارية بين طرفين أو أكثر بدون استخدام المستندات الورقية، حيث يتم تبادل البيانات الكترونيا(EDI)<sup>2</sup> ولذلك فإن التجارة الإلكترونية تعتبر شكل من أشكال التبادل التجاري الذي يعتمد على شبكة الاتصالات بين مؤسسات الأعمال مع بعضها البعض، ومؤسسات الأعمال وزبائنهم، أو بين مؤسسات الأعمال والإدارة العامة .

---

1 : Yvon Merliere, Dominique Jacomet et Evelyne Chaballier, "L'impact du Commerce Electronique en Matiere de Soldes et de Promotions", Institut Français de la Mode ,s.l, Avril 2011, p.6.

2 : حسني ثابت، "التجارة الإلكترونية تحول من التقليدية إلى الآلية" ، 2009/08/31 ، ([www.egynews.net](http://www.egynews.net)) .

كما تعتبر التجارة الإلكترونية نظام تبادل غير ورقي لصفقات ومعلومات تجارية ومصرفية باستخدام وسائل تكنولوجية حديثة<sup>1</sup>.

كما عرفت أيضا بأنها عرض متزايد للنشاطات تجري داخل شبكة مفتوحة للوصول إلى مبادلة قيم بين طرفين، ومصطلح الكترونية يعبر عن أداة حديثة في الاتصال هي الإنترنت التي من خلالها يتم مبادلة المعلومات<sup>2</sup>.

إن هذه التعاريف ركزت على وسائل تبادل المعلومات التجارية، وهي الوسائل الإلكترونية دون التركيز على مضمون هذا النوع من التجارة، لكن الذي يهمننا في هذا الموضوع من البحث هو مستويات هذه التجارة و تأثيرها على طبيعة المعاملات من الناحية القانونية، ولذلك سنركز على زاوية معينة في تعريف التجارة الإلكترونية وهي التي تتعلق بالتغيير في نمط وطبيعة المعاملات التجارية، وبالتالي أثر ذلك على طبيعة الوثيقة المتداولة لإنجاز هذه المعاملات، حيث عرفت التجارة الإلكترونية بأنها أسلوب من الأساليب التجارية والتي تكون فيها المعاملات التجارية بين المشاركين الكترونياً. بمعنى إجراء المعاملات التجارية بواسطة الحاسب الآلي عن طريق الشبكات الإلكترونية (الإنترنت)، أو عن طريق استخدام شبكات خاصة مثل الشبكة الوسيطة، أو عن طريق اتصال مباشر بحسابات الشركاء التجاريين<sup>3</sup>.

---

1 : راسم سميح محمد عبد الرحيم، التجارة الإلكترونية في خدمة التجارة والمصارف العربية. مكتبة البنك المركزي، القاهرة، 1997، ص.30.

2 : كمال رزيق، مسدور فارس، "التجارة الإلكترونية وضرورة اعتمادها في الألفية الثالثة"، نادي الدراسات الاقتصادية، كلية العلوم الاقتصادية وعلوم التسيير، جامعة سعد دحلب، البلدة، ب.ت.

3 : محمد بن أحمد السديري، "التجارة الإلكترونية، تقنيات واستراتيجيات التطبيق"، 2012/03/23، (faculty-ksu.edu.sa)، ص.ص. 4، 5.



ولذلك سنعرض في العنصر الموالي مستويات التجارة الإلكترونية لتمييز أنواع المعاملات الإلكترونية التي تتم في هذه البيئة، ثم نبين الإطار القانوني للتجارة الإلكترونية.

### ثانيا : مستويات التجارة الإلكترونية

يشمل نظام تبادل البيانات الكترونيا المعاملات الإلكترونية من شركة إلى شركة، والمعاملات الإلكترونية بين شركة ومستهلك<sup>1</sup>، وكذا المعاملات التي تتم بين حكومة وشركة أو مستهلك في إطار الحكومة الإلكترونية، ولذلك تمتد التجارة الإلكترونية لتشمل مجموع المعاملات التجارية التي تتم بين أطراف متعددة .

1-المعاملات بين شركة وشركة أخرى (B2B) : هذه المعاملات تشمل بيع المنتجات والخدمات، حيث يلتقي مجموع البائعين والمشتريين في مكان واحد هو السوق الإلكتروني...، كما تتم العملية الكترونيا بين هذه الشركات (تجار الجملة، تجار التجزئة، المصدريين والموردين) وفق نظام معين ونموذج محدد يتم الإتفاق والتوقيع عليه مسبقا. فيتم إبرام عقد يتفق فيه الطرفان على طريقة الإتصال والدفع والشخص المفوض بإرسال الأوامر وكذلك الشخص المفوض بتنفيذها<sup>2</sup> .

2- المعاملات بين شركة ومستهلكين (B2C): تعتمد هذه المعاملات على بيع المنتجات والخدمات مباشرة إلى المستهلك بدون وسيط. فيتم عرض السلع والخدمات على الشبكة

---

1: Steven Globerman, " Définition et Evaluation des Liens Entre Commerce Electronique et Croissance de la productivité ", Programme des Publications de Recherche d'industrie , Canada , Avril 2001,p.3.

2 : محمد بن أحمد السديري، مرجع سابق، ص 6 .

العنكبوتية من خلال متاجر إلكترونية أو أسواق افتراضية. تقوم الشركات بفتح المتاجر الإلكترونية وعرض السلع، ويقوم ومن خلال البطاقات الذكية، أو بواسطة بطاقات الدفع<sup>1</sup>.

3- **المعاملات بين شركة وحكومة (B2G)** : ويشمل هذا النوع من التعامل دفع الضرائب، وكذا المعاملات بين الشركات والإدارة المحلية حيث يتم إجراء المعاملة الكترونياً دون التنقل إلى المكاتب الحكومية، ودون استخدام المستندات الورقية .

4- **المعاملات بين الحكومة والأفراد (G2C)**: ويعتبر هذا النوع من التعامل جزء من مفهوم الحكومة الإلكترونية، ويتضمن دفع الضرائب، استخراج الشهادات والوثائق، وغيرها من الخدمات.

### ثالثاً: الإطار القانوني للتجارة الإلكترونية

تهدف التجارة الإلكترونية بمختلف مستوياتها إلى خلق بيئة من المعاملات اللاورقية، لتجنب استخدام الوثائق الورقية الذي يؤدي إلى بطء المعاملة مقابل السرعة التي تتميز بها الوثائق المعلوماتية، وهو ما يشجع هذه التجارة ويزيد من انتشارها وحجمها .

غير أن الإ اعتماد على هذا النوع من المعاملات يعني بالضرورة أن الوثيقة المعلوماتية ستصبح هي السند القانوني المعتمد بين الأطراف .

ولذلك واجهت التجارة الإلكترونية في البداية مشكلة اعتراف التشريعات بالوثيقة المعلوماتية

---

1 : محمد بن أحمد السديري ، مرجع سابق ، ص 6 .

ومدى حجية الدليل الإلكتروني، خاصة مع تزايد الاعتماد على الوثائق المعلوماتية مقابل الوثائق الورقية .

هذه العقبة كانت تهدد ازدهار التجارة الإلكترونية، ولذلك كان لابد من وضع الإطار القانوني المناسب لحل المشكلة، وهو ما جعل لجنة الأمم المتحدة للقانون التجاري الدولي (UNCITRAL) تعكف على تنظيم هذه التجارة دولياً من خلال إعداد قانون الأونسترال النموذجي للتجارة الإلكترونية الذي تم اعتماده في 16/12/1996، والذي نظم المعاملات التجارية الإلكترونية وحدد المصطلحات الخاصة بها، كما بين القيمة القانونية للرسائل الإلكترونية(الوثائق المعلوماتية) .

وقد كان من أهداف هذا القانون وضع القواعد القانونية الملائمة لإزالة العقبات القانونية في مجال التجارة الإلكترونية، بالإضافة إلى المساواة في القيمة القانونية بين الوثائق الورقية ونظيرتها الإلكترونية، ومواجهة قصور بعض التشريعات في مجال التعامل الإلكتروني .

### الفرع الثاني : الإنترنت

ساهمت الإنترنت بشكل بارز في التحول إلى العالم اللورقي من خلال تأثيرها على طبيعة المعاملات القانونية في مختلف المجالات .

### أولاً : نبذة عن ظهور الإنترنت

ظهرت الإنترنت لأول مرة لأغراض عسكرية، ففي نهاية الستينات من القرن الماضي وفي خضم الحرب الباردة أرادت الولايات المتحدة الأمريكية تأمين نفسها ضد أي هجوم نووي يؤدي إلى تعطيل الاتصال بين قواتها العسكرية وقواعدها في مختلف أنحاء العالم، وهو ما جعل وزارة

الدفاع الأمريكية تطالب البنثاغون بإيجاد وسيلة اتصال جديدة ومأمونة حتى لا تتأثر بالهجوم النووي خلال الحرب .

وفي عام 1964 أوجد (Paul Baran) شبكة اتصالات تتحمل روابط مطولة وقادرة على تحمل الإنقطاع وبالتالي أي هجوم نووي<sup>1</sup>، ثم تم تكوين شبكة اتصالات موحدة (NETWORK) التي كان لها مركز تحكم رئيسي ، حيث إن إتلاف جزء من الشبكة لا يؤثر على البقية.

ولكن نظرا للغاية الأمنية لهذه الشبكة لم يكن متاحا للأفراد استخدامها، وقد عرفت باسم (شبكة وكالة مشروع الأبحاث المتقدمة:ARPANET) التي تم توسيعها لتضم شبكات عديدة لنقل المعلومات، ولكن الهدف من هذه الشبكة كان ذو طبيعة إستراتيجية وهو إرسال تعليمات إصابة الصواريخ لأهدافها من خلال مركز تحكم، على أن يبقى الاتصال مستمر مع القطاعات العسكرية حتى لو دمرت أجزاء من الشبكة إذا ما تعرضت لهجوم عسكري<sup>2</sup>.

وفي بداية السبعينات اتسعت الشبكة بين حواسيب مراكز البحث العسكرية الأمريكية<sup>3</sup>، ثم أصبحت خدمة الإنترنت متاحة للأفراد سنة 1985، حيث تبنت المؤسسة القومية العلمية (NSF) شبكة (ARPA) لتحقيق الاستفادة في المجال العلمي والبحوث، من خلال تمكين الباحثين من الوصول إلى المعلومات المخزنة على الشبكة .

---

1 : Pascal Renand , "Historique de l'internet du Nord au Sud ",S.D,(www.africanti.Org).P.4

2 : داوود عبد الرزاق الباز، الحكومة الإلكترونية وأثرها على النظام القانوني للمرفق العام. منشأة المعارف، الإسكندرية، 2007، ص23 .

3 : Pascal Renand , Op.Cit , P 4 .

وفي سنة 1989 أنشأت الحكومة الأمريكية شبكة الانترنت التي أصبح لها أغراض تجارية، خاصة بعد نهاية الحرب الباردة بداية التسعينات، حيث أصبح للشبكة صبغة مدنية، وهذا ما ساعد على ظهور التجارة الإلكترونية بمساعدة نظام الإدارة الإلكترونية<sup>1</sup>، ثم بدأت الحكومات في التحول في أداء أعمالها وخدماتها إلى الشكل الإلكتروني.

### ثانيا : تعريف الإنترنت

الإنترنت عبارة عن مجموعة هائلة من الحواسيب الآلية موجودة في أماكن مختلفة موصولة مع بعضها البعض عن طريق الأسلاك التليفونية أو كوابل أخرى، كما يمكن إستخدام الأقمار الصناعية لربطها إذا كانت الأماكن بعيدة ومتفرقة، وبالتالي يتحقق الاتصال الدولي عبر الإنترنت<sup>2</sup>.

ويتطلب عمل الشبكة جهاز كمبيوتر، وجهاز مودم يقوم بتحويل البيانات المستقبلية من أرقام ثنائية إلى إشارات مناسبة يمكن فهمها، مع وجود خط هاتفي يعمل على نقل البيانات الإلكترونية بعد أن يقوم المودم بتحويلها إلى إشارات ضوئية<sup>3</sup>.

### ثالثا : تأثير الانترنت على التنظيم القانوني للمعاملات

سيتم التركيز في هذا العنصر على أهم المجالات المرتبطة بالبحث، ذلك أن تأثير الإنترنت على القانون بصفة عامة له مجالات متعددة ومتشعبة .

---

1 : داوود عبد الرزاق الباز ، مرجع سابق، ص . ص . 2524.

2 : عبد الفتاح بيومي حجازي ، الجريمة في عصر العولمة . دار الفكر الجامعي، الإسكندرية ، 2007 ، ص 15 .

3 : عباس العبودي، الحجية القانونية لوسائل التقدم العلمي في الاثبات المدني. الدار العلمية، ط1، عمان، الأردن، 2002، ص.140.

قد كان لهذه الشبكة العالمية الأثر البالغ على الكثير من التشريعات، من بينها تشريعات التجارة والبنوك، نظم الإثبات، التشريعات الإدارية، تنظيم الجهاز القضائي وغيرها.

### 1- تأثير الانترنت على القوانين المدنية والتجارية :

لعبت الانترنت دورا مهما في تسهيل عملية التعاقد، بالإضافة إلى الإثبات وهو ما فتح الباب أمام تحديد طبيعة التعاقد وأحكامه، ومدى حجية العقد الإلكتروني في الإثبات أمام الجهاز القضائي، وكذا بقية المستخرجات والبيانات المخزنة في النظام .

ونظرا لأهمية هذه العقود الالكترونية سواء في المعاملات المنجزة بين شركة ومستهلك، أو بين شركة وشركة، أو حتى بين الجهات الحكومية فقد كان لابد من تنظيمها قانونيا، وهو ما أدى بالمشرع الدولي والوطني إلى الاعتراف بحجيتها في الإثبات، بالإضافة إلى إحاطتها بأمن معلوماتي قوي، وضمان الثقة عند التعامل بها من خلال التوقيعات الرقمية وشهادات التصديق الإلكتروني .

### 2- تأثير الانترنت على تشريعات البنوك :

أثرت التقنية الحديثة على الخدمات المصرفية والبنكية، حيث ظهرت أنظمة الدفع الإلكتروني ، البطاقات الائتمانية ، النقود الالكترونية ، والتبادل الإلكتروني للأموال .

### 3- تأثير الانترنت على تنظيم الجهاز القضائي :

من أهم استخدامات الانترنت في هذا المجال ظهور ما يسمى بالسجل الإلكتروني على مستوى كتابة الضبط لقيود صحائف الدعاوى، وذلك من خلال وثائق معلوماتية عبر الشبكة، وبالتالي أصبح التقاضي يعتمد على مستندات الكترونية من خلال نفس الفكرة المعتمدة في

التجارة عبر الانترنت، حيث إن نظام إرسال وقبول المستندات الإلكترونية(EDI) هو نظام إلكتروني خاص بفتح قنوات الإتصال بين المتقاضين والمحكمة من خلال نافذة الكترونية، وبالتالي يختلف الأمر عن الوضع المعتاد، حيث أن المعلومات تصبح ذات طبيعة الكترونية، كما أنها موثقة من خلال نظام التصديق الإلكتروني<sup>1</sup>.

#### 4- تأثير الانترنت على التشريعات الإدارية :

ساهمت الانترنت في تغيير نمط الأعمال الإدارية، مما أدى إلى تطور الإدارة الإلكترونية، ومن أوجه هذا التغيير اختلاف طريقة التعبير عن الإرادة المنفردة في شكل قرارات إدارية، أو تلك التي تقتن بإرادة طرف آخر من خلال العقود الإدارية إذ أصبحت هذه العمليات تتم عن طريق البريد الإلكتروني أو الموقع، كما أن عملية توثيق هذه التصرفات الإدارية يتم من خلال التوقيع الإلكتروني .

كل هذا انعكس على الإطار التشريعي الإداري من خلال توجه غالبية القوانين إلى الإقرار بصحة الوثائق المعلوماتية وإمكانية التعامل بها مع الإدارة\*.

---

1 : لمزيد من التفاصيل أنظر: خالد ممدوح ابراهيم، التقاضي الإلكتروني. دار الفكر الجامعي، الإسكندرية، 2007، ص.ص 24 – 35 .

\* : من بين هذه القوانين القانون الفدرالي الأمريكي لسنة 1998 الذي طبق نظام الشراء الحكومي الإلكتروني للتخلص من العمل الورقي ، قانون المناقصات في فرنسا لسنة 1999 الذي نظم كيفية إجراء المعاملات الإدارية عبر الإنترنت، إعلان حكومة دبي في 2001 بتحويل كل مشتريات الدوائر الحكومية إلى النظام الإلكتروني عبر الإنترنت .

## الفرع الثالث: الإدارة الإلكترونية

إن الصلة بين المعاملات الإلكترونية والإدارة الإلكترونية وطيدة، ذلك أن الإدارة الإلكترونية تقوم على الأنشطة ذات الطبيعة الإلكترونية بدل المعاملات الورقية، مستفيدة بذلك من الوسائل التكنولوجية الحديثة، ولذلك فإن ظهور هذا النوع من المعاملات كان مرتبطاً بظهور الإدارة الإلكترونية وتطورها، ولذلك سنبحث عن بدايات هذه الإدارة ونبين مفهومها وعناصرها، وكذا أهميتها ومستوياتها .

### أولاً: نبذة عن الإدارة الإلكترونية

إن بداية ظهور الإدارة الإلكترونية تقنياً كان نتيجة تطور التبادل الإلكتروني للبيانات، حيث كان العمل بين المنظمات أو المؤسسات داخلياً من خلال العمل ببيانات إلكترونية موحدة غير إن هذا التبادل في البداية كان محدوداً في مجالات معينة، حيث استخدمت في البداية الإنترنت وهي شبكة داخلية يمكن أن تزود جميع الموظفين في المؤسسة بالمعلومات، بالإضافة إلى شبكة الإكسترانت وهي شبكة خارجية تزود المؤسسة بالمعلومات في علاقتها بالموردين والزبائن. ثم تطور هذا التبادل الإلكتروني بظهور شبكة الإنترنت، كما اتسعت الإدارة الإلكترونية مع اتساع التجارة الإلكترونية، واتسعت أكثر مع توسع الحكومة الإلكترونية<sup>1</sup> .

---

1: عادل حرشوش، أحمد علي صالح ، ستار البياتي، الإدارة الإلكترونية مرتكزات فكرية ومتطلبات تأسيس عملية. المنظمة العربية للتنمية الإدارية، القاهرة، 2007، ص.ص 6-9 .



## ثانيا : مفهوم الإدارة الإلكترونية

هناك تداخل بين مفهوم الإدارة الإلكترونية والحكومة الإلكترونية، إذ يرى البعض أن تطبيق الإدارة الإلكترونية هو الخطوة السابقة لتطبيق الحكومة الإلكترونية. ونرى أن الإدارة الإلكترونية مختلفة من حيث نوع النشاط الذي تؤديه، ونطاقه، وهو ما يظهر من خلال تعريفها .

### I- تعريف الإدارة الإلكترونية

عرفت الإدارة الإلكترونية بأنها " تحويل كافة الأعمال والخدمات الإدارية التقليدية إلى أعمال وخدمات إلكترونية تنفذ بسرعة عالية ودقة متناهية"<sup>1</sup> .

كما عرفت بأنها "إدارة عامة مسؤولة عن تقديم المعلومات والخدمات الإلكترونية بطريقة رقمية للموظفين ومنشآت الأعمال القادرة على الاتصال الكترونيا عن بعد"<sup>2</sup> .

أما الحكومة الإلكترونية فترتبط بتيسير سبل أداء الإدارات الحكومية لخدماتها العامة بواسطة استثمار التطورات العلمية المذهلة في مجال تقنية الإتصالات والمعلومات<sup>3</sup> .

ولذلك كان مصطلح الحكومة الإلكترونية أوسع، بينما ترتبط الإدارة الإلكترونية بالأنشطة والمهام الإدارية ولذلك فهي تعني "عملية ميكنة جميع مهام وأنشطة المؤسسة الإدارية بالاعتماد

---

1: عبد الله بن سليمان، "الأثر الاقتصادي لتطبيق الأعمال الحكومية الإلكترونية" ، منتدى الأعمال الحكومية الثالث، السعودية، 18-20 سبتمبر 2006 .

2: محمد محمد الهادي، "الحكومة الإلكترونية وسيلة للتنمية والإصلاح الإداري"، Cybrarians journal ، عدد 11، (ديسمبر 2006).

3: علي السيد الباز، "الحكومة الإلكترونية والإدارة المحلية"، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، مركز البحوث، الإمارات العربية المتحدة، 26/04/2003 .

على جميع تقنيات المعلومات الضرورية للوصول إلى تحقيق أهداف الإدارة الجديدة في تقليل استخدام الورق، وتبسيط الإجراءات والقضاء على الروتين والإنجاز السريع والدقيق للمهام والمعاملات لتكون كل إدارة جاهزة لربطها مع الحكومة الإلكترونية لاحقاً<sup>1</sup>، مع ضمان بيئة من الثقة تحمي فيها المعطيات الشخصية وتتخذ فيها إجراءات التحقق من الهوية وصدق المعلومات<sup>2</sup>.

يبدو واضحاً أن الإدارة الإلكترونية تعتمد على تقديم الأعمال والخدمات بشكل إلكتروني (نوع النشاط) إلى جمهور المتعاملين معها، بشكل سريع ودقيق، من خلال إعادة تنظيم مهامها وأنشطتها بالإعتماد على المعلوماتية لتحقيق أهدافها (نطاق الإدارة).

لكن هذا لا يعني أن الإدارة الإلكترونية تتحقق بمجرد وجود مواقع إلكترونية أو بوابات لها على شبكة الإنترنت، بل لابد أن تمارس نشاطها فعلاً من خلال هذه المواقع والبوابات، مغيرة بذلك أساليبها باستخدام التكنولوجيا والتقنية الرقمية، فتتغير الأعمال والخدمات من النمط التقليدي (الشكل الورقي) إلى نمط جديد (الشكل الإلكتروني)، وهذا يجعل الإدارة الإلكترونية تتميز أيضاً من حيث طبيعة أهدافها، فهي تعمل على :

1- تطوير العمل الإداري باستخدام التقنيات الرقمية الحديثة .

2- توفير المعلومات والبيانات لإتخاذ القرار الإداري بشكل سريع وملائم في نفس الوقت.

---

1: علي السيد الباز ، مرجع سابق .

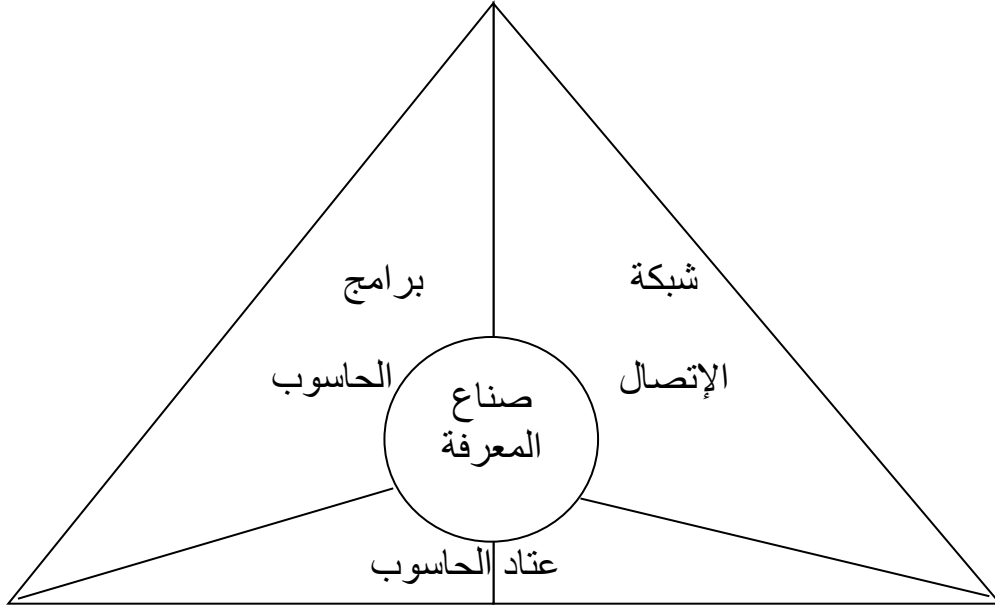
2 : Aminata Bal, "Quelque réflexions sur l'administration Electronique",Revue Française d'administration Publique, N° 110 ,2004, P . 6.

- 3- خفض حجم الإستخدام الورقي، ومشكلة الحيز المكاني المستخدم للحفظ.
- 4- السرعة في إنجاز المعاملات القانونية ، وشفافيتها بتوفير كل المعلومات اللازمة حولها في فضاء الكتروني .
- 5- الإتصال بين الإدارات المختلفة، بتوفير البيانات وربطها ببعضها من أجل أداء إداري أفضل .
- 6- رقمنة الإجراءات مما يؤدي إلى اختصار الوقت في إنجاز المعاملة الإدارية .
- 7- أداء الأعمال والخدمات الإدارية من خلال الشبكة في أي وقت، وفي أي مكان.
- 8- خفض التكاليف في إنجاز المعاملة ، وتجنب سلبيات المعاملات الورقية.

## II- العناصر التقنية للإدارة الإلكترونية :

إن الإدارة الإلكترونية لا يمكن أن تحقق هذه الأهداف من الناحية التقنية إلا من خلال أربعة عناصر مترابطة وهي : عتاد الحاسوب، البرمجيات، شبكة الإتصال، صناع المعرفة من خبراء ومختصين وفق ما يوضحه الشكل الموالي :

## شكل رقم (1) يوضح عناصر الإدارة الإلكترونية



المصدر : سعد ياسين، الإدارة الإلكترونية وآفاق تطبيقاتها

العربية، معهد الإدارة العامة السعودية ، 2005، ص 24 .

إن شبكة الإتصال كما هو مبين في الشكل أعلاه ، هي أهم عناصر الإدارة الإلكترونية، لأنها تضيف على الإدارة ذلك الطابع الإلكتروني، وتغير من نمط نشاطها كما ذكرنا سابقا، وذلك من خلال شبكة الحواسيب وهي مجموعة من الأجهزة الحاسوبية المرتبطة بخطوط اتصال تمكن من نقل وتبادل المعلومات، وتتكون من الأجزاء التالية<sup>1</sup> :

---

1 : يوسف محمد يوسف، "واقع إدارة الموارد البشرية الكترونيا في الجامعات الفلسطينية النظامية"، (مذكرة ماجستير)، تخصص إدارة أعمال، كلية الدراسات العليا، الجامعة الإسلامية، غزة، 2009، ص.ص 38-40 .

## 1- جهاز الخادم الرئيسي :

هو عبارة عن جهاز حاسوب ذو مواصفات عالية، يقوم بالتحكم في أنظمة برمجية وقواعد بيانات، ويربط المستخدمين بالتطبيقات المختلفة ويطلق عليه خادم التطبيقات، أما خادم الويب فهو عبارة عن برنامج يقوم بتخزين وحفظ مواقع الويب، وتحديد مكانها لدى طلبها من المستخدم، وربط المستخدمين مع قواعد البيانات والتطبيقات عن طريق الإنترنت. من خلال واجهات الإستخدام .

## 2- الأجهزة الملحقة :

مثل الطابعات والراسمات، ويستطيع المستخدم استخدام هذه الأجهزة الموصلة .

## 3- الكابلات ووحدات الشبكة :

الكابلات هي المكونات التي تقوم بتوصيل أجزاء الشبكة بعضها ببعض وتجعلها تستخدم بكفاءة، وبذلك يمكن إرسال الرسائل من مكان إلى آخر. وتستخدم الشبكات المحلية أنواع مختلفة من الكابلات منها الأسلاك الهاتفية المزدوجة النقل ، الكابلات المحورية ذات القناة الواحدة أو متعددة القنوات، الألياف الضوئية ذات الأداء والكلفة العالية .

كما لا بد أن تتوفر مشغلات وحدة الشبكة، وهي برامج تسمح للأجهزة بالإتصال والتخاطب مع نظام التشغيل للكمبيوتر، حيث لا يمكن لنظام التشغيل التعامل مع هذه الوحدة ما لم يتوفر مشغل الوحدة، الذي يمكن من التخاطب بين النظام والوحدة .

أما الشبكات فهي أشكال مختلفة وعديدة، وأهم هذه الشبكات المستخدمة في مجال الإدارة الإلكترونية ما يلي :

## أ- الشبكة الواسعة :

هي الشبكات التي تغطي مساحة جغرافية واسعة، على مستوى مدينة كبيرة الحجم أو على مستوى دولة، وتكون قادرة على تحمل عبء العمل اليومي لكافة الأنشطة التجارية والحكومية

## ب- الشبكات المحلية :

هي شبكة ضيقة تستعمل لربط أجهزة الحاسوب ضمن مجال فيزيائي صغير.

## ج- الإنترنت :

هي شبكة داخلية محمية قد تكون مرتبطة عن طريق الإنترنت أو من خلال برامج معينة داخل شبكة محلية، تسمح بتبادل البيانات والمعلومات داخل الشبكة عن طريق حاسبات خاصة.

## د- الإكسترانت :

هي شبكات خاصة تقوم بربط شبكات الإنترنت الخاصة بالشركات والعملاء ومراكز الأبحاث الذين تجمعهم أعمال مشتركة، وتؤمن لهم تبادل المعلومات والمشاركة فيها مع الحفاظ على خصوصية الإنترنت المحلية لكل مؤسسة .

## ثالثا : أهمية الإدارة الإلكترونية

تبدو أهمية الإدارة الإلكترونية من خلال ما توفره من مزايا بالمقارنة مع الإدارة التقليدية، خاصة من حيث طبيعة المعاملات المنجزة، وكيفية حفظها واسترجاعها وتأمينها ضد المخاطر والإعتداءات ، وهي العناصر التي سنركز عليها باعتبارها ذات صلة مباشرة بموضوع البحث .

## 1- خفض الوثائق الورقية :

يؤدي العمل بنظام الإدارة الإلكترونية إلى الاعتماد على الرسالة الإلكترونية كوثيقة أساسية في إجراء المعاملات، مما يؤدي إلى التخلص من الأوراق، فكل المعاملات تتم عن بعد<sup>1</sup> ، ويقضي على مشكلة حفظ المعاملات الورقية وتخزين ملفاتها التي قد تتجاوز أعدادها أرقاما تتخطى حاجز الأصفار الستة، وهي من أكبر المشكلات التي تواجه الإدارة التقليدية<sup>2</sup> .

## 2- التفاعلية بين الموظفين :

حيث يتم التفاعل بين الموظفين ورؤسائهم من خلال التواصل عبر البريد الإلكتروني، التصديق على الوثائق الكترونيا ، وإتمام المعاملات من خلال الموقع على الشبكة .

## 3- تغيير أسلوب التواصل بين الأجهزة الإدارية :

حيث عملت نظم المعلومات والشبكات داخل هذه الأجهزة على تلاشي الاتصال التقليدي بين الأجهزة المركزية واللامركزية، بالتنسيق بين الجهات اللامركزية وسلطة الوصاية عن طريق الشبكة، وإمكانية تدفق البيانات والمعلومات إلى الوحدات الإدارية الفرعية مما يساعدها في اتخاذ القرار<sup>3</sup> .

---

1 : Gilles St . Amant, Gouvernement en Ligne . ESG , Montréal, 2004, P . 12 .

2 : حسين بن محمد الحسن، "الإدارة الإلكترونية بين النظرية والتطبيق"، المؤتمر الدولي للتنمية الإدارية، معهد الإدارة العامة، الرياض، 1-4 نوفمبر 2009، ص 9 .

3 : داوود عبد الرزاق الباز ، مرجع سابق، ص . 241 .

#### 4- نظام حفظ المعاملة :

أصبحت الإدارة تعتمد في حفظ المعاملات والوثائق على الملفات الإلكترونية التي توجد في مأمّن من التلف والتقادم في ذلك الحيز الإلكتروني المخصص لذلك، وكذا من خلال تأمين هذه الوثائق باستخدام أكثر من وسيط تخزين الكتروني احتراز من حدوث أي عارض للشبكة الأم<sup>1</sup> .

#### 5- استرجاع الوثائق :

إن نظام الأرشيف الورقي يصعب الحصول على المعلومة عند الحاجة إلى استرجاعها من أحد الملفات الورقية، فقد يحتاج الأمر إلى ساعات أو أيام نظرا لتكدس الملفات والمعاملات، فالإنقال إلى الأرشيف للبحث عن ملف تائه بين مئات وربما آلاف الملفات رحلة شاقة<sup>2</sup> ، في حين لا تواجه الإدارة الإلكترونية هذه المشكلة لإعتمادها على الأرشيف الإلكتروني على الشبكة، حيث مهمة البحث عن الملف، أو إحدى الوثائق لا يتطلب سوى ثوان معدودة .

#### 6- حماية المعاملة :

تمنح الإدارة الإلكترونية للمتعامل ميزة تأمين المعاملة والوثيقة ضد التلاعب عن طريق الحذف أو الإضافة ، أو الدخول غير المشروع، وذلك من خلال برامج وتقنيات لحماية البيانات والمعلومات المخزنة على الشبكة الإلكترونية .

---

1 : حسين بن محمد الحسن ، مرجع سابق ، ص 8 .

2 : نفس المرجع ، ص 8 .



ولتحقيق أمن المعلومات لابد للإدارة الإلكترونية أن تتخذ مجموعة من الإجراءات الأمنية في المجال المعلوماتي من خلال: وضع السياسات الأمنية لتقنيات المعلومات، وتبني استراتيجية وطنية لأمن المعلومات. وكذا المحافظة على الخصوصية وتطوير أدوات التشفير في البرمجيات الحديثة لتمكين المستخدم من المحافظة على سرية شخصيته وتعاملاته عبر الشبكة.

#### رابعاً : مستويات الإدارة الإلكترونية

تمر الإدارة بمستويات متعددة لتصل إلى الإدارة الإلكترونية الحقة .

#### I- المستوى الأول :

إن الإدارة الإلكترونية قد تعتمد في مستواها الأول على تقديم المعلومات من خلال مواقع إلكترونية على شبكة الإنترنت لتحقيق الشفافية، حيث يمكن لأي متعامل أن يطلع على هذه المعلومات، وهو ما يسمى أيضاً بمرحلة الإتصال الأحادي الجانب<sup>1</sup> . وهو مستوى بسيط جداً كبداية للإدارة الإلكترونية، ولا يمكن التوقف عنده لأنه لا يعني أن الإدارة أصبحت تمارس نشاطها فعليا في شكل الكتروني .

رغم ذلك يحتاج هذه الإدارة لبلوغ هذا المستوى مجموعة من الإجراءات اللازمة لذلك

وهي<sup>2</sup>:

---

1 : حماد مختار، "تأثير الإدارة الإلكترونية على إدارة المرفق العام وتطبيقاتها في الدول العربية"، (مذكرة ماجستير)، تخصص تنظيم سياسي وإداري، قسم العلوم السياسية والعلاقات الدولية، كلية العلوم السياسية والإعلام، جامعة يوسف بن خدة، الجزائر، 2007، ص 26 .

2 : نفس المرجع، ص . ص 27 ، 28 .

- 1- تطوير البنية التحتية التي تشمل نظم الاتصالات .
- 2- العمل على دعم أسعار الحواسيب لإقتنائها من جميع فئات المجتمع .
- 3- إتخاذ التدابير والإجراءات المساعدة على زيادة التنافس بين الشركات المستثمرة في مجال خدمات الإنترنت .
- 4- تبني الحكومة إستراتيجية تهدف إلى زيادة نسبة إستخدام الإنترنت .
- 5- تقليص الفجوة الرقمية بين شرائح المجتمع لتحقيق الوصول الشامل لخدمات الإتصالات.

## II- المستوى الثاني :

تعتمد الإدارة في هذا المستوى على تحقيق التفاعل مع المتعاملين عبر شبكة الانترنت بشكل مستمر، وذلك عن طريق النماذج الإلكترونية، البريد الإلكتروني، الإتصال عبر الموقع، حتى يتسنى التأكد من المعلومات، أو طبع الاستمارات والنماذج، أو الإستفسار عن بعض المعلومات.

إن الإدارة تحتاج في هذا المستوى إلى مجموعة من الإجراءات اللازمة لهذا الغرض

وهي<sup>1</sup>:

- 1- توفير المعلومات والبيانات وحمايتها بالقوانين المناسبة .
- 2- تمويل البرامج التدريبية لإستخدام تكنولوجيا المعلومات .
- 3- توفير الإمكانيات المادية لتحقيق العمليات التقنية من تصميم ونشر، تحديث، صيانة مواقع.

---

1 : حماد مختار ، مرجع سابق ، ص 29 .

### III- المستوى الثالث :

تقوم الإدارة في هذا المستوى بإنجاز جزء من المعاملات أو جميعها عن طريق شبكة الإنترنت، ويتطلب هذا وضع الإطار القانوني لهذا النوع من المعاملات .  
فالإدارة ستتعامل مع المواطن أو بقية المتعاملين بوثائق إلكترونية، وسيتم أيضا تأدية الخدمات بشكل إلكتروني مثل تسديد الرسوم، دفع الضرائب وغيرها .

### IV- المستوى الرابع :

تعمل الإدارة في هذا المستوى على تقديم الخدمات وأداء الأعمال من موقع واحد، ولذلك يسمى بمستوى التكامل الأفقي الذي يتطلب قواعد بيانات عملاقة عن كافة الأفراد والمؤسسات لتقديم الخدمة من خلال أي وحدة مهما تعددت الجهات المتعامل معها<sup>1</sup> .

### الفرع الرابع : الحكومة الإلكترونية

الحكومة الإلكترونية هي البوابة الرئيسية للمعاملات الإلكترونية ، كما إن تطبيقها يضمن التحول الكلي إلى العالم اللأورقي.

### أولا : بدايات الحكومة الإلكترونية

بدأت تجربة الحكومة الإلكترونية في أوساط الثمانينات من القرن الماضي في الدول "الاسكندنافية"، حيث ربطت القرى البعيدة بالمركز وسميت بالقرى الإلكترونية، وأصبحت تعرف

---

1 : حماد مختار ، مرجع سابق ، ص 31 .

بمركز الخدمة عن بعد ، وقد أطلق هذه الفكرة البروفسور "LARS" من جامعة "AODNEIS" بالدنمارك .

أما في "بريطانيا" فكانت التجربة عام "1989" ضمن مشروع قرية مانشيستر، حيث بدأ تقديم بعض الخدمات بشكل الكتروني وهذا حتى نهاية القرن، ثم قدم مشروع الحكومة الإلكترونية عام "2000" وفق إستراتيجية متكاملة تهدف إلى التحول كلياً نحو هذه الحكومة بحلول عام "2005".

وفي "الولايات المتحدة الأمريكية" انطلق مشروع الحكومة الإلكترونية عام "1995" في ولاية فلوريدا، حيث تعود جذوره إلى سنة "1993" عندما أعد نائب الرئيس الأمريكي "ALGORE" تقرير حول تحسين أداء الحكومة لأعمالها<sup>1</sup>.

وقد انتشر نظام الحكومة الإلكترونية في العديد من الدول الأوربية، غير أن الميلاد الرسمي والسياسي لهذه الحكومة كان بمؤتمر "نابولي" بإيطاليا في مارس 2001<sup>2</sup> .

وفي الدول العربية بدأ مشروع الحكومة الإلكترونية بصورة جزئية بداية القرن "21" استجابة لتوصيات "مؤتمر القمة العالمية لمجتمع المعلومات" الذي عقد في جنيف (10-12 كانون الأول 2003) وضم 18 دولة عربية<sup>3</sup> منها "الجزائر" .

---

1: لمزيد من التفاصيل أنظر : عبد الفتاح بيومي حجازي، "الحكومة الإلكترونية". دار الفكر الجامعي ، ط1، الإسكندرية، 2008، ص.ص 119-122 .

2: خالد ممدوح إبراهيم، "أمن الحكومة الإلكترونية". الدار الجامعية، الإسكندرية، 2008، ص.ص 15-17 .

3: ذاكر محي الدين، "آفاق استراتيجية : دور الحكومة الإلكترونية في التنمية المستدامة"، جريدة الصباح، يومية، العراق 19 أوت 2009، (www.Alsabah.com).

وتعتبر الإمارات العربية المتحدة الأولى عربياً في مجال تطبيق الحكومة الإلكترونية ، فقد أعلن عن هذه الفكرة صاحب السمو الشيخ "محمد بن راشد آل مكتوم" نائب رئيس الدولة حاكم دبي بداية عام "2000"، بينما كان الانطلاق الرسمي للحكومة الإلكترونية في 29 أكتوبر 2001، وفي مارس 2009 أصدر صاحب السمو قانون رقم 07 لسنة 2009 الذي قضى بإنشاء دائرة حكومة دبي الإلكترونية \* .

وتحتل الإمارات العربية المتحدة المرتبة الثانية والثلاثين عالمياً بين 192 دولة عضو في الأمم المتحدة حسب تقرير الأمم المتحدة 2008 المتعلق بترتيب الحكومات الإلكترونية حول العالم.

وقد انتشر هذا النظام في العديد من الدول العربية في مطلع القرن 21 في كل من السعودية، الكويت، البحرين، الأردن، لبنان، تونس، مصر، وغيرها. إذن يمكن القول أن الحكومة الإلكترونية مرت بعدة مراحل وهي:

**1- المرحلة الأولى:** وذلك ببداية استخدام الحاسب الآلي في العمل الإداري وتقديم الخدمات، لكن بوجود الموظف والمواطن في مكان ثابت، وقد بدأت هذه المرحلة في النصف الثاني من القرن 20.

**2- المرحلة الثانية :** وهي مرحلة السبعينات والثمانينات حيث بدأ العمل بأنظمة المعلومات في الأعمال الإدارية، وأصبح بإمكان المواطن الحصول على الخدمة أو المعلومة عن بعد .

---

\* : البوابة الرسمية لحكومة دبي : [www.dubai.ae/ar.portail](http://www.dubai.ae/ar.portail)

3- المرحلة الثالثة : وهي مرحلة منتصف التسعينات التي ارتبطت بظهور الانترنت، وهي مرحلة الذروة، حيث تم الاعتماد على هذه الشبكة في المعاملات وتقديم الخدمات، وأصبح بإمكان كل من المواطن والموظف التعامل عن بعد<sup>1</sup> .

### ثانيا : مفهوم الحكومة الإلكترونية

يعرف البعض الحكومة الإلكترونية بالمعنى الواسع بأنها "الإستخدام الواسع للتكنولوجيا الحديثة لإعادة تنظيم الإدارات الحكومية وتطوير البنية التحتية المحلية اللازمة لذلك، بشكل يؤدي إلى استفادة الحكومة من الانترنت والمعلومات والاتصالات التكنولوجية لانجاز معاملات الأفراد بسهولة وسرعة"<sup>2</sup> .

أما المعنى الضيق لها فيشير إلى أنها مجموع الأنشطة الحكومية المعتمدة على الانترنت والاتصالات الإلكترونية عبر جميع طبقات ومستويات الحكومة ، لتقديم جميع الخدمات والمعاملات للأفراد والحصول على المعلومات في شتى المجالات ببسر وسهولة، ويطلق على هذه الأنشطة الإجراءات الإدارية الإلكترونية<sup>3</sup> .

وهناك اتجاه آخر يمزج بين معنى الحكومة الإلكترونية ومصطلح الإدارة الإلكترونية بالمعنى الواسع، فيعرفها بأنها قدرة القطاعات الحكومية على تبادل المعلومات وتقديم الخدمات فيها بينها وبين المواطن، وبين قطاعات الأعمال بسرعة ودقة عالية وبأقل تكلفة عبر شبكة

1 : نوبي محمد حسن، "منظومة الحكومة الإلكترونية"، ب.ت، ([www.Publications.Ksu.edu.Sa/Conférences](http://www.Publications.Ksu.edu.Sa/Conférences)).

2 : سهيل ياسين، "الحكومة الإلكترونية"، جريدة الصباح يومية، العراق، 2009/09/20، ([www.Alsabah.com](http://www.Alsabah.com)).

3 : أنظر في هذه التعاريف : داوود عبد الرزاق الباز، مرجع سابق ، ص.ص 74 ، 75 .

الإنترنت، أو وسائل الاتصال الأخرى مع ضمان سرية وامن المعلومات المتناقلة في أي وقت وأي مكان .

إلا أن البعض الآخر يرى تعارض المعنيين حيث إن الحكومة الإلكترونية لها معني خاص في القانون الدستوري، ولذلك من الأنسب استخدام مصطلح الادارة الإلكترونية لان المراد من مصطلح الحكومة الإلكترونية ليس ممارسة الحكم بطريقة الكترونية وإنما المقصود إدارة النشاط الحكومي بطريقة الكترونية<sup>1</sup>، حيث يركز تعريف الحكومة الإلكترونية على فكرتين هما استعمال تكنولوجيا المعلومات والاتصال وتغيير العلاقات مع مجموع الأطراف الداخلية والخارجية<sup>2</sup> .  
ولذلك فان هذه الحكومة تقوم على مبدئين الأول فني يتمثل في إعداد المعلومات الكترونيا وتناقلها عبر شبكة الانترنت وضمان دقتها وسريتها، والثاني إجرائي ويتمثل في تنفيذ المعاملات والخدمات عن بعد مع ضمان صدقها ومصداقيتها .

### ثالثا : مستويات الحكومة الإلكترونية

صنف الكاتب "ريتشارد هيكس" في كتابه "الحكومة الإلكترونية" هذه المستويات إلى خمس<sup>3</sup>:

#### 1 – المستوى الأول:

في هذا المستوى تقوم المؤسسة الحكومية بحفظ البيانات وتحديثها، وعرضها على

---

1 : عبد الفتاح بيومي حجازي، "الحكومة الالكترونية بين الواقع والطموح". دار الفكر الجامعي، ط1، الإسكندرية، 2008، ص. 25 .

2 : Gilles St Am ant, Op.Cit, P. 3.

3 : كتب المدير رجل الأعمال ، مجلة خلاصات ، عدد 19، (أكتوبر 2003).

المواطن، ولا تقوم بأكثر من ذلك فمهمتها هنا استعلامية فقط حيث تعرض ما لديها من بيانات حول الخدمات العامة، ولا تستطيع استقبال بيانات من المستخدمين لتعطي نتائج جديدة، ولذلك تعتبر هذه الخدمات صماء.

## 2 . المستوى الثاني:

تصبح المؤسسة الحكومية في هذا المستوى أكثر ايجابية، حيث تشرع في تقديم بعض الخدمات البسيطة، إذ يمكن للمستخدم إدخال البيانات الخاصة به، حيث يتم اعتمادها وتسجيلها ضمن الأرشيف (مثل طلبات الترخيص أو الدفع بواسطة بطاقة الائتمان).

## 3 . المستوى الثالث:

في هذا المستوى يصبح التفاعل بين المؤسسة الحكومية والمستخدم ثنائياً، إذ يمكن للمستخدم إدخال بياناته، ليتم معالجة هذه البيانات، ثم عرض النتيجة عبر الموقع الإلكتروني (مثل خدمة استخراج شهادة رسمية).

في هذه المرحلة تبرز العلاقة بين هذه الحكومة والتعامل بالوثائق المعلوماتية، ومن ثم يصبح من الضرورة حماية هذه الوثائق ضد الاعتداءات المختلفة ومن أشكالها التزوير.

## 4 . المستوى الرابع:

في هذا المستوى يتم إيجاد ربط شبكي بين المؤسسات الحكومية المختلفة، حيث يحصل المستخدم على ما يريد من الخدمات من أي جهة حكومية من موقع الكتروني واحد دون الحاجة إلى التنقل بين أكثر من موقع كلما اختلفت الخدمة المطلوبة .



## 5 . المستوى الخامس:

في هذا المستوى تأخذ المؤسسة الحكومية دور المبادر، فبدل من أن يطلب المواطن الخدمة، يتم الاتصال به رقمياً لطلب البيانات التي تمكنه من الحصول على الخدمة. إن الذي أضافته الحكومة الإلكترونية اليوم هو قدرات التواصل من خلال الاتصال، التفاعل، المساهمة بين عدة أشخاص، وحدات إدارية ومنظمات .

### المطلب الثاني: متطلبات التحول إلى المعاملات الإلكترونية

إن استخدام المعاملات الإلكترونية في المؤسسات الحكومية والتحول من البيئة الورقية إلى البيئة اللورقية يستوجب مجموعة من المتطلبات القانونية والتقنية الضرورية لضمان هذا الإستخدام .

### الفرع الأول: المتطلبات القانونية للتحول إلى المعاملات الإلكترونية

هذه المتطلبات القانونية هي من المتطلبات الأساسية لتطبيق الحكومة الإلكترونية، ويتحقق ذلك من خلال جهودات تشريعية ومخصصة لبناء الإطار القانوني المناسب لكل ما يتعلق بالمعاملات الإلكترونية سواء من حيث التعامل بها، أو من خلال ضبط المصطلحات القانونية والتقنية المرتبطة بها، وكذا من حيث استحداث نصوص جنائية لمواجهة الجرائم المتعلقة بها .

وتتمثل الخطوات التشريعية اللازمة لتحقيق ذلك فيما يلي :

1- قيام الحكومات بعمليات مسح تشريعي لكل الأنظمة واللوائح والتشريعات للوصول إلى أطر قانونية محددة.

2- مراجعة المفاهيم والأطر التشريعية التقليدية للعمل على تعديلها أو استبعادها<sup>1</sup>.

3- استنباط قواعد ومفاهيم جديدة ومستحدثة نتجت عن النظام الإلكتروني الجديد، وهي مستخدمة في هذه البيئة من المعاملات، مع ضبط التعاريف القانونية والتقنية المتعلقة بها مثل المعاملات الإلكترونية، المعاملات الإلكترونية المؤتمنة، الرسالة الإلكترونية، الوسيط الإلكتروني، توثيق المعاملة الإلكترونية، التوقيع الإلكتروني، جهات التصديق الإلكتروني، وغيرها من المصطلحات ذات الصلة بهذا المجال .

4- وضع الإطار التشريعي المناسب لصحة المعاملات الإلكترونية وذلك من خلال الاعتراف بحجية الرسائل الإلكترونية التي تتم بها هذه المعاملات، لحسم الجدل الفقهي والقضائي في هذه المسألة.

ويبقى الأمر في مجال وضع الأطر التشريعية المتعلقة بالمعاملات الإلكترونية يتأرجح بين ثلاث توجهات، حيث يمكن لكل دولة أن تحسم التوجه الخاص بها، إذ يمكن لها تعديل القواعد والنصوص التنظيمية المطبقة على المعاملات الإدارية السارية بالوسائل التقليدية لتشمل المعاملات الإلكترونية .

كما يمكن الاستغناء عن القواعد التقليدية، ووضع نصوص مستقلة وخاصة بتطبيق المعاملات الإلكترونية. وقد يتم اختيار التوجهين معا .

---

1: علي محمد عبد العزيز، "تطبيقات الحكومة الإلكترونية"، (رسالة ماجستير)، كلية الدراسات العليا ، قسم العلوم الإدارية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2005/06/07 ، ص . 51 .

ومن بين الجهود الدولية لمساعدة الدول في وضع قوانينها المتعلقة بالمعاملات الإلكترونية (أيا كان التوجه التشريعي الذي تختاره) ، ما قامت به لجنة الأمم المتحدة للقانون التجاري الدولي من أجل وضع قانون للمعاملات الإلكترونية التجارية<sup>1</sup> .

كما تم الاستفادة من هذا القانون في تنظيم المعاملات الإلكترونية الحكومية أيضا، وذلك من أجل مواجهة الفراغ التشريعي الموجود في بعض القوانين الوطنية والذي يقف عائقا أمام اعتماد هذه المعاملات، وكذا محاولة إيجاد مجموعة من القواعد المقبولة دوليا بحيث يمكن للدول الاستفادة منها مهما اختلفت أنظمتها وتوجهاتها الاقتصادية والاجتماعية، ولتجنب أية عقبات قد تواجهها نتيجة استعمال الوسائل الإلكترونية كبديل للوسائل التقليدية.

ومن أجل ضبط المصطلحات القانونية والتقنية المرتبطة بالمعاملات الإلكترونية، فقد تضمن الفصل الأول من هذا القانون تعريفات لمجموعة من المصطلحات .

كما تضمن الفصل الثاني كيفية تطبيق الإشتراطات القانونية المتعلقة بالكتابة والتوقيع عندما يتعلق الأمر برسائل بيانات، وبالتالي إبراز مسألة القيمة القانونية للمستندات الإلكترونية، وصحة التعامل برسائل البيانات. ولذلك تناول هذا القانون المتطلبات الواجب توافرها في رسالة المعلومات لتؤدي وظيفة الوثائق الورقية .

---

**1** : صدر هذا القانون بقرار من الجمعية العامة 162/51 المؤرخ في 16 ديسمبر 1996 المتضمن قانون الأونسترال النموذجي بشأن التجارة الإلكترونية. متوفر على موقع : [www.uncitral.org/uncitral/ar/uncitral-texts/electronic-modelcommerce/1996](http://www.uncitral.org/uncitral/ar/uncitral-texts/electronic-modelcommerce/1996)

## الفرع الثاني : المتطلبات التقنية للتحويل إلى المعاملات الإلكترونية

ترتبط المتطلبات التقنية بجوانب فنية، وأخرى تتعلق بتوفير الأمن المعلوماتي، حيث لا يكفي وضع الإطار القانوني بدون تهيئة القاعدة التقنية التي تمكن من إنجاز المعاملات الإلكترونية بأمان .

### أولاً : إتاحة المعلومات عبر الشبكة

من أجل إتاحة المعلومات للجميع عبر الشبكة بكثافة وشفافية لا بد من توسيع قاعدة الوصول إلى المعلومات والخدمات الحكومية، وذلك من خلال توفير المعلومات اللازمة لجمهور المواطنين، العملاء، والمؤسسات المتعاملة مع الحكومة بغرض إنجاز المعاملات بسرعة ويسر .

ويمكن للحكومات التي تدخل مشروع الحكومة الإلكترونية في مستوياته الأولى أن تقوم بنشر المعلومات الخاصة بها على الشبكة مبتدئة بنشر الوثائق، النماذج، والإستمارات لتقديم الخدمات الحكومية<sup>1</sup> ، حتى يتجنب المتعامل التوجه شخصياً إلى الإدارة أو المؤسسة مقدمة الخدمة .

وللقيام بهذا الدور لا بد من القيام بالخطوات التالية<sup>2</sup> :

---

1: سحر قدوري الرفاعي، "الحكومة الإلكترونية وسبل تطبيقها"، مجلة اقتصاديات شمال إفريقيا، عدد07، ب.ت، ص. 317.  
2: نفس المرجع، ص . 318 .

1- البدء بإعداد استراتيجية واضحة لوضع وتحميل المعلومات على الشبكة وإتاحتها للمستفيدين.

2- تكليف المؤسسات الحكومية بنشر معلومات محددة على الشبكة تسهم في تيسير تعامل جمهور المواطنين والأعمال لقضاء حاجاتهم على الشبكة .

3- تصميم المواقع على الشبكة ، وصيانتها، وتحديثها باستمرار .

وفي مرحلة لاحقة عندما يتم الانتقال من مستوى تقديم المعلومات فقط، إلى مستوى تقديم الخدمة على الشبكة، ستظهر تطبيقات مختلفة لتقديم هذه الخدمة منها<sup>1</sup> :

### 1- الإدارة الافتراضية لتقديم الخدمة على الشبكة :

حيث تهدف البرامج المستخدمة لذلك إلى تنمية وتفعيل الخدمات الإلكترونية للإدارة، تقليل حجم العمل وازدحام المتعاملين، تقليل العمل اليدوي، السرعة والدقة في إنجاز المعاملات .

### 2- خدمة العملاء :

حيث يتم تزويد العملاء بكافة المعلومات وتحديثها دوريا بما يضمن توفير الوقت والجهد على العميل لإنجاز معاملته .

---

1 : علي محمد عبد العزيز، مرجع سابق ، ص . ص 121 - 124 .

### 3- خدمة تقديم طلب الخدمة الكترونيا :

حيث يحصل المستفيد على نموذج الطلب عبر الانترنت ليقوم بتعبئته، وإعادته للإدارة على الشبكة، وبالتالي يمكن إنجاز المعاملة دون الحاجة لمراجعة الإدارة .

### 4- خدمة تسديد الرسوم :

ترتبط هذه الخدمة بالدفع الإلكتروني، الذي يختصر على المواطن كما كبيرا من الإجراءات والمعاملات التي تستوجب تسديد رسوم .

### ثانيا : الأمن المعلوماتي

يتطلب تحقيق الأمن المعلوماتي توافر العناصر التالية 1 :

- 1- المحافظة على المعلومات وسلامتها وسريتها وملكيته .
- 2- المحافظة على المعلومات من تداخل إستخدامها أو تخريبها أو استخدام معلومات مضللة، أو تحريفها أو استبدالها أو سوء استخدامها .
- 3- معالجة جميع الخروقات المتعلقة بالسلامة والسرية والملكية .
- 4- الإجراءات التي تحقق الحماية .
- 5- الحماية الدقيقة من خلال صياغة ضوابط واضحة ومحددة بشكل سليم للمراقبة الأمنية وتطبيقها بفاعلية .

---

1: عمر بن محمد العتيبي، الأمن المعلوماتي، "أطروحة دكتوراه في العلوم الأمنية" ، كلية الدراسات العليا، قسم العلوم الإدارية، جامعة نايف، الرياض ، 2010 ، ص . 15 .

كما أنه لا بد من حماية الأنظمة المعلوماتية ، والذي يتضمن عدة جوانب مترابطة <sup>1</sup> :

1. صلابة الشبكات ضد الاعتداءات .

2. الحماية ضد التعدي الفيزيائي والمعلوماتي .

3. بنية الشبكات المحمية .

4. مراقبة الدخول إلى الخدمات .

5. علم التشفير .

6. الحماية ضد الفيروسات .

### المبحث الثاني : ظهور الجرائم المتعلقة بالمعلوماتية

إن انتشار استخدام المعلوماتية في الأنشطة الحياتية المختلفة أدى إلى تنوع أشكال الإستفادة منها في مختلف المجالات .

ومع هذا الانتشار وذلك التنوع بدأت أشكال الإستعمال غير المشروع للمعلوماتية تطفو على السطح، وبالتالي تعددت أيضا أنماط السلوك غير المشروع المرتكبة باستخدام الكمبيوتر ومع خطورة بعض هذه الأنماط ومساسها بالمصالح الجديرة بالحماية فيما يتعلق باستخدام المعلوماتية، أصبحت تشكل أفعالا إجرامية .

ولذلك تنطوي الجريمة المعلوماتية على كل استعمال احتيالي أو غير قانوني للشبكات

---

1 : Laila Zouak, "Sécurité et confiance dans les Réseaux et Systèmes d'information", Atelier sur la Sécurisation des Réseaux et Systèmes d'information, Rabat ,19-20Juin 2006, P.5

المعلوماتية، والاعتداءات على أنظمة المعلومات أو المعطيات المعالجة، الإعتداء على الحياة الخاصة والمعلومات الشخصية، الإحتيال بالبطاقة البنكية، نشر الفيروسات المعلوماتية، تبييض الأموال، الإحتيال والنصب على الأشخاص، تنظيم الشبكات الإرهابية وغيرها <sup>1</sup> .

ويرى البعض أن الجريمة المعلوماتية تتطوي على صنفين من الجرائم: الجرائم المرتبطة مباشرة بتكنولوجيا المعلومات والاتصال والتي تتضمن الاعتداءات الموجهة ضد سرية وتكامل وموثوقية الأنظمة والمعطيات المعالجة، والجرائم المرتكبة بواسطة الكمبيوتر حيث تستخدم تكنولوجيا المعلومات كأداة لارتكاب هذا النوع من الجرائم، وهي تتضمن الجرائم التي تواجه في العالم المادي، أما اليوم فهي تواجه في العالم الافتراضي للإنترنت <sup>2</sup> .

### المطلب الأول : جرائم ضد سرية المعلومات وسير النظام

المعلومة هي "مجموعة من الرموز أو الحقائق أو المفاهيم، أو التعليمات التي تصلح لتكون محلا للتبادل والاتصال، أو التفسير والتأويل، أو المعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة حيث يمكن تغييرها وتجزئتها، وجمعها، أو نقلها بوسائل وأشكال مختلفة" <sup>3</sup> .

وحتى تكون المعلومة جديرة بالحماية لا بد أن تكون محددة ومبتكرة، سرية ومستأثر بها.

---

1 : Mukadi Musuyi, "Cybercriminalité, le Sida Informatique", *Revue Lubila*, n° 01, 18 Janvier 2008 .

2 : نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية. منشورات حلبي الحقوقية، ط1، بيروت، لبنان، 2005، ص97.

3 : Melanie Kowalski, "Cybercriminalité", Centre Canadien de la Statistique Juridique, Décembre 2002, P . 6 .



وتتسم المعلومة بالسرية كلما كان المجال الذي تتحرك فيه الرسالة التي تحملها محددًا بمجموعة معينة من الأشخاص، وهذه الخاصية هي التي تحدد نطاق استعمالها في دائرة محددة، بحيث يستفيد أصحابها من الخاصية الثانية، وهي الاستثناء بالمعلومة<sup>1</sup> .

ولذلك جرمت الأفعال التي يتم الاعتداء فيها على سرية المعلومات أو الاستثناء بها ومن هذه الجرائم جريمة الدخول غير المشروع للنظام ، وجريمة تعطيل نظام المعالجة الآلية .

### الفرع الأول : جريمة الدخول غير المشروع للنظام

تنص المادة الثانية من اتفاقية بودابست<sup>2</sup> على: "على كل طرف تبني التدابير التشريعية وغيرها من التدابير حيثما كان ذلك لازماً لاعتبار الدخول إلى كل أو جزء من نظام حاسب دون وجه حق جريمة طبقاً لقانونه الداخلي إذا ما ارتكبت عمداً .

وقد يتطلب الطرف الموقع أن يكون الفعل المقترف قد تم بمخالفة تدابير الأمن وذلك بنية الحصول على بيانات حاسب أو لغاية أخرى غير شريفة أو أن تكون اقترفت نظراً للصلة بنظام حاسب آخر" .

إذن هذا الفعل يتحقق بإساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه ، للوصول إلى المعلومات والبيانات المخزونة بداخله لاستخدامها في غرض ما، أو لمجرد التسلية والرغبة في الاستطلاع، أو لإشباع الشعور

---

1 : نائلة عادل محمد فريد قورة، مرجع سابق، ص . 114 .

2 : قرار 185 صادر عن المجلس الأوربي مؤرخ في 2001/11/23 حول الإجراء المعلوماتي .

بالنجاح في اختراق الحاسب الآلي على الرغم من الإحتياطات الأمنية التي يحتويها نظامه للحيلولة دون ذلك<sup>1</sup> .

ولذلك فإن هذا الدخول هو بغرض الوصول إلى المعلومات التي تمت معالجتها في النظام، والإطلاع غير المصرح به على تلك المعلومات المخزنة داخله<sup>2</sup> .

وعلى هذا الأساس تعتبر هذه الجريمة من جرائم الخطر أو السلوك المجرد، حيث لا يشترط فيها حصول نتيجة معينة، ولذلك فمجرد الاتصال غير المشروع بالنظام الذي يخزن مستندات وسجلات الكترونية، ومجموعة بيانات يؤدي إلى قيامها، لأن المصلحة المحمية في هذه الحالة هي سرية المعلومات .

ويرى البعض خلاف هذا الرأي ، حيث طالما المصلحة المحمية هي سرية المعلومات، فلا بد أن يؤدي الدخول غير المشروع إلى الوصول للمعلومات المخزنة داخل النظام وإلا لا يكتمل الركن المادي للجريمة .

ويتحقق الدخول غير المشروع<sup>3</sup>، إذا كان مخالفا لإرادة صاحب النظام أو من له حق

---

1 : نائلة عادل محمد فريد قورة، مرجع سابق ، ص . 316 .

2 : أحمد خليفة الملط، الجرائم المعلوماتية. دار الفكر الجامعي، ط2، الإسكندرية، 2006 ، ص . 190 .

3 : عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، مرجع سابق، ص . 82 .

السيطرة عليه، أو إذا كان الدخول مقيد من طرف صاحب النظام بقيود لم يتم احترامها\* .

إن فعل الدخول لا يرتبط بمعنى مادي ، وإنما بمدلول معنوي يشبه الذي نعرفه عندما نقول

الدخول إلى فكرة أو إلى ملكة التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات<sup>1</sup> .

ويعرف النظام بأنه كل وحدة أو عدة وحدات للمعالجة أو الذاكرة أو البرامج أو البيانات،

أو وحدات الإدخال أو الإخراج أو الموصلات التي تساعد في الوصول إلى نتيجة محددة<sup>2</sup> .

ويعرفه الفقه الفرنسي بأنه وحدة أو مجموعة وحدات معالجة والتي تتكون من الذاكرة

والبرامج والمعطيات، وأجهزة الإدخال والإخراج، وأجهزة الربط، والتي يربط بينها مجموعة من

العلاقات التي عن طريقها تحقق نتيجة معينة وهي معالجة المعطيات<sup>3</sup> .

أما فكرة عدم المشروعية فتربط بمعرفة من له الحق أو السلطة في الدخول إلى النظام،

ويؤدي هذا إلى اعتبار الدخول غير مشروع في حالتين تتعلق الأولى بالدخول إلى نظام

---

\*: أدان القضاء الأمريكي أحد الأشخاص بتهمة الدخول غير المشروع إلى سجلات إحدى المحاكم الاتحادية، وهي تحوي سجلات الكترونية خاصة تضم أحكام وقرارات ومستندات خاصة بدعاوى عرضت على المحكمة، أو صدر قرار فيها، بالإضافة إلى تقارير إحصائية تتعلق بعمل هذه المحاكم، حيث إن نظام حفظ هذه المعلومات مفتوح للجمهور، إلا أن حق النسخ أو الإنزال مقيد بسداد مقابل نقدي. لكن الجاني تمكن من نسخ الملايين من الصفحات باستخدام برنامج خاص لوضع ملفات الكترونية خفية في النظام حتى لا يتم احتساب نفقات النسخ (أنظر : أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني. دار النهضة العربية، ط1، القاهرة، 2006، ص . 145).

1 : آمال قارة، الحماية الجزائرية للمعلوماتية في التشريع الجزائري. دار هومة، ط1 ، الجزائر، 2006، ص . 107.

2 : محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات. دار النهضة العربية، القاهرة، 2003، ص.181.

3 : أنظر : آمال قارة ، مرجع سابق، ص . 102 .

المعالجة الآلية دون تصريح من المسؤول عنه، أما الثانية فتتعلق بالدخول إلى النظام في غير الحالات المرخص فيها بالدخول<sup>1</sup> .

إن الدخول بشكل غير مشروع للنظام بسبب الثغرات الموجودة به أو خرقاً لإجراءات أمن المعلومات، أو اختراق آليات التشفير وكلمات السر قد يكون بغرض الحصول على أغراض مادية ومعنوية من المعطيات الموجودة بالنظام<sup>2</sup> .

وتعتبر هذه الجريمة من الجرائم العمدية إذ لا بد من توافر القصد الجنائي العام المتكون من العلم والإرادة ، حيث لا بد أن يعلم الجاني بعدم أحقيته بالدخول إلى النظام ، ومع ذلك تنصرف إرادته لإثبات هذا السلوك الإجرامي مخالفة للقانون، ولا يتأثر ذلك بالباعث من الدخول حتى لو كان الفضول أو التنزه أو إثبات القدرة على الانتصار على النظام<sup>3</sup> .

### الفرع الثاني : جريمة تعطيل نظام المعالجة الآلية

تنص المادة 05 من إتفاقية بودابست على : "على كل طرف تبني التدابير التشريعية وغيرها إذا كان ذلك ضروريا لاعتبار الأفعال التالية جرائم طبقا للقانون الداخلي إذا ارتكبت عمدا إعاقة خطيرة ودون وجه حق لعمل نظام المعالجة الآلية عن طريق إدخال بيانات، أو نقلها، أو إفساد، محو، تعديل، أو حذف للمعطيات" .

---

1 : نائلة عادل محمد فريد قورة، مرجع سابق ، ص . 333 .

2 : محمد علي قطب، "الجرائم المعلوماتية وطرق مواجهتها"، الأكاديمية الملكية للشرطة، البحرين، مارس 2010.

3 : علي عبد القادر القهوجي، "الحماية الجنائية للبيانات المعالجة الكترونيا"، بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الإمارات العربية المتحدة، 1-3 مايو 2000، ص . 54 .

ترتبط جريمة تعطيل نظام المعالجة بجريمة الدخول غير المشروع، حيث يترتب على ذلك التلاعب في نظام معالجة البيانات بالتدمير أو التغيير أو الإتلاف، أو إعاقة النظام بأية وسيلة سواء كانت الإعاقة مادية عن طريق أعمال العنف المادية على مكونات الحاسب وشبكات الإتصال، أو عن طريق برنامج معلومات من خلال فيروس أو تعديل كلمة السر أو كيفية أداء النظام لوظيفته بوسيلة تؤدي إلى توقف أو تعطيل في أداء وظيفة داخل النظام المعلوماتي<sup>1</sup> .

ويتكون السلوك الإجرامي في هذه الجريمة من الأعمال التي تترك عمل نظام معالجة البيانات، بحيث يؤدي ذلك إلى إعاقة أو إفساد نظام التشغيل، سواء أدى ذلك إلى توقف النظام عن العمل بصورة دائمة أو مؤقتة<sup>2</sup> .

أما فعل الإفساد فقد لا يؤدي إلى التعطيل، بل يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم بأن يعطي نتائج غير تلك التي ينتظر حصولها، ووسائله مختلفة مثل استخدام الفيروسات التي تعمل على تغيير البرامج و المعطيات أو جعل مخرجات النظام غير تلك التي كان يتوجب إخراجها<sup>3</sup> .

ويمكن أن تؤدي إلى التعطيل كلية فهي عبارة عن مجموعة من التعليمات التي تتكاثر بمعدل سريع جدا لدرجة تصيب النظام المعلوماتي بالشلل التام<sup>4</sup> .

---

1 : علي عبد القادر القهوجي، مرجع سابق ، ص . 56 .

2 : عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، مرجع سابق ، ص . 90 .

3 : علي عبد القادر القهوجي، مرجع سابق ، ص . 57 .

4 : محمد سامي الشوا، مرجع سابق ، ص . 166 .

ويتميز الفيروس بقدرته على التخفي عند مستخدم النظام، وقدرته على الانتشار من جهاز لآخر، وكذلك داخل الشبكات، والتسلل داخل النظم المعلوماتية لاختراقها مباشرة أو عن كسر نظام الحماية لتدميرها أو تعطيلها، أو إيقاف تشغيلها، أو إتلاف أو محو أو تغيير البيانات والمعلومات المخزنة على وسائط التخزين<sup>1</sup>.

إن هذا التغيير، أو التعديل، أو حذف البيانات، أو محوها قد يستخدم لارتكاب جريمة التزوير المعلوماتي إذا كانت هذه المعلومات ضمن وثيقة معلوماتية، وهنا تظهر العلاقة بين هذه الجريمة وجريمة التزوير .

### **المطلب الثاني : جرائم ضد سلامة المعلومات وقيمتها الاقتصادية**

أشكال هذه الجرائم متعددة بتعدد أنماط السلوك الذي يؤدي إلى الاعتداء على المعلومات، أو المعطيات والبرامج أو قيمتها الاقتصادية حيث قد تأخذ شكل جريمة الاعتداء العمدي على المعطيات، وقد تشكل جريمة الإتلاف، وقد ترتبط بالإحتيال، كما قد تؤدي إلى التزوير .

### **الفرع الأول : جريمة الاعتداء العمدي على المعطيات**

نصت الاتفاقية الدولية حول الإجرام المعلوماتي ببودابست في المادة الرابعة منها على الاعتداءات الواقعة ضد تكاملية المعطيات (سلامتها) كالتالي : "على كل طرف تبني التدابير التشريعية وغيرها التي تعتبر ضرورية لتجريم الأفعال التالية طبقا لقانونه الداخلي إذا ارتكبت عمدا ودون وجه حق إتلاف أو محو أو إفساد أو تعديل أو حذف المعطيات".

---

1 : بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات. دار الفكر الجامعي، الإسكندرية، 2008، ص.372.

إن السلوك الإجرامي في هذه الجريمة يتحقق بالإتلاف أو المحو أو تعديل أو حذف المعطيات الموجودة داخل النظام، ولا يقع هذا الإعتداء إذا كان خارج النظام، سواء قبل دخول المعطيات إليه، أو بعد خروجها منه عندما تكون مفرغة على قرص أو شريط ممغنط خارج النظام .

هذه الأفعال قد لا تجتمع جميعها في فعل واحد، ولكن يكفي أن يتحقق إحداها، غير أن محل الجريمة في كل الأحوال هي معطيات أي معلومات تمت معالجتها آليا وأصبحت مجرد إشارات أو رموز تمثل تلك المعلومات<sup>1</sup> .

وتعتبر هذه الجريمة جريمة عمدية تتطلب القصد الجنائي بعنصرية العلم والإرادة، حيث تتجه إرادة المجرم إلى الاعتداء على المعطيات بأحد أنماط ذلك مع علمه بان ذلك مخالف للقانون .

إن الجرائم الماسة بقيمة معطيات الحاسوب، أو الواقعة على ذات المعطيات، كجرائم الإتلاف، وتشويه البيانات والمعلومات وبرامج الحاسوب بما في ذلك استخدام الفيروسات، وكذا الجرائم الواقعة على ما تمثله المعطيات من أموال، كجرائم غش الحاسوب، وجرائم التلاعب في المعطيات المخزنة داخل النظام من خلال تزوير المستندات المعالجة آليا واستخدامها، ليست ذات حدود قاطعة ومانعة بينها ، فالداخل حاصل ومتحقق ، حيث الاعتداء على معطيات الحاسوب بالنظر لقيمتها الذاتية أو ما تمثله، هو في ذات الوقت اعتداء على امن المعطيات<sup>2</sup> .

---

1 : علي عبد القادر القهوجي، مرجع سابق ، ص . 58.

2 : يونس عرب، "جرائم الكمبيوتر والانترنت"، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، الإمارات العربية المتحدة، 10-12 ديسمبر 2002 ، ص . 7 .

ويقصد بالمعطيات في هذا القانون طبقاً للمادة 1/ب "أية عمليات عرض للوقائع أو المفاهيم في شكل مناسب لعملية المعالجة داخل منظومة الكمبيوتر بما في ذلك البرنامج المناسب لجعل منظومة الكمبيوتر تؤدي وظائفها".

أما منظومة الكمبيوتر فيقصد بها في المادة 1/أ : "جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو التي ذات صلة بذلك ويقوم احدها أو أكثر من واحد منها، تبعا للبرنامج بعمل معالجة آلية للبيانات".

### الفرع الثاني : جرائم الإلتلاف والإحتيال

هذه الجرائم تقع على المعطيات أو المعلومات المعالجة باعتبارها ذات قيمة اقتصادية، حيث تعتبر مال وبالتالي تشملها الحماية الجنائية لكن بنصوص خاصة باعتبارها كيانات منطقية وليست مادية .

كما أن هذه الجرائم قد تكون نتيجة الدخول غير المشروع للنظام، كما قد تؤدي إلى تعطيل نظام المعالجة الآلية، أو الاعتداء على المعطيات نتيجة استخدام طرق تقنية وفنية لذلك

**أولاً : جريمة الإلتلاف\***

يعني الإلتلاف تخريب الشيء أو التقليل من قيمته بجعله غير صالح للاستعمال، أو تعطيله<sup>1</sup>.

---

\* : من التشريعات التي جرمت الإلتلاف المعلوماتي: قانون العقوبات الفرنسي رقم 88/19 (م462) .  
1 : فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون. منشورات الحلبي الحقوقية، بيروت، لبنان، 2003، ص . 200 .



وقد يقصد بالإتلاف إفناء مادة الشيء أو هلاكه كلياً أو جزئياً، أما التخريب فهو توقف الشيء تماماً عن أداء منفعته كلياً أو جزئياً دون إتلاف مادته .

أما عدم الصلاحية للإستعمال فتعني جعل الشيء لا يقوم بوظيفته على النحو الأكمل، ويعني التعطيل توقف الشيء عن القيام بوظيفته فترة مؤقتة<sup>1</sup> .

وقد يتحقق الإتلاف أو التخريب بوسائل مختلفة مادية أو معنوية سواء بالإعتداء على المعطيات والدعامة الموجودة عليها، أو محو المعطيات دون إصابة الدعامة، أو تعطيل البرامج أو محوها باستخدام أداة لهذا الغرض<sup>2</sup> .

ويشمل التعريف الواسع للبرنامج عناصر ثلاث وهي<sup>3</sup> :

(أ) البرنامج بمعناه الضيق الذي يعرف بأنه مجموعة التعليمات التي من شأنها ، عقب نقلها

على دعامة مقروءة من الآلة أن تؤدي إلى الإشارة أو التحقق أو الحصول على وظيفة أو غاية أو نتيجة معينة عن طريق آلة قادرة على معالجة المعلومات .

(ب) وصف البرنامج وهو التقديم الكامل المفصل بصورة كافية لعمليات، بغية تحديد مجموعة التعليمات المشكلة لبرنامج الحاسب الالكتروني وصلة كل منها بالأخرى.

(ج) المستندات الملحقة وهي المستندات التي ليست ببرنامج الحاسب الالكتروني ولا بوصف له، المستهدفة تبسيط فهم وتطبيق البرنامج .

---

1 : علي عبد القادر القهوجي، مرجع سابق، ص . 35 .

2 : نفس المرجع ، ص . 36 .

3 : محمد حسام محمود لطفي، الحماية القانونية لبرامج الحاسب الالكتروني. دار الثقافة للطباعة والنشر، القاهرة، 1987،

ص.ص 18-19 .

ويشكل الفعل إتلافا بالمعنى القانوني إذا كان محله المعلومات والبرامج على النحو السابق بيانه، عندما يهدف الجاني الإضرار بالغير الذي يقصد به صاحب النظام المعلوماتي الذي قد يكون مالكه أو مستأجره، أو المنتفع به أو مزوده، وبصفة عامة كل شخص له مصلحة في الاحتفاظ بالبيانات<sup>1</sup> .

ويحصل الإتلاف بعدة صور منها وسائل التخريب المنطقي ومن أهمها الفيروسات وهي برامج صغيرة لها خاصية التكاثر آليا ، وهدفها الغالب إلحاق الأضرار<sup>2</sup> ، ومن بينها<sup>3</sup> :

- 1- تعديل البيانات أو تحريفها بالإضافة أو الحذف .
  - 2- التدخل أو الاعتراض عند الاستخدام القانوني للبيانات .
  - 3- تعطيل أجزاء من مكونات الحاسب أو جعلها بلا معنى .
  - 4- تغيير وظائف البرامج مما يسبب أضرار مادية ومعنوية .
- وتترك الفيروسات في الملف المصاب أثرا خاص بكل فيروس يسمى توقيعه<sup>4</sup> .

كما قد يحصل الإتلاف عن طريق تعديل برنامج ، أو اصطناع برنامج كلية، وقد يحصل التعديل في برامج التشغيل عن طريق إضافة تعليمات يتم الوصول إليها عن طريق كلمة السر، ومن خلالها يمكن الوصول إلى جميع التعليمات التي تحويها ذاكرة الجهاز .

---

1 : محمد أمين الشوابكة، جرائم الحاسوب والانترنت. مكتبة دار الثقافة للنشر والتوزيع، ط1، عمان، الأردن، 2004، ص . 230 .

2 : "Virus Informatiques", Atelier Interne-Sécurité , Genève , 4 Juin 2004 , P . 1 .

3 : فتوح الشاذلي ، عفيفي كامل ، مرجع سابق، ص . 219 .

4 : " Virus Informatiques", Op . Cit , P . 1 .

ومن الوقائع التي تذكر في هذا الشأن قيام مجموعة من المبرمجين بشركة أمريكية بلوس أنجلس باصطناع وثائق تأمين لمؤمن عليهم وهميين اقتصر دورها على إدارة الحسابات، حيث وضعوا شفرة خاصة بالبرامج حتى لا تظهر هذه المعلومات عند الطباعة بل تظهر الوثائق السليمة فقط، وقد حصلوا من هذه العملية 200 مليون دولار<sup>1</sup> .

وكذا قضية (Cox.v.Riely) وهو مبرمج باحدى الشركات من أجل تشغيل شبكة المعلومات بها التي تعتمد في أداء عملها على بطاقة بلاستيكية ، حيث قام هذا المبرمج بمحو البرامج المخزنة عليها عن طريق خاصية الحذف ، مما أدى إلى توقف الشبكة.

وقد أدانت محكمة أول درجة المتهم بجريمة الإتلاف ، وسببت المحكمة حكمها بأن البطاقة هي من قبيل الممتلكات، وهي ملك للشركة التي يعمل بها المتهم<sup>2</sup> .

كذلك قضية (Regina.V.Turner) التي قام فيها المتهم باستخدام شبكة اتصالات في مدينة تورونتو بكندا للوصول إلى أقراص ممغنطة بها معلومات خاصة بشركات أمريكية ، حيث قام بتشفيرها مما أدى إلى إتلاف المعلومات ولذلك اعتبرت المحكمة العليا في أونتاريو أن عملية التشفير تعد حائلا دون استخدام الأقراص الممغنطة، وبالتالي وجوب تطبيق النص الخاص بجريمة الإتلاف<sup>3</sup> .

---

1 : محمد أمين الشوابكة ، مرجع سابق ، ص . 231 .

2 : نائلة عادل محمد فريد قورة ، مرجع سابق ، ص . 197 .

3 : نفس المرجع ، ص . 201 .

## ثانيا : جريمة الإحتيال

الاحتتيال هو الاستيلاء بطريق الاحتيال على شيء مملوك للغير بنية تملكه<sup>1</sup> ، ولذلك يستخدم الجاني طرق احتيالية ليستولي على مال الغير .

هذه الطرق متعددة فقد يتم تقديم بيانات غير حقيقية بتزوير بيانات شخصية، أو تزوير بطاقات ائتمانية، أو عن طريق التلاعب في بيانات السجلات أو التقارير أو غيره<sup>2</sup> .

أما عندما يتعلق الأمر بالإحتيال المعلوماتي فيسميه البعض نصب الكمبيوتر وهو يعني "أي سلوك يستلزم معالجة الكمبيوتر أو بياناته بأي طريقة للحصول على المال أو أي ميزة أخرى لها قيمة أو للإعتداء على الملكية أو التسبب في خسارة " .

إن الاستيلاء على الأموال المعلوماتية بالاحتيال كثيرا ما يرتبط بالتلاعب في مستحقات مالية وإيداعات مصرفية، وبطاقات الائتمان<sup>3</sup> .

ولذلك فالطرق الاحتيالية تعتمد على التلاعب في البرامج والبيانات والتغيير فيها مما يؤدي إلى إيهام المجني عليه بصحتها، ويعتبر الحاسوب وسيط لهذا التحايل<sup>4</sup> .

ولذلك يعرف الإحتيال المعلوماتي بأنه " التلاعب العمدي بمعلومات وبيانات تمثل قيما مادية، يخترنها نظام الحاسب الآلي، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة،

---

1 : محمد سامي الشوا ، مرجع سابق ، ص . 121 .

2 : حسين محمد الشبلي، مهند فايز الدويكات، الاحتيال المصرفي. دار مجدلوي، ط1، عمان، الأردن، ب.ت، ص.53 .

3 : أحمد خليفة الملت ، ، مرجع سابق ، ص . 324 .

4 : هدى حامد قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن . دار النهضة العربية، القاهرة، 1992، ص.133.

أو التلاعب في لأوامر والتعليمات التي تحكم عملية البرمجة، أو أية وسيلة أخرى من شأنها التأثير على الحاسب الآلي حتى يقوم بعملياته بناء على هذه الأوامر أو التعليمات، من أجل الحصول على ربح غير مشروع وإلحاق ضرر بالغير"<sup>1</sup>.

وبالتالي فإن الركن المادي في هذه الجريمة هو التلاعب في معلومات وبيانات لها قيمة مالية بطرق احتيالية ، قد لا تكون محصورة تماشياً مع طبيعة الاحتيال المعلوماتي، فالجريمة المعلوماتية بصفة عامة جريمة متطورة ومتجددة لارتباطها بتكنولوجيا المعلومات فلا يمكن التنبؤ مستقبلاً بالوسائل التي يمكن أن يلجأ إليها الجاني في مجال الجريمة المعلوماتية حيث إن التطور التكنولوجي قد يسفر دائماً عن وسائل جديدة لم تكن معلومة من قبل<sup>2</sup> . ولكنها تؤدي بالضرورة إلى نتيجة وهي الإستيلاء على مال الغير، أو الحصول على كسب مادي غير مشروع، وبالتالي فإن الطرق الاحتيالية التي اتخذها الجاني تربط بينها وبين المال الذي حصل عليه علاقة هي السبب في هذه الجريمة، ولولا هذه الطرق الاحتيالية لما تمت الجريمة التي أوقعت المجني عليه في الخطأ نتيجة لها وجعلته يسلم ماله<sup>3</sup> .

وعندما يتم استخدام الكمبيوتر فإن هذه الوسيلة تضع المال تحت تصرف الجاني نتيجة هذه الأساليب والطرق الاحتيالية .

---

1 : نائلة عادل محمد فريد قورة ، مرجع سابق ، ص . 425 .

2 : نفس المرجع ، ص . 463 .

3 : أحمد خليفة الملط ، مرجع سابق ، ص . 346 .

أما الضرر الذي قد ينجم عن هذا الاستيلاء فهو عنصر مختلف فيه، حيث يعتبر البعض هذه الجريمة من جرائم الضرر وبالتالي لا بد من وقوعه، بينما لا يراه البعض الآخر ضروريا لاكتمال الركن المادي .

وتعتبر هذه الجريمة جريمة قصدية ، حيث لا بد أن يعلم الجاني أنه يستخدم طرق احتيالية، وهو يريد من وراء ذلك سلب مال الغير بالغش والتحايل على النظام المعلوماتي. إن الجرائم السابقة تتداخل مع بعضها البعض في كثير من الأحيان، وقد ترتبط بجريمة التزوير المعلوماتي، أو قد تشته به في بعض العناصر ولذلك انتهجت التقسيم السابق للجرائم الواقعة على المعلومات.

فقد ترتبط جرائم الاعتداء على المعلومات بجريمة التزوير عندما يحصل إدخال معلومات مصطنعة لنظام المعالجة الآلية، أو التعديل في البيانات المخزنة داخله . كما قد ترتبط جريمة التزوير بجريمة الاحتيال على النظام عندما تستخدم بطاقات ائتمان مزورة .

وقد تتداخل جريمة الإتلاف مع جريمة التزوير باعتبار أن الركن المادي فيهما يتعلق بأفعال المحو أو التعديل أو التغيير في معلومات معالجة آليا .

## الباب الأول

### الوثيقة المعلوماتية محل التزوير

ترتبط جريمة التزوير المعلوماتي بوجود وثيقة بالمفهوم القانوني، فهذه الجريمة تدور وجودا وعلما بوجود هذه الوثيقة أو انعدامها.

ولذلك تسعى بعض التشريعات إلى تعريف الوثيقة سواء عند تجريم التزوير المعلوماتي بنصوص خاصة، أو عند تنظيم الوثيقة باعتبارها دليل إثبات في القانون المدني أو قانون الإثبات .

إن هذه الصلة الوطيدة بين قيام هذه الجريمة ووجود الوثيقة يوجب التطرق لمفهومها وقيمتها الثبوتية في باب مستقل ، خاصة بظهور هذه الطائفة المستجدة من الوثائق ذات الطبيعة المعلوماتية وما تثيره من إشكالات في تحديد مدلولها، ومدى قيمتها كدليل إثبات باعتبار أن جريمة التزوير لا تقع إلا إذا كان لهذه الوثيقة قيمة قانونية .

إن تحديد هذه المسائل يستوجب البحث في الإتجاهات التشريعية والفقهية لتحديد مدلول الوثيقة المعلوماتية بصفة عامة ، وتحديد قيمتها القانونية الذي يؤدي بالضرورة إلى تحديد الشروط الواجب توافرها فيها للتمتع بالحماية القانونية ضد التزوير .

## الفصل الأول : مفهوم الوثيقة المعلوماتية تشريعا وفقها

لتحديد مفهوم الوثيقة المعلوماتية لا بد من الرجوع إلى مجموع التشريعات المقارنة التي نظمت التعامل بها من خلال النصوص التي تضمنتها في المعاملات القانونية المختلفة، بالإضافة إلى استعراض الآراء الفقهية في مفهوم الوثيقة المعلوماتية ومحاولة تقديم نماذج للوثيقة المعلوماتية الرسمية الصادرة عن جهات إدارية .

### المبحث الأول : مفهوم الوثيقة المعلوماتية في التشريعات المقارنة

تناولت مجموعة من التشريعات - السبّاقة في تنظيم التعامل بالوثائق المعلوماتية- مفهوم الوثيقة المعلوماتية عند تنظيم المعاملات الإلكترونية المختلفة سواء على صعيد المعاملات التجارية، أو عند تنظيم المعاملات الحكومية الإدارية وهو الجانب الذي يخصنا في هذا البحث. ولذلك سنحاول التركيز على أهم القوانين الدولية والداخلية التي وضعت إطارا قانونيا للتعامل بالوثيقة المعلوماتية .

### المطلب الأول : مفهوم الوثيقة المعلوماتية في القانون الدولي

من القوانين الدولية المهمة والسبّاقة في تنظيم التعامل بالوثيقة المعلوماتية نجد قانون الأونسترال باعتباره نموذجا وضع في متناول الدول التي تسعى إلى التحول إلى المعاملات الإلكترونية خاصة التجارية، ومساعدتها على وضع الأطر القانونية لذلك .



## الفرع الأول : عناصر الوثيقة المعلوماتية في قانون الأونسترال النموذجي

أشار قانون الأونسترال النموذجي للتجارة الإلكترونية إلى الوثيقة المعلوماتية باستخدام مصطلح رسالة البيانات في المادة 02 فقرة 01 حيث عرفها بأنها: "المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل الكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكترونية، أو البريد الإلكتروني، أو البرق، أو التلكس، أو النسخ البرقي".

يشير منير محمد الجنبهي وممدوح محمد الجنبهي في تعليقهما على هذا النص<sup>1</sup>، إلى أن مفهوم الرسالة يشمل مفهوم السجل، غير أنه يمكن إضافة تعريف للسجل وفقا للعناصر المميزة للكتابة الواردة في المادة 06 (من هذا القانون)، وهو يقصد هنا بالسجل الوثيقة .

وبالرجوع إلى هذا النص نجد ينص على: "(1) عندما يشترط القانون أن تكون المعلومات مكتوبة، تستوفي رسالة البيانات ذلك الشرط إذا تيسر الإطلاع على البيانات الواردة فيها على نحو يتيح استخدامها بالرجوع إليه لاحقا .

(2) تسري أحكام الفقرة (1) سواء اتخذ الشرط المنصوص عليه فيها شكل التزام أو اكتفى في القانون بمجرد النص على العواقب التي تترتب إذا لم تكن المعلومات مكتوبة " .

هذا يعني أن رسالة البيانات تعتبر وثيقة عندما تتضمن معلومات مكتوبة، وذلك عندما يمكن الإطلاع على هذه المعلومات ، والرجوع إليها كلما دعت الحاجة .

---

1 : منير محمد الجنبهي، ممدوح محمد الجنبهي، تزوير التوقيع الإلكتروني. دار الفكر الجامعي، الإسكندرية، 2006 ، ص.

وبالتالي فإن رسالة البيانات في هذا القانون قد تعبر عن معنى الوثيقة، إذا اشترط القانون أن تكون هذه المعلومات مكتوبة .

كما أن المادة 07 تشير إلى عنصر التوقيع في رسالة البيانات وهو من عناصر الوثيقة المعلوماتية، حيث تنص على ما يلي :

"(1) عندما يشترط القانون وجود توقيع من شخص ، يستوفي ذلك الشرط بالنسبة إلى رسالة البيانات إذا :

(أ) استخدمت طريقة لتعيين هوية ذلك الشخص والتدليل على موافقة ذلك الشخص على المعلومات الواردة في رسالة البيانات.

(ب) كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشئت أو أبلغت من أجله رسالة البيانات في ضوء كل الظروف بما في ذلك أي اتفاق متصل بالأمر " .

كما تشير المادة 08 من هذا القانون إلى عنصر سلامة المعلومات من التغيير، وهو عنصر أساسي في الوثيقة، إذ تنص على ما يلي :"(1) عندما يشترط القانون تقديم المعلومات أو الإحتفاظ بها في شكلها الأصلي تستوفي رسالة البيانات هذا الشرط إذا :

(أ) وجد ما يعول عليه لتأكيد سلامة المعلومات منذ الوقت الذي أنشئت فيه للمرة الأولى في شكلها النهائي، بوصفها رسالة بيانات أو غير ذلك .

(ب) كانت تلك المعلومات مما يمكن عرضه على الشخص المقرر أن تقدم إليه وذلك عندما يشترط تقديم تلك المعلومات " .

وتنص الفقرة (3) على : "لأغراض الفقرة الفرعية (أ) من الفقرة (1) :

(أ) يكون معيار تقدير سلامة المعلومات هو تحديد ما إذا كانت قد بقيت مكتملة ودون تغيير، باستثناء إضافة أي تظهير يطرأ أثناء المجرى العادي للإبلاغ والتخزين والعرض.

(ب) تقدير درجة التعويل المطلوب على ضوء الغرض الذي أنشئت من أجله المعلومات على ضوء جميع الظروف ذات الصلة".

هذا يعني أن أي إضافات لازمة لرسالة البيانات حسب المجرى العادي للإبلاغ والتخزين والعرض لا يعتبر تغيير في هذه المعلومات مثل إضافة تصديق الكتروني، أو إضافة بيانات في بداية الرسالة أو نهايتها لغرض إرسالها .

وفي سياق تنظيم مسألة حجية رسالة البيانات في الإثبات، أشارت المادة 09 من هذا القانون إلى ضرورة المحافظة على سلامة المعلومات، إذ نصت الفقرة (2) من هذه المادة على: "يعطى للمعلومات التي تكون على شكل رسالة بيانات ما تستحقه من حجية في الإثبات. وفي تقدير حجية رسالة البيانات في الإثبات، يولى الاعتبار لجدارة الطريقة التي استخدمت في إنشاء أو تخزين أو إبلاغ رسالة البيانات بالتعويل عليها، ولجدارة الطريقة التي استخدمت في المحافظة على سلامة المعلومات بالتعويل عليها، وللطريقة التي حددت بها هوية منشئها ولأي عامل آخر يتصل بالأمر".

وهذا يعني أن رسالة البيانات قد يعول عليها كدليل إثبات بنفس قوة الدليل الكتابي إذا توافرت الشروط المطلوبة والمنصوص عليها في هذا القانون.

أما الدعامة التي تثبت عليها هذه المعلومات فهي غير محددة بنوع معين، ولذلك فإن هذا القانون يغطي كل الحالات الواقعية التي تنشأ فيها معلومات أو تخزن أو تبلغ بصرف النظر

عن الوساطة التي قد تثبت عليها هذه المعلومات...، غير أن مرتكز القانون النموذجي هو وسائط الإتصال غير الورقية<sup>1</sup> .

ومن أجل ذلك فقد أشارت المادة 02 السابقة الذكر إلى وسيلة إنشاء أو إرسال أو استلام أو تخزين المعلومات وهي الوسائل الإلكترونية أو الضوئية أو وسائل مشابهة، والتي يقصد بها جميع وسائل إبلاغ المعلومات وتخزينها التي قد تستعمل لأداء وظائف موازية للوظائف التي تؤدي بالوسائل المذكورة في التعريف<sup>2</sup>، وهذا حتى يتم استيعاب أي وسيلة مستجدة تفضي إليها التكنولوجيا المتطورة .

ويلاحظ أن هذا التشريع قد استخدم مصطلح "رسالة البيانات"، رغم أن البيانات تعني "كلمات وأرقام ورموز وحقائق وإحصاءات خام لا يوجد أي صلات بينها، وهي صالحة لتكوين فكرة أو معرفة بواسطة الإنسان أو الأدوات والأجهزة وهي ما تسمى بالمعالجة الآلية"<sup>3</sup>، كما تعني "مجموعة من الأرقام والكلمات والرموز أو الحقائق أو الإحصاءات الخام التي لا علاقة بين بعضها البعض ولم تخضع بعد للتفسير أو التجهيز للإستخدام والتي تخلو من المعنى الظاهر في أغلب الأحيان"<sup>4</sup> .

---

1: منير محمد الجنبهي، ممدوح محمد الجنبهي، مرجع سابق، ص. 191 .

2: نفس المرجع، ص 195 .

3: أحمد خليفة الملط ، مرجع سابق، ص. 77 .

4: نائلة عادل محمد فريد قورة ، مرجع سابق، ص . 99 .

وبذلك تختلف البيانات عن المعلومات في أن هذه الأخيرة هي "مجموعة رموز يستخلص

منها معنى معين في مجال محدد، وتتمتع بالتحديد والإبتكار والسرية والإستثناء"<sup>1</sup>.

ولذلك فإن مدلول المحرر الإلكتروني (الوثيقة المعلوماتية) يرتبط برسالة المعلومات

باعتبارها تحمل معنى معين ومحدد، حيث هذا التحديد ضروري في مجال الإعتداء على القيم،

لأن هذا التعدي يفترض دائماً شيئاً محدداً وينبغي على هذا الشيء بدوره أن يكون محلاً لحق

محدد<sup>2</sup>.

### الفرع الثاني : مبدأ النظير الوظيفي لتحديد مفهوم الوثيقة المعلوماتية

نظم القانون النموذجي للتجارة الإلكترونية رسائل البيانات وما يتعلق بها عندما تستخدم في

سياق أنشطة تجارية، وهذا ما أشارت إليه المادة الأولى "ينطبق هذا القانون على أي نوع من

المعلومات يكون في شكل رسالة بيانات مستخدمة في سياق أنشطة تجارية".

غير أن هذا القانون يقدم نصوص بديلة للدول التي قد ترغب في قصر نطاق تطبيق

قوانينها المستدة إلى القانون النموذجي على رسائل البيانات الدولية، أو تلك التي ترغب في

توسيع مدى انطباقه ليتجاوز نطاق الأنشطة التجارية<sup>3</sup>.

كما يمكن أن نستنتج أن هذا القانون قد اشتمل على ما يمكن اعتباره العناصر الرئيسية

المطلوبة من أجل إعطاء رسائل البيانات ذات المركز القانوني الذي تتمتع به المستندات

---

1: أحمد خليفة الملط، مرجع سابق، ص. 74 .

2: محمد سامي الشوا، مرجع سابق، ص. 157 .

3: عمر حسن المومني، التوقيع الإلكتروني وقانون التجارة الإلكترونية. دار وائل للنشر والتوزيع، ط1، عمان، الأردن،

2003، ص. 78 .

الورقية<sup>1</sup>، وهذا بالرجوع إلى الفصل الثاني منه المتعلق بتطبيق الإشتراطات القانونية على رسائل البيانات الذي يضم ستة مواد، وهذه العناصر تضم الكتابة، التوقيع، الشكل الأصلي للرسالة، الإحتفاظ برسائل البيانات .

إن قانون الأونسترال يعتمد على نهج " النظرير الوظيفي " في تحديده لمفهوم رسالة البيانات وقيمتها القانونية، أي محاولة تحديد مقاصد ووظائف الإشتراطات الشكلية المرتكزة على المستندات الورقية بغية تحديد المعايير التي يجب أن تفي بها رسالة بيانات من أجل إعطائها نفس الإعتراف القانوني الذي يعطي للمستند الورقي<sup>2</sup> .

ولذلك نجد في دليل الإشتراع المرفق بهذا القانون\* ضمن البند (هـ) نهج "النظرير الوظيفي" فقرة 15 أن هذا القانون يقوم على التسليم بأن الإشتراطات القانونية التي تفرض استخدام مستندات ورقية تقليدية يشكل العائق الرئيسي الذي يحول دون استحداث وسائل إبلاغ عصرية، ومن تلك الإشتراطات "الكتابة" المتطلبة ضمن القوانين الوطنية .

ومن أجل ذلك سعى هذا القانون إلى توسيع مفاهيم "الكتابة" ، "التوقيع" ، "الأصل" لتشمل التقنيات المستحدثة حاسوبيا، وهو بذلك يسمح للدول بتكييف تشريعاتها المحلية مع التطورات

---

1: عمر حسن المومني، مرجع سابق، ص . 79 .

2: نفس المرجع ، ص . 80 .

\*: هذا الدليل يوفر معلومات أيضا حية للحكومات والهيئات المشرفة لتساعدها على استخدام القانون النموذجي، كما يساعد أيضا مستعملي وسائل الإتصال الإلكترونية والباحثين في هذا المجال، ولذلك يعتبر دليل إرشادي .

الحاصلة في تكنولوجيا الإتصالات دون أن يقتضي ذلك إزالة الإشتراطات الورقية الأساس بكاملها أو التأثير على المفاهيم التي تقوم عليها تلك الإشتراطات .

وفي الفقرة 16 يشير دليل الإشتراع إلى أن القانون النموذجي يعتمد على نهج جديد هو "نهج النظرير الوظيفي" الذي يقوم على تحليل الوظائف الذي يقوم عليها الإشتراط الورقي الأساس، بهدف تقرير كيفية أداء تلك الوظائف من خلال التقنيات الحديثة، ومن بين الوظائف التي يؤديها المستند الورقي مايلي :

1- أن يكون المستند مقروء للجميع.

2- توفير إمكانية بقاء المستند بلا تحوير بمرور الزمن وإتاحة المجال لإستنساخ المستند لكي يحوز كل طرف نسخة من البيانات نفسها.

3- إتاحة المجال لتوثيق البيانات بواسطة التوقيع.

4- إتاحة وضع المستند في شكل مقبول لدى السلطات العامة والمحاكم .

إن هذه الوظائف جميعها تتوافر في السجلات الإلكترونية بمستوى الأمان نفسه بشرط الوفاء بعدد من الإشتراطات التقنية والقانونية .

لقد ارتكز قانون الأونسترال على مبدأ "النظرير الوظيفي"، لأن هذا القانون يهدف إلى إزالة العقبات والمشكلات القانونية التي تقف عائقا أمام استخدام وانتشار وسائل التبادل اللاورقي في إنجاز المعاملات القانونية المختلفة ، وفي إثباتها .

هذه العقبات نتجت أساساً عن اشتراط الكتابة بمفهومها التقليدي لإثبات المعاملات، ولذلك انطلق القانون النموذجي في العديد من قواعده من مبدأ المعاملة المتساوية بين رسائل البيانات (الوثيقة المعلوماتية) والمستندات الورقية وهذا هو مبدأ النظر الوظيفي<sup>1</sup>.

### **المطلب الثاني : مفهوم الوثيقة المعلوماتية في التشريعات الوطنية**

نظمت مجموعة من الدول العربية – التي كانت من أوائل هذه الدول التي اعتمدت نظام الحكومة الإلكترونية – كيفية التعامل بالوثيقة المعلوماتية في المعاملات التجارية، أو المعاملات الإدارية والحكومية، وخصتها بمجموعة من النصوص الخاصة، حددت من خلالها المفاهيم والمصطلحات، كما بينت القيمة القانونية لهذه الوثيقة .

ولذلك سنعرض ثلاث نماذج من هذه القوانين حسب صدورها وهي قانون المعاملات الإلكترونية في الأردن، قانون المعاملات والتجارة الإلكترونية لدولة الإمارات العربية المتحدة، قانون التوقيع الإلكتروني في مصر .

بينما سنعرض التجربة الفرنسية باعتبارها من النماذج التشريعية التي نظمت التعامل بالوثيقة المعلوماتية بصفة عامة ضمن القواعد العامة في القانون المدني المتعلقة بالإثبات.

### **الفرع الأول : مفهوم الوثيقة المعلوماتية في التشريع الأردني**

استخدم المشرع الأردني مصطلح السجل الإلكتروني بمعنى الوثيقة المعلوماتية، إذ نص

---

1: أحمد شرف الدين، " حجية المحررات الإلكترونية في الإثبات"، ورقة عمل مقدمة لندوة المعاملات القانونية الإلكترونية وعقود التجارة الإلكترونية، دبي، فيفري 2007، ص. 11 .



في المادة 10 من القانون 2001/85 المتعلق بالمعاملات الإلكترونية<sup>1</sup> على :

أ- "إذا استوجب تشريع نافذ توقيع عام على المستند أو نص على ترتيب أثر على خلوه من

التوقيع فإن التوقيع الإلكتروني على السجل الإلكتروني يفى بمتطلبات ذلك التشريع .

ب- يتم إثبات صحة التوقيع الإلكتروني ونسبته إلى صاحبه إذا توافرت طريقة لتحديد هويته

والدلالة على موافقته على المعلومات الواردة في السجل الإلكتروني الذي يحمل توقيععه..".

والسجل الإلكتروني هو قيد أو عقد أو رسالة معلومات تنشأ أو ترسل أو تسلم أو تخزن

بوسائل الكترونية حسب المادة 02 من هذا القانون، وهي تتطلب قدر من المعلومات والبيانات

التي في جزء منها تحويل المعلومات الشخصية التي تحدد هوية صاحب السجل وبالتالي

إمكانية إثبات التوقيع الإلكتروني إليه من عدمه<sup>2</sup> .

ولذلك أشار المشرع الأردني إلى التوقيع الإلكتروني الموثق المرتبط بالسجل الإلكتروني

عندما نص في المادة 31 على اعتبار التوقيع الإلكتروني موثقاً إذا توفرت فيه الشروط التالية:

أ- تميز بشكل فريد بارتباطه بالشخص صاحب العلاقة .

ب- كان كافياً للتعرف بشخص صاحبه .

ج- تم إنشاؤه بوسائل خاصة بالشخص وتحت سيطرته .

---

1 : قانون رقم 2001/85 المؤرخ في 2001/12/11 المتعلق بالمعاملات الإلكترونية، الجريدة الرسمية، عدد 4524،

(2001/12/31)، ص 6010 ، النسخة الكاملة متوفرة على موقع: <http://www.lob.gov.jo/ui/laws/print.jsp>

2 : خالد عبد الفتاح محمد، التنظيم القانوني للتوقيع الإلكتروني (دراسة مقارنة). المركز القومي للإصدارات القانونية، ط1،

دم، 2009، ص.272.

د- ارتبط بالسجل الذي يتعلق به بصورة لا تسمح بإجراء تعديل على القيد بعد توقيعه دون إحداث تغيير في التوقيع .

كما جاء في المادة 33 أنه "يعتبر السجل الإلكتروني أو أي جزء منه يحمل توقيعاً إلكترونياً موثقاً سجلاً موثقاً بكامله أو فيما يتعلق بذلك الجزء ، حسب واقع الحال، إذا تم التوقيع خلال مدة سريان شهادة توثيق معتمدة ومطابقتها مع رمز التعريف المبين في تلك الشهادة " .  
إن المشرع الأردني في النصوص السابقة يشير إلى السجل الإلكتروني بمعنى الوثيقة المعلوماتية، عندما اعتبره رسالة معلومات في المادة 02 من القانون السابق الذكر، وكذا عندما ربطه بالتوقيع الإلكتروني للتمتع بالقيمة القانونية التي يتمتع بها المستند الموقع خطياً، واعتبر التوقيع الإلكتروني جزء من السجل، وهذا يعني أنه يقصد بهذا المصطلح "الوثيقة المعلوماتية" باعتبار أن التوقيع الإلكتروني أحد عناصرها .

ولذلك نصت المادة 07 على "أ- يعتبر السجل الإلكتروني والعقد الإلكتروني والرسالة الإلكترونية والتوقيع الإلكتروني منتجا للآثار القانونية ذاتها المترتبة على الوثائق والمستندات الخطية والتوقيع الخطي بموجب أحكام التشريعات النافذة من حيث إلزامها لأطرافها أو صلاحيتها في الإثبات .

ب- لا يجوز إغفال الأثر القانوني لأي مما ورد في الفقرة (أ) من هذه المادة لأنها أجريت بوسائل الكترونية شريطة اتفاقها مع أحكام هذا القانون" .

كما نصت المادة 08 على : "يستمد السجل الإلكتروني أثره القانوني ويكون له صفة النسخة الأصلية إذا توافرت فيه مجتمعة الشروط التالية :

1- أن تكون المعلومات الواردة في ذلك السجل قابلة للإحتفاظ بها وتخزينها بحيث يمكن في أي وقت الرجوع إليها .

2- إمكانية الإحتفاظ بالسجل الإلكتروني بالشكل الذي تم به إنشاؤه أو إرساله أو تسلمه أو بأي شكل يسهل به إثبات دقة المعلومات التي وردت فيه عند إنشائه أو إرساله أو تسلمه

3- دلالة المعلومات الواردة في السجل على من ينشأه أو يتسلمه وتاريخ ووقت إرساله وتسلمه".

وما يلاحظ على نصوص هذا القانون أنها وسعت نطاق تطبيقه ، حيث ينطبق على أي رسالة معلومات الكترونية يتم تداولها بما في ذلك المعاملات الإلكترونية المعتمدة في الدوائر الحكومية أو المؤسسات الرسمية بصورة كلية أو جزئية، بالإضافة إلى المعاملات الإلكترونية ذات الطابع المدني أو التجاري ، وهذا ما نصت عليه المادة 04 : " تسري أحكام هذا القانون على ما يلي :

أ- المعاملات الإلكترونية والسجلات الإلكترونية والتوقيع الإلكتروني وأي رسالة معلومات الكترونية .

ب- المعاملات الإلكترونية التي تعتمدها أي دائرة حكومية أو مؤسسة رسمية بصورة كلية أو جزئية " .

غير أنه استثنى في المادة 06 التعامل برسائل المعلومات في المعاملات التالية :

أ/ العقود والمستندات والوثائق التي تنظم وفقا لتشريعات خاصة بشكل معين أو تتم بإجراءات محددة ومنها:

1- إنشاء الوصية وتعديلها .

2- إنشاء الوقف وتعديل شروطه .

3- معاملات التصرف بالأموال غير المنقولة بما في ذلك الوكالات المتعلقة بها وسندات

ملكيتها وإنشاء الحقوق العينية عليها باستثناء عقود الإيجار الخاصة بهذه الأموال.

4- الوكالات والمعاملات المتعلقة بالأحوال الشخصية .

5- الإشعارات المتعلقة بإلغاء أو فسخ عقود خدمات المياه والكهرباء والتأمين الصحي

والتأمين على الحياة .

6- لوائح الدعاوى والمرافعات وإشعارات التبليغ القضائية وقرارات المحاكم .

ب/ الأوراق المالية إلا ما تنص عليه تعليمات خاصة تصدر عن الجهات المختصة استنادا

لقانون الأوراق المالية النافذ المفعول .

### الفرع الثاني : مفهوم الوثيقة المعلوماتية في التشريع الإماراتي

بين القانون الخاص بالمعاملات والتجارة الإلكترونية الإماراتي<sup>1</sup> في المادة 02 منه مفهوم

الوثيقة المعلوماتية مستخدما مصطلح المستند الإلكتروني حيث اعتبره : "مستند يتم إنشاؤه أو

تخزينه أو استخراجة أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة الكترونية، على وسيط

لملموس أو على أي وسيط الكتروني آخر، ويكون قابلا للاسترجاع بشكل يمكن فهمه " .

---

1: قانون رقم 2002/02 المؤرخ في 12 فبراير 2002 ، بشأن المعاملات والتجارة الإلكترونية ، الجريدة الرسمية، عدد 277،

(2002/02/16)، متوفر على موقع : (Arab e-law) .

يبدو أن المشرع الإماراتي لم يضع فارقاً بين المستند والسجل الإلكتروني، فهو يستخدم مصطلح السجل الإلكتروني عند الحديث عن المعاملات الإلكترونية حيث خصص الفصل السادس لتنظيم الإستخدام الحكومي للسجلات والتوقيعات الإلكترونية، إذ نص في المادة 27 على بعض الصلاحيات والسلطات الممنوحة في هذا المجال وهي :

- أ- قبول إيداع أو تقديم المستندات أو إنشائها أو الإحتفاظ بها في شكل سجلات الكترونية .
  - ب- إصدار أي إذن أو ترخيص أو قرار أو موافقة في شكل سجلات الكترونية.
  - ج- قبول الرسوم أو أية مدفوعات أخرى في شكل الكتروني.
  - د- طرح العطاءات واستلام المناقصات المتعلقة بالمشتريات الحكومية بطريقة الكترونية .
- إذا قررت أية دائرة أو جهة تابعة للحكومة تنفيذ أي من المهام المذكورة في الفقرة (أ) من هذه المادة فيجوز لها عندئذ أن تحدد :

أ. الطريقة أو الشكل الذي سيتم بواسطته إنشاء أو إيداع أو حفظ أو تقديم أو إصدار تلك السجلات الإلكترونية .

ب. الطريقة والأسلوب والكيفية والإجراءات التي يتم بها طرح العطاءات واستلام المناقصات، وإنجاز المشتريات الحكومية .

ج. نوع التوقيع الإلكتروني المطلوب بما في ذلك اشتراط أن يستخدم المرسل توقيعاً رقمياً أو توقيعاً الكترونياً محمياً آخر .

د. الطريقة والشكل الذي سيتم بها تثبيت ذلك التوقيع على السجل الإلكتروني والمعيار الذي يجب أن يستوفيه مزود الخدمات الذي يقدم له المستند للحفظ أو الإيداع .

هـ. عمليات وإجراءات الرقابة المناسبة للتأكد من سلامة وأمن وسرية السجلات الإلكترونية أو المدفوعات أو الرسوم " .

كما استخدم المشرع الإماراتي في المادة 03 مصطلحي السجل الإلكتروني والمستند في نفس الوقت، إذ نص على ما يلي "يفسر هذا القانون طبقاً لما هو معقول في المعاملات والتجارة الإلكترونية وبما يؤدي إلى تحقيق الأهداف التالية :

- 1- تسهيل المراسلات الإلكترونية بواسطة سجلات الكترونية يعول عليها .
- 2- تسهيل وإزالة أية عوائق أمام التجارة الإلكترونية والمعاملات الإلكترونية الأخرى والتي قد تنتج عن الغموض المتعلق بمتطلبات الكتابة والتوقيع، ولتعزيز تطور البنية التحتية القانونية والتجارية لتطبيق التجارة الإلكترونية بصورة مضمونة .
- 3- تسهيل نقل المستندات الإلكترونية إلى الجهات والمؤسسات الحكومية وتعزيز توفير خدمات هذه الجهات والمؤسسات بكفاءة عن طريق مراسلات الكترونية يعول عليها .
- 4- التقليل من حالات تزوير المراسلات الإلكترونية والتعديلات اللاحقة على تلك المراسلات من فرص الإحتيال في التجارة الإلكترونية والمعاملات الإلكترونية الأخرى.
- 5- إرساء مبادئ موحدة للقواعد واللوائح والمعايير المتعلقة بتوثيق وسلامة المراسلات الإلكترونية .

- 6- تعزيز ثقة الجمهور في سلامة وصحة المعاملات والمراسلات والسجلات الإلكترونية.
- كما جاء في المادة 05 : " يسري هذا القانون على السجلات والتوقيعات الإلكترونية ذات العلاقة بالمعاملات والتجارة الإلكترونية..."، ونصت المادة 2/6 على : " يجوز أن يتفق

الأطراف الذين لهم علاقة بإنشاء أو إرسال أو استلام أو تخزين و معالجة أية سجلات الكترونية، على التعاقد بصورة مغايرة لأي من الأحكام الواردة في الفصل الثاني حتى الفصل الرابع من هذا القانون " .

إن المشرع الإماراتي في هذه النصوص القانونية يستخدم مصطلح "السجل الإلكتروني" و"المستند الإلكتروني" بمفهوم الوثيقة التي تنشأ أو تخزن أو تستخرج أو ترسل أو تستلم بوسائل الكترونية على وسيط الكتروني، ويمكن استرجاعها بصورة مفهومة.

وبالرجوع إلى المادة 08 من هذا القانون، ضمن الفصل الثاني "متطلبات المعاملات الإلكترونية"، نجد أنها تنص في الفقرة (1) على ما يلي :

"إذا اشترط القانون حفظ مستند أو سجل أو معلومات لأي سبب، فإن هذا الشرط يتحقق عندما يتم حفظ ذلك المستند أو السجل أو المعلومات في شكل سجل إلكتروني، شريطة مراعاة ما يلي:

(أ) حفظ السجل الإلكتروني بالشكل الذي أنشئ أو أرسل أو استلم به ، أو بشكل يمكن من إثبات أنه يمثل بدقة المعلومات التي أنشأت أو استلمت في الأصل .

(ب) بقاء المعلومات محفوظة على نحو يتيح استخدامها والرجوع إليها لاحقاً .

(ج) حفظ المعلومات إن وجدت التي تمكن من إستبانة منشأ الرسالة الإلكترونية وجهة وصولها وتاريخ ووقت إرسالها واستلامها" .

وتنص الفقرة (4) : "ليس في هذه المادة ما يؤثر على ما يلي:

(أ) أي قانون آخر ينص صراحة على الإحتفاظ بالمستندات أو السجلات أو المعلومات في

شكل سجلات الكترونية وفق نظام معلومات الكتروني معين أو باتتبع إجراءات معينة، أو الحفظ أو المراسلة عبر وسيط إلكتروني".

إن المشرع الإماراتي في هذه المادة وهو ينظم كيفية حفظ المستند الإلكتروني عن طريق سجل الكتروني نجده يستخدم هذا المصطلح باعتباره وسيلة لحفظ المستندات الإلكترونية، وبالتالي فهو يخلط هنا بين مفهوم المستند والسجل .

بينما نجده في المادة 11 يعود مجددا ليستخدم مصطلح السجل الإلكتروني بمعنى المستند، حيث تنص هذه المادة على: "يكون المستند أو السجل الإلكتروني أصليا عندما تستخدم بشأنه وسيلة:

- (1) توفر ما يعول عليه فنيا للتأكد من سلامة المعلومات الواردة في ذلك المستند أو السجل من الوقت الذي أنشئ فيه للمرة الأولى بشكله النهائي كمستند أو سجل الكتروني .
- (2) وتسمح بعرض المعلومات المطلوب تقديمها متى طلب ذلك" .

يتبين من النصوص السابقة أن المشرع الإماراتي لم يكن دقيقا في استخدام المصطلحات، حيث بدا الخلط بين المستند الإلكتروني ، والسجل الإلكتروني، إذ تارة يستخدم المصطلحين بنفس المعنى في بعض النصوص، وفي نصوص أخرى يعتبر السجل الإلكتروني وسيلة لحفظ المستند الإلكتروني (الوثيقة المعلوماتية).



## الفرع الثالث : مفهوم الوثيقة المعلوماتية في التشريع المصري

بين المشرع المصري مفهوم الوثيقة المعلوماتية من خلال مصطلح المحرر الإلكتروني، كما بين مفهوم المحرر الإلكتروني الرسمي من خلال قانون التوقيع الإلكتروني.

### أولاً : مفهوم الوثيقة المعلوماتية

تنص المادة 01/ب من القانون الخاص بالتوقيع الإلكتروني في مصر<sup>1</sup> على : "المحرر الإلكتروني كل رسالة بيانات تتضمن معلومات تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل كلياً أو جزئياً بوسيلة الكترونية أو رقمية أو ضوئية أو بأي وسيلة أخرى مشابهة" . يعقب "د.أشرف توفيق" على منهج المشرع المصري في تحديده لمدلول المحرر الإلكتروني<sup>2</sup> ، بأن هذا المحرر قد لا يكون عبارة عن رسالة فهذا المدلول مضيق، ذلك أن المحرر قد يكون عبارة عن معلومات مخزنة ضمن سجلات الكترونية أو قواعد بيانات الكترونية كشهادات الميلاد أو الوفاة أو الزواج أو غيرها. وهذه البيانات لا تعتبر رسالة موجهة إلى شخص .

كما يرى أن المشرع المصري قد ركز في تعريفه للمحرر على الجانب الفني لا على الجانب القانوني، وهو ما جعل المحرر يشمل كل البيانات والمعلومات حتى تلك التي ليس لها أهمية قانونية ذلك أن هذه الأخيرة هي أساس الحماية .

---

1 : قانون رقم 2004/15 المؤرخ في 21 /02/2004 المتعلق بتنظيم التوقيع الإلكتروني، الجريدة الرسمية، عدد 17 ، (2004/04/22)، ص 17 .

2 : أشرف توفيق شمس الدين، مرجع سابق، ص.ص 32-35 .

وإذا كان المشرع المصري قد ضيق من مدلول المحرر من حيث طبيعته، فإنه من جهة أخرى قد وسع من هذا المدلول من حيث الوسيلة المستخدمة في إنشائه أو دمج أو تخزينه باستخدامه عبارة " بأي وسيلة أخرى مشابهة " وهذه النتيجة - في نظر هذا المؤلف - لم يقصدها المشرع المصري عندما صاغ هذه النصوص .

بينما يرى " د. عبد الفتاح بيومي حجازي " أن المشرع المصري اعتمد في تعريفه للمحرر الإلكتروني على الوسيلة التي أنشأ، أو خزن، أو أرسل، أو استقبل بها، وهي الوسيلة الإلكترونية وما في حكمها<sup>1</sup> .

وهذا يعني أنه على العكس من الرأي السابق، فإن المشرع المصري قد قصد توسيع نطاق الوسيلة التي تضي على هذا المحرر الصفة الإلكترونية .

ويرى "محمد أمين الرومي" أن المشرع المصري عندما عرف المحرر الإلكتروني لم يشترط تضمينه توقيعاً إلكترونياً، رغم أن المحرر لن يكون له قيمة في الإثبات إذا لم يقترن بتوقيع، كما أن التوقيع الإلكتروني يرتبط دائماً بالمحرر الإلكتروني<sup>2</sup> .

### ثانياً : مفهوم الوثيقة الرسمية الإدارية المعلوماتية

أشار المشرع المصري في المادة 15 من قانون التوقيع الإلكتروني إلى مفهوم الوثيقة الرسمية الإدارية المعلوماتية عند بيان الحجية التي يتمتع بها المحرر الإلكتروني، حيث اعتبره

---

1 : عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة. دار الفكر الجامعي، الاسكندرية، ب.ت، ص.50.

2 : محمد أمين الرومي، المستند الإلكتروني. دار الكتب القانونية، المحلة الكبرى، 2008، ص.ص 51-53 .

ذلك المحرر الإلكتروني الصادر عن جهة إدارية والذي يحمل توقيعاً إلكترونياً من موظف مختص .

وقد أشارت المذكرة الإيضاحية لهذا القانون إلى أن الاعتراف بحجية المحررات الإلكترونية سواء كانت رسمية أو عرفية يؤدي إلى تكوين منظومة قانونية متكاملة في المجال الإلكتروني تظاهي تلك التي للمحررات العادية في قانون الإثبات في المادة المدنية والتجارية الأمر الذي يدعم استخدام الوسائل الإلكترونية، ويشجع تعامل الأفراد والجهات الحكومية بها، فتتحقق بذلك فكرة الحكومة الإلكترونية .

وبذلك يتمكن كل فرد من الحصول على الوثائق الرسمية إلكترونياً، وبعد ذلك مكسباً مهماً حيث سييسر ذلك أداء الخدمات للجميع .

أما ما يتعلق بمصطلح "السجل الإلكتروني" فإن جانب من الفقه المصري لا يعتبره محرراً إلكترونياً، رغم أن المشرع المصري تدخل وجرم تزوير هذا السجل في قانون الأحوال المدنية<sup>1</sup> بمقتضى المادة 72، إذ اعتبر أن البيانات المسجلة بالحاسبات الآلية وملحقاتها بمراكز معلومات الأحوال المدنية ومحطات إصدار الوثائق وبطاقات تحقيق الشخصية بيانات واردة في محررات رسمية .

كما جاء في المادة 12 من نفس القانون " تعتبر السجلات التي تمسكها المصلحة (مصلحة الأحوال المدنية) وفروعها بما تشمل عليه من بيانات وصور رسمية مستخرجة منها حجة

---

1: قانون رقم 94/143 المؤرخ في 09/06/1994 المتعلق بسجلات الحالة المدنية، الجريدة الرسمية، عدد 23 ، (1994/06/10).

بصحتها ما لم يثبت عكسها أو بطلانها أو تزويرها بحكم قضائي".

نستنتج من النصوص السابقة أن المشرع المصري قد وفق من حيث توسيع صيغة النص المتعلق بتحديد مفهوم الوثيقة المعلوماتية ليشمل الأشكال المستحدثة تكنولوجيا ، كما أنه أعمل مبدأ النظر الوظيفي لمعادلة الوثيقة المعلوماتية بالوثيقة الورقية، باشتراط التوقيع الإلكتروني للتمتع بالقيمة الثبوتية، رغم ما يؤخذ عليه عند استخدام مصطلح السجل الإلكتروني كمرادف للوثيقة المعلوماتية .

ويعتبر الفقه السجل الإلكتروني عبارة عن " مجموعة من النصوص أو الرسوم أو البيانات أو الأصوات أو الصور أو غيرها من المعلومات تتمثل في صورة رقمية، ويتم إنشاؤها أو تعديلها أو حفظها أو فهرستها أو استرجاعها أو توزيعها بواسطة نظم الحاسب الآلي<sup>1</sup> . ويشبه السجل الإلكتروني السجل الورقي الذي يحفظ به الأشخاص تصرفاتهم اليومية<sup>2</sup> مثل سجلات التجار، سجلات مصالح الأحوال المدنية، السجلات الطبية، سجلات قيد صحائف الدعاوى القضائية .

#### الفرع الرابع : مفهوم الوثيقة المعلوماتية في التشريع الفرنسي

إن التشريع الفرنسي هو من النماذج التشريعية التي اعتمدت على تعديل القواعد العامة للإثبات في القانون الخاص بها، دون اللجوء إلى وضع نصوص خاصة لتنظيم الوثيقة المعلوماتية باعتبارها دليل إثبات وتحديد مفهومها .

1 : محمد أمين الرومي ، مرجع سابق، ص.151.

2 : عيسى غسان الرضي، القواعد الخاصة بالتوقيع الإلكتروني. دار الثقافة، ط1، عمان، الأردن، 2009، ص.189 .

فقد تم تعديل النصوص المتعلقة بالإثبات في القانون المدني الفرنسي بالقانون رقم 1230/2000 لتشمل الوثيقة المعلوماتية، وتحديد الشروط المتطلبة لإعتبرها دليل إثبات من أجل مواجهة المشكلات القانونية في قبول التعامل بمثل هذه الوثائق، ومدى قيمتها القانونية تحقيقاً لمسعى قانون الأونسترال النموذجي، واستجابة أيضاً لتوجيهات الإتحاد الأوروبي بشأن الإعراف بالوثيقة المعلوماتية في إثبات المعاملات وتداولها .

وبالتالي مواجهة المشكلات التي كانت موجودة من قبل فيما يخص الارتباط بين مدى قبول الوثيقة المعلوماتية وتقدير حجيتها في الإثبات بالسلطة التقديرية لقضاء الموضوع في إطار نصوص القانون المدني، مما أدى إلى صعوبة ارتفاع حجية المحررات الإلكترونية إلى مستوى القواعد العامة، عدا الحالات الخاصة التي اعترف فيها المشرع بتلك الحجية بالنسبة للمحركات الإلكترونية، مما مؤداه فقد الثقة فيها<sup>2</sup> . غير أنه لا بد من التنويه بفضل السبق للقضاء الفرنسي في إقرار انفصال الكتابة عن الأدوات المستخدمة في إحداثها ، إلا أن التدخل التشريعي كان له الفضل في وضع المبدأ المذكور في قاعدة قانونية ملزمة للقضاء مما يكفل استقرار الأحكام وتوحيدها<sup>3</sup> .

وبذلك تمت صياغة المادة 1316 من القانون المدني الفرنسي كالتالي "ينشأ الإثبات

---

**1 :** Loi n 230/2000 du 13/03/2000 portant adaptation du droit de la preuve aux technologies de l'information et relative a la signature electronique journal officiel, n°62, (14/03/2000), p . 391 .

**2:** أحمد شرف الدين، مرجع سابق، ص. 13 .

**3:** نفس المرجع ، ص . 15 .

الخطي أو بالكتابة من تتابع أحرف أو أشكال أو أرقام أو أية إشارات أو رموز لها دلالة قابلة للإدراك أيا كانت دعامتها أو وسيلة نقلها <sup>1</sup> .

لقد وسع المشرع الفرنسي مفهوم الدليل الكتابي ليشمل الوثيقة المعلوماتية بعدم اشتراط نوع معين من الوسائط التي تحمل عليها هذه الأحرف أو الأشكال أو الأرقام أو الإشارات ذات الدلالة الواضحة والمفهومة، وبالتالي يمكن تصور الكتابة على وسائط إلكترونية تختلف أشكالها وأنواعها حسب التطور التكنولوجي ، وبذلك أخذ المشرع الفرنسي بمبدأ "النظير الوظيفي" الذي أقره قانون الأونسترال حول التجارة الإلكترونية، حيث تؤدي الوثيقة المعلوماتية نفس وظيفة الوثيقة الورقية- وإن اختلفت الدعامة الحاملة للمعلومات - كلما أمكن الإطلاع على هذه المعلومات واسترجاعها لاحقا .

وتعني إمكانية الإطلاع أن هذه المعلومات لها دلالة قابلة للإدراك من الغير، وهو ما نص عليه قانون الأونسترال النموذجي في المادة 1/6 "عندما يشترط القانون أن تكون المعلومات مكتوبة تستوفي رسالة البيانات ذلك الشرط إذا تيسر الإطلاع على البيانات الواردة فيها على نحو يتيح استخدامها بالرجوع إليها لاحقا " .

غير أن الذي يميز المعلومات الموجودة على وثيقة معلوماتية أنها غير قابلة للإدراك مباشرة، بل عن طريق الكمبيوتر ، فالمعلومات الموجودة على قرص مرن أو قرص ضوئي لا يمكن قراءتها بمجرد النظر إلى القرص، وإنما لابد من وضع القرص في الكمبيوتر ، كذلك

---

**1 :** " La preuve littéral ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles doté d'une signification intelligible, quels que soient leur support et leur modalités de transmission ."

المحرر الموجود على ذاكرة الكمبيوتر، لا يمكن قراءته إلا من خلال شاشة الكمبيوتر وذلك باستدعائه من ذاكرة الكمبيوتر وإظهاره على الشاشة<sup>1</sup>.

كما أضاف المشرع الفرنسي في تعريفه للوثيقة المعلوماتية عنصر " التداول" وهو عنصر جديد من عناصر التعريف، حيث يعطي هذا العنصر شكلا حركيا للتعريف الساكن للمحرر الكتابي،... فبظهور تكنولوجيا المعلومات أصبحت لمسألة تداول المحرر آفاق جديدة أدت إلى اعتبار عنصر التداول من أهم عناصر تعريف المحرر<sup>2</sup>.

وبذلك عدل المشرع الفرنسي النصوص المتعلقة بالدليل الكتابي على أساس مبدأ "المعادلة الوظيفية" التي تعني البحث عن الوظائف التي يمتلكها الدليل القانوني ونقلها إلى جميع الدعامات الأخرى المحتمل أن تنتج نفس الوظائف<sup>3</sup>، وهو يهدف إلى إحداث توازن مع الأوضاع القانونية المعروفة في عالم الكتابة الورقية من أجل نقلها وإعادة إنتاجها في بيئة الكترونية<sup>4</sup>.

كما نص المشرع الفرنسي في المادة 1317 عن إمكانية تحرير الوثيقة الرسمية على دعامة الكترونية إذا أمكن حفظها في الشروط المطلوبة قانونا<sup>5</sup>.

---

1: سامح عبد الواحد التهامي، *التعاقد عبر الإنترنت*. دار الكتب القانونية، المجلة الكبرى، مصر، 2008، ص. 521 .  
2: نفس المرجع، ص. 499 .

3 : Stéphane Caïdi *la preuve et la conservation de l'écrit dans la société de l'information*, Mémoire présenté à la faculté de droit pour l'obtention du grade Maîtrise en droit (LLM), université de Montréal, Décembre 2002, P.24

4 : Ibid, P.25 .

5 : Art 1317 : "L'acte authentique est celui qui a été reçu par officiers publics ayant le droit d'instrumenter dans le lieu ou l'acte a été rédigé, et avec les solennités requise. Il peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par décret en conseil d'état" .

وتجسيدا لهذا النص صدر المرسوم رقم 2005/973 المؤرخ في 10 أوت 2005 المعدل للمرسوم رقم 1971/941 الخاص بالوثائق الرسمية، حيث وضع هذا المرسوم شروط إنشاء وحفظ هذه الوثائق التي يمكن أن تنشأ على دعامة إلكترونية .

وقد ساعد على صدور هذا المرسوم وجود شبكة داخلية تربط مكاتب التوثيق تسمى (REAL)\* ، حيث يتم تداول الوثائق الرسمية الإلكترونية داخلها .

وتتم عملية التوثيق بين أكثر من موثق، حيث يوقع الأطراف على الوثيقة- كل أمام موثقه- بصيغة رقمية عن طريق نقل التوقيع الخطي بالماسح الضوئي إليها أو عن طريق القلم الإلكتروني، ثم يقوم الموثق بالتوقيع إلكترونيا. ليتولى موثق رئيسي إرسال الوثيقة بعد تمام تحريرها وتوقيعها إلى الموثق الآخر .

وقد وفر المجلس الأعلى للموثقين بباريس شبكتان محميتان من أجل نقل المعطيات بين الموثقين، تديران أكثر من 9000 عنوان خاص بالموثقين ويتم عن طريقها تبادل أكثر من مليون رسالة شهريا .

كما وضع المجلس إجراء للتوقيع الرقمي الآمن عن طريق الشريحة الإلكترونية "REAL" التي تخص التوقيع من طرف الموثقين على العقود الرسمية الإلكترونية ونسخها<sup>1</sup>.

---

\* Reseau – Electronique notarial

1: Thierry Blanchet, "La Realisation du minutier central de notaires de France" 7 decembre 2004, (www.frili.org/spip.php? Article 60) .



## المبحث الثاني : مفهوم الوثيقة المعلوماتية فقها

إن تحديد مفهوم الوثيقة المعلوماتية يتطلب البحث في الإتجاهات الفقهية التي تناولت هذه المسألة، من خلال تحديد عناصر هذه الوثيقة والبحث في مدلولاتها .

وانطلاقاً من هذا يمكن إعطاء نماذج عن الوثائق المعلوماتية التي يتم تداولها في إنجاز المعاملات الإدارية أو المعاملات المختلفة.

### المطلب الأول : الإتجاهات الفقهية في تحديد مفهوم الوثيقة المعلوماتية

لقد تجاذب مفهوم الوثيقة المعلوماتية عدة اتجاهات فقهية بحسب الزاوية التي ينظر منها إليها، ولذلك تعددت المفاهيم وعلى هذا الأساس لابد من الرجوع إلى مفهوم الوثيقة بوجه عام لفهم هذا المدلول .

### الفرع الأول : مفهوم الوثيقة بوجه عام

إن تحديد مفهوم الوثيقة يقتضي الرجوع إلى المعنى اللغوي والإصطلاحي، ثم استنتاج عناصر هذه الوثيقة .

### أولاً : تعريف الوثيقة

إذا عدنا إلى لفظ الوثيقة نجده أيضاً تحت مسمى "المحرر" والذي يعني لغة: "تنقية الشيء من كل شائبة وجعله نقياً خالصاً، واستعير للكتابة ليدل على إقامة حروفها وإصلاح السقط فيها"<sup>1</sup> .

---

1: ابن منظور، لسان العرب. دار المعارف، القاهرة، ب.ت .

يبدو من هذه اللفظة لغة أنها غير مرتبطة تماما بالكتابة على الورق، ولذلك يمكن لأي مادة أن تشكل هذا المحرر .

أما إذا عدنا إلى التعاريف الإصطلاحية فنجدها تنطلق من هذا التأصيل اللغوي لتوسيع مفهوم المحرر، وتغيير التصور الشائع حول معناه المرتبط بالكتابة على الورق .

ولذلك عرف المحرر بأنه : " كل كتابة مقروءة تعبر عن معنى معين، سواء كانت مركبة من حروف أو أرقام أو علامات أو رموز"<sup>1</sup>، أو هو " كل مسطور مثبت على وسيلة معينة، يحوي علامات أو رموز تعبر عن إرادة أو أفكار أو معان صادرة عن شخص معين، بحيث يمكن إدراكها من الآخرين بمجرد الإطلاع عليها"<sup>2</sup>.

كما عرف بأنه " كل مكتوب يفصح عن شخص من صدر عنه، ويتضمن ذكرا أو تعبيراً عن إرادة، من شأنه إنشاء مركز قانوني معين أو تعديله أو إنهائه أو إثباته سواء أعد المحرر أساساً لذلك أو ترتب على هذا الأثر بقوة القانون"<sup>3</sup> ، كما يعتبر المحرر بحسب غايته كل ما حرر لإثبات تصرف أو واقعة قانونية، سواء أعد باعتباره دليلاً، أو كان غير ذلك"<sup>4</sup>.

ويفرق البعض بين مدلول المحرر والمستند<sup>5</sup> ، حيث لا يكون المحرر مستندا إلا إذا تضمن

---

1: عمر السعيد رمضان، شرح قانون العقوبات، القسم الخاص .دار النهضة العربية، 1986 ، ص.144 .

2: أمال عثمان، شرح قانون العقوبات ، القسم الخاص، د.ن ، ص.361 .

3: عوض محمد ، الجرائم المضرة بالمصلحة العامة. دار المطبوعات الجامعية، الإسكندرية، 1985، ص.174 .

4 : thuy – nam – Trân Tren , L'acte Authentique Notarié Electronique, thèse présenté a la faculté de droit, Institut de loi comparé, université de Montreal, Août 2001, p.42 .

5: أحمد محمود خليل، جرائم تزوير المحررات .د.ن،د.م ، 2008 ، ص.ص . 92 – 95 .

واقعة أو تعبير عن إرادة بحيث يوجد بين عباراته ترابط فكري يؤدي معنى معين معقول ، ويكون منسوب لصاحبه من خلال توقيع أو ما يشير إلى ذلك ضمن المحرر وأن تكون له صلاحية في إقناع الغير به .

ويلاحظ من التعاريف السابقة أن المحرر يتكون من كتابة وحامل ، أما الكتابة فهي عبارة عن علامات، أو رموز، أو أرقام، أو حروف، أو أشكال أو غيرها مما يؤدي معنى معين، أي تحوي معلومة يمكن الإطلاع عليها، حيث تتعلق هذه المعلومة بمركز قانوني معين، ويمكن إسنادها إلى صاحبها بطريقة ما . بينما لا يؤثر نوع الحامل على اعتبار هذه الكتابة محررا إلا بالقدر الذي يكون فيه صالحا لتثبيتها عليه، وضمان ديمومتها واستمرارها أي حفظها، وإمكانية قراءتها.

ولذلك عرف المجلس الدولي للأرشيف في دليله الخاص بالأرشفة لسنة 1997 المحرر بأنه المعلومة المستلمة، أو المنشأة، أو المستقبلة في لحظة بدأ أو إجراء أو تنفيذ الأنشطة من قبل مؤسسة أو شخص، ويحمل مضمون يسمح بإثبات وجود هذه الأنشطة بشكل مستقل عن الشكل أو الحامل<sup>1</sup> .

## ثانيا : عناصر الوثيقة

مما سبق يمكن القول أن عناصر الوثيقة تتمثل فيما يلي :

---

1 : Stephane Caidi , Op.Cit , P . 63 .

## 1- مجموعة من المعاني المترابطة :

إن المعاني والأفكار التي يتضمنها المحرر تتكون من خلال العلامات والرموز، الحروف والأرقام، بحيث تعبر عن فكرة معينة. كما لا بد أن تكون هذه الأفكار مترابطة، وبالتالي تنتقي هذه الصفة عن مجموعة الألفاظ التي لا تفيد في ذاتها هذه المجموعة من الأفكار<sup>1</sup>.

وإذا خصصنا هذا الشرط في مجال القانون ، نجد أن هذه الأفكار المترابطة تعبر عن إرادة معينة في إنشاء مركز قانوني، أو تعديله أو إنهائه .

## 2- الكتابة :

الكتابة هي مجموع الأحرف والأشكال والرموز والإشارات، أو العلامات والأرقام المتسلسلة على أن تكون قابلة للقراءة .

وتخصيص مفهوم الكتابة في المجال القانوني يقتضي التفرقة بين نوعين منها، حيث يتعلق الأول باعتبارها دليل أصلي لإثبات التصرفات والوقائع القانونية، بينما يتعلق الثاني باعتبارها ركنا شكليا في التصرف القانوني، وهذا الوصف يؤدي إلى اشتراط وجودها لقيامه.

## 3- مدى إمكانية قراءة الكتابة :

نعني بذلك إمكانية الإطلاع من طرف الغير على المعنى الذي تضمنته تلك الرموز أو الحروف، العلامات، الإشارات أو غيرها حيث يمكن فهم ذلك المعنى وإدراكه .

بل يذهب البعض إلى القول بأن المحرر لا يكون مقروءا إذا كان مدونا بحروف أو رموز

---

1 : محمد أمين الرومي، مرجع سابق، ص.46 .

معروفة ومفهومة للشخص الذي يراد الإحتجاج عليه بهذا المحرر<sup>1</sup> .

أما الإطلاع على المعنى فيخصصه البعض بما يستشف من معنى بالنظر إلى المحرر عن طريق العين، فهي الحاسة التي تكشف الفكرة<sup>2</sup> .

غير أن هذا الإتجاه ضيق فهو يستبعد أي طريقة أخرى للإطلاع على هذا المعنى، وهذا يجعل المحرر مرتبط بالكتابة الموجودة على حامل معين، يمكن من إدراك معناها مباشرة عن طريق العين، وبالتالي الربط مجددا بين الكتابة والورق أو ما شابهه وهو ما ليس له أصل كما ذكرنا .

#### 4- إسناد المحرر لصاحبه :

إن المعاني التي يتضمنها المحرر تدل بالضرورة عن صاحبها ، وليس بالضرورة أن يكون هو مدونها، فلا بد من اليقين فيما اتجهت إليه إرادته<sup>3</sup> .

وللتعرف على شخصية صاحب المحرر، وتأكيد هذا الإرتباط والإسناد وجد ما يسمى بالتوقيع الذي يؤدي هذه الوظيفة-أي وظيفة الإسناد- أو كما يسميها البعض نسب المحرر لصاحبه. ولذلك عرف التوقيع بأنه وضع علامة على السند للتعبير عن القبول بما ورد فيه<sup>4</sup>.

---

1 : حسين عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت . دار النهضة العربية، القاهرة، 2000، ص.20.

2 : محمود نجيب حسني، شرح قانون العقوبات (القسم الخاص). دار النهضة العربية، القاهرة 1987 ، ص.247 .

3: Martine Boudreau, "La Nouvelle définition de l'Écrit en Matière de preuve", Revue Experts, n°47, (06/2000), P3

4 : عباس العبودي، شرح أحكام قانون الإثبات. دار الثقافة، ط1، عمان، الأردن، 2005، ص.ص 137 ، 138 .

كما يؤدي التوقيع وظيفة مهمة وهي إضفاء الحجية القانونية على المحرر، فهو شرط لقبول الكتابة كدليل<sup>1</sup>، ولذلك اشترط الفقه في هذا التوقيع مجموعة من الشروط لتحقيق هذه الوظيفة.

### الفرع الثاني : مفهوم الوثيقة المعلوماتية

تجاذب مفهوم الوثيقة المعلوماتية اتجاهان فقهيان أحدهما يتناول هذا المفهوم من جانب مادي، بينما يركز الإتجاه الثاني على الجانب الموضوعي .

### أولاً : مفهوم الوثيقة المعلوماتية من جانب مادي

يستخدم البعض مصطلح الوثيقة المعلوماتية للدلالة على الدعامة أو الوعاء بكافة الأشكال المقررة، حيث تحمل فكرة أو يمكن أن ينتج عنها دليل على حق أو واقعة ذات آثار قانونية<sup>2</sup> .

### 1- مفهوم الدعامة الإلكترونية :

إن الدعامة الإلكترونية هي تلك الأجسام المادية المعدة لإستقبال المعلومات عن طريق طبعتها بصورة أو بأخرى بشرط أن تكون سجلت عليها المعلومات بأحد الأساليب المعلوماتية<sup>3</sup>. وهي أيضا كل جسم منفصل، أو يمكن فصله عن نظام المعالجة الآلية للمعلومات، وقد سجلت عليه معلومات معينة سواء كان معد للإستخدام بواسطة نظام المعالجة الآلية للمعلومات أو مشتقا من هذا النوع<sup>4</sup> .

---

1 : Martine Boudreau , Op-Cit , P . 3

2 : بيومي حجازي، الجريمة في عصر العولمة ، مرجع سابق، ص. 107 .

3 : علي عبد القادر القهوجي، مرجع سابق، ص. 38.

4 : بيومي حجازي، الحكومة الإلكترونية، الكتاب الثاني ، دار الكتب القانونية ، د.م، 2007 ، ص . 192 .

وهذا يعني أنه يشترط أن تنفصل هذه المعلومات أو البيانات المعالجة عن طريق الحاسب الآلي على شرائط أو تسجيلات مغناطيسية أو أقراص مدمجة أو المخرجات الكومبيوترية الورقية التي تنتجها الطابعات<sup>1</sup> .

كما عرفت الدعامة بأنها الأقراص الإلكترونية التي تسجل فيها المعلومات من خلال مغنطتها بشكل يرمز إلى كتابة غير مرئية مدونة بلغة الآلة المعتمدة على نظام الترقيم الثنائي<sup>2</sup>.

وخلافا للآراء السابقة يرى "د.سامي الشوا" أن الوثيقة المعلوماتية هي دعائم معلوماتية خالية من المعلومات فإذا ما تلقت هذه الدعائم معلومات ممغنطة أصبحت وثائق مبرمجة<sup>3</sup> . وفي كل الأحوال فإنه يخرج عن مفهوم الوثيقة المعلوماتية أو الوثيقة المبرمجة العدد والآلات كأجهزة الحاسب الآلي والطابعات .

ومن جهة أخرى يستخدم البعض مصطلح المستند المعلوماتي باعتباره كل شيء مادي متميز يصلح لأن يكون دعامة أو محل لتسجيل المعلومات المعالجة بواسطة نظام معالجة آلية، بينما المستند المعالج آليا هو كل دعامة مادية مهيأة لإستقبال المعلومات والتي تسجل عليها المعطيات من خلال تطبيق إجراءات المعالجة الآلية<sup>4</sup> .

---

1 : بيومي حجازي، الحكومة الإلكترونية، الكتاب الثاني، مرجع سابق، ص.ص 201 ، 202 .

2 : نبيل زوين، "السندات الإلكترونية"، 2009/10/29، (www.dahsha.com/uploads/muharriat-electronyya.pdh)

3 : محمد سامي الشوا، مرجع سابق، ص. 150 .

4 : آمال قارة ، مرجع سابق، ص. 135 .

## 2- أنواع الدعامات الإلكترونية :

إن الأجسام أو الدعامات المادية عديدة، كما أنها متغيرة ومتطورة بحسب ما تفرزه تكنولوجيا المعلومات، ومن بين هذه الأجسام نذكر :

### 1. القرص الصلب :

هو قرص معدني رقيق مطلي بمادة مغناطيسية، له قدرة عالية في تخزين المعلومات وسرعة فائقة في تسجيل البيانات واسترجاعها. فهو ذاكرة تخزين موجودة عادة داخل الكمبيوتر حيث تعمل على تخزين معلومات متعددة منها نظام التشغيل، التطبيقات، المعطيات المدخلة. يتكون القرص الصلب من مسارات دائرية وأقسام، وللولوج إلى البيانات لابد من تحديد عنوان المسار والقسم لتسهيل عملية البحث، ولذلك تتحدد قدرة القرص الصلب حسب سطحه، وعدد المسارات والأقسام، وتقاس سعته بوحدة الأوكتي<sup>1</sup> .

### 2. القرص المضغوط :

القرص المضغوط هو قرص بصري أو ضوئي (Optical disque) مسطح ودائري، تخزن فيه البيانات في شكل إشارات رقمية، حيث تظلي الجهة التي تخزن عليها المعلومات بطبقة من الألمنيوم النقي، وتستخدم أشعة الليزر في تسجيل البيانات كفجوات محفورة على مسارات حلزونية ضيقة جدا غير منظورة على سطحه<sup>2</sup> .

---

1: "Disque Dur" Fiche thématique 009, CASES, Luxembourg, S.D. ([www.cases.Public.lu/fr/publications/fiches/pdf](http://www.cases.Public.lu/fr/publications/fiches/pdf)).

2: Disque compact, 11 octobre 2011. ([fr.wikipedia.org](http://fr.wikipedia.org)).



أما القرص المضغوط القابل لإعادة الكتابة فيمتاز عن القرص المضغوط المعتاد بأنه قابل لمسح محتوياته وإعادة الكتابة ولذلك يرمز له اختصاراً (CD-RW) .

### 3. القرص الوميض :

هو قرص خارجي بحجم صغير، يمكن حمله ، ويتصل بمأخذ (USB) للكمبيوتر. وهو مثل القرص الصلب حيث تخزن عليه المعلومات، كما يسهل عملية نقل هذه المعلومات من كمبيوتر لآخر .

يأخذ هذا القرص أشكال وأحجام مختلفة، ويتميز بسعة عالية في التخزين<sup>1</sup> .

### ثانياً : مفهوم الوثيقة المعلوماتية من جانب موضوعي

عرفت الوثيقة المعلوماتية بأنها " رسالة بيانات تتضمن معلومات تنشأ أو ترسل أو تستلم أو تخزن باستخدام وسائل إلكترونية"<sup>2</sup> .

كما تعتبر "معلومات تم إنشاؤها أو إرسالها أو تخزينها أو استلامها بوسيلة إلكترونية أو ضوئية ورقمية أو صوتية ما دام يتضمن إثبات واقعة أو تصرف قانوني محدد، ويتضمن توقيع إلكتروني ينسب هذه الواقعة أو التصرف لشخص محدد"<sup>3</sup> .

---

1: "Qu'est-ce qu'un disque mémoire flash USB",2011, ( windows. microsoft. com/ fr/ windows) .

2: ناهد فتحي الحموري، الأوراق التجارية الإلكترونية. دار الثقافة، ط1، عمان، الأردن، 2009، ص.36 .

3: محمد أمين الرومي، المستند الإلكتروني، مرجع سابق، ص.55 .

وبذلك تتميز الوثيقة المعلوماتية بأن المعطيات التي تتضمنها موجودة على حامل إلكتروني، على شكل لغة رقمية ثنائية<sup>1</sup> .

يلاحظ على هذه التعاريف أنها تستخدم مصطلح "المعلومات" أو "البيانات" ويرى البعض أن هناك فرق بينهما، حيث تعني المعلومات رسالة معبر عنها في شكل يجعلها قابلة للنقل أو الإبلاغ للغير، أو هي " تعبير يستهدف جعل رسالة قابلة للتوصيل إلى الغير بفضل علامة أو إشارة من شأنها أو توصل المعلومة لهذا الغير " .

كما تعتبر " رمز أو مجموعة رموز تنطوي على إمكانية الإفضاء إلى معنى أو تعبير مجرد قابل لأن يصف عنصرا أو موقفا أو خصائص"<sup>2</sup> .

وهي أيضا عبارة عن " مجموعة من الرموز أو الحقائق والمفاهيم أو التعليمات تصلح أن تكون محلا للتبادل والاتصال، أو التفسير والتأويل، أو المعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية وهي تتميز بالمرونة حيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة"<sup>3</sup> .

أما البيانات فهي عبارة عن كلمات وأرقام ورموز وحقائق وإحصاءات خام لا يوجد أي صلات بينها، وهي صالحة لتكوين فكرة أو معرفة بواسطة الإنسان أو الأدوات والأجهزة<sup>4</sup>.

---

1 : Stephane Caidi, Op.Cit, p. 65 .

2: أنظر في هذه التعاريف: محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن. دار الجامعة الجديدة، الإسكندرية، 2007، ص. 88 .

3: نائلة محمد فريد قورة، مرجع سابق، ص. 97 .

4 : أحمد خليفة الملط، مرجع سابق، ص. 77 .

## المطلب الثاني : نماذج من الوثائق المعلوماتية

إن أشكال الوثيقة المعلوماتية غير محصورة، باعتبارها مرتبطة بالتطور التكنولوجي والعالم الرقمي الذي يشهد تغيرا باستمرار .

ولذلك سنعرض في هذا المطلب نماذج فقط من هذه الوثائق، والتي يتم تداولها بكثرة في المعاملات الإلكترونية سواء عند إتمامها في شكل عقود الكترونية، أو عند تنفيذها عن طريق البطاقات الإلكترونية .

### الفرع الأول : العقود الإلكترونية

إن العقد الإلكتروني هو من الوثائق المعلوماتية الشائعة في عالم المعاملات الرقمية، ولذلك كان محل اهتمام التشريع والفقهاء لتعريفه وبيان كيفية إبرامه، وبحث مسألة توثيقه لضمان الثقة فيما يتضمنه .

### أولا : مفهوم العقد الإلكتروني

إهتم التشريع والفقهاء بوضع تعريف للعقد الإلكتروني، غير أننا إذا عدنا إلى التشريعات المقارنة الدولية أو المحلية نجدها بصفة عامة تشير إلى تعريف رسالة البيانات أو المعلومات ويندرج ضمنها العقد الإلكتروني.

### 1- تعريف العقد الإلكتروني تشريعا :

عرف قانون الأونسترال للتجارة الإلكترونية رسالة البيانات في المادة 02 بأنها "المعلومات التي يتم إنشاؤها أو إرسالها أو إستلامها أو تخزينها بوسائل الكترونية أو ضوئية أو بوسائل مشابهة " .

وفي المادة 1/11 أشار إلى أن هذه الوسائل هي للتعبير عن العرض والقبول، حيث نص على: " 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 يفقد ذلك العقد صحته أو قابليته للتنفيذ لمجرد استخدام رسالة بيانات لذلك العرض".

أما التوجيه الأوربي رقم 97/07 المؤرخ في 1997/05/20 المتعلق بحماية المستهلك في العقود المبرمة عن بعد فقد عرف العقد الإلكتروني تحديدا بأنه " عقد متعلق بالسلع والخدمات يتم بين مورد ومستهلك من خلال الإطار التنظيمي الخاص بالبيع عن بعد أو تقديم الخدمات التي ينظمها المورد، والذي يتم باستخدام واحدة أو أكثر من وسائل الإتصال الإلكترونية حتى إتمام العقد".

## 2- تعريف العقد الإلكتروني فقها :

عرف العقد الإلكتروني بأنه "التقاء إيجاب صادر من الموجب بشأن عرض مطروح بطريقة الكترونية سمعية أو مرئية أو كليهما على شبكة الإتصالات والمعلومات، بقبول مطابق له صادر من الطرف المقابل بذات الطرق بهدف تحقيق عملية أو صفقة معينة يرغب الطرفان في إنجازها 1 .

---

1: خالد ممدوح إبراهيم، إبرام العقد الإلكتروني دراسة مقارنة. دار الفكر الجامعي، الإسكندرية، 2005، ص. 51

كما عرف بأنه "اتفاق يتم فيه التقاء الإيجاب بالقبول على شبكة إتصالات دولية مفتوحة بطريقة سمعية بصرية بفضل التفاعل بين الموجب والقابل" <sup>1</sup> .

إن هذا التفاعل بين الموجب والقابل يتم من خلال تبادل رسائل المعلومات، أي عن طريق معلوماتي على الشبكة، بأشكال مختلفة سمعية، أو مرئية، للوصول إلى التطابق بين الإيجاب والقبول .

### ثانيا : التعبير عن الإرادة الكترونيا :

لقد كانت مسألة التعبير عن الإرادة محل جدل فقهي وقانوني، حيث لم يجز البعض هذا النوع من التعبير، مما استدعى إلى الفصل في المسألة بنصوص قانونية .

### 1- جواز التعبير عن الإرادة الكترونيا :

حسم قانون الأونسترال للتجارة الإلكترونية هذه المسألة في المادة 11 التي نصت على :  
"في سياق العقود وما لم يتفق الطرفان على غير ذلك، يجوز استخدام رسائل البيانات للتعبير عن العرض وقبول العرض .

وعند استخدام رسالة البيانات في إنشاء العقد، لا يفقد ذلك العقد صحته أو قابليته للتنفيذ لمجرد استخدام رسالة البيانات لذلك الغرض " .

---

1 : Beare Augère, Pierre Bresse et Stéphanie Thuilier, Paiement Numérique Sur Internet. Thomson publishing, S.L, 1997 , p.76 .

## 2- طرق التعبير عن الإرادة الكترونيا :

للتعبير عن الإرادة صيغ متعددة فقد يكون باللفظ عند المحادثة المباشرة، وقد يكون كتابة عن طريق البريد الإلكتروني ، أو باتخاذ إشارة متداولة في العالم الرقمي، أو موقف لا يدع شكاً في الدلالة على نية صاحبه .

### أ- التعبير عن طريق المحادثة والمشاهدة :

إن أجهزة الكاميرا الموصولة بالكمبيوتر تساعد الطرفين الموصولين بالشبكة العالمية على التحدث إلى بعضهما البعض، وبالتالي في حال صدر من أحدهما إيجاباً ارتبط به قبول فإن العقد ينعقد نتيجة اقتران الإيجاب بالقبول وتطابقهما .

ويساعد على إتمام هذا النوع من التعاقد تلك البرامج الخاصة بالتواصل صوتياً مع الطرف الآخر، وكذا حركياً عن طريق صور الفيديو .

### ب- التعبير عن الإرادة عن طريق الموقع الإلكتروني :

يتم الإعلان عن السلع والخدمات في مواقع خاصة عبر شبكة المواقع "web"، ويعتبر هذا الإعلان إيجاب موجه للجمهور إذا تضمن العناصر الأساسية للعقد، ويحصل القبول بالنقر على مفتاح الموافقة، خاصة إذا كان العقد بصيغة نموذجية حيث لا يملك الموجب له سوى القبول أو الرفض .

### ج- التعبير عن الإرادة عن طريق البريد الإلكتروني :

البريد الإلكتروني هو بريد يضمن التراسل بين الأفراد رقمياً، حيث ترسل رسائل المعلومات وتستقبل بين أجهزة الحواسيب باستخدام شبكة الإنترنت من خلال العنوان الخاص بكل مرسل،

واكتساب البريد الإلكتروني يعني أن للمشارك مساحة على القرص الصلب يستقبل ويرسل الرسائل من خلالها .

#### د- التعبير عن الإرادة عن طريق التنزيل :

التنزيل هو نقل أو استقبال أحد البرامج أو الرسائل أو البيانات عبر شبكة المعلومات الدولية إلى الكمبيوتر الخاص بالعميل، ويسمى في التجارة الإلكترونية بالتسليم المعنوي .  
والتعبير الرقمي عن طريق التنزيل يمكن اعتباره موقف لا يدع شكاً في دلالاته على مقصود صاحبه<sup>1</sup> .

#### ثالثاً: توثيق العقد الإلكتروني

ترتبط مسألة توثيق العقد الإلكتروني بتحديد هوية طرفي العقد، والتأكد من مضمون رسائل المعلومات من طرف جهات التوثيق الإلكتروني أو ما يسمى بسلطات التصديق ، والتي تجسد مبدأ الثقة فيما يتلقاه الموثق من ذوي الشأن وما يقوم بتدوينه في العقد<sup>2</sup> .

وتعتبر جهات التوثيق الإلكتروني جهات محايدة موثوق بها من كلا المتعاقدين، حيث قد تكون هيئة عامة أو خاصة مهمتها تحديد هوية الطرفين عن طريق إصدار شهادات إنشاء توافيق الكترونية لمطابقة المعلومات والتأكد من صحتها، وإسنادها لصاحبها ، بفضل مفتاحين

---

1: الصالحين محمد العيش، الكتابة الرقمية طريقاً للتعبير عن الإرادة ودليلاً للإثبات. منشأة المعارف، ط1، الإسكندرية، 2008 ، ص.ص 65 ، 66 .

2: مولود قارة، "التعبير عن الإرادة في عقود التجارة الإلكترونية"، ب.ت، ( Tadrib. hmsageria. net/ hanme/ pièces/ ) ، ص 1 .

أحدهما خاص وسري ، والآخر عام ترسله جهات التصديق إلى كل من يرغب في التعامل مع صاحب التوقيع الإلكتروني<sup>1</sup> .

وتعتبر الرسالة الإلكترونية المرفقة بالتوقيع صادرة ممن نسبت إليه، ويعتبر التوقيع صحيحا، والبيانات الموقع عليها ليس بها تلاعب، ولم يطرأ عليها تبديل، أو حذف، أو إضافة أو تغيير، وبالتالي تصبح موثقة ولا يمكن إنكارها<sup>2</sup> .

### الفرع الثاني : البطاقات الإلكترونية

تتخذ البطاقات الإلكترونية أشكالا متعددة ووظائف مختلفة، كما أنها قد تصدر عن جهات حكومية، أو عن مؤسسات مالية خاصة من أجل المبادلات التجارية أو الإستفادة من بعض الخدمات. ومن بينها البطاقات البنكية أو المصرفية. ولذلك تختلف التعاريف الواردة بشأنها، غير أنها تتشابه من حيث تكوينها وبنائها المادي والمعلوماتي.

إن هذا البناء هو الذي يدعونا إلى البحث في مدى اعتبارها وثيقة معلوماتية بعد عرض تعريفها، وكيفية تكوينها .

---

1: إياد عبد الرزاق سعد الله، "التجارة الإلكترونية بين القانون النموذجي للأونسترال والتشريع الكويتي"، بحث مقدم لندوة الجوانب القانونية والتنظيمية للاتصال الإلكتروني، الكويت، 3-5 نوفمبر 2001 .

2: سليم سعادوي، عقود التجارة الإلكترونية دراسة مقارنة. دار الخلدونية، ط1، الجزائر، 2008، ص. 93 .



## أولاً: تعريف البطاقة الإلكترونية

ذكرنا سابقاً أن هذا التعريف يختلف بحسب نوع البطاقة الإلكترونية والذي يرتبط بالوظيفة التي تؤديها، وهذه بعض الأنواع الشائعة من البطاقات الإلكترونية، كبطاقة التعريف الوطنية، جواز السفر الإلكتروني، بطاقة الضمان الإجتماعي، رخصة القيادة، والبطاقات البنكية .

### 1 . بطاقة التعريف الإلكترونية

إن انتشار هذه البطاقات بوحدة المعالجة المصغرة ، مع إضافة وظيفة التشفير لها جعلها دعائم للتعريف يمكنها أداء وظيفة التوثيق بقوة<sup>1</sup>. (أنظر الشكل رقم (2) الموالي)



### نموذج بطاقة تعريف الكترونية

<sup>1</sup> : Dominique Launay, "Etat des lieux et orientation des projets concernant les cartes a puce et autre Supports d'Identité" , S.D ( [www.Jres.org/paper/53](http://www.Jres.org/paper/53) pdf) .

لقد حلت بطاقة التعريف الإلكترونية محل بطاقة التعريف التقليدية ، إذ أصبحت تتضمن التعريف بالشخص من خلال معلومات مرئية ظاهرة على البطاقة، ومعلومات غير مرئية موجودة على المنطقة المعالجة إلكترونياً<sup>1</sup>، من خلال الشريحة الإلكترونية التي تسمح بالتعريف بالشخص وكذا التوثيق من صحة البيانات، وهي الوظيفة المستجدة والتي لم تكن موجودة في البطاقة القديمة حيث تتضمن هذه الشريحة شهادة رقمية تسمح بالتأكد بطريقة الكترونية من هوية حائز البطاقة<sup>2</sup>.

## 2. جواز السفر الإلكتروني :

جواز السفر الإلكتروني هو وثيقة تعريف وسفر عالية الأمان تحمل صورة وبصمات رقمية وخصائص بيومترية لصاحبها مخزنة ضمن شريحة إلكترونية، حيث تسمح هذه الشريحة بقراءة الجواز إلكترونياً وبشكل سريع للتعرف على هوية الشخص عند السفر ، كما تسمح بالتأكد من صحة البطاقة .

وتتضمن الشريحة المعطيات الشخصية مثل الإسم وتاريخ الميلاد ورقم الجواز وغيرها.

(أنظر الشكل رقم (3) الموالي).

---

1 : "Document de réflexion sur la Question des Cartes d'identité au Québec", Octobre 1996, ([www.Cai.gov.qc.ca/06-documentatio/01/pdf](http://www.Cai.gov.qc.ca/06-documentatio/01/pdf)), p . 8 .

2 : "La carte d'identité Electronique(EID)",Fiche de l'AWT (agence wallonne de Télécommunication ) ,07/07/2005, ([www.awt.be/contenu/tel/gov/fr](http://www.awt.be/contenu/tel/gov/fr)) .





## Exemple de recto

نموذج بطاقة ضمان اجتماعي

4- رخصة القيادة الإلكترونية : (أنظر الشكل رقم (5) الموالى)



نموذج رخصة قيادة الكترونية

## 5- بطاقة الوفاء :

بطاقة الوفاء هي "عبارة عن أداة وفاء تصطبغ - بالنظر لظروف إصدارها والتعامل بها- بصبغة مصرفية وتسمح لحاملها باتخاذ الإجراءات اللازمة لخصم و تحويل مبلغ محدد من المال من حسابه لدى البنك المصدر للبطاقة لمصلحة وحساب شخص آخر" <sup>1</sup> .

## 6 . بطاقة الإئتمان :

بطاقة الإئتمان هي "بطاقة خاصة يصدرها المصرف لعميله كي تمكنه من الحصول على السلع والخدمات من محلات وأماكن معينة عند تقديمه هذه البطاقة، ويقوم بائع السلع أو الخدمات بتقديم الفاتورة الموقعة من العميل إلى المصرف مصدر الإئتمان فيسدد قيمتها له ، ويقدم المصرف للعميل كشفا شهريا بإجمالي القيمة لتسديدها أو يخصمها من حسابه الجاري لطرفه" <sup>2</sup> .

## 7 . بطاقة الصراف الآلي :

هذه البطاقة مخصصة للقيام بالعمليات المصرفية عبر الصراف الآلي ، كعمليات السحب وكشف الحساب<sup>3</sup> ، والعمليات الممكنة بواسطة هذا الجهاز .

إذ يمكن سحب مبالغ نقدية بسقف محدد متفق عليه، بإدخال البطاقة في الفتحة الخاصة

---

1: عماد علي الخليل، الحماية الجزائرية لبطاقات الوفاء، دراسة تحليلية مقارنة. دار وائل للنشر، عمان، الأردن، د.ت، ص.7 .  
2: محمد رأفت عثمان، "ماهية بطاقة الإئتمان وأنواعها وطبيعتها القانونية وتمييزها عن غيرها" ، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية، 2003، ص.618 .  
3: نادر عبد العزيز شافي، المصارف والنقود الإلكترونية. المؤسسة الحديثة للكتاب، ط1، طرابلس، لبنان، 2007، ص.236 .

بالجهاز، وإدخال الرقم السري ليتم صرف المبلغ آليا وتسجيل المبلغ في الجانب المدين من حساب الحامل<sup>1</sup>.

## ثانيا : بناء البطاقة الإلكترونية

تتكون البطاقة الإلكترونية من مكونات مادية ومعلوماتية لها مواصفات خاصة .

### 1 . المكونات المادية :

من المكونات المادية جسم البطاقة الذي يتميز بأبعاد معينة من حيث الطول والعرض والسماك ، فهي أبعاد معيارية .

بالإضافة إلى تموضع كل مكونات البطاقة من حيث المسافات الرأسية والأفقية بين الحروف والأرقام والصورة وشريط التوقيع والشريط الممغنط<sup>2</sup> .

كما تتميز البطاقة بخواص تكوينية و يقصد بها نوع اللدائن التي يتكون منها جسم وغلاف البطاقة وما يتميز به من خواص نوعية، وأساليب الطباعة وأنواع الأحبار المستخدمة ودرجاتها اللونية<sup>3</sup> ، والمواد المكونة للشريط الممغنط وشريط التوقيع. ويوجد على البطاقة معلومات أو بيانات يمكن إدراكها بالعين وهي البيانات المتعلقة بالجهة المصدرة، الشعار، رقم البطاقة، اسم

---

1 : فداء يحي أحمد المحمود ، النظام القانوني لبطاقة الإئتمان . دار الثقافة، دم، د.ت ، ص. 18 .

2 : محمد أحمد وقيع الله، أساليب التزييف والتزوير وطرق كشفها. أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003. ص. 170 .

3 : نفس المرجع، ص. 171 .

حاملها وصورته، تاريخ الصلاحية، وتتميز الحروف والأرقام الغائرة على البطاقة بالتجانس في الحجم و المسافات البيئية 1.

أما ظهر البطاقة فيحوي الشريط المغناطيسي (الممغنت)، وشريط التوقيع الذي يظهر عليه توقيع صاحب البطاقة يدويا، حيث يلصق أسفل الشريط الممغنت بمسافة معينة. ويصنع كل من الشريط الممغنت وشريط التوقيع من مواد خاصة.

وتستخدم في صناعة هذه البطاقات طبقة بلاستيكية خاصة تغطيها لحماية المعلومات والبيانات من العوامل البيئية المحيطة والحرارة 2.

## 2 . المكونات المعلوماتية :

يحوي الشريط الممغنت أو الشريحة الإلكترونية بيانات معالجة الكترونيا تتعلق بصاحب البطاقة، حيث لا يمكن إدراك هذه البيانات بصريا ، إلا انه من الممكن قراءتها وفقا للأصول الفنية الخاصة بها 3 .

## ثالثا : مدى إعتبار البطاقة الإلكترونية وثيقة

إن الجدل الحاصل في هذه المسألة هو ذاته المتعلق بمدى الإعتراف بفكرة الوثيقة

---

1 : عمر الشيخ الأصم، "البطاقات الإئتمانية المستخدمة والأكثر انتشارا في البلاد العربية". أعمال ندوة تزوير البطاقات الإئتمانية. أكاديمية نايف العربية للعلوم الأمنية، ط1، الرياض، 2001، ص.18.

2 : محمد عبد الرسول خياط، "عمليات تزوير البطاقات الإئتمانية"، أعمال ندوة تزوير البطاقات الإئتمانية. أكاديمية نايف العربية للعلوم الأمنية، ط1، الرياض، 2002، ص.50 .

3 : عبد الجبار الحنيص، "الحماية الجزائرية لبطاقات الإئتمان الممغطة من التزوير"، مجلة جامعة دمشق للعلوم الإقتصادية والقانونية، العدد 02، 2008، ص. 21 .

المعلوماتية، حيث يرى جانب من الفقه أن فكرة الوثيقة تقوم على إمكانية إدراك المعاني والأفكار التي تضمنها عن طريق العين، أي إدراكها بطريقة مباشرة، فإذا كان ذلك ممكناً بالنسبة للمعلومات الظاهرة على البطاقة فهو غير ممكن بالنسبة للبيانات الموجودة على الشريط المغنط أو الشريحة الإلكترونية حيث تسجل على هيئة جزئيات دقيقة مجهزة ومثبتة بشكل إلكتروني...، لا تتاح قراءتها إلا بجهاز معين<sup>1</sup>.

بالإضافة إلى فكرة الكتابة والتي ترتبط بما هو مدون على الورق، وبالتالي لا تتوافر الكتابة في مجموع البيانات والمعلومات المثبتة على الشريط المغناطيسي أو الشريحة الإلكترونية لأنها معالجة إلكترونياً. كما أن من عناصر الوثيقة إمكانية نسبها إلى صاحبها، مع دوامها وثباتها، ولا يتوافر هذا بالنسبة للكيان المعلوماتي للبطاقة.

غير أن كل هذه الحجج يمكن مجابتهها، فالبطاقة الإلكترونية تحمل مجموعة من المعلومات والبيانات التي ترتبط بمركز مالي أو قانوني معين لصاحبها، سواء كانت ظاهرة أو كانت إلكترونية.

أما المعلومات الإلكترونية الموجودة على الشريط المغنط فهي جزء من هذه الوثيقة، ولا ينفي عنها ذلك أنها غير مرئية حيث لا يمكن الإطلاع عليها بمجرد النظر إليها، ولكن يمكن إدراكها عن طريق أجهزة مخصصة لذلك، ولا يشترط لإدراك المعاني المكونة للوثيقة أن يكون ذلك بطريقة مباشرة.

---

1 : عماد علي الخليل، مرجع سابق، ص 62.



## الفصل الثاني: القيمة القانونية للوثيقة المعلوماتية

منذ ظهور الوثيقة المعلوماتية بانتشار المعاملات عن طريق الوسائط الإلكترونية، بدأ الجدل حول قيمتها القانونية في مسائل الإثبات، والتحقق من الهوية والتوثيق ، خاصة في غياب النصوص التشريعية الناظمة لذلك وهو ما جعل القضاء يجتهد في هذا الباب .

لكن هذا الوضع بات يهدد حجم المعاملات الإلكترونية الدولية والمحلية، ويزعزع الثقة في مثل هذه الوثائق ، ولذلك حسم الأمر تشريعيا وفق الإتجاهات التي سنبينها في المبحثين المواليين .

### المبحث الأول: الإتجاهات التشريعية حول القيمة القانونية للوثيقة المعلوماتية

بدأ الإهتمام التشريعي بتنظيم الوثيقة المعلوماتية وتقدير حجيتها القانونية على الصعيد الدولي، باعتباره نموذجا يساعد الدول على حسم المسألة عند وضع تشريعاتها الوطنية .

### المطلب الأول : الإتجاهات التشريعية الدولية حول القيمة القانونية للوثيقة المعلوماتية

يعتبر قانون الأونسترال والتوجيه الأوربي من النماذج الدولية التي بينت القيمة القانونية للوثيقة المعلوماتية في مجموعة من النصوص ولذلك سنتناولها في الفرعين المواليين .

## الفرع الأول : قانون الأونسترال

بين قانون الأونسترال النموذجي المتعلق بالتجارة الإلكترونية، وكذا التوقيع الإلكتروني القيمة القانونية للوثيقة المعلوماتية حيث ساوى بينها وبين الوثيقة العادية وذلك من خلال مجموعة من النصوص.

### أولا : قانون الأونسترال حول التجارة الإلكترونية

أعطى قانون الأونسترال للتجارة الإلكترونية قيمة قانونية للرسالة الإلكترونية في المادة 05 مكرر عندما اعتبر أن هذه رسالة لا تفقد مفعولها أو قابليتها للتنفيذ من الناحية القانونية لمجرد أنها في شكل رسالة بيانات .

وتستوفي رسالة البيانات شرط الكتابة كلما أمكن الإطلاع على البيانات الموجودة ضمنها بالشكل الذي يمكن معه الرجوع إليه لاحقا.

ولأن المعلومات المكتوبة لا تكون لها قيمة إلا إذا احتوت الوثيقة توقيع يمكن من نسبة هذه المعلومات إلى صاحبها، فإن هذا القانون اعتبر أن رسالة البيانات تستوفي هذا الشرط إذا:

(أ) استخدمت طريقة لتعين هوية ذلك الشخص، والدلالة على موافقته على ما جاء في الرسالة من معلومات .

(ب) كانت تلك الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي أنشئت أو بلغت من أجله رسالة البيانات، وفي ضوء كل الظروف بما في ذلك أي إتفاق متصل بالأمر.

وحتى عندما يشترط القانون أصل الوثيقة للإثبات فإن رسالة البيانات تستوفي هذا الشرط إذا وجد ما يعول عليه لتأكيد سلامة المعلومات منذ الوقت الذي أنشأت فيه لأول مرة بصفة نهائية على أنها رسالة بيانات.

وتقدر سلامة المعلومات التي تتضمنها الوثيقة بحسب ما إذا بقيت مكتملة ولم يطرأ عليها أي تعديل.

كما يقدر أيضا في إعطاء قيمة قانونية للرسالة في الإثبات الطريقة التي استخدمت في إنشائها أو تخزينها أو إبلاغها ، وكذلك الطريقة التي استخدمت في المحافظة على سلامة المعلومات الواردة فيها والطريقة التي تحدد هوية المنشئ ولأي عامل آخر يتصل بالأمر<sup>1</sup> .

كما تعطي المادة 06 من نفس القانون معيارا موضوعيا لجعل المعلومات التي تنشأ في بيئته الكترونية ذات قيمة عند الإحتجاج بها، وهو أن تكون رسالة البيانات في المتناول حيث يمكن الرجوع إليها، بالإضافة إلى إمكانية قراءتها وقابليتها للتفسير.

ويرى البعض أن معيار إمكانية الرجوع لرسالة البيانات لاحقا يفضل مفاهيم أخرى مثل الدوام ، عدم القابلية للتحريف، التي قد تضع معايير صارمة أكثر مما ينبغي، وعلى مفهوم سهولة القراءة أو سهولة الفهم التي قد تشكل معايير ذاتية أكثر مما ينبغي<sup>2</sup>.

ولذلك أشار قانون الأونسترال للتجارة الإلكترونية في المادة 10 إلى الشروط الواجب توافرها عند حفظ رسالة البيانات وهي :

---

1: أمير فرج يوسف ، عالمية التجارة الإلكترونية وعقودها . المكتب الجامعي الحديث ، دم ، 2009 ، ص .59.

2: نفس المرجع ، ص .76.

- 1 . تيسير الإطلاع على المعلومات الواردة بها على نحو يتيح استخدامها بالرجوع إليها لاحقاً .
- 2 . الإحتفاظ بالشكل الذي أنشأت أو أرسلت أو استلمت به، أو بشكل يمكن إثبات انها يمثل بدقة المعلومات التي أنشأت أو أرسلت أو استلمت .
- 3 . الإحتفاظ بالمعلومات إن وجدت التي تمكن من إستبانة منشأ الرسالة وجهة وصولها ، وتاريخ ووقت إرسالها واستلامها .

### ثانيا : قانون الأونسترال حول التوقيع الإلكتروني<sup>1</sup>

إن مساواة رسالة البيانات (الوثيقة المعلوماتية) بالوثيقة الورقية من حيث القيمة القانونية مرهون بتوافر الشروط اللازمة في التوقيع الإلكتروني حتى يؤدي وظيفته، بل قد يؤدي ذات الدور الذي يؤديه التوقيع التقليدي، ذلك أن التوقيع الأخير قد لا يجد له مكانا في ظل تقدم نظم المعالجة الإلكترونية للبيانات والمعلومات<sup>2</sup>.

ومن الشروط التي يجب توافرها كي يؤدي التوقيع الإلكتروني وظيفة التوقيع العادي، وجوب استيعاب قواعد الإثبات لما هو مستجد من أحكام التوقيع الإلكتروني، وإعطاء الحجية لهذا الأخير تقاديا لصعوبة الإثبات بالوثيقة المعلوماتية .

ولذلك نظم قانون الأونسترال النموذجي للتوقيع الإلكتروني هذه المسائل حيث نص في

المادة 06 على :

---

1 : قرار 80/56 المؤرخ في 12 ديسمبر 2001 المتضمن قانون الأونسترال النموذجي بشأن التوقيعات الالكترونية متوفر على

موقع: [www.uncitral.org/uncitral/ar/uncitral-texts/electronic-commerce/2001Model-signatures.html](http://www.uncitral.org/uncitral/ar/uncitral-texts/electronic-commerce/2001Model-signatures.html)

2 : عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، مرجع سابق، ص. 279 .

"1- حيثما يشترط القانون وجود توقيع من شخص يعد ذلك الإشتراط مستوفى بالنسبة لرسالة البيانات إذا استخدم توقيع الكتروني موثوق به بالقدر المناسب للغرض الذي أنشأت أو بلغت من أجله رسالة البيانات في ضوء كل الظروف بما في ذلك أي إتفاق ذي صلة.

2- تنطبق الفقرة (1) سواء كان الإشتراط المشار إليه فيها في شكل التزام أم كان القانون يكتفي بالنص على تبعات تترتب على عدم وجود توقيع .

3- يعتبر التوقيع الإلكتروني موثوقا به لغرض الوفاء بالإشتراط المشار إليه في الفقرة (1) إذا :  
أ- كانت بيانات إنشاء التوقيع مرتبطة في السياق الذي تستخدم فيه بالموقع دون أي شخص آخر .

ب- كانت بيانات إنشاء التوقيع خاضعة وقت التوقيع لسيطرة الموقع دون أي شخص آخر .

ج- كان أي تغيير في التوقيع الإلكتروني يجري بعد حدوث التوقيع قابلا للاكتشاف.

د- إذا كان الغرض من اشتراط التوقيع قانونا هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع، وكان أي تغيير يجري في تلك المعلومات بعد وقت التوقيع قابلا للاكتشاف".

لقد أعطت هذه المادة لرسالة البيانات نفس القيمة القانونية للوثيقة الورقية التي تقترن بتوقيع، إذا اقترنت هذه الرسالة بتوقيع الكتروني موثوق منه، حيث يمكن نسبة الرسالة لصاحبها، ويتحقق ذلك إذ كانت بيانات إنشاء هذا التوقيع خاضعة عند التوقيع لسيطرة الموقع، وكان بالإمكان اكتشاف أي تغيير يطرأ على الرسالة بعد ربطها بهذا التوقيع .

وتقوم شهادة المصادقة الإلكترونية بهذا الدور فهي عبارة عن بيانات رقمية غير مكررة خاصة بالشخص ، حيث هذه البيانات مشفرة لا يمكن قراءتها <sup>1</sup>.

وبذلك استكمل قانون الأونسترال النموذجي للتوقيع الإلكتروني مسألة القيمة القانونية لرسالة البيانات التي نظمها قانون الأونسترال للتجارة الإلكترونية عندما أعطى لهذه الرسالة نفس القيمة القانونية التي للوثيقة الورقية كلما أمكن الإطلاع على البيانات الموجودة بها ، واسترجاعها عند الحاجة .

ولذلك قرن المشرع في هذا القانون هذه القيمة القانونية بمدى ارتباط رسالة البيانات بتوقيع يؤدي وظيفة نسبة المعلومات لصاحبها .

### الفرع الثاني : التوجيه الأوربي حول التوقيع الإلكتروني

سعت الدول الأوروبية من أجل تطوير أنظمتها القانونية لتساير التطورات الحاصلة، والتنسيق فيما بينها كدول أعضاء ضمن الإتحاد الأوربي فيما يخص تشريعاتها الداخلية، وذلك من أجل بعث الثقة في المعاملات التي تتم داخل السوق الأوربية، وجعل القانون النموذجي للتجارة الإلكترونية (قانون الأونسترال) المرجعية في سن هذه التشريعات .

وفي هذا السياق أصدرت اللجنة الأوربية في 7 أكتوبر 1997 بيانا تعلن فيه رغبتها في إعداد مشروع توجيه أوربي يخص التوقيع الإلكتروني من أجل بث الثقة في المبادلات الإلكترونية.

---

1: محمد أمين الرومي، مرجع سابق، ص.69 .

وفي 13 ماي 1998 عرض المشروع على مجلس وزراء الإتحاد الأوربي، فوافق عليه في 30 نوفمبر 1999 ، ثم وافق عليه البرلمان الأوربي في 13 ديسمبر 1999 ، وأصبح من الواجب على الدول الأعضاء أخذ الإجراءات اللازمة لدمج أحكام التوجيه الأوربي ضمن التشريعات الداخلية لكل دولة عضو خلال ثمانية عشر شهرا من تاريخ نفاذ التوجيه الذي حدد بالتاسع عشر يوليو 2001<sup>1</sup> .

وقد جاء في المادة 02/05 من هذا التوجيه<sup>2</sup> الإعتراف بالحجية القانونية للتوقيع الإلكتروني مثل التوقيع الخطي، مع إلزام الدول الأعضاء بإصدار تشريعات بالصياغة التي تضمن إعطاء قيمة قانونية للتوقيع الإلكتروني أو الوثيقة المعلوماتية في الإثبات. وألا ينتقص من هذه القيمة لمجرد أن التوقيع أو الوثيقة جاء في شكل الكتروني، مع وجوب أن يتضمن هذا التوقيع نفس المتطلبات والشروط التي تتوفر في التوقيع العادي الذي تحويه الوثيقة الورقية.

ولذلك بينت المادة 02 من هذا التوجيه الشروط الواجب توافرها في التوقيع الإلكتروني وهي:

- أ- أن يكون مرتبط بالموقع وحده .
- ب- يمكن من تحديد هوية الموقع .
- ج- أن ينشأ بوسائل تمكن الموقع من إبقائه تحت رقابته.

---

1: أنظر : ثروت عبد الحميد، التوقيع الإلكتروني. دار الجامعة الجديدة، الإسكندرية، 2007، ص.ص 157 ، 158 .

2 : Directive 1999/93/ce du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques , **Journal officiel des communautés européennes**, n° 013 , (19/01/2000).

د- أن يرتبط بالمعطيات التي يتضمنها بالشكل الذي يمكن من اكتشاف أي تعديلات تطرأ عليها.

غير أن الملاحظ على هذا القانون أنه أشار في الفقرة الأولى من المادة 05 إلى التوقيع الإلكتروني الذي تتوفر فيه الشروط التقنية اللازمة لضمان الثقة والأمان مما يجعل الوثيقة تتمتع بالحجية القانونية.

ثم تناول في الفقرة 02 التوقيع الإلكتروني الذي لا يتوافر على المتطلبات المنصوص عليها في هذا التوجيه، حيث ألزم الدول الأعضاء بإصدار تشريعاتها بما يضمن عدم إهدار قيمته في الإثبات، وقبوله كدليل أمام القضاء .

ويرى الأستاذ "ثروت عبد الحميد" في تعقيبه على هذا النص، أن الإعراف بالحجية لهذا التوقيع لا يساوي الإعراف المقرر في الفقرة الأولى من المادة 05 ، إذ يجب على من يتمسك بالتوقيع الإلكتروني الذي لا تتوفر فيه المتطلبات الواردة في هذا التوجيه أن يقيم الدليل أمام المحكمة على جدارة التقنية المستخدمة في إنشاء وإصدار التوقيع<sup>1</sup>.

وهذا يعني أن تقدير حجية هذا التوقيع تبقى ضمن سلطة قاضي الموضوع الواسعة لتقرير مدى قيمته الثبوتية .

وفي إطار تحقيق المتطلبات اللازمة في التوقيع الإلكتروني لأداء وظائفه، نظم التوجيه الأوربي خدمات التوثيق خاصة فيما يتعلق بالشهادات الصادرة عن جهات التصديق الإلكتروني،

---

1: ثروت عبد الحميد، مرجع سابق، ص 162 .



حيث ألزم الدول الأعضاء بإصدار نصوص تسمح لجهات عامة أو خاصة مرخص لها من قبل الدولة باعتماد التوقيع الإلكتروني، وإصدار شهادات توثيق تدل على إستيفاء هذا التوقيع للشروط اللازمة مما يجعله موثوقا فيه .

وفي إطار تحقيق هذه الثقة أوجب هذا التوجيه على مقدمي خدمات التوثيق توفير شروط الأمان اللازمة في التوقيع وفقا للمواصفات القياسية الواردة ضمن ملاحقه .

ويعتبر مقدم خدمات التوثيق مسؤولا عن الثقة في التوقيع الإلكتروني فيما يتعلق بـ:

- صحة البيانات الواردة في الشهادة .
- ارتباط التوقيع بصاحبه .
- تسجيل ونشر القرار الخاص بإلغاء شهادة التوقيع أو إبطالها .

#### **المطلب الثاني: الإتجاهات التشريعية الوطنية حول القيمة القانونية للوثيقة المعلوماتية**

حذت التشريعات المحلية حذو تشريع الأونسترال النموذجي حول التجارة الإلكترونية والتوقيع الإلكتروني، من حيث الإعتراف بالقيمة القانونية للوثيقة المعلوماتية، وكذا معادلتها وظيفيا بالوثيقة الورقية .

إلا أن هذه التشريعات تباينت من حيث كيفية تنظيم هذه المسألة، حيث لجأت بعض الدول إلى تعديل قوانين الاثبات القائمة، فيما أصدرت دولا أخرى تشريعات خاصة بذلك .

## الفرع الأول : التشريع الفرنسي

توجه الفقه الفرنسي نحو المناداة بتعديل قانون الإثبات من خلال تحديد معنى الكتابة الإلكترونية والتوقيع الإلكتروني، وإعطاء قيمة قانونية للوثيقة المعلوماتية .

ومن هؤلاء الفقيه الفرنسي "LORENTZ" الذي أكد ضرورة إزالة كل الشكوك فيما يخص قيمة الوثيقة المعلوماتية ، كما طالب بتعديل نصوص الإثبات بحيث تصبح الوثيقة المعلوماتية مساوية للوثيقة الورقية، وإلا فإن المحررات التقليدية تبقى أعلى درجة من المحررات الإلكترونية وهذا يعرقل تطور التعامل بالوسائط الإلكترونية<sup>1</sup> .

كما اجتهد القضاء الفرنسي في تحديد هذه القيمة، فقد أكدت الغرفة التجارية لمحكمة النقض الفرنسية أن الكتابة لم تعد قاصرة على الوثائق الورقية، وإنما يمكن أن تكون مقبولة كدليل إثبات حتى لو دونت على دعائم أخرى متعارف عليها في التعامل بين المتخصصين في مجالات متعددة، ومنها على سبيل المثال الفاكس مادام محتوى الوثيقة يمكن نسبته إلى من أنشأه مع إمكانية التحقق منه دون منازعة<sup>2</sup>.

واستجابة للتطور التكنولوجي، وتوجه الفقه والقضاء الفرنسي تم تعديل المادة 1/1316 من القانون المدني الفرنسي حيث تم تقرير المساواة في القيمة القانونية بين الكتابة العادية والكتابة الإلكترونية حيث أصبحت تنص على ما يلي: "تتمتع الكتابة الإلكترونية بنفس القيمة المعترف

1: أنظر: رحيمة الصغير، العقد الإداري الإلكتروني. دار الجامعة الجديدة، دم، 2007، ص . ص 124 ، 125 .

2: نفس المرجع ، ص. 126 .

بها للكتابة على دعامة ورقية في الإثبات شريطة أن يكون بالإمكان تحديد شخص مصدرها، وأن يكون تم عقد إنشاؤها وحفظها في ظروف تضمن سلامتها" \* .

وفي مجال الإثبات بالوثيقة المعلوماتية بين المتعامل والجهات الإدارية تدخل المشرع الفرنسي بالمرسوم 99/68 المؤرخ في فيفري 1999 المتعلق بتنظيم الإثبات بهذه الوسيلة الإلكترونية حيث نص في المادة 04 على " لا تستطيع الوزارات وجهات الإدارة والمصالح تعديل فيها على الموقع الخاص بجهة الإدارة " .

وفي قانون العقود الإدارية المعدل بالمرسوم 2004/15 ثم الاعتراف بالوثيقة المعلوماتية وإعطاء قيمة قانونية كاملة لها من خلال المادة 3/56: التي تنص على "كل النصوص للمرسوم الحالي الخاصة بالكتابة، يمكن تحويلها إلى كتابة على وسيط الكتروني"

وبالتالي أصبحت الوثائق الخاصة بكراسة الشروط والعطاءات ومحاضر اللجان كلها يمكن أن تكون في شكل الكتروني، ولها الحجية الكاملة في الإثبات، حيث تم تطبيق المادة 1316 من القانون المدني فيما يخص الوثائق اللازمة لإبرام العقد الإداري الإلكتروني، وهو مانتشير إليه نصوص قانون العقود الإدارية.

وتعتبر هذه النصوص تطبيق لنصوص قانون الأونسترال النموذجي وكذا التوجيه الأوربي حول التجارة الإلكترونية والتوقيع الإلكتروني التي ساوت بين الوثيقة المعلوماتية والوثيقة الورقية من حيث القيمة القانونية في الإثبات.

---

\* "L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane, et qu'il soit établi et conservé dans des conditions de nature à garantir l'intégrité".

وبذلك ألغى القانون الفرنسي التدرج بين الوثائق على أساس الدعامة التي يتم الكتابة عليها، فلا فرق بين الوثيقة الورقية والوثيقة المعلوماتية من حيث القيمة الثبوتية إذا توافرت الشروط المطلوبة قانوناً، حيث لن تكون هذه الوثيقة مقبولة في الإثبات فقط ولكنها تتمتع بنفس القوة الثبوتية للمحرر العرفي الورقي<sup>1</sup>.

كما يمكن أن تكون الوثيقة المعلوماتية رسمية مثل الوثيقة الورقية إذا حررت أمام موثق أو موظف عام مكلف بتحريرها، ولذلك أصدر المشرع الفرنسي المرسوم 2005/973 الخاص بتوثيق هذه الوثيقة حيث نص في المادة 16 على ضرورة قيام الموثق بإنشاء نظام المعالجة ونقل البيانات، وأن يتوافر في هذا النظام الشروط التالية :

- 1- أن يتم اعتماده من المجلس الأعلى للموثقين .
- 2- أن يضمن سلامة وسرية محتويات الوثائق التي يتم نقلها من خلال هذا النظام.
- 3- أن يكون هذا النظام متصل مع الأنظمة الأخرى التي يتم إنشاؤها من قبل الموثقين الآخرين في فرنسا<sup>2</sup>.

ويلتزم الموثق بإنشاء فهرس الكتروني يسجل عليه كل البيانات الخاصة بالوثائق التي قام بإنشائها، ليتم توقيع هذا الفهرس الكترونياً من قبل رئيس مجلس الموثقين.

---

1: سامح عبد الواحد التهامي، التعاهد عبر الانترنت دراسة مقارنة. دار الكتب القانونية، دم، 2008، ص.552 .

2 : N.Samarc, "Les Actes Authentiques électroniques" , 14 Novembre 2005, ([www.droit.ntic.com](http://www.droit.ntic.com))

كما يجب أن تحفظ هذه الوثائق في ظروف تضمن سلامتها، وتجعلها قابلة للقراءة، من خلال حفظها في سجل مركزي للنسخ الأصلية الذي يعتبر قاعدة بيانات مركزية تجمع فيها الوثائق الرسمية الأصلية وتصنف حتى يسهل الرجوع إليها .

ويمكن للموثق توقيع العقد من خلال مفتاح "REAL" الذي هو عبارة عن مفتاح مؤمن يضمن صحة البيانات الموقع عليها، ويعتبر هذا المفتاح شخصي ومؤمن بفضل شفرة خاصة ومكون من مجموعة من العناصر التي تميز شخص الموثق وتوقيعه الرقمي.

وبالتالي أصبح للموثق في إطار العقود الرسمية الإلكترونية، أن يستعمل هذا المفتاح ليوقع العقد بالدخاله في مأخذ (USB) الخاص بجهاز حاسوبه الخاص<sup>1</sup>.

إن هذه الشريحة الإلكترونية "REAL" لا تسمح فقط بإنشاء وحفظ العقود الرسمية ، وإنما أيضا بتحرير نسخ على دعائم الكترونية والتوقيع عن بعد . وهذه العقود سيكون لها نفس القيمة القانونية التي للعقود الورقية<sup>2</sup>.

### الفرع الثاني : نماذج من التشريعات العربية

اتجهت بعض النماذج التشريعية العربية- السبابة في تنظيم التعامل بالوثائق المعلوماتية - إلى سن تشريعات خاصة بهذه الوثائق خلاف النموذج السابق "النموذج الفرنسي"، ومن بينها التشريع الأردني، الإماراتي والمصري.

---

1 : "L'acte Authentique sur Support Electronique", S.D, ([www.pargade - notaires.fr/equipe et compétences/missions et activités/acte authentique sur support électronique](http://www.pargade-notaires.fr/equipe-et-compétences/missions-et-activités/acte-authentique-sur-support-électronique))

2 : " La Signature électronique est maintenant une réalité pour les Notaires Français " , S . D , ([www.gautrais.com](http://www.gautrais.com)).

## أولاً : التشريع الأردني

نظم المشرع الأردني التعامل بالوثائق المعلوماتية بالقانون 2001/85 الذي يخص المعاملات الإلكترونية الخاصة، أو المعاملات التي تعتمد على أي دائرة حكومية أو مؤسسة رسمية بصورة كلية أو جزئية وهو ما نصت عليه المادة 04 من هذا القانون .

وقد أخذ المشرع الأردني بمبدأ المساواة في القيمة القانونية بين الوثيقة المعلوماتية والوثيقة الورقية من خلال المادة 07 التي نصت على :

" أ- يعتبر السجل الإلكتروني والعقد الإلكتروني والرسالة الإلكترونية والتوقيع الإلكتروني منتجا للآثار القانونية ذاتها المترتبة على الوثائق والمستندات الخطية والتوقيع الخطي بموجب أحكام التشريعات النافذة من حيث إلزامها لأطرافها أو صلاحيتها في الإثبات.

ب- لا يجوز إغفال الأثر القانوني لأي مما ورد في الفقرة (أ) من هذه المادة لأنها أجريت بوسائل الكترونية شريطة اتفاقها مع أحكام هذا القانون".

كما أجاز هذا القانون التعامل بالوثائق الرسمية بشكل الكتروني مع الإستثناءات الواردة بهذا الخصوص، كما يمكن للجهات الحكومية كأصل عام إجراء معاملاتها الكترونياً، غير أن ذلك مقترن بمدى اعتماد الدوائر الحكومية على الضوابط المشروطة لذلك، ذلك أن السند الرسمي هو حجة على الكافة في الإثبات لا يطعن فيه إلا تزويراً وهناك شرائط معينة لصحة الإحتجاج به<sup>1</sup>.

---

1: يوسف أحمد النوافلة، حجية المحررات الإلكترونية في الإثبات. دار وائل للنشر، ط1، عمان، 2007، ص.ص 129، 128.

ولذلك اشترط المشرع الأردني في المادة 08 مجموعة من الشروط حتى تتمتع الوثيقة المعلوماتية بالقيمة القانونية المطلوبة وهي :

"1- أن تكون المعلومات الواردة في ذلك السجل قابلة للإحتفاظ بها وتخزينها بحيث يمكن الرجوع إليها في أي وقت.

2- إمكانية الإحتفاظ بالسجل الإلكتروني بالشكل الذي تم به إنشاؤه أو إرساله أو تسلمه

3- دلالة المعلومات الواردة في السجل على من ينشأه أو يتسلمه وتاريخ ووقت إرساله وتسلمه".

كما نصت المادة 32 على أن السجل الإلكتروني أو التوقيع الإلكتروني غير الموثق

ليس له أي قيمة ثبوتية، ويكون التوقيع الإلكتروني موثقا طبقا للمادة 31 التي تنص على:

" أ- إذا تميز بشكل فريد بارتباطه بالشخص صاحب العلاقة .

ب- إذا كان كافيا للتعريف بشخص صاحبه .

ج- إذا تم إنشاؤه بوسائل خاصة بالشخص وتحت سيطرته.

د- ارتبط بالسجل الذي يتعلق به بصورة لاتسمح بإجراء تعديل على القيد بعد توقيعه دون

إحداث تغيير في التوقيع".

## ثانيا : التشريع الإماراتي

نظم المشرع الإماراتي التعامل بالوثائق المعلوماتية بالقانون 2002/02 المتعلق بالمعاملات

والتجارة الإلكترونية، حيث بينت المادة 1/07 القيمة القانونية للرسالة الإلكترونية بنصها على:

"لا تفقد الرسالة الإلكترونية أثرها القانوني أو قابليتها للتنفيذ لمجرد أنها جاءت في شكل الكتروني".

كما جاء في المادة 09 "إذا اشترط القانون أن يكون خطيا أي بيان أو مستند أو سجل أو معاملة أو بينة أو نص على ترتيب نتائج معينة في غياب ذلك، فإن المستند أو السجل الإلكتروني يستوفي هذا الشرط طالما تم الإلتزام بأحكام الفقرة (1) من المادة السابقة".

وهذه الأحكام طبقا للمادة 08 تتمثل في :

"(أ) حفظ السجل الإلكتروني بالشكل الذي أنشئ أو أرسل أو أستلم به، أو بشكل يمكن من إثبات أنه يمثل بدقة المعلومات التي أنشأت أو أرسلت أو استلمت في الأصل.

ب - بقاء المعلومات محفوظة على نحو يتيح استخدامها والرجوع إليها لاحقا .

ج - حفظ المعلومات ان وجدت التي تمكن من استبانته منشأ الرسالة الإلكترونية وجهة وصولها وتاريخ ووقت إرسالها واستلامها."

وتؤكد المادة 12 القيمة القانونية للرسالة الإلكترونية والتوقيع الإلكتروني في الإثبات، إذ تنص على "لايحول دون قبول الرسالة الإلكترونية أوالتوقيع الإلكتروني كدليل إثبات: لمجرد أن الرسالة أو التوقيع قد جاء في شكل الالكتروني"، أما الفقرة 02 فنصت على: "يكون للمعلومات الالكترونية ما تستحقه من حجية في الاثبات ، وفي تقدير هذه الحجية يعطى الاعتبار كما يلي:

(أ) مدى إمكانية التعويل على الطريقة التي تم بها تنفيذ واحدة أو أكثر من عمليات الإدخال أو الإنشاء أو التجهيز أو التخزين أو التقديم أوالارسال.



- (ب) مدى إمكانية التعويل على الطريقة التي استخدمت في المحافظة على سلامة المعلومات.
- (ج) مدى إمكانية التعويل على مصدر المعلومات إذا كان معروفا .
- (د) مدى إمكانية التعويل على الطريقة التي تم بها تأكد المنشئ إذا كان ذلك ذا صلة.
- (هـ) أي عامل آخر يتصل بالموضوع " .

كما أجاز هذا القانون للجهات الحكومية التعامل بالوثائق المعلوماتية طبقا للمادة 1/27 "على الرغم من وجود أي نص مخالف في أي قانون آخر، يجوز لأية دائرة أو جهة تابعة للحكومة في أداء المهام المناطة بها بحكم القانون، أن تقوم بما يلي :

- (أ) قبول إيداع أو تقديم المستندات أو إنشائها أو الإحتفاظ بها في شكل سجلات الكترونية.
- (ب) إصدار أي إذن أو ترخيص أو قرار أو موافقة في شكل سجلات الكترونية.
- (ج) قبول الرسوم أو أية مدفوعات أخرى في شكل الكتروني.
- (د) طرح العطاءات واستلام المناقصات المتعلقة بالمشتريات الحكومية بطريقة الكترونية.

إذا قررت أي جهة حكومية التعامل بهذه المستندات عليها أن تحدد :

(أ) الطريقة التي سيتم بواسطتها إنشاء أو إيداع أو حفظ أو تقديم أو إصدار تلك السجلات الإلكترونية .

(ب) الطريقة والاجراءات التي يتم بها طرح العطاءات واستلام المناقصات وانجاز المشتريات الحكومية.

(ج) نوع التوقيع الإلكتروني المطلوب بما في ذلك اشتراط أن يستخدم المرسل توقيعاً رقمياً أو توقيعاً إلكترونياً محمياً آخر .

(د) الطريقة والشكل الذي سيتم به تثبيت ذلك التوقيع على السجل الإلكتروني والمعيار الذي يجب أن يستوفيه مزود خدمات التصديق الذي سيقدم له المستند للحفظ أو الإيداع.

(هـ) عمليات وإجراءات الرقابة المناسبة للتأكد من سلامة وأمن وسرية السجلات الإلكترونية أو المدفوعات أو الرسوم".

### ثالثاً : التشريع المصري

ساوى المشرع المصري بين الكتابة الإلكترونية والكتابة العادية من حيث القيمة القانونية في الإثبات، حيث نص في المادة 15 من قانون التوقيع الإلكتروني على " للكتابة الإلكترونية وللمحركات الإلكترونية في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للكتابة والمحركات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية متى استوفت الشروط المنصوص عليها في هذا القانون وفقا للضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون".

كما أعطى المشرع المصري للتوقيع الإلكتروني ذات القيمة القانونية المقررة للتوقيع الخطي، وذلك من خلال المادة 14 التي تنص على "للتوقيع الإلكتروني في نطاق المعاملات المدنية والتجارية والإدارية ذات الحجية المقررة للتوقيعات في أحكام قانون الإثبات في المواد المدنية والتجارية، إذا روعي في إنشائه وإتمامه الشروط المنصوص عليها في هذا القانون، والضوابط الفنية والتقنية التي تحددها اللائحة التنفيذية لهذا القانون".

إن المشرع المصري لم يخرج عن نهج بقية التشريعات التي أخذت بمبدأ النظير الوظيفي أو المعادلة الوظيفية المقررة في قانون الأونسترال، حيث ترتبط المساواة بين الوثيقة الورقية

والوثيقة المعلوماتية من حيث القيمة القانونية بمدى تحقق الوظائف التي تؤديها الكتابة العادية عندما يتعلق الأمر بالكتابة الإلكترونية والتوقيع الإلكتروني.

### **المبحث الثاني : شروط تمتع الوثيقة المعلوماتية بالحماية القانونية**

كل التشريعات التي ساوت بين الوثيقة الورقية والوثيقة المعلوماتية من حيث قيمتها في الإثبات ربطت ذلك بمجموعة من الشروط الفنية والتقنية التي تضمن لهذه الوثيقة أداء وظيفتها في ذلك، ويتعلق الأمر بشروط الكتابة الإلكترونية والتوقيع الإلكتروني ، وظروف حفظ الوثيقة لتحقيق سلامة المحتوى وثباته.

#### **المطلب الأول : الكتابة الإلكترونية**

من أجل تحديد شروط الكتابة الإلكترونية حتى تؤدي الوظيفة التي تؤديها الكتابة على الورق، استوجب ذلك تحديد مفهومها باعتبارها مرتبطة ببيئة مختلفة عن الكتابة العادية، وهو ما سعت إليه مختلف التشريعات التي نظمت التعامل بالوثيقة المعلوماتية.

#### **الفرع الأول : مفهوم الكتابة الإلكترونية**

سنحاول استقراء بعض التشريعات الغربية والعربية في تحديد مفهوم الكتابة الإلكترونية من خلال قانون الأونسترال ، التشريع الفرنسي ، التشريع المصري.

## أولاً: مفهوم الكتابة الإلكترونية في قانون الأونسترال

إن معنى الكتابة لا يرتبط بالضرورة بتدوين الأفكار على الورق، وبالتالي يكفي أن يكون هناك وسيط قادر على نقل الرموز والأشكال وماتضمنته الوثيقة أياً كان الوسيط المستعمل لنقل هذه التعابير المتعلقة بحق أو مركز قانوني معين .

وبالتالي ينعقد الإرتباط بين الكتابة والوسيط الورقي، حيث أية دعامة قادرة على عكس مضمون الكتابة فإنه من الممكن أن يأخذ بها في الإثبات<sup>1</sup> .

وبذلك تم الفصل بين شرط الكتابة الورقية وحماية الوثيقة المعلوماتية، وهو ما كرسه قانون الأونسترال النموذجي المتعلق بالتجارة الإلكترونية في المادة 1/06 التي تنص على: "عندما يشترط القانون أن تكون المعلومات مكتوبة تستوفي رسالة البيانات ذلك الشرط إذا تيسر الإطلاع على البيانات الواردة فيها على نحو يتيح استخدامها بالرجوع إليها لاحقاً".

لقد جعل قانون الأونسترال النموذجي المتعلق بالتجارة الإلكترونية البيانات المعالجة والمحمولة على وسيط الكتروني بإمكانها أن تؤدي نفس الوظيفة التي تؤديها الورقة بما عليها من كتابة مقروءة وواضحة تثبت حق أو مركز قانوني، طالما أمكن الإطلاع على البيانات والرجوع إليها.

وبالتالي فقد ركزت هذه المادة على المفهوم الأساسي للبيانات المستنسخة والمقروءة دون النص على الشرط القاضي بوجود أن تقي رسائل البيانات في جميع الحالات بكل ما يمكن

---

1: ناهد فتحي الحموري، مرجع سابق ، ص.ص 66 ، 67 .

تصوره من وظائف الكتابة، مع عدم الإعتداد بنوع الوسيط الحامل للبيانات في مسألة الإثبات، فقدرة الوسيط على الإحتفاظ بما دون عليه يتحقق معه الإعتراف بهذا الوسيط في الإثبات، ومن ثم ينعلم أي ارتباط قانوني بين المحرر ووجوب تدوينه على وسيط ورقي أو شكل كتابي معين<sup>1</sup>. ولذلك فالمفهوم المعبر عنه في هذه المادة يتعلق بمعيار موضوعي وهو أن المعلومات الواردة في رسالة البيانات يجب أن تكون في المتناول حتى يتسنى استخدامها للإحالة المرجعية لاحقاً<sup>2</sup>.

### ثانياً : مفهوم الكتابة الإلكترونية في التشريع الفرنسي

نص المشرع الفرنسي في المادة 1316 من القانون المدني على: "يشمل الإثبات عن طريق الكتابة كل تدوين للحروف أو العلامات أو الأرقام أو أي رمز أو إشارة أخرى ذات دلالة تعبيرية واضحة ومفهومة، أي كانت الدعامة التي تستخدم في إنشائها، أو الوسيط الذي تنقل عبره".

لقد وسع المشرع الفرنسي في هذا النص من مفهوم الكتابة ليشمل جميع أشكالها، وبالتالي أعاد تعريف الدليل الكتابي بشكل مستقل عن دعامته<sup>3</sup>، وفي نفس الوقت كرس مبدأ عدم التمييز بين أنواع الكتابة بسبب الدعامة الموجودة عليها، فلا يهتم الوعاء الذي يحوي هذه الحروف أو العلامات أو الأرقام التي تعبر عن فكرة معينة، سواء كان هذا الوعاء مادي أو غير مادي،

---

1 : ناهد فتحي الحموري، مرجع سابق، ص.ص 68 ، 69 .

2 : عمر حسن المومني ، مرجع سابق ، ص . 198 .

3 : Valérie Sédallian, "Preuve et Signature Electronique", 09 Mai 2000 ,(Juriscom.net) .voir aussi :  
Thuy – Trần Tran, Op.Cit, P.44 .

وبالتالي لا يمكن إنكار القوة الثبوتية لهذه الكتابة أو درجتها بسبب الطريقة المستخدمة في تحرير المعلومات، أو الوسيلة التي تم عبرها نقل هذه المعلومات<sup>1</sup>.

إن التطور المستمر في وسائل الإتصال هو الذي أدى إلى إعادة النظر في مفهوم الكتابة، إذ الهدف من استلزام أن يأخذ عقد أو إتفاق شكل الكتابة ليس هو الدعامة الورقية ذاتها، وإنما هو وسيلة لتثبيت المعلومات التي تتضمنها<sup>2</sup>.

ولذلك فإن الكتابة الرقمية في نظر المتخصص في الإعلام الآلي ماهي إلا تسلسل رموز ثنائية مكونة من صفر وواحد، لأن الأمر يتعلق بمعطيات يتم إنشائها، أو تخزينها، أو نقلها أو معالجتها أو عرضها بواسطة نظام رقمي<sup>3</sup>.

وبالتالي فالكتابة لا تعني بالضرورة تدوين الأفكار على ورق، بل يكفي أن يكون هناك وسيط قادر على نقل الرموز والأشكال والإشارات والحروف والأرقام التي تكون معنى مهما كان نوع هذا الوسيط، ولذلك بين الاتحاد الأوروبي في الدراسات التي أعدها أن اشتراط توافر الكتابة لصحة صفقة قانونية ما يمثل بوضوح عقبة بديهية مطلقة تعترض تبادل البيانات الكترونياً، وتبادل البيانات الكترونياً لا يمكن أن يستخدم لإنجاز الصفقات القانونية طالما ظل هذا الشرط قائماً<sup>4</sup>.

1 : ثروت عبد الحميد، مرجع سابق، ص. 176 .

2 : فيصل سعيد الغريب، التوقيع الإلكتروني وحججه في الإثبات. المنظمة العربية للتنمية الإدارية، القاهرة، 2005، ص. 104.  
3 : Françoise Banat-Berger , Anne Canteant, "Intégrité, Signature et Processus d'Archivage", Direction des Archives de France, S.D, p 16,17 .

4 : نادر فاحوش، العمل المصرفي عبر الإنترنت. الدار العربية للعلوم، ط1، بيروت، لبنان، 2001، ص. 82.

### ثالثا : مفهوم الكتابة الإلكترونية في التشريع المصري

عرف المشرع المصري الكتابة الإلكترونية في قانون التوقيع الإلكتروني في المادة 01 بأنها " كل حروف أو أرقام أو رموز أو أي علامات أخرى تثبت على دعامة الكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك " .

يقول الدكتور بيومي حجازي في تعقيبه على هذا النص<sup>1</sup> ، أن المشرع المصري قد عول في تعريفه للكتابة الإلكترونية على مسألتين الأولى هي الدعامة المادية المثبتة عليها الكتابة، وهذا يعني أن الكتابة الموجودة داخل الجهاز أو على شبكة الانترنت التي لا يمكن فصلها لاتعد كتابة الكترونية حسب التعريف المذكور ، ولكن من ناحية أخرى فتح المجال أمام تعدد نماذج الدعامات المادية التي قد تثبت عليها الكتابة الإلكترونية لتستوعب أي وسيلة تظهر في المستقبل .

ويقول د. سامح عبد الواحد التهامي أن هذا النص اتبع أسلوب الحياد التقني الذي يسمح بقبول أية صورة حديثة<sup>2</sup>، وهو النهج الذي اتبعه قانون الأونسترال من أجل المعادلة الوظيفية بين الكتابة الإلكترونية والكتابة الورقية. ذلك أن الاعتماد الهائل على المعلوماتية وشبكة الإنترنت في المعاملات اليومية أدى إلى ظهور نظام تبادل المعلومات الكترونيا، الأمر الذي

---

1 : عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، مرجع سابق، ص.45 .

2 : سامح عبد الواحد التهامي، مرجع سابق، ص . 513 .

غير من مفهوم الكتابة حيث أصبح إرسال ونقل البيانات يتم من خلال سلسلة رموز وأرقام محملة على دعامات غير ورقية<sup>1</sup> .

وبالتالي أصبح من غير المنطقي التمييز بين الكتابة الورقية والكتابة المعلوماتية على أساس الوعاء الذي يحوي تلك الأفكار أو المعاني المثبتة لحق أو مركز قانوني، أو إنكار قوة تلك الكتابة بسبب هذا الحامل ، بل العبرة بتلك المعلومات التي لها دلالة قابلة للإدراك . ومن البديهي أن إدراك هذه الدلالة لا يتم مباشرة بسبب طبيعة هذه الكتابة، ولذلك بين قانون الأنسترال ضرورة تيسير الإطلاع على هذه المعلومات واسترجاعها، وهو المعيار المعول عليه

### الفرع الثاني : شروط الكتابة الإلكترونية

حتى تؤدي الكتابة وظيفتها لابد من توافر عدة شروط تتعلق بمدى إمكانية قراءتها، وثباتها وديمومتها .

### أولا : مدى إمكانية قراءة الكتابة الإلكترونية

لابد أن تكون الكتابة ذات مضمون واضح ومفهوم يمكن ادراكه من خلال الكلمات أو الرموز أو الإشارات أو بقية العلامات المكونة لها، حيث يتم ادراكها مباشرة بواسطة العين . غير أن الأمر يختلف عندما يتعلق الأمر بالبيانات الإلكترونية التي تتم في صورة غير مادية، وقد تكون مشفرة أحيانا<sup>2</sup> ، حيث لا يمكن قراءتها مباشرة بل لابد من وسيط إلكتروني،

1 : عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة ، مرجع سابق ، ص 44 .

2 : الصالحين محمد العيش، مرجع سابق ، ص . 165 .



ولكن لاينفي عن الكتابة خاصية امكانية القراءة أنها في هذا الشكل الإلكتروني ، حيث تأتي الوثيقة الإلكترونية في شكل تتابع رقمي 0 و 1 اللذان يميزان هذه الكتابة، وبالتالي فإن هذا التتابع الزوجي ومن خلاله فقط يمكن تقنيا ضمان سلامة الوثيقة،...التي تضمن امكانية قراءتها إذا تم حفظها<sup>1</sup> .

إن الوصول إلى المعلومة وادراكها إذا كانت ضمن وثيقة معلوماتية يستدعي معالجة الكترونية معقدة ومتتابعة بوساطة مجموع المكونات المادية والبرامج وأنظمة التشغيل ، ولذلك فإن امكانية القراءة تعني " إمكانية الدخول - في لحظة استرجاع الوثيقة- إلى مجموع المعلومات التي تتضمنها<sup>2</sup> .

ولعل هذه العمليات المركبة لإدراك مضمون الوثيقة هي التي جعلت جانب من الفقه يتمسك بالمعنى الضيق للكتابة التي يعتمد ادراكها على حاسة العين ، وبالتالي فإن أي كتابة من نوع آخر لا يمكن ادراكها مباشرة لن يكون لها قيمة قانونية .

غير أن شرط امكانية قراءة الكتابة والإطلاع عليها متوافر أيضا بالنسبة للوثيقة المعلوماتية في اللحظة التي تستعمل فيها العدة المناسبة للقراءة لإمكانية فهم الكتابة من طرف الإنسان<sup>3</sup> ، وذلك من خلال العتاد المعلوماتي ونظام التشغيل المناسب لإمكانية إدراك مضمون الكتابة<sup>4</sup> .

---

1 : Francaise Banat-Berger, Anne Canteau, Op.Cit, P16,17.

2 : Ibid , P . P , 19 - 21 .

3 : Stephane Caidi,Op.cit, P. 20 .

4 : Najoua Djerad,"Cycle de vie du Document Électronique et Obligations de conservation" . S.D. ([www.ebsi.umontreal.ca/rech/ebsi-enssib/pdf/Djerad.pdf](http://www.ebsi.umontreal.ca/rech/ebsi-enssib/pdf/Djerad.pdf)), P 7 .

## ثانيا : ثبات الكتابة الإلكترونية وديمومتها

إن شرط الثبات والديمومة أو الإستمرار يرتبط بأداء وظيفة الكتابة في الإثبات ، حيث إن تدوينها على وسيط يمنح لها الثبات والديمومة يمكن من العودة إليها عند الحاجة<sup>1</sup> .

ولذلك فقد نص قانون الأونسترال النموذجي للتجارة الإلكترونية على ذلك في المادة 1/06:

"عندما يشترط القانون أن تكون المعلومات مكتوبة ، تستوفي رسالة البيانات ذلك الشرط إذا تيسر الإطلاع على البيانات الواردة فيها على نحو يتيح استخدامها بالرجوع إليها لاحقا " .

إن الإطلاع على المعلومات الواردة في الرسالة الإلكترونية كلما دعت الحاجة إلى ذلك يتطلب ثبات الكتابة ودوامها، ولذلك كان هذا شرطا من شروط الكتابة الإلكترونية. ويعني هذا الشرط اتصاف العلامات والرموز المكونة للكتابة الإلكترونية بالثبات النسبي ، حيث لاتزول تلقائيا ، بل تبقى طالما لم يتعرض للإتلاف، وذلك لأن من وظائف الكتابة كفالة بقاء الوثيقة وعدم زوالها بمرور الزمن ، وهذا ما يشير إليه دليل تشريع قانون الأونسترال النموذجي للتجارة الإلكترونية .

كما أن مسألة ثبات الكتابة وديمومتها مرتبط أيضا بالوسيط الذي يحمل عليه ، حيث لابد أن يوفر هذه الخاصية ولذلك تعددت وسائط تخزين المعلومات وما تزال تتطور بتطور التكنولوجيا الرقمية .

---

1 : محمد أمين الرومي ، مرجع سابق ، ص . 48 .

## المطلب الثاني : التوقيع الإلكتروني

يلعب التوقيع الإلكتروني دورا مهما بالنسبة للوثيقة المعلوماتية، فهو أحد العناصر المهمة لتمتع هذه الوثيقة بالحجية، ومن ثم إضفاء الحماية القانونية عليها، ولكن لا بد أن يؤدي هذا التوقيع وظائف التوقيع العادي، وهذا ما سعت إليه التشريعات الدولية والوطنية التي نظمت التعامل به، حيث بينت مفهومه وشروطه لآداء هذه الوظيفة .

### الفرع الأول : مفهوم التوقيع الإلكتروني

حاولت القوانين الدولية والوطنية النازمة للتوقيع الإلكتروني أو المعاملات الإلكترونية بصفة عامة تحديد مفهوم التوقيع الإلكتروني كما حاول الفقه وضع تعريف له على غرار التوقيع العادي .

### أولا : مفهوم التوقيع الإلكتروني تشريعا

بينت عدة قوانين دولية ووطنية مفهوم التوقيع الإلكتروني نظرا لأهميته في إثبات صحة الوثيقة المعلوماتية، من أهمها قانون الأونسترال النموذجي للتوقيعات الإلكترونية، والتوجيه الأوربي للتوقيع الإلكتروني ، وكذا التشريع الفرنسي وبعض التشريعات العربية .

#### 1- مفهوم التوقيع الإلكتروني في قانون الأونسترال والتوجيه الأوربي للتوقيع الإلكتروني :

عرف التوقيع الإلكتروني في قانون الأونسترال النموذجي للتوقيعات الإلكترونية في المادة 02/أ بأنه " بيانات في شكل الكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا ، مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا ، يجوز أن تستخدم

لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات " .

أما المشرع الأوربي فقد عرفه في التوجيه الأوربي للتوقيع الإلكتروني في المادة 02 بأنه " البيانات في الشكل الإلكتروني التي تلحق أو ترتبط مع بيانات الكترونية أخرى والذي يساعد كطريقة للتوثيق " .

من خلال التعريفين السابقين يتبين أن التوقيع الإلكتروني هو جزء من الوثيقة المعلوماتية باعتبارها تذييل به لآداء وظيفة معينة، لكنه لا يعتبر من محتواها ، ولذلك عرفه كلا التشريعين بأنه عبارة عن " بيانات " فهو لا يتضمن مجموعة أفكار مثل الرسالة إلا أنه يؤدي وظيفة مهمة أجزها المشرع الأوربي في وظيفة التوثيق التي تتعلق بصحة محتوى الوثيقة المعلوماتية وعدم التلاعب بها ، ونسبتها إلى صاحبها وعدم إنكارها ، لكنه ميز بين التوقيع الإلكتروني البسيط والتوقيع الإلكتروني المتقدم ، حيث يتطلب التوجيه الأوربي في التوقيع الإلكتروني المتقدم عددا من الشروط الخاصة بضمان الأمان والموثوقية ، والتي لاتعتبر مطلوبة في حال ذلك البسيط ، وبالمقابل أعطى للتوقيع المتقدم ميزة أكبر من حيث الاعتراف الكامل بحجته<sup>1</sup> .

ولكي يؤدي التوقيع الإلكتروني وظيفته لابد أن يتوافر على مجموعة من الشروط التقنية اللازمة لضمان الثقة في الوثيقة المعلوماتية كي تتمتع بالحجية القانونية ، حيث لابد من ارتباطه بالموقع وحده ، وأن يمكن من تحديد هويته ، وأن ينشأ بوسائل تمكن الموقع من إبقائه

---

1: عدنان برنو، "قانون التوقيع الإلكتروني" مجلة المعلوماتية، عدد5، (تموز 2006). على موقع: (<http://infmag.news.sy>)

تحت سيطرته ، بالإضافة إلى ارتباطه بالوثيقة بالشكل الذي يمكن من اكتشاف أية تعديلات تطراً عليها .

وفي إطار تحقيق المتطلبات اللازمة في التوقيع الإلكتروني لأداء وظيفته نظم المشرع خدمات التوثيق، وما يتعلق بالشهادات الصادرة عن جهات التصديق الإلكتروني الخاصة أو العامة المرخص لها ، حيث تسمح هذه الشهادات باعتماد توقيع الكتروني معين لضمان الثقة في المعاملات الإلكترونية الخاصة أو الحكومية .

## 2- مفهوم التوقيع الإلكتروني في التشريعات الوطنية :

اهتمت التشريعات الوطنية بتنظيم التوقيع الإلكتروني لإرتباطه بالوثيقة المعلوماتية (رسالة المعلومات) ارتباطاً وثيقاً ، حيث سيؤدي نفس الدور الذي يؤديه التوقيع الخطي على الوثيقة الورقية .

### أ. مفهوم التوقيع الإلكتروني في التشريع الأردني :

عرف المشرع الأردني التوقيع الإلكتروني في قانون المعاملات الإلكترونية في المادة 2 بأنه "البيانات التي تتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها وتكون مدرجة بشكل الكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مماثلة في رسالة معلومات أو مضافة عليها أو مرتبطة بها ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره من أجل توقيعه وبغرض الموافقة على مضمونه" .

إن المشرع الأردني لم يورد حصراً لصور التوقيع الإلكتروني عندما عرفه ، وذلك ليتسع مستقبلاً لأي صور أو أشكال قد تظهر متفقاً بذلك مع قواعد قانون الأونسترال النموذجية ، كما

أبدى اهتمامه بضرورة أن يكون التوقيع الإلكتروني ممثلاً لشخص الموقع ومعبراً عن رغبته في الإلتزام بما وقع عليه<sup>1</sup> .

### ب. مفهوم التوقيع الإلكتروني في التشريع الإماراتي :

عرف المشرع الإماراتي التوقيع الإلكتروني في قانون المعاملات والتجارة الإلكترونية في المادة 02 بأنه "توقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذي شكل إلكتروني وملحق أو مرتبط منطقياً برسالة إلكترونية وممهور بنية توثيق أو اعتماد تلك الرسالة". لقد بين المشرع الإماراتي الصلة بين التوقيع الإلكتروني والرسالة الإلكترونية كما هو الحال بالنسبة للتوقيع العادي على الوثيقة الورقية ، ولكن نظراً لإختلاف طبيعة هذا التوقيع الذي يأتي في شكل إلكتروني، فقد بين أن هذا الارتباط هو ارتباط منطقي ، وليس ارتباطاً مادياً بوجود التوقيع على الوثيقة الورقية .

إن هذا الارتباط المنطقي يعني أن التوقيع الإلكتروني هو جزء من الرسالة الإلكترونية، أو قد يكون ملحق بها ، وذلك لأداء وظيفة مهمة هي وظيفة توثيق الرسالة الإلكترونية .

لقد جمع المشرع الإماراتي في تعريفه للتوقيع الإلكتروني بين الجانب التقني والوظيفي كما جاء في تشريع الأونسترال النموذجي للتوقيعات الإلكترونية ، وكذا التوجيه الأوربي للتوقيع الإلكتروني، وقد كان أقرب لهذا الأخير من حيث الصياغة ، فقد أوجز وظيفة التوقيع في التوثيق كما جاء في المادة 02 من التوجيه الأوربي .

---

1: يوسف أحمد النوافلة ، مرجع سابق ، ص . 69 .

## ج. مفهوم التوقيع الإلكتروني في التشريع المصري :

عرف المشرع المصري التوقيع الإلكتروني في القانون 04/15 في المادة 01/ج بأنه "كل ما يتم وضعه على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو رسوم أو غيرها ، ويكون له طابع متفرد، يسمح بتحديد شخص صاحب التوقيع ويميزه عن غيره " .

لم يبين المشرع المصري بدقة طبيعة التوقيع الإلكتروني مثل نظيره الأردني على ضوء قواعد قانون الأونسترال والتوجيه الأوربي، التي بينت أن التوقيع الإلكتروني عبارة عن بيانات إلكترونية مضافة لرسالة المعلومات، مما يجعله متميز عن محتواها ، بينما لم يوفق المشرع المصري بالصياغة الواردة أعلاه في بيان ذلك عندما اعتبره بأنه كل ما يوضع على محرر إلكتروني متخذا أشكال مختلفة كالحروف أو الأرقام أو الرموز أو الإشارات أو الرسوم أو غيرها، حيث هذه الأشكال في حد ذاتها قد تكون محتوى المحرر (الوثيقة) .

ولكي يؤدي التوقيع الإلكتروني وظيفته المذكورة في المادة السابقة نصت اللائحة التنفيذية لهذا القانون<sup>1</sup> على مجموعة من الضوابط الفنية والتقنية من أجل تأمين بيانات التوقيع الإلكتروني وهي التفرد في بيانات إنشائه والسرية فيها ، وعدم قابليتها للإستنتاج والإستنباط وحمايتها ضد التزوير .

وتعتبر هيئة تنمية صناعة التكنولوجيا في مصر - وهي من الهيئات الإقتصادية التابعة للدولة - هي الجهة التي لها سلطة التصديق الإلكتروني ، حيث تتولى إصدار المفاتيح الشفوية

---

1: قرار وزاري 05/108 المتضمن اللائحة التنفيذية للقانون 04/15 المتعلق بالتوقيع الإلكتروني .

الجزرية الخاصة للجهات المرخص لها بإصدار شهادات التصديق الإلكتروني طبقا للمادة 05 من قانون التوقيع الإلكتروني ، وهي التي تتحقق قبل منح ترخيص مزاولة نشاط إصدار شهادات التصديق الإلكتروني أن منظومة تكوين بيانات إنشاء التوقيع الإلكتروني لدى الجهة المرخص لها مؤمنة وتتضمن الضوابط الفنية والتقنية. كما تقدم خدمة فحص التوقيع الإلكتروني بعد التحقق من سلامة شهادة التصديق الإلكتروني، وموافقتها لبيانات إنشاء التوقيع الإلكتروني، وإمكانية تحديد مضمون الوثيقة الموقعة وشخص موقعها .

#### د. مفهوم التوقيع الإلكتروني في التشريع الفرنسي :

لقد وضع المشرع الأوربي-من خلال أحكام التوجيه الأوربي- الإطار المشترك للتوقيع الإلكتروني في الدول الأوربية، ولذلك سعى المشرع الفرنسي إلى تنظيم التوقيع الإلكتروني على ضوء هذه الأحكام من خلال تعديل نصوص القانون المدني المتعلقة بالدليل الكتابي، حيث أعطى المشرع الفرنسي للتوقيع الإلكتروني نفس القيمة القانونية التي يتمتع بها التوقيع الخطي على وثيقة ورقية، وذلك من خلال المادة 3/1316 من القانون المدني ولكن بتوافر شروط تقنية معينة.

ويصدر المرسوم 2001/272<sup>1</sup> تم تحديد الشروط الواجب توافرها في التوقيع الإلكتروني لكي يحقق الموثوقية التي تطلبها المادة 04/1316 من القانون المدني، حيث تتعلق بالبرامج

---

**1:** décret d'application 272/2001 du 30 mars 2001 relatif a l'application des articles modifiés du droit civil journal officiel, n° 77,(31 Mars 2001), P. 5070 .



والأدوات المستعملة في إنشاء توقيع إلكتروني وبمضمون الشهادة التي تضمن هوية الموقع <sup>1</sup> .

وأمام هذه الشروط سيكون التوقيع الإلكتروني أقل تزويراً من التوقيع الخطي، حيث يرتبط

التوقيع الإلكتروني فيما يتعلق بإجراءات الأمان والحماية بعلم التشفير <sup>2</sup> .

### ثانياً : مفهوم التوقيع الإلكتروني فقها :

يعرف التوقيع الإلكتروني بأنه " جزء صغير مشفر من بيانات يضاف إلى رسالة

إلكترونية، فهو مجتزأ من الرسالة ذاتها يشفر ويرسل مع الرسالة ، ليتم التوثق من صحة الرسالة

بفك التشفير وانطباق محتواه على الرسالة" <sup>3</sup> .

يشير المؤلف إلى أن التوقيع الإلكتروني عبارة عن بيانات مرتبطة بالرسالة الإلكترونية

(الوثيقة المعلوماتية)، تعتمد على نظام التشفير، وتؤدي وظيفة مهمة وهي التوثيق كما أوجزها

التوجيه الأوربي، إلا أن هذا التعريف اقتصر على نوع من أنواع التوقيع الإلكتروني وهو التوقيع

الرقمي . كما يعرف بأنه " كل حروف أو أرقام أو رموز أو أصوات أو نظام معالجة ذي شكل

إلكتروني أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموقع ويميزه عن غيره، بحيث

يعبر عن رضا الموقع بمضمون التصرف ويضمن سلامته <sup>4</sup> . لقد جمع هذا التعريف بين

عناصر التوقيع وخصائصه، ووظيفته في القبول بمضمون الوثيقة وضمن سلامتها .

---

1 : Maximilien Amegee, *la Signature Electronique* . BEDA, S . L, 2002 , P . 11 .

2 : Ibidem .

3 : خالد عبد الفتاح محمد، مرجع سابق ، ص . 15 .

4 : أسامة روبي، " حجية التوقيع الإلكتروني في الإثبات والإدعاء مدنياً بتزويره " ، مؤتمر المعاملات الإلكترونية، جامعة الإمارات العربية المتحدة ، دب ، ص . 509 .

إن المقارنة بين وظائف التوقيع الإلكتروني والتوقيع التقليدي التي تتمثل في التحقق من شخصية الموقع، وإقرار الموقع بمضمون الوثيقة الموقعة منه، وعدم إنكارها، يمكن من اعتبار التوقيع الإلكتروني أشد ثقة من التوقيع التقليدي، فهو لا يدلنا فقط على شخصية الموقع، وإنما يؤكد أيضا أن الوثيقة لم تحرف بعد توقيعها، وهو ما لا يستطيع التوقيع اليدوي التقليدي تحقيقه، خاصة عندما يتعلق الأمر بالتوقيع الرقمي المعتمد على تقنية المفاتيح<sup>1</sup>. (أنظر الشكل رقم 6)

إن هذه التقنية تعتمد على اللوغاريتمات التي تستعمل بطريقة متكاملة فيما بينها ، حيث تتعلق الأولى باللوغاريتم الأسيمتري وهذا النظام يقوم على زوج مفاتيح رقمية مبنية بطريقة بحيث لا يمكن إيجاد إحدى هذه المفاتيح إلا من خلال الآخر<sup>2</sup> . وتسمح هذه المفاتيح بالتوقيع الكترونيا على الوثيقة ، كما تستعمل في فك تشفير المعطيات لضمان السرية، فإذا أراد شخص إرسال رسالة (وثيقة) مشفرة فإنه يستعمل المفتاح العام للمرسل لتشفير المحتوى، غير أن المفتاح الخاص – المرتبط بالمفتاح العام – وحده قادر على فك التشفير<sup>3</sup> .

إن التوقيع الرقمي هو شكل فقط من أشكال التوقيع الإلكتروني، فهذا الأخير يشير إلى جميع الوسائل والأساليب الممكنة لإنتاج الموقع لتوقيعه بصورة الكترونية بقصد الإلتزام بمضمون السند الموقع ، فهو مصطلح أوسع<sup>4</sup> .

---

1 : عدنان برنو ، مرجع سابق .

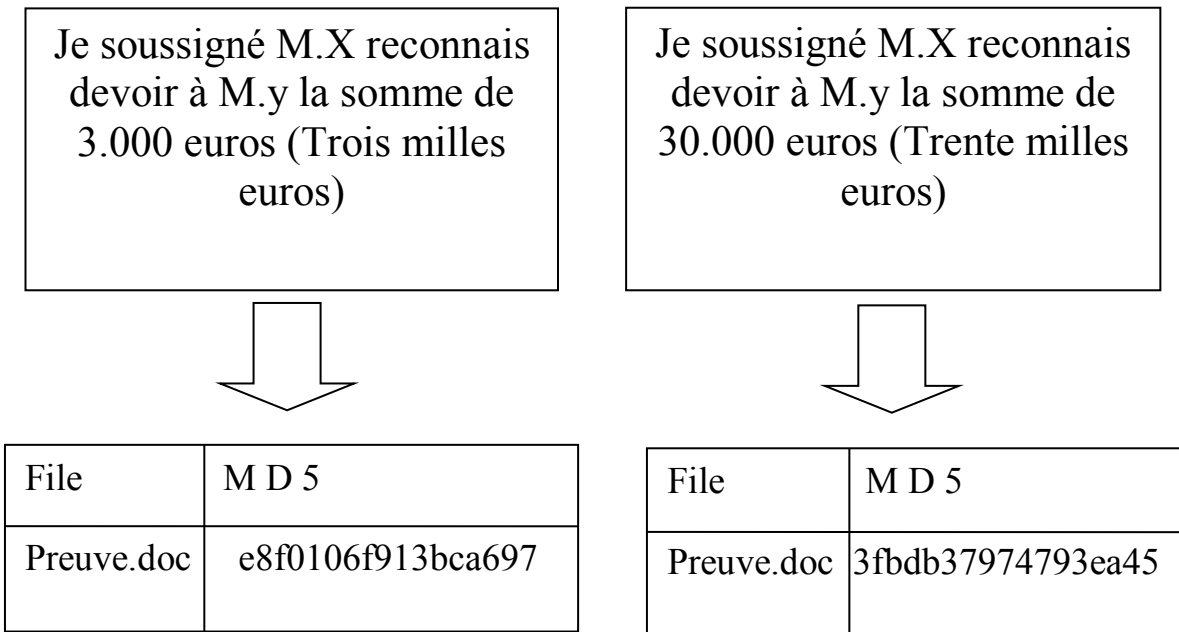
2 : Jean-luc parouty, " La Signature électronique ", S.D, ([www.jres.org/actes/79 . pdf](http://www.jres.org/actes/79.pdf)).

3 : Carine Bernard, L'utilisation de la signature électronique au CNRS, (stage d'application), Institut régional d'administration de lille, 2003/2004, P.20 .

4 : حاتم محمود عبد الرزاق ، " تعريف وخصائص التوقيع الإلكتروني " ، 11 سبتمبر 2012 ، ([www.ksp.gov.Sd](http://www.ksp.gov.Sd)) .

ولذلك فإن مفهوم التوقيع الإلكتروني لا يجب أن يحدد بصورة أو شكل معين من أشكال التوقيع ، خاصة وأن هذه الأشكال غير محصورة بسبب التطور المستمر في مجال المعلوماتية، والتعريف الأنسب هو الذي لا يخوض في ذكر أشكال التوقيع الإلكتروني حتى لا يقف عائقاً في وجه أي تطور تقني لاحق<sup>1</sup> .

### شكل رقم (6) : شكل توضيحي للتوقيع الإلكتروني



**La Source :** Lucien pauliac , " la face cachée de la signature Electronique " ,  
27 Septembre 2010, ( [www.megapreuve.org/cariboost-files/signature-electronique.pdf](http://www.megapreuve.org/cariboost-files/signature-electronique.pdf) ).

**1:** حاتم محمود عبد الرزاق ، مرجع سابق.

## الفرع الثاني : أشكال التوقيع الإلكتروني

للتوقيع الإلكتروني أشكال عديدة ، يمكن استخدامها للتوقيع على الوثيقة المعلوماتية ، حيث تتمتع بقدر من الأمان ولكن بنسب متفاوتة ، كما أن النماذج الموجودة ليست على سبيل الحصر فقد تفرز التكنولوجيا أشكالا جديدة. ومن بين النماذج الشائعة نجد التوقيع البيومتري، التوقيع بالقلم الإلكتروني، التوقيع بالرقم السري، التوقيع الرقمي .

### 1- التوقيع البيومتري :

يعتمد هذا التوقيع على السمات الخاصة بكل شخص والتي تميزه عن غيره ، ولذلك فهو يؤدي نفس وظيفة التوقيع من حيث تحديد هوية الشخص إذا تم تخزين إحدى هذه الوسائل على بطاقة بصورة رقمية مضغوطة<sup>1</sup> .

ويمكن التمييز في هذا المجال بين ثلاث فئات من الخصائص البيومترية وهي الخصائص البيولوجية مثل الدم ، اللعاب ، الرائحة، الحمض النووي والخصائص الذاتية مثل التوقيع ، حركات الجسم ، والخصائص الشكلية مثل بصمات الأصابع ، الوجه ، العين ، وشكل اليد<sup>2</sup> . ويوضح الشكل الموالي صور للتوقيع البيومتري .

---

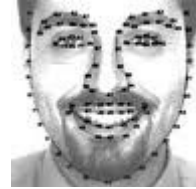
1: خالد عبد الفتاح محمد، مرجع سابق ، ص . 25 .

2 : Hocine Boutella, **Système Biometrique de Vérification de Signature Manuscrite en Ligne**, (Mémoire de Magister),Systemes informatiques,Ecole Nationale d'informatique,Alger,S.D,p 5

## شكل توضيحي رقم (7): صور التوقيع البيومتري



بصمة الأصبع



الوجه



بصمة العين



بصمة اليد و الصوت

Source :Hocine Boutella ,Op.cit ,p06 .

تخزن هذه الخصائص - بعد أخذ صورة دقيقة لها - داخل الكمبيوتر لمنع استخدامها بشكل غير قانوني، حيث يتم التقاط صورة دقيقة لإحدى هذه الخواص التي يراد استعمالها كتوقيع، ثم تخزن بطريقة مشفرة في ذاكرة الكمبيوتر، لتتم برمجته بعدم التعامل إلا في حال

مطابقة البصمة لتلك البرمجة في ذاكرته، وبالتالي لن يتمكن من فتح الحاسب الإلكتروني أي شخص غير المصرح لهم بذلك<sup>1</sup> .

ولذلك يستخدم النظام البيومتري بطريقتين<sup>2</sup> : تتعلق الأولى بالتعريف بالشخص حيث يحدد النظام الشخص الذي يمتلك المعطيات البيومترية التي تم إدخالها ، ثم يقارنها بتلك المخزنة في النظام المتعلقة بجميع المستعملين ليحدد هوية الشخص .

أما الطريقة الثانية فتتعلق بالتحقق والتأكد من الشخص صاحب الخصائص البيومترية المدخلة بمقارنها مع تلك المخزنة داخل النظام ، حيث يمكن القول أن الطريقة الأولى هي الإجابة عن السؤال : من هو الشخص الذي يملك هذه المعطيات البيومترية المدخلة للنظام ؟، فيما تتعلق الطريقة الثانية بالإجابة عن السؤال : هل هذا الشخص هو (س) ؟

لكن هذا النوع من التوقيع قد يكون عرضة للتزوير بطرق مختلفة مثل تسجيل بصمة الصوت، مطابقة بصمة الشفاه من خلال طلائها بمادة معينة ، تزوير بصمة العين من خلال استخدام العدسات اللاصقة ، كما يمكن نسخ بصمة الصوت أو الوجه ، كما يواجه هذا التوقيع عدة عقبات منها احتمال تغير بعض خصائص الإنسان بفعل الظروف ، كتآكل بصمات الأصابع ، تأثير التوتر على نبرة الصوت ، وغيرها ولذلك فإن هذا النوع من التوقيع الإلكتروني نادر الإستعمال عبر شبكات الإنترنت الإلكترونية<sup>3</sup> .

---

1 : عطا السنباطي، "الإثبات في العقود الإلكترونية – دراسة فقهية مقارنة-"، أعمال مؤتمر الأعمال المصرفية الإلكترونية، الإمارات العربية المتحدة، 10-12 ماي 2003 ، ص 471 .

2 : Hocine Boutella, Op. Cit , p 6 .

3 : نادر شافي ، " التوقيع الإلكتروني الإعراف التشريعي به وتعريفه القانوني "، مجلة الجيش، عدد 249 ، (آذار 2006)

## 2- التوقيع بالقلم الإلكتروني :

يعتبر التوقيع بالقلم الإلكتروني صورة من صور التوقيع البيومترية لأنه يعتمد على التوقيع الشخصي، حيث يوقع الشخص على شاشة الحاسب الآلي باستخدام قلم الكتروني خاص، وهذا يستوجب جهاز حاسب آلي ذا مواصفات خاصة تمكنه من أداء مهمته في النقاط التوقيع من شاشته<sup>1</sup> . وهو ما يوضحه الشكل الموالي .

### شكل توضيحي رقم (8): التوقيع بالقلم الإلكتروني



يتم التأكد من صحة هذا التوقيع بمضاهاة التوقيع الخطي المرسل بهذا القلم الإلكتروني الخاص بالتوقيع المخزن في ذاكرة الكمبيوتر، وذلك من خلال الإستناد إلى حركة القلم الإلكتروني والأشكال التي يتخذها من إنحناءات أو إتواءات وغيرها من السمات الخاصة بالتوقيع الخاص بالموقع<sup>2</sup> .

1 : إيمان مأمون أحمد سليمان، إبرام العقد الإلكتروني وإثباته . دار الجامعة الجديدة، الإسكندرية، 2008، ص 258 .  
2 : Caprioli , " Le juge et la preuve Electronique " , Revue de droit des technologies de l'information, N°10, (10 Janvier 2000) ([www.juriscom.net](http://www.juriscom.net)) .

غير أن هذا التوقيع لم يعرف على نطاق واسع في مجال التجارة الإلكترونية التي تفضل التوقيعات الرقمية، فضلا عن أن التوقيع بالقلم الإلكتروني يحتاج جهاز كمبيوتر بمواصفات خاصة تمكنه من التقاط التوقيع والتأكد من صحته ومطابقته للتوقيع المخزن في الذاكرة<sup>1</sup>.

### 3- التوقيع بالرقم السري :

يرتبط هذا النوع من التوقيع بالبطاقات الممغنطة التي تصدر عن البنوك والمؤسسات المالية لعملائها كوسائل دفع أو سحب، حيث تحمل هذه البطاقات أرقاما سرية خاصة بالعميل، يستخدمها عند ادخال البطاقة في جهاز الصراف الآلي، حيث يكون ذلك بمثابة توقيع على العملية البنكية أو المصرفية التي قام بها. أما عند استخدام بطاقة الوفاء في المحلات التجارية، فإن العملية تتم بين التاجر والبنك، حيث يرتبط الجهاز الخاص بتمرير البطاقة بنظم المعلومات الخاصة بالبنك للتأكد من رصيد صاحبها بعد إدخال الرقم السري، ليتم السداد عن طريق التحويل من حساب العميل لدى البنك إلى حساب التاجر لدى نفس البنك أو بنك آخر<sup>2</sup>.

إن ما يميز هذا النوع من التوقيع هو الأمان الذي يوفره إلى حد ما، حيث من الصعب الحصول على الرقم السري الذي لا يعلمه إلا صاحب البطاقة، إذ ترسله الجهة المختصة بذلك بمراسلة رسمية ، وعليه الإحتفاظ به وعدم إطلاع الغير عليه .

---

1 : خالد عبد الفتاح محمد ، مرجع سابق ، ص . 25 .

2 : ثروت عبد الحميد ، مرجع سابق ، ص 57 .



وفي حال سرقة أو ضياع الرقم السري يمكن لصاحب البطاقة إبلاغ البنك بأسرع وقت ليتم إيقاف العمل بها، هذا بالإضافة إلى اعتماد تقنية البرمجة الذاتية داخل ماكينات السحب النقدي، والتي تتعلق بإمكانية إعطاء حامل البطاقة ثلاث محاولات لإدخال الرقم السري بصورة صحيحة، فإن لم يتمكن يتم سحب البطاقة تلقائياً ولا يجوز لأي شخص سوى صاحبها أن يحصل عليها من الفرع الذي يوجد به حسابه، حيث يتم إرسال البطاقات لكل فرع صدرت منه<sup>1</sup>. لكن رغم ذلك فإن هذا التوقيع عرضة أيضاً لمخاطر التزوير، حيث كلما تطورت التقنية في هذا الجانب، كلما تناسبت الأساليب الإجرامية معها، وبالتالي تطورت تقنيات التزوير .

#### 4- التوقيع الرقمي :

يعتبر التوقيع الرقمي أحدث أشكال التوقيع الإلكتروني وأكثرها أماناً نظراً لطبيعته ، وتلك الشروط الفنية والتقنية الخاضع لها .

#### أ- طبيعة التوقيع الرقمي :

يعتمد التوقيع الرقمي على اللوغاريتمات أو المعادلات الرياضية ، حيث تتحول الكتابة العادية المقروءة إلى لغة الأرقام وهي لغة خاصة غير مقروءة ، ولذلك يقوم هذا التوقيع على عملية التشفير<sup>2</sup> .

---

1 : سعيد السيد قنديل ، مرجع سابق ، ص 69 .

2 : عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة ، مرجع سابق ، ص 400 .

إن نظام التشفير هو سلسلة من الهندسة العكسية التي تستخدم مفاتيح، حيث يعتبر المفتاح الخاص محقق هوية رقمي يمكن أن يدمج على وسائط متعددة ، يحل محل الإستعمال البيومترى، ويسمح بالتوقيع على الوثيقة المعلوماتية ، وهو بذلك يعادل القلم الذي يضع به الموقع توقيعه<sup>1</sup> .

إن هذه العناصر تجعل التوقيع على الوثيقة مرتبط بمجموعة من الأرقام المبرمجة ، التي تسمح بالثبوت من شخص الموقع ، حيث ترتبط هذه الأرقام بمعلومات مبرمجة واحدة يمتلكها شخص الموقع ، فالأمر يشبه شق ورقة إلى نصفين ، وحسب الشكل الحاصل نتيجة ذلك ، يمكننا إعادة بناء هذه الورقة مع نصفها الآخر الوحيد ، ومن العسير أن نجد نصفاً آخر له نفس الشكل<sup>2</sup> .

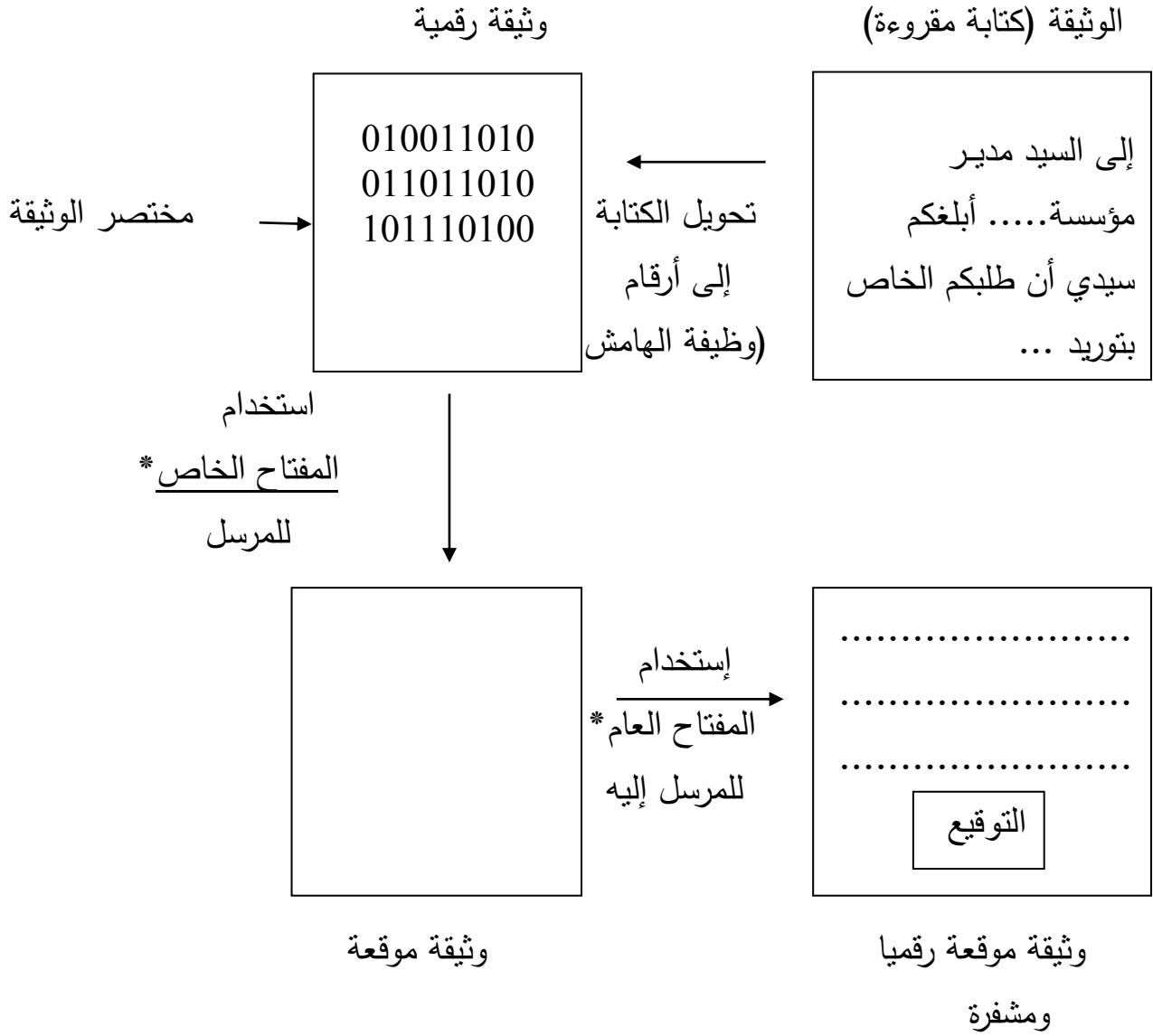
وتتم عملية التوقيع الرقمي على الرسالة (الوثيقة المعلوماتية) عن طريق تحويلها إلى أرقام، ثم استخدام المفتاح الخاص للمرسل والمفتاح العام للمرسل إليه، لينتج في الأخير رسالة موقعة الكترونياً حسب ما يوضحه الشكل الموالي :

---

1 : Julien Esnault, La Signature Electronique, (Mémoire de Dess de droit du Multimédia et de l'informatique), Université de droit , paris, 2002/2003, p 08 .

2 : Pierre Florent , "Signature Electronique " , 2/07/2009,([www.telio.be/blog/2009/07/24/Signature.electronique](http://www.telio.be/blog/2009/07/24/Signature.electronique))

## شكل وضيحي رقم (9): كيفية التوقيع الرقمي



أما عملية استقبال الوثيقة الموقعة رقميا، وقراءتها، وكذا التأكد من صحتها فتتم وفق سلسلة أيضا من الإجراءات حيث يقوم المستقبل عن طريق المفتاح العام بفك التشفير، واستنتاج مختصر الرسالة عن طريق وظيفة الهامش، ثم مقارنة هذا المختصر مع نظيره الناتج من الرسالة المستقبلية، فإن تطابقا كانت الوثيقة صحيحة .

\* تعتمد هذه المفاتيح على الخوارزميات والصيغ الرياضية المعقدة.

وتلعب شهادة التوثيق الإلكتروني دوراً مهماً في عملية التوقيع الرقمي، حيث تؤكد صحة المفتاحين العام والخاص للمستخدمين في ذلك، حسب المعلومة الواردة بهذه الشهادة الخاصة بصاحبها، والمنشئة من جهة محايدة.

ذلك أن منح هذه الشهادة من جهة التوثيق الإلكتروني يتطلب تقديم المعلومات الخاصة بطلب التوقيع والتأكد من صحتها، ليتم منح هذا الشخص مفتاح تشفير خاص يتسم بالسرية، حيث يحتفظ به الموقع، ويتم تثبيت نصفه في جهاز الكمبيوتر الخاص به، والنصف الآخر في بطاقة إلكترونية .

أما جهة التوثيق فتحتفظ بالمفتاح العام ، حيث تقوم بإرساله بالبريد الإلكتروني إلى الأشخاص الذين يتعامل معهم الموقع، وذلك لإستخامه في فك التشفير .

هذه العناصر تجعل التوقيع الرقمي يتمتع بنسبة عالية من الأمان لكن بمراعاة شروط فنية وتقنية<sup>1</sup> هي :

- أ- إختبار الأنظمة المعتمدة لإنشاء التوقيع الرقمي للتأكد من أمنه .
- ب- المحافظة على سرية المفتاح الخاص .
- ج- اعتماد سلطات تصديق تزود المشتركين لديها بشهادات تعترف بهويتهم .

---

1 : عمر حسن المومني ، مرجع سابق ، ص.ص 59 ، 60 .

## الفرع الثالث : شروط التوقيع الإلكتروني

إن أهم خاصية في التوقيع الإلكتروني لكي يؤدي الوظيفة المنوطة به هي خاصية الموثوقية\*، والتي ترتبط بمجموعة من العناصر تتعلق بارتباط التوقيع بصاحبه وتمييزه عن غيره، ومدى سيطرته عليه ، وإمكانية كشف أي تغيير فيه .

### أولا : ارتباط التوقيع بصاحبه

لابد أن يبين التوقيع شخصية صاحبه ، ولما كان الأمر يتعلق ببيئة افتراضية يغيب فيها الحضور المادي للأطراف ، حيث لا نستطيع تحديد الطرف الموقع والتعرف عليه ماديا من خلال حضوره ووضع توقيعه الدال على شخصيته ، فقد أصبح ارتباط هذا التوقيع بصاحبه مسألة تقنية تتعلق بوضع التكنولوجيا اللازمة لتأمين المواقع ومتابعة رقابية من جهات معتمدة لها القدرة على التوثق من شخصية أصحاب التوقيع باستخدام مفاتيح شفرة يتم وضعها على المحررات الإلكترونية<sup>1</sup> ، هذا الذي يجعل التوقيع مميزا وفريدا وقادرا على التعريف بشخص الموقع<sup>2</sup> ، حيث يأتي هذا التوقيع في شكل أرقام أو رموز أو أشكال الكترونية تصدر عن جهات متخصصة موثوق بها، أو باستخدام طرق تكنولوجية مختلفة، ولذلك فإن نوع التكنولوجيا

---

\* : La cour de cassation, chambre civile, 30 septembre 2010 .

1: خالد مصطفى فهمي، النظام القانوني للتوقيع الإلكتروني في ضوء التشريعات العربية والاتفاقيات الدولية. دار الجامعة الجديدة، الإسكندرية، 2007، ص 52 .

2: يوسف أحمد النوافلة ، مرجع سابق ، ص 86 .

المستخدمة في إنشاء التوقيع الإلكتروني يؤثر على درجة الموثوقية التي يتمتع بها التوقيع الإلكتروني<sup>1</sup> .

ولذلك تعتمد جهات التوثيق كما ذكرنا آنفا على تقنية التشفير المعتمدة على مفاتيح مفتاح عام ومفتاح خاص يتسم بالسرية، بحيث يحتفظ به صاحبه ولا يمكن الوصول إليه، أما المفتاح العام فهو متاح لمن يريد التعامل مع هذا الشخص للتأكد من صحة توقيعه، وتنفيذ هذه التقنية بطريقة مأمونة يجعل من المستحيل عمليا اشتقاق المفتاح الخاص انطلاقا من معرفة المفتاح العام<sup>2</sup> .

### ثانيا : سيطرة الموقع على التوقيع

تتحقق سيطرة الموقع على التوقيع إذا كان بإمكانه السيطرة على الوسيط الإلكتروني المتضمن هذا التوقيع ، وذلك لضمان أن يكون صاحب التوقيع منفردا به سواء عند التوقيع أو استعماله بأي شكل من الأشكال<sup>3</sup> .

ولضمان هذه السيطرة لابد من بقاء منظومة إحداث ذلك التوقيع سرا لا يطلع عليها أحد ، حتى لا يساء استعماله من قبل الغير سيما وأن التوقيع يترتب عليه آثار قانونية في حق الموقع وحق الغير<sup>4</sup> .

---

1 : منير محمد الجنبهي، ممدوح محمد الجنبهي ، مرجع سابق ، ص 141 .

2 : نفس المرجع ، ص 141 .

3 : بيومي حجازي ، التوقيع الإلكتروني في النظم القانونية المقارنة ، مرجع سابق ، ص 444 .

4 : نفس المرجع ، ص . ص 444 ، 445 .

### ثالثاً : سلامة الوثيقة الموقعة من التغيير

للتأكد من سلامة محتوى الوثيقة من أي تعديل أو تغيير قد يطرأ عليها فإن شهادات التوثيق ضرورية لذلك ، حيث تؤكد أن التوقيع الرقمي توقيع صحيح ينسب إلى من أصدره ، ويستوفي الشروط والضوابط المطلوبة فيه باعتباره دليل إثبات يعول عليه<sup>1</sup> ، كما تؤكد صحة البيانات الموقع عليها وصدورها من موقعها، وعدم التلاعب بها، فتصبح بذلك بيانات موثقة لا يمكن إنكارها<sup>2</sup> .

إن التأكد من سلامة المحتوى يضمن الثقة خاصة إذا لم يكن هناك علاقات أو تعاملات سابقة بين الأطراف مع ما تحمله التكنولوجيا الحديثة والإنترنت من مخاطر، ولتوفير هذه الثقة لابد من وجود بيئة إلكترونية آمنة<sup>3</sup> .

وقد ذكرنا سابقاً أن من التقنيات المستخدمة في ذلك تقنية التشفير بزوج المفاتيح العام والخاص، إذ يقوم المرسل بتشفير الرسالة بالمفتاح العام، ثم يتم اختصار الرسالة إلى خانات رقمية لها قيمة معينة وفريدة لكل رسالة، بعد ذلك يشفر المرسل رسالته بالمفتاح الخاص، مما ينشئ توقيعاً رقمياً مميزاً، ومن ثم ترسل الرسالة للمستقبل الذي يقوم بدوره بعملية معاكسة، حيث إن استعمال المفتاح العام للمرسل من طرف المستقبل لفك شفرة التوقيع الرقمي يضمن أن

---

1 : ابراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية. مجلس النشر العلمي، جامعة الكويت، 2003، ص 183.

2 : الصالحين محمد العيش ، مرجع سابق ، ص 194 .

3 : خالد مصطفى فهمي، مرجع سابق ، ص 55 .

هذه الرسالة قد أنشأت من قبل حامل المفتاح السري المحاكي للمفتاح العام للمرسل ، وأن أي تغيير في محتوى الرسالة سوف يؤدي إلى عدم فك الشفرة الأمر الذي يضمن سلامة الرسالة<sup>1</sup> .

### **المطلب الثالث : حفظ الوثيقة المعلوماتية**

إن شرط الحفظ هو شرط يرتبط بتحقيق السلامة في محتوى الوثيقة المعلوماتية وثباتها، ولذلك فإنه يرتبط بجوانب تقنية في تأمين الوثائق ضد التغيير والتحريف ، عن طريق وسائل الحفظ كالسجل الإلكتروني، وشهادات التوثيق، وتوفير الشروط التقنية اللازمة المنصوص عليها قانونا لحفظها .

### **الفرع الأول : وسائل حفظ الوثيقة المعلوماتية**

نظم قانون الأونسترال للتجارة الإلكترونية - باعتباره قانونا نموذجيا - مجموعة من الوسائل لحفظ الوثيقة المعلوماتية من خلال ضوابط تقنية مهمة أشار إليها في نصوصه .

### **أولا : السجل الإلكتروني**

يعتبر السجل الإلكتروني من الوسائل التي تؤدي وظيفة حفظ الوثيقة المعلوماتية ، ولذلك اشترط قانون الأونسترال توافر سجل الكتروني يتضمن مجموعة من البيانات الخاصة بالأطراف، تاريخ ومكان إرسال واستلام الرسائل الإلكترونية، وهو ما نصت المادة 1/10: "عندما يقضي القانون بالإحتفاظ بمستندات أو سجلات أو معلومات بعينها ، يتحقق الوفاء بهذا المقتضى إذا تم الإحتفاظ برسائل البيانات ، شريطة مراعاة الشروط التالية :

---

1 : عمر حسن المومني ، مرجع سابق ، ص 58 .



(أ) تيسير الإطلاع على المعلومات الواردة فيها على نحو يتيح استخدامها في الرجوع إليها لاحقاً .

(ب) الإحتفاظ برسالة البيانات بالشكل الذي أنشأت أو أرسلت أو أستلمت به أو بشكل يمكن إثبات أنه يمثل بدقة المعلومات التي أنشأت أو أرسلت أو أستلمت.

(ج) الإحتفاظ بالمعلومات إن وجدت التي تمكن من استبانة منشأ رسالة البيانات وجهة وصولها وتاريخ ووقت إرسالها واستلامها " .

إن هذه الفقرة وهي تشير إلى شروط الحفظ تعيد الشروط المحددة بموجب المادة 06 لكي تلبى رسالة البيانات القاعدة التي تقضي بتقديمها " كتابة "1، وتتناول الفقرة (ج) جميع المعلومات الواجب تخزينها من منشأ الرسالة ، وجهة إرسالها، وتاريخ إرسالها وإستلامها .

إن السجل الإلكتروني يعتبر وسيلة مهمة للإحتفاظ بالوثيقة المعلوماتية، من حيث أنه يمكن من الإطلاع على المعلومات كلما دعت الحاجة إلى ذلك، كما يحافظ على شكل الوثيقة الذي أنشأت أو أرسلت أو استلمت به. ويمكن من تخزين المعلومات المتعلقة بمصدرها وجهة وتاريخ إرسالها .

### ثانياً : شهادات التوثيق الإلكتروني

إن شهادة التوثيق الإلكتروني هي من وسائل حفظ الوثيقة المعلوماتية والتوقيع الإلكتروني، بالإضافة إلى أنها وسيلة للتحقق من هوية أطراف المعاملة الإلكترونية ، وهي تعتبر وسيلة

---

1: عمر حسن المومني ، مرجع سابق ، ص 58 .

حفظ لأنها تثبت صحة التوقيع الإلكتروني ، كما تثبت صحة رسالة البيانات المذيلة به، مما يضمن عدم وجود تغيير، أو تحريف أو تلاعب بها .

كما تضمن شهادة التوثيق عدم إنكار أي من طرفي المعاملة الإلكترونية توقيعه ، إذ يتم التوقيع بالمفتاح الخاص ، وعدم إدعائه أن مضمون المحرر قد تم تعديله أو تغييره <sup>1</sup> .

ولما كانت شهادة التوثيق تؤدي هذا الدور، وجب على جهات التوثيق أن تضمن استمرار القيام بدورها هذا، ولذلك تتولى جهات التوثيق الإلكتروني إنشاء أرشيف الكتروني متضمنا التوقيعات الإلكترونية، والشهادات الصادرة عنها، حيث يتم حفظ البيانات المتعلقة بالشهادات، وحفظ المعاملات الإلكترونية، وكل وثيقة حررت في ذلك <sup>2</sup> .

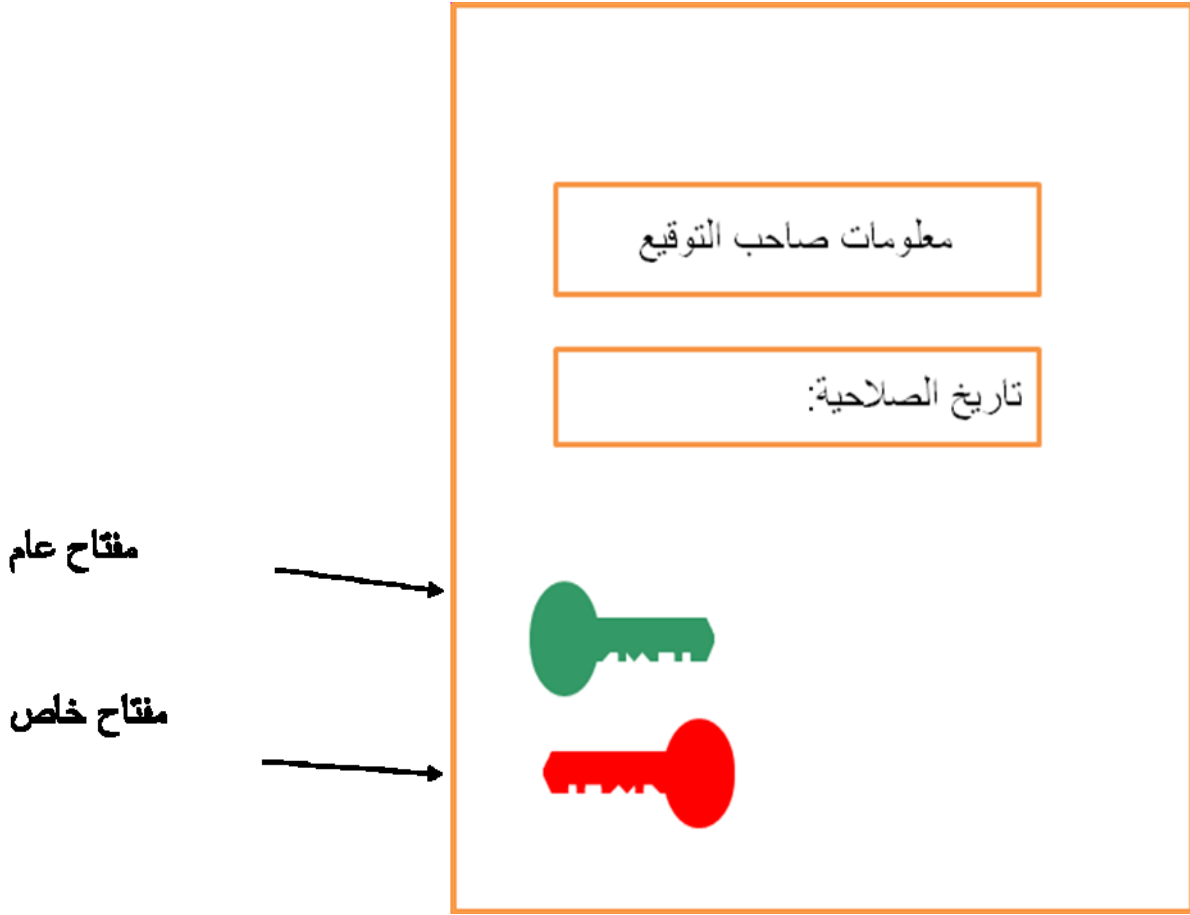
وتتضمن شهادة التوثيق الإلكتروني معلومات عن صاحبها، تاريخ صلاحيتها، تاريخ نشأتها، المفتاح العام لصاحب الشهادة، ويوضح الشكل الموالي نموذج لهذه الشهادة.

---

1 : إيمان مأمون أحمد سليمان ، مرجع سابق ، ص 328 .

2 : مولود قارة ، " التوثيق الإلكتروني "، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية حول بيئة المعلومات الآمنة، الرياض ، 06-07 أبريل 2010 ، ص 10 .

## شكل توضيحي رقم (10) : نموذج شهادة توثيق إلكتروني



### الفرع الثاني : شروط حفظ الوثيقة المعلوماتية

لا يمكن للوثيقة المعلوماتية أن تؤدي دورها كأداة إثبات إلا إذا تم حفظها وفق الشروط المنصوص عليها قانونا، ولذلك فإن غياب أي شرط من هذه الشروط سيجرد هذه الوثيقة من قيمتها القانونية، وهو ما جعل الجهود الدولية والوطنية تتجه نحو تنظيم شروط الحفظ في مجموعة من النصوص القانونية ، وهو ما احتواه قانون الأونسترال النموذجي للتجارة الإلكترونية لتنظيم شروط حفظها .

## أولاً : شروط حفظ الوثيقة المعلوماتية في قانون الأونسترال

نص قانون الأونسترال النموذجي للتجارة الإلكترونية في المادة 10 على مجموعة من

الشروط الواجب توافرها عند حفظ الوثيقة المعلوماتية وهي :

1. تيسير الإطلاع على المعلومات الواردة برسالة البيانات بشكل يتيح استخدامها والرجوع إليها

لاحقاً.

2. الحفاظ على الشكل الذي أنشأت أو أرسلت أو أستلمت به بشكل يمكن من إثبات أن

المعلومات الواردة بها صحيحة .

3. الإحتفاظ بالمعلومات التي تبين منشأ رسالة البيانات وجهة وصولها وتاريخ ووقت إرسالها

واستلامها .

ومن أجل ذلك نظم قانون التوقيع الإلكتروني النموذجي الأحكام المتعلقة بمزودي خدمات

التصديق ، ومحتوى شهادة التصديق الإلكتروني ، حيث بمقتضى المادة 09 منه أوجب على

مقدم خدمة التصديق الإلكتروني توفير وسائل يمكن الوصول إليها بيسر ، وتمكن من التأكد

من العناصر التالية في الشهادة :

1- هوية مقدم خدمات التصديق .

2- سيطرة الموقع على بيانات إنشاء التوقيع في وقت صدور الشهادة .

3- صحة بيانات إنشاء التوقيع في الوقت الذي صدرت فيه الشهادة .

4- عدم تعرض بيانات إنشاء التوقيع لأي تغيير .

## ثانيا : شروط حفظ الوثيقة المعلوماتية في التشريعات الوطنية

نص المشرع الأردني في المادة 08 من قانون المعاملات الإلكترونية على مجموعة من

الشروط الواجب توافرها في السجل الإلكتروني لحفظ الوثيقة المعلوماتية وهي :

" 1/ أن تكون المعلومات الواردة في ذلك السجل قابلة للإحتفاظ بها وتخزينها بحيث يمكن في أي وقت الرجوع إليها .

2/ إمكانية الإحتفاظ بالسجل الإلكتروني بالشكل الذي يتم به إنشاؤه أو إرساله أو تسلمه أو بأي شكل يسهل به إثبات دقة المعلومات التي وردت فيه عند إنشائه أو إرساله أو تسلمه .

3/ دلالة المعلومات الواردة في السجل على من أنشأه أو تسلمه وتاريخ ووقت إرساله وتسلمه".

كما نص المشرع الإماراتي في المادة 08 من قانون المعاملات والتجارة الإلكترونية على

مجموعة من الضوابط التي يجب مراعاتها في السجل الإلكتروني لحفظ الوثيقة المعلوماتية وهي: "أ- حفظ السجل الإلكتروني بالشكل الذي أنشئ أو أرسل أو استلم به أو بشكل يمكن

من إثبات أنه يمثل بدقة المعلومات التي أنشأت أو أرسلت أو استلمت في الأصل .

ب- بقاء المعلومات محفوظة على نحو يتيح استخدامها والرجوع إليها لاحقا .

ج- حفظ المعلومات إن وجدت التي تمكن من استبانة منشأ الرسالة الإلكترونية وجهة وصولها

وتاريخ ووقت إرسالها واستلامها" .

إن حفظ الوثيقة المعلوماتية يحقق مجموعة من الأغراض<sup>1</sup> :

1- إمكانية الإطلاع على محتوى الوثيقة ما دامت صالحة ولم يتم إلغاؤها أو العبث بها .

2- حفظ الوثيقة في الشكل النهائي يضمن سلامة محتواها .

3- حفظ المعلومات التي وردت بالوثيقة والتي تخص المصدر والجهة وتاريخ ومكان استلامها

وكذلك إرسالها .

---

1 : خالد عبد الفتاح محمد ، مرجع سابق ، ص 230 .

## الباب الثاني

### الصيغ التشريعية في تجريم تزوير الوثيقة الرسمية الإدارية المعلوماتية

لقد تبين الاختلاف في تحديد مفهوم الوثيقة المعلوماتية من حيث توسيع مفهوم الوثيقة التقليدية لتشمل هذه الطبيعة المستجدة، أو من خلال استحداث مفهوم خاص بالوثيقة المعلوماتية، مما انعكس على الصيغ التشريعية عند تجريم تزوير هذه الوثيقة، حيث تنوعت بين توسيع مفهوم التزوير في إطار نصوص قانون العقوبات، وبين تحديد مفهوم تزوير الوثيقة المعلوماتية بنصوص خاصة، وبالتالي فإن تحديد أركان هذه الجريمة وعقوباتها سيرتبط بصيغة التجريم .

## الفصل الأول

### تحديد مفهوم تزوير الوثيقة الرسمية الإدارية المعلوماتية

هناك عدة صيغ تشريعية لتحديد مفهوم تزوير الوثيقة المعلوماتية بصفة عامة - ومن أصنافها الوثيقة الرسمية الإداري المعلوماتية-، ومن هذه الصيغ نجد صيغة نصوص قانون العقوبات الفرنسي كنموذج لتوسيع مفهوم التزوير في إطار نصوص قانون العقوبات، أما صيغ بعض القوانين العربية - القانون المصري والقانون الإماراتي نموذجا - فتعتمد على تحديد مفهوم تزوير الوثيقة المعلوماتية في قوانين مستقلة ، كما تحدد بعض أشكال تزوير هذه الوثيقة منها جريمة تزوير التوقيع الإلكتروني ، وجريمة تزوير البطاقة الإلكترونية .

### المبحث الأول : توسيع مفهوم التزوير في إطار نصوص قانون العقوبات

لقد اعتمدت بعض الدول نهجا معينا في تجريم التزوير في الوثيقة المعلوماتية بصفة عامة، حيث تم توسيع نصوص قانون العقوبات ليشمل هذا النوع من التزوير ، ومن هذه الدول نجد فرنسا ، وذلك من خلال تعديل نصوص قانون العقوبات المتعلقة بالتزوير . لكن الإشكال يبقى قائما بالنسبة للدول التي لم تعدل النصوص المتعلقة بالتزوير ، من حيث مدى إمكانية تطبيق هذه النصوص على هذا النوع المستجد من التزوير .



## المطلب الأول : مفهوم التزوير في قانون العقوبات الفرنسي

توسع المشرع الجنائي الفرنسي في تجريم التزوير ليمتد إلى الوثيقة المعلوماتية في القسم الأول ضمن الكتاب الرابع من قانون العقوبات تحت عنوان " الاعتداءات ضد الثقة العامة " في المادة 1/441 المعدلة في 14 ماي 1993 .

### الفرع الأول : توسيع مفهوم الوثيقة محل التزوير

تنص المادة 1/441 من قانون العقوبات الفرنسي على :

"Constitue un faux toute altération frauduleuse de la vérité, de nature a causer un préjudice et accomplie par quelque moyen que ce soit , dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques " .

يستنتج من النص السابق أن الوثيقة تشمل إلى جانب الشكل التقليدي لها - وثيقة ورقية - كل وسيط آخر للتعبير عن فكرة أو معاني معينة لكن يجب أن يكون لها قيمة ثبوتية بمعنى أنها تصلح قانونا لإستخدامها كدليل إثبات حق أو واقعة لها آثار قانونية .

ولما كان التزوير هو تغيير للحقيقة في الوثيقة غشا، فقد أصبح للوثيقة مفهوم أوسع وهو التعبير المستخدم في النص السابق "dans un écrit" و "support d'expression de la pensée" ، وبالتالي فقد شمل هذا المعنى كل الأشكال الحديثة التي نتجت عن استخدامات المعلوماتية والتي تحمل هذه الأفكار، ومن بينها الدعامات المادية مثل الأقراص الإلكترونية، أو البطاقات

أو الشرائح المغناطيسية وغيرها ، ولا يكون التزوير معتبرا إلا إذا كانت الوثيقة لها قيمة قانونية حيث أنها تثبت حقا أو مركزا قانونية ، أو يمكن استخدامها كدليل لإثبات واقعة قانونية كما ذكرنا سالفًا.

إلا أن المشرع الفرنسي كان قد نظم الجرائم المعلوماتية بقانون خاص رقم 19/88 المؤرخ في 5 يناير 1988\*، حيث نص في المادة 5/462 على :

"Quiconque aura procédé à la falsification de documents informatisés , quelle que soit leur forme, de nature a causer un préjudice a autrui , sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20.000 francs a 2.000.000 Francs " .

إن هذا النص يجرم تزوير الوثيقة المعالجة آليا مهما كان شكلها إذا سبب ذلك ضررا للغير .

وبالتالي فقد كان منهج المشرع الجنائي الفرنسي من خلال هذا القانون هو إفراد نص مستقل في قانون العقوبات لمواجهة تزوير الوثائق المعلوماتية ، وقد إعتبر الفقه الفرنسي هذه المواد مكملة للمادة 150 الخاصة بتزوير المحررات<sup>1</sup> ، وبذلك اعتبرت جريمة تزوير الوثائق المعلوماتية جريمة مستقلة عن جريمة التزوير في المحررات<sup>2</sup> .

---

\*: يعرف هذا القانون ب " Loi Godfrain " نسبة إلى النائب الذي تقدم به (Jacques Godfrain) .

1: نائلة عادل محمد فريد قورة، مرجع سابق ، ص 587 .

2: أشرف توفيق شمس الدين، مرجع سابق ، ص 108 .

لكن بعد تعديل قانون العقوبات الفرنسي لم يأخذ المشرع بالمادتين 5/462 و 6/462 المتعلقة بتزوير الوثيقة المعالجة آليا واستعمال الوثيقة المزورة باعتبار أن المادة 1/441 قد وسعت من مفهوم الوثيقة ، كما أن هذين المادتين لاقتا اعتراضات في مجلس الشيوخ عند مناقشة هذا القانون ، لما يترتب عليهما من مساواة بين المعطيات المعلوماتية بصفة عامة وبين المحررات من حيث القيمة القانونية<sup>1</sup> . لذلك غير المشرع الجنائي الفرنسي خطته بشأن تجريم تزوير الوثيقة المعلوماتية باعتبار أن المصلحة المحمية في جرائم المساس بالأنظمة المعلوماتية أو المعطيات والبيانات مختلفة عن تلك المتعلقة بجرائم التزوير في المحررات التي تتعلق بحماية الثقة العامة فيها . وبذلك اختفت جريمة تزوير المستندات المعالجة آليا واستعمالها من الباب الثالث (المتعلق بالجرائم المعلوماتية) ، وأضافها إلى جريمة التزوير العادية بعد تطويع نصوصها بما يتلاءم وتلك المستندات<sup>2</sup> .

كما لم يحدد المشرع الفرنسي في المادة 441 طرق معينة لإرتكاب التزوير\* ، وهذا يعني استخدام شتى الطرق والأساليب المعلوماتية أيا كانت لإرتكاب الفعل الإجرامي المتمثل في تزوير المستندات المعلوماتية<sup>3</sup> .

---

1: نائلة عادل محمد فريد قورة ، مرجع سابق ، ص 588 .

2: علي عبد القادر القهوجي ، مرجع سابق ، ص 41 .

\* : Article 441/1 : <<..... par quelque moyen que ce soit....>>

3: بلال أمين زين الدين ، مرجع سابق ، ص 354 .

وقد كان الفقه الفرنسي متباين في مواقفه قبل صدور قانون 19/88 بين مؤيد ومعارض لإمكانية تطبيق النصوص التقليدية لجريمة التزوير على التلاعب في البيانات والبرامج<sup>1</sup>، حيث اعتبر الإتجاه المعارض أن جريمة التزوير المنصوص عليها في المادة 145 من القانون الجنائي الفرنسي تفترض وجود محرر وهذا يعني وجود كتابة ، بينما المعلومات الإلكترونية لا تعتبر كتابة ، بالإضافة إلى افتراض تمتع المحرر بقيمة ثبوتية ، بينما لا تتمتع الوثائق المعلوماتية بهذه القيمة. ولم يكن هذا الإتجاه يرى امكانية تطبيق النص التقليدي لجريمة التزوير بالنسبة للوثائق المعلوماتية إلا في حالة اخراج هذه الوثائق عن طريق مخرجات الحاسب الآلي في شكل ورقي، إذ كان لهذه الورقة قيمة في الإثبات .

لقد تطور القانون الفرنسي في مجال تجريم التزوير في الوثيقة المعلوماتية باعتباره من أخطر صور الغش في نطاق المعلوماتية بسبب خطورة الدور الذي يقوم به الحاسب الآلي في الوقت الحاضر وفي كل المجالات ، فقد أصبحت تتم من خلاله عمليات هائلة ترتب آثار قانونية خطيرة<sup>2</sup> .

وبذلك حسم المشرع الجنائي الفرنسي الجدل الذي كان قائماً من خلال المادة 1/441 من قانون العقوبات، كما قطع كل خلاف حول مفهوم المحرر الذي أصبح ينصرف إلى الورقة المكتوبة والوثيقة المعلوماتية التي عبر عنها بلفظ أي دعامة أخرى، حيث ينصرف هذا التعبير

---

1: محمد سامي الشوا ، مرجع سابق ، ص 144 .

2: عبد الفتاح بيومي حجازي ، الجريمة في عصر العولمة ، مرجع سابق ، ص 106 .

إلى كافة الأشكال المقررة التي يمكن أن تكون وعاء للتعبير عن فكرة أو يمكن أن ينتج عنها دليل على حق أو واقعة ذات آثار قانونية<sup>1</sup> .

كما حقق المشرع الجنائي الفرنسي من خلال المادة 441 من قانون العقوبات هدفين ، تمثل الهدف الأول في استيعاب هذا النص حالات التزوير التقليدي في المحررات إلى جانب تزوير الوثيقة المعلوماتية ، وذلك بتجريم التزوير على وثيقة معلوماتية مطبوعة على سند أو دعامة مادية كشريط ممغنط أو قرص مدمج وبأي وسيلة ،..... أما الهدف الثاني فهو خروج جريمتي تزوير المستندات المعالجة آليا واستعمالها من بين جرائم الإعتداء على نظم المعالجة الآلية للمعطيات<sup>2</sup> .

### الفرع الثاني : عناصر التزوير في الوثيقة المعلوماتية

يشمل التزوير في الوثيقة المعلوماتية التحريف المادي أو المعنوي ويشمل التحريف المادي خلق وثيقة أو تقليد توقيع ، أما التزوير المعنوي فيشمل ذكر عناصر مخالفة للحقيقة أو غير صحيحة<sup>3</sup> .

كما أن فعل التزوير لا يشكل جرما في حد ذاته إلا إذا أدى إلى ضرر ، أو أنتج آثارا من الناحية القانونية لم تكن لتنتج في غياب هذا الفعل .

---

1 : عبد الفتاح بيومي حجازي ، التجارة الإلكترونية ، مرجع سابق ، ص 165 .

2 : خالد محمد كدفور المهيري، جرائم الكمبيوتر والأنترنت والتجارة الإلكترونية . معهد القانون الدولي ، ط2 ، دبي ، د.ت ، ص . ص 646 ، 647 .

3 : Maitre Anthony Ben, "Définition et sanction pénales du faux", 23/08/2011, (www. Legavox. Fr/blog/maitre – anthony-bem/defir)

ولذلك فإن تزوير دليل يتضمن تعديل كتابة موجودة من أجل تحريف المضمون بحذف معلومات أو إضافة أخرى جديدة ، أما التزوير من خلال خلق دليل محرف فالهدف منه جعل هذا الدليل وسيلة من أجل غايات معينة ، حيث بخلق هذا الدليل تنتج آثار قانونية لمصلحة منشئه<sup>1</sup> .

إن هذا التحريف في الوثيقة المعلوماتية مختلف عنه في الوثيقة الورقية ، حيث لا تظهر هذه التعديلات في مضمون الوثيقة ، في حين تظهر الآثار المادية على الورقة ، وإذا أردنا إخفاء هذا التعديل فسيؤدي ذلك إلى فقدان المعلومات الأصلية ، وبالتالي لابد من محاولة إعادة إنتاجها<sup>2</sup> ، بينما إضافة معلومات في الوثيقة المعلوماتية لا يبق أثرا .

فقد يقوم الجاني بإضافة معلومات لم تكن موجودة في الوثيقة لتغيير مضمونها<sup>3</sup> ، وبالتالي تغيير الحقيقة مما يرتب آثار قانونية معينة ، مثل إضافة أرقام أو كلمات أو حروف إلى البيانات الأصلية كبيانات العملاء لزيادة أرصدهم أو أرقام فاتورة الهاتف أو الكهرباء ، أما حذف المعلومات فيتم بمحو بعض البيانات الكائنة على المستند الأصلي أو طمسها أي إخفائها عن مستخدميها ، كما يمكن جعل واقعة غير صحيحة في صورة واقعة صحيحة أو غير معترف بها في صورة واقعة معترف بها<sup>4</sup> ، كما يمكن اصطناع الوثيقة بأكملها مثل اصطناع بطاقة انتمانية باسم مزور .

---

1 : Fabien Kerbouci, "La preuve Ecrite Electronique et le droit Français", 21/01/2010, ([www.e-juristes.org](http://www.e-juristes.org)), p.26.

2 : Ibid , p . p , 26 , 27 .

3 : بلال أمين زين الدين ، مرجع سابق، ص . ص 355 ، 356 .

4 : نفس المرجع ، ص. ص 355 ، 356 .

ولأن التكنولوجيا قد تفرز وسائل وتقنيات جديدة للتزوير فإن المشرع لم يحصر هذه الطرق، فهي متعلقة بالتقنية التكنولوجية المعلوماتية التي يلجا إليها المجرم المعلوماتي في تزوير الوثائق المعالجة وفقا للنظم المعلوماتية<sup>1</sup> .

كما أن من عناصر التزوير وجود تلك النية الإجرامية بحيث يقوم الجاني بتغيير الحقيقة وهو يعلم بذلك من خلال الإصطناع أو التعديل والتغيير في الوثيقة المعلوماتية، وهذا هو مقتضى القصد الجنائي العام في جريمة التزوير، والذي أشار إليه المشرع الجنائي الفرنسي في المادة 1/441 بعبارة "كل تغيير تدليسي للحقيقة"، بالإضافة إلى القصد الجنائي الخاص والذي يتعلق بنية الإضرار بالغير .

وقد أشارت إلى هذه العناصر المادة 07 من اتفاقية بودابست المتعلقة بالإجرام المعلوماتي بنصها على " يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية وفقا لقانونه الداخلي لتجريم الإدخال أو الإتلاف أو المحو أو الطمس العمدي وبدون حق للبيانات المعلوماتية الذي يتولد عنه بيانات غير صحيحة بقصد أخذها في الحسبان أو استخدامها لأغراض قانونية كما لو كانت صحيحة بصرف النظر عما إذا كانت سهلة القراءة مباشرة وواضحة أم لا . ويمكن لأي طرف أن يشترط في قانونه الداخلي نية الغش أو أي نية إجرامية مشابهة من أجل تقرير المسؤولية الجنائية " .

---

1 : بلال أمين زين الدين ، مرجع سابق ، ص 352 .

## المطلب الثاني: مدى تطبيق نص التزوير التقليدي على تزوير الوثيقة المعلوماتية

إن التشريعات الجنائية في مختلف الدول تجرم فعل التزوير سواء كان في وثيقة عرفية أو رسمية، لكن هذه الجريمة في كل الأحوال تتطلب لقيامها وجود وثيقة لها قيمة ثبوتية، فهي العنصر الأساسي في التزوير والمحل الذي يقع عليه ، ومناطق الحماية وعلة التجريم تلك الثقة المنبعثة منها، خاصة تلك الوثيقة الرسمية الصادرة عن الجهات الإدارية .

ولذلك يثور الإشكال في مدى إنطباق نص التزوير التقليدي على التزوير في الوثيقة المعلوماتية، مما يؤدي بالضرورة إلى مناقشة مدى امكانية انطباق معنى الوثيقة على المعلومات المعالجة آليا والتي تحمل معنى يثبت حق أو مركز قانوني معين ، وهي المسألة التي تجاذبها اتجاهان انطلاقا من النصوص الجنائية القائمة، ومبادئ التفسير .

### الفرع الأول : عدم تطبيق نص التزوير التقليدي على تزوير الوثيقة المعلوماتية

يرى جانب من الفقه أن تطبيق النص الجنائي الخاص بجريمة التزوير على التلاعب في البيانات يصطدم بعقبة منيعة ألا وهي وجود محرر<sup>1</sup> .

ولذلك يرى هذا الإتجاه عدم انطباق النص الجنائي الخاص بالتزوير في الوثيقة الرسمية أو العرفية الورقية على الوثيقة ذات الطبيعة المعلوماتية لأنها ليست وثيقة بالمعنى القانوني .  
إن الوثيقة ترتبط بالكتابة ، ومما يتفق مع أصول التفسير في هذه الحالة أن يفترق المدلول الإصطلاحي للكتابة عن المدلول اللغوي، ولذلك يرى د.أشرف توفيق شمس الدين في مؤلفه

1 : محمد سامي الشوا ، مرجع سابق ، ص 141 .



الحماية الجنائية للمستند الإلكتروني أنه لا يجوز تفسير النصوص المتعلقة بالوثيقة والكتابة لتشمل الكتابة التي تتم بوسيلة الكترونية، والعلة في ذلك أنها ما زالت عرضة للتطور التقني مما قد يعرض المعاملات لعدم الاستقرار، كما أن اقتران الوثيقة بالتوقيع يوجب للأخذ بفكرة التوقيع الإلكتروني وجود تشريع دقيق يبين نظم حمايته وتأمينه ليؤدي دوره في الإثبات ، ولذلك لا يجوز التوسع في تفسير هذه النصوص لأن هذا التوسع لا يلتقي مع المعنى الإصطلاحي للكتابة<sup>1</sup> .

كما ترى الدكتورة نائلة عادل محمد فريد قوره عدم امكانية تطبيق النصوص المتعلقة بالتزوير على تغيير الحقيقة في المعلومات المبرمجة لأنها لا تعتبر محرر من حيث أنه لا يمكن مشاهدة المعلومات المخزنة على وسائط التخزين الخاصة بها عن طريق النظر، وبالتالي فهي ليست مقروءة ولا يمكن للمعنى الذي تحمله أن ينتقل عن طريق العين المجردة<sup>2</sup> .

ويرى د. عبد الفتاح بيومي حجازي أن هناك فرق بين تغيير المعلومات المخزنة في ذاكرة الجهاز أو المدخلة في البرامج ، وإثبات هذه المعلومات المحرفة على الورق عن طريق مخرجات النظام وبالتالي يصبح لها وصف المحرر لتشملها الحماية القانونية بمقتضى نصوص التزوير<sup>3</sup> .

---

1 : محمد سامي الشوا ، مرجع سابق ، ص . ص 29 ، 30 .

2 : نائلة عادل محمد فريد قوره ، مرجع سابق ، ص . ص 584 ، 585 .

3 : عبد الفتاح بيومي حجازي ، الجريمة في عصر العولمة، مرجع سابق ، ص . 102 .

إن الإتجاه السابق يربط قيام جريمة التزوير بوجود الوثيقة الورقية، حتى في حال تغيير الحقيقة في الوثيقة المعلوماتية من خلال تغيير المعلومات المخزنة داخل الجهاز أو الموجودة على دعامة الكترونية حيث لا بد لها من وجود ورقي ، وبالتالي فإن هذا الإتجاه لم يضيف جديدا طالما بقي التلازم بين الوثيقة والطبيعة الورقية .

ولذلك فإنه في إطار نص التزوير التقليدي لا يمكن مد هذا النص ليشمل التزوير في الوثيقة ذات الطبيعة المعلوماتية لسببين :

- 1- جمود النص الجنائي مما يصعب معه التأويل، لعدم وجود أي إشارة إلى الأشكال المستحدثة من الوثائق، طالما هناك ربط بين الوثيقة والكتابة التي لها مدلول ورقي غالبا .
- 2- التلازم بين قيام جريمة التزوير وشرط وجود وثيقة لها قيمة ثبوتية يقتضي الرجوع إلى قوانين الإثبات وكيفية تنظيمها للدليل المكتوب ، فإن كانت هذه النصوص جامدة بحيث تربط الكتابة بالشكل الورقي ، أو لا يمكن التوسع في تفسيرها فإن هذا سيخلق الباب أمام تفسير النص الجنائي، وبالتالي لا يمكن تطبيقه على الوثيقة ذات الطبيعة المعلوماتية باعتبار أن مفهوم الكتابة لا يشملها .

### الفرع الثاني : تطبيق نص التزوير التقليدي على تزوير المعلوماتية

يرى جانب من الفقه امكانية تطبيق نص التزوير القائم على فعل تزوير الوثيقة المعلوماتية، وهو ما حصل في فرنسا قبل صدور قانون الغش المعلوماتي السابق الذكر ، حيث

أيد البعض فكرة تطبيق النص التقليدي لجريمة التزوير على كل تلاعب أو تغيير في الوثيقة المعلوماتية معتمدا في ذلك على التطبيق والتفسير القضائي ، ونصوص قانون الإثبات .

**1- التفسير القضائي الموسع لمعنى الوثيقة :** أصبح تفسير القضاء للوثيقة تفسيرا موسعا جدا كما هو الحال لدى القضاء الفرنسي ، حيث يشمل كل وثيقة لها قيمة تصلح في الإثبات مهما كانت دعائها ، وبما أن الواقع أصبح يفرض التعامل بالوثيقة المعلوماتية ، فإن هذه الوثيقة قد تكون لها قيمة تصلح في الإثبات، إذا تم المحافظة على محتواها، وتحديد منشئها<sup>1</sup> .

**2- تمتع الوثيقة المعلوماتية بقيمة ثبوتية بمقتضى قوانين الإثبات:** لقد أصبحت الوثيقة المعلوماتية - خاصة تلك الصادرة عن الجهات الإدارية العامة - لها قيمة قانونية في الإثبات، ولما كانت العلاقة قائمة بين جريمة التزوير وتمتع الوثيقة بهذه القيمة، أمكن مد النص الجنائي التقليدي ليشمل تزوير الوثيقة المعلوماتية .

## **المبحث الثاني : تحديد مفهوم تزوير الوثيقة الرسمية الإدارية المعلوماتية**

### **بنصوص خاصة**

لقد ساهمت الصعوبات التي واجهت تطبيق النص المتعلق بتجريم تزوير الوثيقة الورقية ليشمل الوثيقة ذات الطبيعة المعلوماتية في ظهور اتجاه تشريعي يجرم تزوير هذه الوثيقة بنصوص خاصة نظرا لخصائص هذه الأخيرة التي تختلف عن الأولى، وأشكال التزوير الذي

---

1 : Cour de cassation, chambre commerciale , 2 décembre 1997 .

قد يقع عليها، مما جعل مفهوم تزوير الواقع على الوثيقة المعلوماتية ومن أصنافها الوثيقة الرسمية الإدارية - يتحدد بحسب النص الجنائي الوارد في قانون مستقل .

**المطلب الأول : الصيغ التشريعية العربية في تجريم تزوير الوثيقة الرسمية الإدارية**

### **المعلوماتية**

من بين الإتجاهات التشريعية التي جرت تزوير الوثيقة المعلوماتية بنصوص خاصة نجد بعض التشريعات العربية منها التشريع المصري، التشريع الإماراتي، حيث سنعرض كل تجربة على حدى، ثم نحاول استخلاص مفهوم تزوير الوثيقة المعلوماتية من خلال هذه النصوص وتحديد خصائصها .

**الفرع الأول : صيغة التجريم في التشريع المصري من خلال قانون التوقيع الإلكتروني والأحوال المدنية**

جرم المشرع المصري في قانون التوقيع الإلكتروني تزوير الوثيقة المعلوماتية بأشكالها المختلفة ، كما جرم في قانون الأحوال المدنية تزوير الحاصل في المعلومات التي تتضمنها سجلات الأحوال المدنية ذات الطبيعة المعلوماتية وهي سجلات رسمية تمسكها جهات إدارية عامة .

**أولا : قانون التوقيع الإلكتروني**

نصت المادة 23 من قانون التوقيع الإلكتروني على : " 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 باحدى هاتين العقوبتين كل من :

- أتلف أو عيب توقيعاً أو وسيطاً أو محرراً الكترونياً ، أو زور شيئاً من ذلك بطريق

الإصطناع أو التعديل أو التحوير أو بأي طريق آخر .

- استعمل توقيعاً أو وسيطاً أو محرراً الكترونياً معيباً أو مزوراً مع علمه بذلك " .

لقد جرم المشرع المصري التزوير في توقيع أو وسيط أو محرر الكتروني عن طريق القيام

باصطناعه من خلال خلق توقيع أو وسيط أو محرر غير موجود ، أو عن طريق التعديل في

معلومات موجودة أو بأي طريق آخر قد يؤدي إلى تغيير الحقيقة .

ولما كانت علة التجريم تتعلق بالثقة العامة في الوثائق عند تداولها بين الأفراد ، حيث

تنتج هذه الثقة مما تتمتع به هذه الوثائق من قيمة قانونية عند الإثبات ، فإن التجريم يرتبط

بمدى تمتع هذه الوثائق بتلك القيمة، ولذلك أضفى قانون التوقيع الإلكتروني على هذا التوقيع

حجية في الإثبات في نطاق المعاملات الإلكترونية ومن بينها المعاملات الإدارية، وهي ذات

الحجية التي يتمتع بها التوقيع المرتبط بالوثيقة الورقية من خلال أحكام قانون الإثبات\* ، ولكن

بتوافر شروط قانونية وضوابط فنية وتقنية بينها قانون التوقيع الإلكتروني ولائحته التنفيذية

2005/109 الصادرة بقرار من وزير الإتصالات وتكنولوجيا المعلومات .

---

\*: يعترف المشرع المصري للتوقيع الإلكتروني والكتابة الإلكترونية بحجية كاملة في الإثبات في جميع المعاملات المدنية والتجارية والإدارية من خلال المادتين 14 و 15 من قانون التوقيع الإلكتروني .

فقد نصت المادة 18 من قانون التوقيع الإلكتروني على ضرورة توافر الشروط التالية :

أ- إرتباط التوقيع الإلكتروني بالموقع دون غيره .

ب- سيطرة الموقع دون غيره على الوسيط الإلكتروني .

ج- امكانية كشف أي تعديل أو تبديل في بيانات المحرر الإلكتروني أو التوقيع الإلكتروني.

أما المادة 08 من اللائحة التنفيذية فقد بينت الضوابط الفنية والتقنية التالية :

" أ- امكانية تحديد وقت وتاريخ إنشاء الوثيقة الإلكترونية الرسمية أو العرفية من الناحية الفنية،

من خلال نظام حفظ الكتروني مستقل .

ب- تحديد منشئ الوثيقة الإلكترونية الرسمية أو العرفية ، ودرجة سيطرته على الوسائط

المستخدمة في إنشائها .

ج- إذا كانت الوثيقة الإلكترونية أنشأت باستخدام نظام الأتمتة فلا بد من التحقق من وقت

وتاريخ إنشائها".

رغم أن المشرع المصري جرم تزوير التوقيع أو المحرر الإلكتروني في قانون التوقيع

الإلكتروني ، بعد أن ضمن لهذا التوقيع أو المحرر القيمة القانونية اللازمة في الإثبات خاصة

إذا ارتبط بالمعاملات الرسمية الإدارية من خلال الضوابط الفنية والتقنية المشار إليها في نفس

القانون ، إلا أنه لم يوفق في صياغة النص المجرم لهذا الفعل حيث لم يبين أركان التزوير

بدقة، بل اكتفى بالإشارة إلى بعض صور السلوك المادي مثل التعديل والإصطناع .

كما أنه جمع بين جريمتي الإلتلاف والتزوير رغم اختلافهما من حيث نتيجة السلوك المادي، وذلك ظاهر من خلال العبارات المستخدمة مثل أُلّف، عيب توقيعها أو وسيطا أو محررا الكترونيا. كما خلا النص تماما من الإشارة إلى عنصر الضرر في جريمة التزوير .

### ثانيا : قانون الأحوال المدنية

جرم المشرع المصري في قانون الأحوال المدنية تزوير الوثائق الرسمية الإدارية ذات الطبيعة المعلوماتية المخزنة بالكمبيوترات الموجودة بمراكز الأحوال المدنية من خلال المادة 72 التي تنص على: " في تطبيق أحكام هذا القانون وقانون العقوبات تعتبر البيانات المسجلة بالحاسبات الآلية وملحقاتها بمراكز معلومات الأحوال المدنية ومحطات الإصدار الخاصة بها المستخدمة في إصدار الوثائق وبطاقات تحقيق الشخصية بيانات واردة في محررات رسمية. فإذا وقع تزوير في المحررات السابقة أو غيرها من المحررات الرسمية تكون العقوبة الأشغال الشاقة المؤقتة أو السجن لمدة لا تقل عن خمس سنوات "

إن هذا النص خاص بالتزوير الواقع على المعلومات التي تتضمنها الكمبيوترات الخاصة بمصلحة الأحوال المدنية، لكن مع ذلك يسري هذا النص على التزوير الذي يرتكب عن طريق شبكة الإنترنت في هذه المعلومات وتلك الوثائق، إذا كان استخدامها هو الوسيلة للوصول إلى الحاسبات الآلية الخاصة بمصلحة الأحوال المدنية<sup>1</sup> .

---

1 : أشرف توفيق شمس الدين ، مرجع سابق ، ص 108 .

رغم ذلك فإن هذا النص خاص بوثائق الأحوال المدنية ولا يسري على غيرها من الجرائم، وبالتالي تبقى هذه النصوص المتفرقة قاصرة عن استيعاب جريمة التزوير في وثيقة معلوماتية من حيث موضع النص الخاص بها، أو من حيث تحديد أركانها، خاصة في ظل عدم تعديل قانون العقوبات فيما يتعلق بالتزوير ليشمل تزوير الوثيقة المعلوماتية .

## الفرع الثاني : صيغة التجريم في التشريع الإماراتي من خلال القانون الاتحادي لجرائم تقنية المعلومات

جرم المشرع الإماراتي في القانون الاتحادي الخاص بجرائم تقنية المعلومات<sup>1</sup> بعض الأفعال التي تتصل بالأنظمة المعلوماتية أو باستخدام جهاز الكمبيوتر، ومن الأفعال المتعلقة باستخدام هذا الجهاز جرم المشرع الإماراتي في المادة 04 فعل التزوير في مستند من مستندات الحكومة الاتحادية أو المحلية أو المؤسسات العامة الاتحادية والمحلية المعترف بها قانوناً في نظام معلوماتي، حيث شدد العقوبة في هذه الحالة وهي السجن المؤقت فيما تكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين إذا وقع التزوير في مستند غير صادر عن هذه الجهات. وهو ما يوافق اتجاه اتفاقية بودابست المتعلقة بالإجرام المعلوماتية التي تنص على اتخاذ التدابير التشريعية اللازمة لتجريم عدة أفعال ومن بينها التزوير المتعمد باستخدام الكمبيوتر.

---

1 : قانون اتحادي رقم 2006/02 المؤرخ في 30 يناير 2006 المتعلق بمكافحة جرائم تقنية المعلومات، الجريدة الرسمية، عدد 442 ، (31 يناير 2006) ، ص 55 .



وقد نصت المادة 1/04 السابقة الذكر على : "يعاقب بالسجن المؤقت كل من زور مستندا من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية معترفاً به قانوناً في نظام معلوماتي .

وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين إذا وقع التزوير فيما عدا ذلك من المستندات إذا كان من شأن ذلك إحداث ضرر " .

يعتبر القانون الاتحادي المتعلق بجرائم تقنية المعلومات من القوانين العربية السبابة في مكافحة الجرائم المعلوماتية، ذلك أن دولة الإمارات العربية المتحدة هي من الدول العربية الأولى في استخدام المعلوماتية ونظام الحكومة الإلكترونية الذي يسعى إلى تحويل الخدمات والمعاملات الحكومية من الشكل الورقي إلى الشكل الإلكتروني ، من خلال إتاحة كافة الخدمات الاتحادية والمحلية عبر شبكة الإنترنت عن طريق البوابة الاتحادية .

ولمكافحة إحدى أخطر هذه الجرائم شدد المشرع الإماراتي العقوبة عندما يتعلق الأمر بتزوير مستند حكومي ذو طبيعة معلوماتية بالمقارنة مع المستندات غير الحكومية لما لهذا المستند من أهمية باعتباره مستندا رسمياً ، وبالتالي الإعتداء عليه بالتزوير يزعزع الثقة التي يتمتع بها عند تداوله خاصة وأنه يتمتع بالحجية المطلقة في مجال الإثبات، لكن رغم ذلك لم يضع المشرع الإماراتي صيغة تشريعية واضحة في التجريم ، حيث لم يحدد أركان هذه الجريمة فكانت الصياغة مقتضبة، إذ لم يبين السلوك المكون للركن المادي ، ولا نوع القصد المطلوب ، إلا فيما يتعلق بعنصر الضرر الذي ورد ذكره عند تجريم تزوير مستند غير حكومي ، فهل يعتبر عنصر الضرر مرتبطاً بهذا النوع من التزوير فقط .

كما أن المشرع الإماراتي عندما جرم تزوير المستند الإلكتروني الحكومي استخدم مجموعة من المصطلحات المتوالية لتحديد نوع المستند المعاقب على تزويره في الفقرة 01 من المادة 04 من قانون مكافحة جرائم تقنية المعلومات ، وكان يكفيه في هذه الحالة أن يورد عبارة مستند رسمي على غرار ما أورده في المادة 217 من قانون العقوبات الإتحادي<sup>1</sup> ، خاصة أنه استخدم مصطلح المستند الإلكتروني في قانون المعاملات والتجارة الإلكترونية ، مقرا في هذا القانون التعامل بالمستندات أو السجلات الإلكترونية لدى الدوائر الحكومية طبقا للمادة 1/27 التي تنص على :

" على الرغم من وجود أي نص مخالف في أي قانون آخر ، يجوز لأية دائرة أو جهة تابعة للحكومة ، في أداء المهام المناطة بهم بحكم القانون أن تقوم بما يلي :

- (أ) قبول إيداع أو تقديم المستندات أو إنشائها أو الإحتفاظ بها في شكل سجلات الكترونية.
  - (ب) إصدار أي إذن أو ترخيص أو قرار أو موافقة في شكل سجلات الكترونية .
  - (ج) قبول الرسوم أو أية مدفوعات أخرى في شكل الكتروني .
  - (د) طرح العطاءات واستلام المناقصات المتعلقة بالمشتريات الحكومية بطريقة الكترونية".
- وبالتالي تولى هذا القانون شرح فكرة المستند الإلكتروني، والمستند الإلكتروني الرسمي مما يمكن الإحالة إليه .

---

1 : أحمد عبد الواحد أحمد آل علي، جريمة التزوير في التوقيع الإلكتروني (دراسة مقارنة)، (رسالة لنيل درجة الماجستير في القانون الجنائي)، كلية القانون وعلوم الشرطة ، أكاديمية شرطة دبي ، 2011 ، ص 142 .

## المبحث الثالث : مقارنة بين جريمة التزوير التقليدي وجريمة تزوير الوثيقة

### المعلوماتية

لمعرفة مدى اختلاف جريمة التزوير التقليدي عن جريمة تزوير الوثيقة المعلوماتية. لابد من عقد مقارنة بينهما، لمحاولة تحديد ملامح النظرية العامة لجريمة تزوير الوثيقة الرسمية الإدارية المعلوماتية .

### المطلب الأول : جريمة التزوير التقليدية

لابد من تعريف التزوير لدى الفقه ، واستخراج العناصر المكونة له ، ثم بيان الأركان ، المكونة لجريمة التزوير في شكلها التقليدي.

### الفرع الأول : تعريف التزوير فقها

يعرف التزوير بأنه " تغيير الحقيقة في المحرر بإحدى الطرق التي نص عليها القانون على نحو يوقع ضررا بالغير وبنية استعمال هذا المحرر فيما أعد له " <sup>1</sup> .  
كما يعرف بأنه " تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط يحتج به يمكن أن ينتج عنه ضررا أدبيا أو ماديا أو إجتماعيا " <sup>2</sup> .  
ويعتبر التزوير " إظهار للكذب في محرر بمظهر الحقيقة وذلك غشا لعقيدة الغير " <sup>3</sup> .

---

1 : عبد الفتاح بيومي حجازي، الحكومة الإلكترونية الكتاب الثاني ، مرجع سابق ، ص 177 .

2 : محمد عقاد، "جريمة التزوير في المحررات للحاسب الآلي دراسة مقارنة" ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون، القاهرة ، 25-28/10/1993 ، ص 394 .

3 : رمسيس بنهام، الجرائم المضرة بالمصلحة العامة. منشأة المعارف، الإسكندرية، 1986 ، ص 162 .

من هذه التعاريف يتبين أن التزوير يرتبط بوجود محرر له قيمة في مجال الإثبات ، وأن يقع تغيير للحقيقة فيه وهو الأساس الذي تقوم عليه جريمة التزوير<sup>1</sup> ، وذلك بنية الغش على نحو يوقع ضررا بالغير .

إن التزوير باعتباره مرتبط بالكذب قد يشتبه ببعض المصطلحات، إذ قد يقترب من النصب لأنهما يتفقان في الكذب واللباس الأمور على غير حقيقتها ثوب الحقيقة، ولكنهما يختلفان اختلافا جوهريا في أن التزوير يشترط وقوعه على محرر، أما النصب فيمكن وقوعه دون ذلك أو بمحرر كوسيلة لإرتكابه<sup>2</sup> .

ولذلك فالكذب الذي يقع به التزوير هو الكذب المكتوب الذي يقع في محرر، ولا يعد تزويرا تغيير الحقيقة بغير الكتابة .

والعلة في تجريم التزوير في المحررات راجعة إلى رغبة المشرع في حماية الثقة التي تنبعث من هذه المحررات بوصفها وسيلة التعبير عما تتضمنه من بيانات ، لتصبح في نظر الناس معبرة عن الحقيقة فيقدموا على التعامل فيها بثقة واطمئنان<sup>3</sup> ، ذلك أن التزوير يهدد بإضعاف قيمتها الثبوتية التي ينبغي أن تتمتع بها<sup>4</sup> ، وهو خطر يشبه العملة المزورة التي تبقى متداولة في السوق ، حيث يبقى هذا الخطر ساريا مع التزوير<sup>5</sup> .

---

1 : عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق ، ص 137 .

2 : فتوح الشاذلي ، عفيفي كامل عفيفي ، مرجع سابق ، ص 233 .

3 : خالد محمد كدفور المهيري ، مرجع سابق ، ص 633 .

4 : Louis Garron, "L'incrimination du faux et du Mensonge en droit Pénal", 20 juin 2011, (irc – gov – mu ), p.1

5 : Ibid , p. 2 .

ويختلف التزوير عن الصورية رغم أنها تحمل معنى تغيير الحقيقة في مضمون العقد، حيث إن العقد الظاهر مختلف في مضمونه عن العقد الحقيقي، أو قد يكون العقد الظاهر لوجود له حقيقة، ولكن لا تعتبر الصورية تزويرا طالما لم يمس هذا التغيير حقا أو مركزا قانونيا للغير، ولم يهدد المصلحة العامة أو الخاصة ، وكذلك الأمر بالنسبة للإقرارات الفردية فهي لا تكون محلا للتزوير باعتبارها تتعلق بحق المقر أو مركزه القانوني .

### الفرع الثاني : أركان جريمة التزوير

لا تقوم جريمة التزوير إلا بقيام ركنيها المادي والمعنوي ، وتكمن الخصوصية في ركنها المعنوي في اشتراط توافر القصد الخاص، وهونية الإضرار بالغير من وراء تغيير الحقيقة في المحرر .

### أولا : الركن المادي

يشمل الركن المادي ما يقوم به الجاني من سلوك لتغيير الحقيقة في محرر بالطرق المنصوص عليها قانونيا ، مما تترتب عليه ضررا بالغير . ويعني تغيير الحقيقة ابدالها بما يخالفها<sup>1</sup>، ويراد بذلك الحقيقة القانونية، وهي الحقيقة القانونية النسبية وليست الحقيقة الواقعية المطلقة ، لأن تغيير الحقيقة في جريمة التزوير تعني أن يكون هناك مساس بحقوق الغير أو مراكزهم القانونية الثابتة في المحررات<sup>2</sup>. وقد يكون التغيير كلياً أو جزئياً، حيث تتعلق الصورة

1 : فتوح الشاذلي ، عفيفي كامل عفيفي ، مرجع سابق ، ص 236 .

2 : محمود نجيب حسني، مرجع سابق ، ص . 219 .

الأولى باصطناع وثيقة بأكملها مخالفة للحقيقة ، أما الصورة الثانية فتتعلق بتغيير جزء من مضمون الوثيقة، .أما إذا حصل التغيير عن طريق محو مضمون الوثيقة كلها أو إعدام قيمتها بحيث تصبح الكتابة غير مقروءة أو لا يمكن الإحتجاج بها فإن ذلك يؤدي إلى قيام جريمة الإلتلاف إذا توافرت أركانها .

وترتبط الوثيقة في جريمة التزوير بعنصر الكتابة التي ترتبط بالدعامة الورقية، فالوعاء الذي تقع به جريمة التزوير ينصب على ورقة بالمفهوم المتعارف عليه بين الناس<sup>1</sup> . ويشترط أن تكون هذه الكتابة قابلة للإدراك بمجرد النظر إليها فإذا استحال ذلك لا يعتد بتغيير الحقيقة فيها ، ويجب نسبة الكتابة لشخص معين حتى يكون لها قيمة قانونية، وأن تكون لهذه الكتابة آثار قانونية، لأن الحماية القانونية للوثيقة ترتبط بما تتمتع به من قيمة قانونية في إثبات حق أو مركز قانوني معين ، وذلك للمحافظة على الثقة العامة فيها.

إلا أنه لا يمكن الإعتداد بالتزوير إلا إذا تم بالطرق التي نص عليها القانون، وهي على سبيل الحصر تتمثل في محو أو شطب أو إضافة كلمات، وضع امضاءات أو أختام مزورة ، وضع أسماء وصور أشخاص آخرين مزورة، الاصطناع والتقليد، وهي طرق للتزوير المادي. كما قد يكون التزوير معنويا ويتم بطرق محصورة قانونا كتغيير اقرارات أولى الشأن، وجعل واقعة مزورة في صورة واقعة صحيحة .

---

1 : فتوح الشاذلي ، عفيفي كامل عفيفي ، مرجع سابق ، ص 241 .

وسواء كان التزوير ماديا أو معنويا فإنه لا يعتد به إلا إذا أحدث ضررا سواء وقع بالفعل أو كان محتمل الوقوع فقط، وهو ضرر شخصي يصيب شخص محدد، بالإضافة إلى الضرر الإجتماعي أو العام الذي ينال الثقة العامة التي تتمتع بها الوثائق الرسمية وبالتالي هو ضرر يلحق المجتمع .

### ثانيا : الركن المعنوي

تعتبر جريمة التزوير جريمة عمدية لا تقوم إلا بتوافر القصد الجنائي الذي يرتبط بأمرين:

1- العلم : ويقصد به علم الجاني بارتكاب الجريمة بجميع أركانها المكونة لها ، فإذا تعلق الأمر بجريمة التزوير فإن ذلك يعني علم الجاني وادراكه بأنه يقوم بتغيير الحقيقة في وثيقة بأحد الطرق المقررة قانونا تغييرا قد يلحق ضررا بالأفراد والمجتمع .

2- الإرادة : أي إنصراف إرادة الجاني إلى تغيير الحقيقة في وثيقة بالطرق المقررة قانونا، وإلحاق ضرر بالغير أو احتمال حصول ذلك إذا استعملت الوثيقة المزورة فيما زورت من أجله.

### المطلب الثاني : جريمة تزوير الوثيقة المعلوماتية

لابد من وضع تعريف للتزوير المعلوماتي لبيان معالمه واستخراج عناصره، ومن ثم تحديد أركان جريمة تزوير الوثيقة الرسمية الإدارية المعلوماتية، وتمييزها عما يشابهها من الجرائم المعلوماتية.

### الفرع الأول : تعريف التزوير المعلوماتي وأثره على الصيغة التشريعية المجرمة له

عرف الفقه التزوير المعلوماتي بصيغ مختلفة، مما انعكس على الصيغة التشريعية المجرمة

له.

## أولاً : تعريف التزوير المعلوماتي فقها

التزوير في وثيقة معلوماتية هو " تغيير للحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية ، وذلك بنية استعمالها " <sup>1</sup> .

كما عرف بأنه " تغيير للحقيقة بأي وسيلة كانت سواء كان ذلك في محرر أو دعامة طالما أن هذه الدعامة ذات أثر في إنشاء حق، أولها شأن في إحداث نتيجة معينة " <sup>2</sup> .

كما يعتبر التزوير المعلوماتي " تغيير للحقيقة في البيانات أو المعلومات المعالجة عن طريق الحاسب الآلي، والتي أصبح لها كيان مادي ملموس يقابل أصل المحرر المكتوب " <sup>3</sup> .

ويقصد بهذا الكيان المادي مخرجات الحاسب الآلي ، أي البيانات والمعلومات التي تخرج من الحاسب الآلي شرط أن تطبع على دعامة مادية مكتوبة - كورقة أو مسجلة كقرص مرن أو قرص مدمج <sup>4</sup> .

من التعريفات السابقة يتبين أن التزوير المعلوماتي يرتبط بتغيير الحقيقة في وثيقة معلوماتية، وبالتالي هذه الوثيقة لا ترتبط بالشكل الورقي ، فقد تكون دعامة معلوماتية حررت عليها معلومات لها قيمة قانونية . ولذلك فتغيير الحقيقة في هذه المعلومات يجب أن يظهر من خلال هذه الدعامة ، التي تتعدد أشكالها حسب ما تقرزه التكنولوجيا .

---

1 : علي عبد القادر القهوجي، مرجع سابق ، ص . 63 .

2 : أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي دراسة مقارنة. دار النهضة العربية، ط1، القاهرة، 2000 ، ص . 407 .

3 : عبد الفتاح بيومي حجازي، الحكومة الإلكترونية الكتاب الثاني، مرجع سابق ، ص 180 .

4 : خالد محمد كدفوري المهيري، مرجع سابق ، ص 640 .



ويقع التزوير عن طريق التلاعب في المعلومات الموجودة داخل الجهاز عن طريق الحذف أو الإضافة ثم اخراجها عن طريق دعامة معلوماتية، وذلك بنية الإضرار بالغير. ولذلك يرى د. عبد الفتاح بيومي حجازي أن " التزوير في النطاق المعلوماتي يتم عن طريق تغيير الحقيقة على الشرائط أو المستندات التي تمثل مخرجات الحاسب الآلي طالما أن التغيير ذاته قد طال البيانات الموجودة في جهاز الحاسب الآلي، شرط حصول الضرر، والذي يتمثل في اهتزاز الثقة المفترضة في المحررات الرسمية عند وقوع التزوير المعلوماتي في المحرر الرسمي أو المساس بحقوق أحد الأفراد إن كان محل التزوير المعلوماتي محررا عرفيا"<sup>1</sup> .

ويرى د. أحمد حسام طه تمام أن تغيير الحقيقة يمكن تصور وقوعه على المحررات في نطاق المعلوماتية مثل تغيير الحقيقة في محرر من مستخرجات النظام المعلوماتي، وقد يتم الإعتداء عليه قبل خروجه ولكن لا يكون تزويرا إلا بعد خروجه على دعامة مكتوبة أو مسجلة<sup>2</sup>.

وبالتالي فإن تغيير الحقيقة قد يتم في محرر بشكله الورقي أو أي دعامة أخرى تحمل أفكارا ومعان ينتج عنها دليل على حق أو مركز قانوني معين قد لا تدرك مباشرة بل تحتاج إلى وسيط معلوماتي لإدراكها ، وطرق التزوير في هذه الوثيقة غير محصورة كما هو الحال عند تزويرها في شكلها الورقي، وهذا ما يميز أيضا جريمة التزوير المعلوماتي .

---

1 : عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت ، مرجع سابق ، ص 140 .

2 : أحمد حسام طه تمام ، مرجع سابق ، ص 390 .

## ثانيا : أثر التعريف الفقهي للتزوير المعلوماتي على الصيغة التشريعية المجرمة

اختلفت الصيغ التشريعية في تحديد مفهوم تزوير الوثيقة المعلوماتية، حيث نجد صياغة المادة 1/441 من قانون العقوبات الفرنسي التي تشير إلى أن التزوير هو تغيير تدليسي للحقيقة بأي وسيلة في وثيقة أو أي وعاء آخر للتعبير عن الفكر يكون الغرض منه أو كنتيجة له شأن في إثبات حق أو واقعة لها آثار قانونية، ويكون من طبيعة هذا الفعل احداث ضرر .  
وبذلك تستوعب هذه الصيغة التزوير في أي وعاء يحمل أفكار ومعان لها قيمة قانونية في مجال اثبات حق أو مركز قانوني ، متجاوزة معنى المحرر الورقي إلى أشكال أخرى ، بل وحتى تلك التي لم يتوصل إليها العلم بعد<sup>1</sup> .

كما أن هذه الصيغة جاءت مطلقة من حيث بيان طرق وقوع التزوير لأن ذلك يرتبط بجانب تقني أين تتعدد الأساليب وتصبح لاحصر لها .

أما صيغة المشرع المصري في المادة 23 من قانون التوقيع الإلكتروني فنجدها تشير إلى أن التزوير في محرر الكتروني يتم بطريق الإصطناع أو التعديل أو التحوير أو بأي طريق آخر ، وهي صيغة لم تكن موفقة في النص على طرق التزوير لتعدد واختلافها وتجدها ولذلك أرفدها بعبارة " أو بأي طريق آخر"<sup>2</sup> .

---

1 : أشرف توفيق شمس الدين، مرجع سابق ، ص 110 .

2 : نفس المرجع ، ص 112 .

كما أن المشرع المصري لم يبين طبيعة الوثيقة المعلوماتية محل الحماية ، حيث لم يتطرق لتلك القيمة القانونية التي تتمتع بها تلك المعلومات التي تتضمنها، مما سيؤدي إلى الخلط بين فكرة المحرر وأفكار أخرى هي محل حماية من القانون، غير أنها لا تدخل في مدلول المحرر<sup>1</sup>.

كما أن المشرع المصري لم يكن دقيقاً في تنظيمه لجريمة التزوير في وثيقة معلوماتية ، حيث جرم في المادة 74 من قانون الأحوال المدنية بعض الأفعال وأدرج ضمنها صور التزوير، حيث كانت صيغة المادة كالتالي: " مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في غيره من القوانين يعاقب بالحبس مدة لا تجاوز ستة أشهر وبغرامة لا تزيد عن خمسمائة جنيه أو بإحدى هاتين العقوبتين كل من اطلع أو شرع في الإطلاع أو حصل أو شرع في الحصول على البيانات أو المعلومات التي تحتويها السجلات أو الحاسبات الآلية أو وسائط التخزين الملحقة بها أو قام بتغييرها بالإضافة أو بالحذف أو بالإلغاء أو بالتدمير أو بالمساس بها بأي صورة من الصور أو أذاعها أو أفشاها " .

### الفرع الثاني : خصائص جريمة تزوير الوثيقة المعلوماتية

جريمة تزوير الوثيقة المعلوماتية هي نوع من الجرائم المعلوماتية، وهي من أخطر هذه الجرائم خاصة إذا تعلق الأمر بتزوير وثيقة رسمية تمت على يد موظف مكلف بتحريرها مثل العقود، أو وثيقة إدارية تخص جهة حكومية لأن ذلك يمس بالثقة العامة في مثل هذه الوثائق .

وتتميز جريمة تزوير الوثيقة المعلوماتية بمجموعة من الخصائص نوردتها فيما يلي :

---

1 : أشرف توفيق شمس الدين، مرجع سابق ، ص 114 .

## أولاً : إمكانية ارتكاب جريمة التزوير في أي من مراحل تشغيل النظام

يمكن ارتكاب جريمة التزوير في أية مرحلة من مراحل تشغيل نظام المعالجة الآلية وهي مرحلة الإدخال، المعالجة، الإخراج، ففي مرحلة الإدخال حيث تترجم المعلومات إلى لغة مفهومة من قبل الآلة يسهل إدخال معلومات غير صحيحة أو عدم إدخال الوثائق الأساسية والمعلومات المطلوبة<sup>1</sup> ، ولذلك يمكن تصور التزوير المعنوي بإدخال معلومات غير صحيحة للاعتداد بها على أنها معلومات صحيحة، أو ترك إدخال معلومات أساسية وذلك من أجل تغيير الحقيقة ، كقيام موظف بإدراج أسماء أشخاص غير موجودين حقيقة .

أما في مرحلة المعالجة فيمكن إدخال تعديلات على برامج الحاسب الآلي تحقق الهدف الإجرامي عن طريق التلاعب في برامج النظام المعلوماتي كدس تعليمات غير مصرح بها أو تشغيل برامج جديدة تلغي كلياً أو جزئياً عمل البرامج الأصلية<sup>2</sup> ، مثل قيام محاسب بمحو معلومات مخزنة في النظام عن طريق تغيير البيانات الموجودة بالبرنامج المحاسبي ليتم التلاعب بالمستحقات المالية أو الإيداعات المصرفية .

كما يمكن تغيير النتائج عند مرحلة الإخراج بعد أن تم ادخال المعطيات ومعالجتها بطريقة

---

1 : عادل يوسف عبد النبي شكري، " الجريمة المعلوماتية وأزمة الشرعية الجزائية "، مجلة الجريمة المعلوماتية ، عدد 07، 2008 ، ص . 115 .

2 : نفس المرجع ، ص . 115 .

صحيحة، بالدخول إلى نظام المعالجة الآلية من أجل تزيف الحقيقة، مثل قيام أحد الطلبة بالدخول إلى النظام المعلوماتي للكلية لتعديل نقاطه<sup>1</sup> .

### ثانيا : عدم وجود أثر مادي للتزوير المعلوماتي

يتميز التزوير في وثيقة معلوماتية بعدم ترك أثر مادي على الوثيقة المزورة كما هو الحال في الوثيقة الورقية، حيث قد تظهر آثار التغيير بالإضافة أو الحذف باستخدام أدوات أو مواد كيميائية ، بينما لا تظهر هذه الآثار في النوع الأول حيث تتم الجريمة من خلال الوصول إلى المعلومات وتغيير مضمونها ، فهي جريمة فنية غير ملموسة<sup>2</sup> ، وبالتالي يتعذر ترك الدليل المادي على التزوير وبذلك ينذر إثباته حيث إن هذه الجريمة تتم في بيئة افتراضية ، وإذا تم اكتشافها فإن ذلك يحصل بالصدفة .

### ثالثا : تفرد شخصية المجرم ودوافعه

ترتكب جريمة التزوير المعلوماتي بوسائل تقنية،ولذلك يحتاج مرتكبها إلى خبرة وتخصص في مجال المعلوماتية لأنه سيتعامل مع جهاز الكمبيوتر ونظام المعالجة الآلية للبيانات .

---

1 : - أدين أحد طلبة كلية الحقوق والعلوم الاقتصادية بجامعة ( paris II-Assas ) أمام محكمة (Melun) بتهمة الدخول عن طريق الغش لنظام المعالجة الآلية للمعطيات، والتزوير واستعمال المزور بسبب قيامه بتزيف نقاطه خلال ثلاث سنوات (2005-2008) عن طريق الدخول لنظام المعالجة الآلية للمعطيات الخاصة بكليته . 2012/04/12 ([www.mediaetudiant.fr/choc](http://www.mediaetudiant.fr/choc))

- قامت طالبة ماستر بجامعة (Rennes II) بالدخول إلى النظام المعلوماتي التابع للجامعة في جوان 2010، بغرض تعديل نقاطها للحصول على الشهادة ، حيث استفادت من عملها كمستخلفة للحصول على الشفرة التي تسمح لها بالدخول للنظام ، ثم تغيير نقاطها السيئة إلى نقاط ممتازة جعلتها من الأوائل في دفعتها . 2010/09/14 ([www.lefigaro.fr/actualite](http://www.lefigaro.fr/actualite))

2 : عبد الله بن سعود محمد السراني، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني. جامعة نايف العربية للعلوم الأمنية، ط1، الرياض، 2011، ص 66 .

فقد يكون هذا المجرم المعلوماتي من الموظفين المتخصصين في مجال الحاسب الآلي ، وهم يحتلون المرتبة الأولى بين مجرمي المعلوماتية ، أو من القراصنة أو المخترقين وهم أشخاص يستغلون الحاسب الآلي ولكن بشكل غير قانوني ، وهم فئتين الهاكرز القراصنة الهواة، والكرارز وهم القراصنة المحترفون<sup>1</sup> ، حيث يستخدم هؤلاء المعلوماتية لإرتكاب جرائم الحاسوب ، ومن أخطرها جريمة التزوير المعلوماتي ، التي يكون الغرض من ورائها غالبا الحصول على المال .

إن هؤلاء المجرمين لهم طبيعة خاصة وإمكانيات خاصة - علمية معلوماتية - حيث يستخدمون في ارتكاب جريمتهم الموارد المعرفية والأساليب الإحترافية<sup>2</sup> .

ولذلك فجرائم التزوير لا ترتكب بالصدفة أو عن طريق الخطأ، بل هي جرائم يخطط لها بخبرة أشخاص ذوي مهارة فنية عالية وخبرة وذكاء، وهي ذات طابع ذهني علمي تعتمد على المعلومات والمعارف الفنية والتكنولوجية التي فرضها التقدم العلمي والحضاري للمدينة الحديثة<sup>3</sup>. وقد ذكرنا أن الكثير من هذه الجرائم يقع بغرض الحصول على المال كما هو الحال عند تزوير البطاقات الائتمانية، واختراق أنظمة البنوك، وتزوير أوامر الدفع والتحويل الإلكتروني

---

1 : عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماوي، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة. جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص 09 .

2 : نفس المرجع ، ص 10 .

3 : إبراهيم العناني، " تزوير بطاقات الائتمان " ، 2011/11/07 ، ( [www.justice-lawhome.com/vb/](http://www.justice-lawhome.com/vb/) ) ، [www.showthread.php?t=23500](http://www.showthread.php?t=23500) .

للأموال، فالدافع المادي يمثل الحاجة التقليدية لهذا المجرم وهو تأمين متطلبات العيش بطرق غير قانونية وغير مشروعة وغير متعبة<sup>1</sup> .

ولذلك قد تقع هذه الجرائم من طرف موظفي البنوك ممن يملكون التقنية والكفاءة العالية للتلاعب بالبيانات عن طريق إدخال معلومات مصطنعة ، وكذلك المبرمجين الذين يكفون بتحديث وصيانة البرامج المصرفية مما يمكنهم من التلاعب بهذه البرامج<sup>2</sup> .

ولكن رغم ذلك قد تقع هذه الجرائم بدافع معنوي من أجل المتعة الشخصية واللهو وإثبات القدرات والبطش في عالم الحاسوب الافتراضي، من ذلك ما قامت به عصابة "هاكرز" مكونة من خمسة أشخاص بالاستيلاء على أموال من حسابات بطاقات بنكية ، وقد كان من بينهم فرنسي قام بتزوير بطاقات الصراف الآلي واستعمالها في سحب مبالغ مالية، ثم إعادتها للبنك مجددا ليؤكد أن نظام الحماية الذي يوفره البنك لهذه البطاقات ضعيف ويمكن اختراقه<sup>3</sup> .

### الفرع الثالث : علاقة جريمة تزوير الوثيقة المعلوماتية ببعض الجرائم المعلوماتية

قد تكون لجريمة التزوير في وثيقة معلوماتية علاقة بجرائم معلوماتية أخرى كجريمة الإلتلاف وجريمة الإحتيال المعلوماتي ، أو قد تكون لها علاقة بجريمة الدخول غير المشروع لنظام المعالجة الآلية .

---

1 : أسامة سمير حسين، الإحتيال الإلكتروني الوجه القبيح للتكنولوجيا. الجنادرية للنشر والتوزيع، ط1، عمان، الأردن، 2011، ص 96 .

2 : وليد العاكوم، " مفهوم وظاهرة الإجرام المعلوماتي"، بحوث مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 1-3 مايو 2000 ، ص 14 .

3 : أسامة سمير حسين، مرجع سابق، ص 101 .

## أولاً : علاقة جريمة تزوير الوثيقة المعلوماتية بجريمة الإحتيال المعلوماتي

تعددت تعريفات جريمة الإحتيال المعلوماتي ، ولكن التعريفات تلتقي جميعها حول وصف هذا الجرم بأنه سلوك احتيالي أو خداعي مرتبط باستخدام الكمبيوتر يهدف مرتكبه إلى تحقيق فائدة أو مصلحة مالية<sup>1</sup>، حيث يتم الإحتيال المعلوماتي عن طريق التلاعب في البرامج والبيانات وتغييرها لإيهام المجني عليه بصحتها من أجل الحصول على فائدة مالية، ولذلك يرتبط الإحتيال المعلوماتي بالتزوير عندما يتم تزوير بطاقة الدفع الإلكتروني الخاصة بعمل لدى بنك معين من أجل استغلالها في الحصول على السلع والخدمات، ويعتبر استخدام بيانات هذه البطاقة عبر شبكة الإنترنت احتيالا لأن المجرم استخدم صفة غير صحيحة بطرق احتيالية للحصول على قيمة مالية ، كما يعد تخليق بيانات بطاقة الدفع تزويرا، ويعتبر استخدام البطاقة المزورة من قبيل الطرق الإحتيالية<sup>2</sup> . إلا أن الإحتيال هو الإستيلاء على شيء مملوك للغير بطرق احتيالية بقصد تملك ذلك الشيء<sup>3</sup> ، وهذه الطرق الإحتيالية في مضمونها هي تغيير للحقيقة لخداع المجني عليه، للوصول إلى نتيجة وهي تسليم المال للجاني، وفي المجال

---

1 : وليد العاكوم ، مرجع سابق ، ص 14 .

2 : محمد أمين أحمد الشوابكة ، مرجع سابق ، ص 202 .

3 : نجاح محمد فوزي، وعي المواطن العربي تجاه جرائم الإحتيال " بطاقات الدفع الإلكترونية نموذجا"، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص 16 .



المعلوماتي تتخذ هذه الطرق الإحتيالية أشكال متعددة للإستيلاء على مال الغير، وقد تقترن بالتزوير<sup>1</sup> .

وبعد التلاعب في البرامج والبيانات والتغيير فيها بما يترتب عليه إيهام المجني عليه بصحتها مما يجعله يسلم بها ، أحد أساليب التحايل حيث يستخدم الحاسوب كوسيط لذلك<sup>2</sup> .  
غير أنه ليس من السهل في الكثير من الأحيان تحديد الوصف القانوني المناسب لهذه الأفعال، كما هو الحال في جرائم الإحتيال المصرفية ، حيث يتم الإستيلاء على الأموال من حسابات العملاء ، فهو من جهة إجراء تغيير وتلاعب في البيانات لإيهام صاحب الحساب بصحتها مما يجعله يسلم بها، وهو من جهة ثانية إجراء تزوير في البنود المتعلقة بالحسابات ، وهو من جهة ثالثة إستيلاء على أموال الغير دون رضاه ، وهو من جهة رابعة إساءة أمانة إذا حصل من قبل الشخص المكلف بحكم وظيفته بالمحافظة على هذه الأموال<sup>3</sup> .

### ثانيا : علاقة جريمة تزوير الوثيقة المعلوماتية بجريمة الإتلاف المعلوماتي

يتم الإتلاف المعلوماتي بالإعتداء على البرامج والمعلومات المخزنة في النظام، ويكون ذلك بطريق التلاعب بالبيانات سواء بإدخال معلومات مصطنعة أو إتلاف المعلومات المخزنة

---

1 : تمكن هاكرز دولي من اختراق موقع أحد البنوك السعودية واستطاع أن يرسل رسائل الكترونية منسوبة للموقع لعملائه يحثهم فيها على تحديث البيانات الخاصة بهم ليكون التعامل على موقع البنك أكثر أمانا وسرعة، وهو ما مكنه من الإستيلاء على بيانات عملاء البنك، والتي من خلالها استطاع تحويل أموال طائلة من أرصدهم إلى أرصدة وهمية حتى استطاع الإستيلاء على الأموال (إيهاب فوزي السقا، مرجع سابق، ص 66).

2 : هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، ط1، القاهرة، 1992، ص 133 نقلا عن: محمد أمين أحمد الشوابكة ، مرجع سابق، ص 185 .

3 : وليد العاكوم، مرجع سابق ، ص. ص16، 15 .

بمحوها أو تعديلها أو تغيير نتائجها<sup>1</sup> ، ولذلك تتشابه طرق الإلتلاف والتزوير المعلوماتي، لكن جريمة الإلتلاف المعلوماتي تختلف من حيث محلها ونتيجة السلوك المادي فيها، حيث يتم الإعتداء على بيانات وبرامج ويترتب على ذلك أن تصبح غير صالحة للإستعمال، فلا تؤدي وظيفتها المطلوبة، أو يحصل تعديل في برنامج التشغيل من خلال اصطناع برنامج بأكمله، وهذه الصورة قد ينتج عنها عمليات تزوير واحتيال مثل قيام شركة أمريكية باصطناع برنامج تم بواسطته خلق عدد وهمي من المؤمن عليهم، ووضع شفرة خاصة بالبرنامج وبرمجته بحيث لا يظهر عند الطباعة إلا الوثائق الصحيحة<sup>2</sup>، وبالتالي يؤدي هذا التعديل إلى تغيير معلومات لها أثر قانوني مما يحدث ضررا للغير، ويكون الغرض من ذلك استعمالها للإستفادة من مزايا معينة، بينما يؤدي الإلتلاف إلى عدم الصلاحية للإستعمال، وعدم أداء الشيء المتلف لوظيفته المطلوبة .

ولذلك فإن اتلاف البيانات والأموال اللامادية سواء بمحوها وتدميرها الكترونيا أو بتشويهاها أو تعديل طرق معالجتها ووسائل انتقالها يثير تكييفاً جنائياً اختلافاً ملموساً بحسب الغاية التي هدف إليها المجرم المعلوماتي من واقعة الإلتلاف<sup>3</sup> .

أما التزوير فهو تغيير للحقيقة ، بمعنى إدخال تغيير على المحرر المراد تزويره على نحو

---

1 : محمد أمين أحمد الشوابكة ، مرجع سابق ، ص . 216 .

2 : عزة محمود ، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب الآلي، (رسالة مقدمة لنيل درجة الدكتوراه)، كلية الحقوق، جامعة القاهرة، 1994، ص 182 نقلا عن ، ص 237 .

3 : محمد أمين أحمد الشوابكة، مرجع سابق، ص 230 .

يغير مضمونه أو شكله ولكن بشكل لا يعدمه أو يهدر قيمته<sup>1</sup> .

### ثالثا : علاقة جريمة تزوير الوثيقة المعلوماتية بجريمة الدخول غير المشروع للنظام

جريمة الدخول غير المشروع للنظام هي جريمة مستقلة في مختلف القوانين الجنائية باعتبارها من الجرائم المعلوماتية ، حيث المصلحة المحمية من طرف المشرع الجنائي هي مصلحة فردية تتعلق بصاحب النظام .

لكن هذه الجريمة وإن كانت مستقلة إلا أنها قد تكون مقدمة لإرتكاب جرائم معلوماتية أخرى، ومن بين هذه الجرائم جريمة التزوير .

فقد يتمكن الجاني - بعد دخوله بطريقة غير مشروعة للنظام - من القيام بعمليات تزوير<sup>2</sup>، ولذلك فإن تجريم فعل الدخول غير المشروع للنظام وإن كان يهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، إلا أنه يحقق أيضا وبصورة غير مباشرة حماية للمعطيات أو المعلومات ذاتها<sup>3</sup>، وفي موضوع دراستنا يتعلق الأمر بحماية هذه المعلومات ضد التزوير .

---

1 : عبد الرحمان عبد الله حميد آل علي، جرائم التزوير المعلوماتية- دراسة تحليلية تأصيلية، (رسالة ماجستير في العلوم الجنائية)، أكاديمية شرطة دبي، دبي، ب . ت ، ص . 78 .

2 : قام البريطاني " رافايل " الذي لقب نفسه بقديس التجارة الإلكترونية بكشف تفاصيل بطاقات الإئتمان الخاصة ببيل جينس (صاحب شركة مايكروسفت)، و26 ألف حساب آخر في مختلف أنحاء العالم، بعد عمليات اختراق واستخدام هذه البطاقات عبر شبكة الإنترنت مما سبب أضرارا مالية (مصطفى محمد مرسي، مرجع سابق، ص . 63).

- تمكن طالب من اختراق ثلاث بنوك مصرية ، حيث تمكن من الدخول إلى حسابات العملاء وأخذ البيانات الخاصة بهم ، ثم قام بإدراجها على الشريط المغنط لبطاقات ائتمانية مزورة ، ليستخدما في عمليات شراء من محال تجارية .(إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، مرجع سابق ، ص 66).

3 : علي عبد القادر القهوجي، مرجع سابق، ص . 53 .

## الفصل الثاني

### أركان جريمة تزوير الوثيقة الرسمية الإدارية المعلوماتية والعقوبات المقررة

#### لها

لجريمة التزوير في وثيقة رسمية إدارية معلوماتية ركنان هما الركن المادي والركن المعنوي، كما هو الحال في جريمة التزوير التقليدية .

غير أن الركن المادي لهذه الجريمة يقوم بأفعال مختلفة عن التزوير التقليدي ، كما أن هذه الأفعال قد تتشابه مع السلوك المادي لجرائم معلوماتية أخرى ، أو قد تكون مقدمة لإرتكاب فعل التزوير ، ولذلك لا بد من تحديد عناصر الركن المادي والمعنوي لهذه الجريمة بدقة ، وبيان العقوبات المقررة لها ، خاصة وأن التشريعات الجنائية المقارنة قد اختلفت من حيث منهجها في التجريم كما بينا في الفصل الأول من هذا الباب .

#### المبحث الأول : أركان جريمة تزوير الوثيقة الرسمية الإدارية المعلوماتية

تتعدد أركان جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية كباقي الجرائم بين ركن مادي ومعنوي ، لكنها تتميز بخصوصية في الأفعال المكونة لركنها المادي باعتبارها جريمة تقع في بيئة افتراضية غير ملموسة ، وهذا يجعل أشكال وطرق التزوير مختلفة عن تلك المعروفة في جريمة التزوير التقليدية .

## المطلب الأول : الركن المادي

يقوم الركن المادي في جريمة تزوير الوثيقة الرسمية الإدارية المعلوماتية بإتيان أحد الأفعال المتعلقة إما بالتلاعب في محتوى الوثيقة داخل النظام عندما يتعلق الأمر بوثيقة رسمية تخص أحد الجهات الإدارية الحكومية ، أو بخلق وثيقة رسمية إدارية معلوماتية غير صحيحة ، مع اشتراط تحقق الضرر نتيجة هذا الفعل .

### الفرع الأول : السلوك المادي

يتم التزوير في الوثيقة الرسمية الإدارية داخل النظام بالتلاعب في محتواها المعلوماتي مما يتطلب طرق تكنولوجية للقيام بذلك ، أو قد يلجأ الجاني إلى خلق وثيقة بأكملها داخل هذا النظام لم تكن موجودة من قبل وبمحتوى غير صحيح .

### أولا : التلاعب في محتوى الوثيقة الرسمية الإدارية المعلوماتية

إن المعلومات الموجودة على دعامة الكترونية تعتبر وثيقة، سواء كانت هذه المعلومات مخزنة على الجهاز أو على دعامات منفصلة إذا كانت لها قيمة قانونية حيث تثبت حقا أو مركزا قانونيا معينا ، ويعبر عن هذه الوثيقة بمصطلح رسالة المعلومات في التشريعات المقارنة، ويتضمن جزء من محتواها توقيعها الكترونيا أو رقميا يدل على صحتها، كما يجب حفظها وفق شروط تقنية تحافظ على ثبات محتواها وسلامتها\*.

---

\* : أنظر الباب الأول في تفاصيل شروط تمتع الوثيقة المعلوماتية بالحماية القانونية .

لكن رغم هذه الشروط قد يقع التزوير في هذه الوثيقة بالتلاعب في محتواها بطرق مختلفة، وهذا التلاعب في جوهره قائم على أساس تغيير الحقيقة.

## 1- طبيعة التلاعب في محتوى الوثيقة المعلوماتية :

إن السلوك المادي في هذه الحالة يعتمد على تغيير الحقيقة الموجودة في وثيقة افتراضية باستخدام التقنيات الرقمية ، وطرق التغيير لا يمكن حصرها نظرا لطبيعة الوثيقة المعلوماتية، ولذلك تجاوزت التشريعات الجنائية المقارنة التعداد الحصري أو المثالي لصور ومظاهر السلوك، وركزت على إحداث التغيير في الحقيقة بصورة مفتعلة ، توقع الضرر أو تهديد به، دون أن تعير بالا لطريقة أو وسيلة أو مظهر تغيير تلك الحقيقة <sup>1</sup> .

لقد أتاحت الحكومة الإلكترونية تدفقا واسعا للوثائق المعلوماتية في المعاملات الإدارية، كما سهلت وسرعت هذه المعاملات لأنها مخزنة على الشبكة أو نظم المعلومات، ودون مرورها بصورة مخرجات ضمن أية صورة تقليدية ممكنة <sup>2</sup> ، ولذلك يصبح فعل التغيير في الحقيقة الثابتة في هذه الوثيقة واقعا داخل النظام المعلوماتي أو على الشبكة ، حيث يتعلق بتغيير معلومات معالجة آليا ، وهي محمولة على وعاء معلوماتي، مما يجعل طرق تغيير الحقيقة تتناسب مع طبيعة هذه الوثيقة .

---

1 : جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية دراسة مقارنة. دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010، ص . 160 .

2 : نفس المرجع ، ص 160 .

وهنا يفرق بعض الفقه بين تغيير المعلومات المعالجة آليا ، وبين إخراج هذه المعلومات بشكل ورقي عن طريق مخرجات الجهاز ، وحينها تتمتع بالحماية القانونية من خلال نصوص التزوير التقليدية، وبغير ذلك لا تعتبر هذه المعلومات واردة ضمن وثيقة، ولا تصلح لأن تكون محلا للتزوير .

إلا أن هذا الرأي لا يؤدي إلى حلول منطقية لمشكلات التعامل بالوثائق المعلوماتية، حيث يمكن إنجاز المعاملات الإدارية دون إخراجها على ورق ، كما أن ربط قيام الركن المادي باكتمال وصف الوثيقة من خلال الشكل الورقي بعد معالجتها آليا لا يضيف شيئا لجريمة التزوير بل يبقيها في إطارها التقليدي .

ولذلك فإن تغيير الحقيقة في المعلومات المعالجة آليا

قد يظهر على كيان مادي سواء كان ورقي أو دعامة الكترونية كالشروط الممغنطة والأقراص الإلكترونية وغيرها من الدعائم المماثلة ، وفي هذا الغرض يفرق بعض الفقهاء بين تغيير المعلومات المخزنة في الجهاز، وبين إثبات هذه المعلومات في المستندات الصادرة عن النظام المعلوماتي والتي يتحقق فيها وصف المحرر، وبالتالي تتمتع بحماية القانون لها حسب نصوص التزوير باعتبارها معدة للتداول بين الأفراد<sup>1</sup> ، حيث يعتبر التزوير المعلوماتي منصب على مخرجات الحاسب الآلي ، أي البيانات والمعلومات الخارجة منه، بشرط أن تطبع على دعامة مكتوبة أو مسجلة أي يكون لها كيان مادي يمكن إدراكه، ولو تم تغيير الحقيقة دون

---

1 : من هؤلاء الفقهاء : عبد الفتاح بيومي حجازي، الحكومة الإلكترونية، الكتاب الثاني ، مرجع سابق، ص 181 .

طباعة فلا يمكن أن يطلق عليه تزويراً<sup>1</sup> ، فالتجريم وفقاً للنص القانوني لا يتم إلا في حال حدوث التزوير في المعلومات الخارجة من النظام المعلوماتي<sup>2</sup> .

ورغم ذلك يرى البعض الآخر أن ثمة صعوبتين تعترضان هذا الرأي الفقهي أولها التفرقة ما بين المعلومات المخزنة في الحاسب الآلي، وما بين تلك التي طبعت على دعامة أو مستند، والقول بوقوع التزوير في الثانية دون الأولى، والحقيقة أن هذه التفرقة تحكّمية ما بين المعلومات المخزنة في الحاسب الآلي ، وتلك المسجلة على دعامة، فالتزوير لم يقع استقلالاً، بل وقع نتيجة التدخل بالتلاعب في المعلومات المخزنة بالفعل<sup>3</sup> . وهو الرأي الذي نميل إليه باعتبار أن تغيير الحقيقة قد يرد على دعامة معلوماتية متصلة، حيث تخزن المعلومات عليها داخل الجهاز، وتبقى كذلك دون أن يتم تسجيلها على دعامة منفصلة، فقد يتم تبادل هذه الوثائق بين جهتين حكوميتين أو أكثر من شبكة داخلية أو عن طريق شبكة الإنترنت، وهو ما يجعلنا أمام حالة كون المعلومات المزورة ليست محمولة على دعامة منفصلة، ولكنها معلومات معالجة آلياً وهي تتعلق بحق أو مركز قانوني للغير، وإخراجها من نطاق الوثائق التي قد ينصب عليها التزوير غير منطقي، خاصة في ظل مقصد المشرع من وراء تجريم التزوير في الوثائق الرسمية وهو حماية الثقة العامة فيها .

---

1 : أنظر في هذا الرأي : أحمد حسام طه تمام، مرجع سابق ، ص 290 .

2 : عبد الرحمن عبد الله حميد آل علي، جرائم التزوير المعلوماتية. د.ن، ط1 ، د.م ، 2009 ، ص 81 .

3 : خالد محمد كدفور المهيري ، مرجع سابق ، ص 642 .



كما أن الآراء الفقهية السابقة تربط وقوع التزوير بحدوث تغيير في المعلومات المخزنة في الجهاز ابتداءً، لتظهر فيما بعد على مخرجاته ، ومن ثم لا يمكن الإعتداد فقط بما سجل على دعائم منفصلة .

## 2- طرق التلاعب في محتوى الوثيقة المعلوماتية :

يمكن التلاعب في محتوى الوثيقة المعلوماتية بأشكال مختلفة بل يصبح من السهل ذلك في وسط غير ملموس، إذ أن تغيير الحقيقة لن يترك أثراً ظاهراً، لأنه يقع خلال مرحلة المعالجة الآلية بعد تلقي البيانات ضمن النطاق المعلوماتي لجهاز الحاسب الآلي في ضوء طلبات وحاجات الجهة العامة أو الخاصة المستخدمة له<sup>1</sup> ، ويقع التغيير بالإضافة أو الحذف أو التعديل، أو تزوير توقيع أو صورة.

### أ- تغيير الحقيقة عن طريق الحذف أو الإضافة أو التعديل :

إن هذه الطريقة تجعل جريمة تزوير الوثيقة المعلوماتية تشتهه بجريمة الإعتداء العمدي على النظام المعلوماتي التي تتم بأفعال مادية مشابهة عن طريق الإدخال والمحو والتعديل ، حيث يقصد بالإدخال إضافة معطيات جديدة أما المحو فيتمثل في إزالة جزء من المعطيات المخزنة داخل النظام ، بينما يعتبر التعديل تغيير للمعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى<sup>2</sup> . إلا أن الفرق يكمن في طبيعة المعلومات التي يتم الإعتداء عليها، حيث

---

1 : عبد الرحمن عبد الله حميد آل علي ، جرائم التزوير المعلوماتية، مرجع سابق ، ص 96 .

2 : نفس المرجع ، ص 98 .

تكون تلك المعلومات وثيقة في جريمة التزوير إذا كانت تثبت حقا أو مركزا قانونيا معيننا أي لها آثار قانونية بالنسبة للغير .

ويتم التغيير في الوثيقة بحذف كلمة أو رقم أو رمز معين أو بإضافته أو تعديله ، سواء كانت لها معنى مفهوم ومدرك للإنسان ، أو كانت غير مدركة مباشرة ، مثل تغيير الأمر بالدفع الموجه من بنك لآخر وتزوير الرسالة (الوثيقة) ليتم الدفع لحساب المجرم<sup>1</sup>، أو تغيير أرقام موظفين محفوظة داخل النظام والتي لها دلالة مالية<sup>2</sup>، وقد يتم تعديل البيانات باستخدام بعض البرامج المساعدة الجاهزة المصممة خصيصا لتعديل البيانات في أماكنها مباشرة<sup>3</sup>. كما قد يحدث التزوير عن طريق تغيير أمر التحويل المصرفي ، خاصة عندما يعتبر التحويل الإلكتروني للأموال وسيلة قانونية لإجراء المعاملات المصرفية بالنص على ذلك تشريعا .

ويتم التحويل المصرفي الإلكتروني للأموال بوسائل الكترونية متعددة ، كما يتم هذا التحويل الإلكتروني بواسطة أنظمة التحويل الإلكتروني إما فيما بين المصارف أو بواسطة

---

1 : أحمد خليفة الملط ، مرجع سابق ، 467 .

2 : من أمثلة ذلك قيام موظف بتغيير أرقام الموظفين المستفيدين من أجور الساعات الإضافية، والذين لديهم أكثر هذه الساعات الإضافية، حيث لا حظ هذا الموظف المسؤول عن إدخال بيانات ساعات العمل الإضافي لثلاثمائة موظف أن جميع الساعات الإضافية للموظفين تدخل في برنامج حفظ الوقت ودقتر الدفعيات باسم الموظفين وأرقامهم وطباعة شيكات الدفع بناء على ذلك ، إلا أن المراجعة الخارجية تعتمد على اسم الموظف فقط ، ولا أحد يقوم بمراجعة حقوق الأشخاص بأرقامهم ، ومن ثم انتهز الفرصة في استخدام أسماء الموظفين الأكثر عملا إضافيا ، وادخل رقمه الخاص بحيث يضاف أجر الساعات الإضافية لهؤلاء الموظفين إلى هذا الرقم ( عبد الله سعود السراني، مرجع سابق ، ص 54 ).

3 : قام مشرف تشغيل الحاسب في أحد البنوك باستخدام برنامج مساعد لزيادة أرصدة حسابات العديد من أصدقائه، ليتم سحب هذه الأموال من طرفهم ، ثم قام بتفريق ايصالات السحب . ولكن بحلول موعد المراجعة الدورية لحسابات البنك، اكتشف المراجعون هذه العمليات لأنه تم تسجيلها بواسطة نظام أمن سري كان يقوم بتسجيل كل العمليات على الحاسب الموجود في أحد فروع البنك ، ولم يكن المجرم على علم بهذا النظام الأمني (حسن طاهر داود، جرائم نظم المعلومات أكاديمية نايف العربية للعلوم الأمنية، ط1، الرياض، 2000، ص 46).

الوسائل التكنولوجية الحديثة في التحويل المالي والتي ليست مقتصرة على ربطها بين المصارف فقط وإنما تمتد لتشمل المتعاملين مع المصارف<sup>1</sup> .

وأهم هذه الوسائل الإلكترونية نجد الصراف الآلي، مراكز الخدمة الهاتفية والبنك الناطق، البطاقات الذكية، نقاط البيع، جهاز الحاسب الشخصي المرتبط بحاسوب المصرف ، الشيكات الإلكترونية ، شبكة الإنترنت<sup>2</sup> .

ويقع التزوير في أمر التحويل المصرفي الإلكتروني إن لم يكن صادرا عن العميل، وذلك بحصول الجاني على بيانات العميل ورقمه السري، واستعمالها من طرفه لإجراء تحويلات إلكترونية .

وقد تقتزن هذه الطريقة بتزوير توقيع الكتروني، إذا حصل الجاني على منظومة التوقيع الإلكتروني لبطاقة ائتمانية لأحد العملاء، وقام بالتوقيع بها دون رضاه .

#### ب- تزوير التوقيع :

يمكن أن يتم تزوير الوثيقة المعلوماتية الصادرة عن موظف عام أو مكلف بخدمة عامة عن طريق تزوير التوقيع المذيلة به ، باعتبار أن التوقيع يعتبر جزء من هذه الوثيقة وعنصر من عناصرها التي تضفي عليها الحماية القانونية . ويتم تزوير التوقيع بإدخال توقيع أو ختم أو بصمة عن طريق الماسح الضوئي إلى وثيقة مخزنة داخل الجهاز لتنسب إلى صاحب التوقيع ،

1 : حازم نعيم الصمادي، المسؤولية في العمليات المصرفية الإلكترونية. دار وائل للنشر، عمان، الأردن، ب.ت، ص 62.

2 : لمزيد من التفاصيل حول هذه الوسائل أنظر : نفس المرجع ، ص . ص 29 - 33 .

فقد ذكرنا أن عملية التلاعب تتم خلال مرحلة المعالجة الآلية للبيانات لتظهر في شكل مخرجات لها قيمة قانونية ، فقد تكون في شكل قرار إداري من جهة حكومية يرتب أثرا قانونيا معيناً ، حيث وقع من الجهة مصدرة القرار ، فمن السهل إدخال صورة توقيع هذه الجهة عن طريق جهاز الماسح الضوئي ليضاف للوثيقة المزورة ، وبذلك تكون قد اكتسبت صفتها الرسمية بعد أن دون فيها بيانات على غير إرادة صاحبها أو نسب إليه دون أن تنصرف إرادته إلى ذلك<sup>1</sup> .

أما إذا كان التوقيع رقمياً فإن التوقيع المزور يكون مطابقاً للتوقيع الأصلي ، ولكن يتم التوقيع من خلال سرقة منظومة التوقيع والتوقيع بها ، حيث يعتبر التوقيع سليماً إذا تمت مضاهاته ولكنه ليس صادر من مالك منظومة التوقيع الإلكتروني<sup>2</sup> .

ومن تطبيقات هذه الطريقة سرقة منظومة التوقيع الإلكتروني الخاصة ببطاقات ائتمانية والتوقيع بها دون رضا مالكيها ، حيث إن استخدام الرقم السري الخاص بالبطاقة عند استخدامها داخل جهاز السحب الآلي للنقود، إذا تم من شخص غير صاحب البطاقة يعتبر تزويراً للتوقيع، باعتبار أن النقر على لوحة مفاتيح الحاسب الآلي يعتبر توقيعاً إلكترونياً من صاحب الحق في ذلك<sup>3</sup> .

---

1 : عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص 184 .

2 : عبد الله سعود السراني ، مرجع سابق ، ص 56 .

3 : ايهاب فوزي السقا ، مرجع سابق ، ص 63 .

إن هذه الطريقة تتشابه مع طريقة وضع إمضاء مزور في وثيقة ورقية ، والذي يقصد به توقيع الشخص بإمضاء غير إمضائه وليس له حق التوقيع به <sup>1</sup> ، لكنها مختلفة من الناحية لكنها مختلفة من الناحية التقنية حيث أصبح هذا الإمضاء عبارة عن منظومة رقمية \* .

وقد يتم الإعتداء على التوقيع بالتقاط كلمات السر من خلال استخدام برمجيات لإلتقاطها خلال تجوالها في جزء من الشبكة ، حيث عندما يطبع المستخدم كلمة السر أو اسم المستخدم، فإن البرنامج يجمع هذه المعلومات وينسخها، إضافة إلى أن أنواع من هذه البرامج تجمع المعلومات الجزئية وتعيد تحليلها وربطها معا كما تقوم بعضها بإخفاء أنشطة الإلتقاط بعد قيامها بمهمتها <sup>2</sup> .

### ج- تزوير الصورة :

قد يقع التزوير بتغيير الصورة الموجودة في الوثيقة ، إذا كانت الصورة عنصرا جوهريا لا يقل أهمية عن بعض بيانات الوثيقة <sup>3</sup> ، كالبطاقات الشخصية وجوازات السفر و رخص القيادة، وبطاقات التأمين وغيرها. وتعتبر الصورة عنصرا مهما إذا كانت لازمة في الوثيقة، حيث لا تحقق

---

1 : ايهاب فوزي السقا ، مرجع سابق ، ص 61 .

\* : تم ضبط عمليات تزوير من هذا النوع ، حيث تعرضت بنوك بدولة الإمارات العربية المتحدة لعملية قرصنة، من خلال قيام محترفين في المعلوماتية بإدخال جهاز في فتحات إدخال بطاقات السحب بأجهزة السحب الآلي ، ليقوم هذا الجهاز بتسجيل بيانات جميع البطاقات، ونسخ الأرقام السرية الخاصة بالعملاء، ومن ثم استخدام هذه البيانات على بطاقات مزورة، واستعمال هذه البطاقات لسحب مبالغ مالية من أرصدة العملاء . (16 سبتمبر 2008 ، [www.alitihad.ae/details.php?id=384](http://www.alitihad.ae/details.php?id=384) ) ( gy = 2008 384 )

2 : زيان سويدان، " انتحار الهوية الرقمية " ، ب . ت ، (www.urdri.fdspt.mu.tn/zied-souiden-usurpation-id)

3 : عبد الفتاح بيومي حجازي، الحكومة الإلكترونية، الكتاب الثاني، مرجع سابق ، ص 203 .

غرضها الذي أعدت لأجله إلا بوجودها، أو إذا كانت الصورة متصلة عضويا ومندمجة فيها<sup>1</sup>. فإذا كانت الصورة أحد البيانات الجوهرية في الوثيقة المعلوماتية، فإنه يتم تزويرها بالإستبدال باستخدام الماسح الضوئي، حيث توجد برامج متخصصة بتركيب الصور<sup>2</sup>، وبالتالي فإن تزوير الصورة يتم باستخدام الحاسب الآلي وملحقاته حيث تنقل الصورة ضوئيا إليه ثم تعالج ببرامج متخصصة لإدماجها في الوثيقة، سواء تم اخراجها في شكل مخرجات ورقية، أم بقيت في هذا الوسط الافتراضي.

ولذلك فإن تغيير الصورة لا يعد فعلا معاقبا عليه بوصفه تزويرا، إلا إذا كانت الصورة جزءا مكتملا لمحرر على تقدير أن استبدالها يؤدي إلى تغيير في حقيقة معناه أو مضمونه<sup>3</sup>.

### ثانيا : خلق وثيقة معلوماتية مزورة

قد يقوم المجرم بخلق وثيقة معلوماتية لم تكن موجودة من قبل بمحتوى غير صحيح إما عن طريق الإصطناع أو بطرق معنوية .

**1- اصطناع وثيقة معلوماتية مزورة :** فعل الإصطناع يعني خلق وثيقة غير موجودة حقيقة مثل اصطناع شهادة إدارية بالوفاة<sup>4</sup>، أو شهادة إدارية لمؤهل علمي معين، أو شهادة بعدم الملكية وغيرها .

---

1 : عبد الفتاح بيومي حجازي، الحكومة الإلكترونية، الكتاب الثاني، مرجع سابق ، 204 .

2 : عبد الله سعود السراني ، مرجع سابق ، ص 57 .

3 : عبد الرحمن عبد الله حميد آل علي ، مرجع سابق ، ص 86 .

4 : Cour de cassation, chambre criminelle, 22 octobre 2003 .

إلا أنه يجب التفرقة بين هذه الطريقة وبين اصطناع البرنامج حيث لا يعد ذلك تزويرا ، وإنما يعتبر تقليد للمصنف إذا توافرت فيه الشروط القانونية المطلوبة لإعتباره مصنفا وفقا لقانون حماية حق المؤلف<sup>1</sup> .

وعلى خلاف الرأي السابق يرى د.عبد الفتاح بيومي حجازي أن برامج الحاسب الآلي تخضع للتزوير المعلوماتي عن طريق الحذف أو الإضافة أو التعديل باعتبارها مصنف مشمول بالحماية القانونية من خلال قانون حماية حق المؤلف، منعا من الإعتداء عليه بطريقة السرقة والتزوير شرط أن يتحقق للمصنف باقي شروط الحماية ومنها شرط الابتكار، وأن التزوير المعلوماتي يتم بنسخ أو تقليد المصنف باسم المؤلف الحقيقي أو باسم شخص آخر يخلق في الذهن لبسا حول المؤلف الحقيقي أو باسم الجاني نفسه أو باسم خيالي<sup>2</sup>.

إن هذا الرأي مردود عليه لأن البرنامج يعتبر مصنف إذا توافرت فيه شروط المصنف من الناحية القانونية ، وهو مختلف عن الوثيقة المعلوماتية لأنها ترتب أثرا قانونيا معيناً للغير ، ومن ثم كانت حمايتها لما تتمتع به من ثقة عامة لدى تداولها، وهذه المصلحة تختلف عن المصلحة المحمية في المصنف والتي تتعلق بالملكية الفكرية.

ويتم تزوير الوثيقة المعلوماتية عن طريق الإصطناع من خلال إدخال معلومات إلى جهاز

---

1 : فتوح الشاذلي ، عفيفي كامل عفيفي ، مرجع سابق ، ص 239 .

2 : عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت ، مرجع سابق ، ص 189 .

الحاسب الآلي لم تكن موجودة بفرض نسبتها إلى جهة معينة ، ولذلك ترتبط هذه الطريقة بتزوير التوقيع غالبا حتى يتم نسبة الوثيقة للغير .

ويختلف الإصطناع عن التقليد الذي يعتبر طريقة لتزوير الوثيقة الورقية يراعى فيها محاكاة الوثيقة في صلبها و في أختامها أو امضاءاتها<sup>1</sup> ، ولا يتصور وقوع التزوير المعلوماتي بهذه الطريقة لاتصالها بالطبيعة الورقية للوثيقة، كما أن المعلومات المكونة لها غير محررة بخط اليد.

## 2- تزوير الوثيقة المعلوماتية بطرق معنوية:

إن التزوير المعنوي في الوثيقة الورقية يقوم على تغيير الحقيقة في مضمونها، دون وجود أي أثر مدرك على التغيير في ظاهرها، حيث تبقى هذه الوثيقة محافظة على شكلها ، وسلامتها، ودون المساس بطبيعتها<sup>2</sup>. فالاعتداء لا يقع على الوثيقة، ولكن على مضمونها، حيث ما يذكر من بيانات فيها لا يتفق مع الحقيقة<sup>3</sup>.

هذا يعني أن تزوير الوثيقة الرسمية الإدارية بهذه الطريقة لا يتم إلا من طرف القائم على تحريرها أثناء إنشائها، ومن ثم لا يتصور ارتكاب التزوير بها في محرر رسمي من فرد عادي كما هو الحال في التزوير المادي، لأن المحرر الرسمي إنما يكتبه دائما موظف عمومي ، ومن ثم ففاعل التزوير المعنوي لا يمكن أن يكون إلا موظفا<sup>4</sup> .

---

1 : أحمد محمود خليل ، مرجع سابق ، ص 107 .

2 : Louis Garron, op.cit, p 7 .

3 : Geert Delrue, Faux en Ecriture. Maklu, S.L, 2007 , p 17 .

4 : أحمد محمود خليل ، مرجع سابق ، ص 108 .



ويتم التزوير بجعل واقعة غير صحيحة في صورة واقعة صحيحة ، مثل قيام موظف الحالة المدنية بتغيير الحقيقة في شهادة وفاة أو زواج إثباتا لوقائع غير صحيحة، سواء بتدوين بيانات معنية أو بترك تدوين بيانات معنية لها أثرها من الناحية القانونية.

كما قد يتم بتغيير المعلومات التي طلب تدوينها عند إنشاء الوثيقة من طرف من هو قائم بتحريرها محرفا مضمونها ابتداء، مثل قيام موظف بتغيير البيانات المدخلة لبرنامج يعتمد على عبارة نعم أولا في تصنيف الموظفين الحاصلين على قرض من عدمه<sup>1</sup>، ليقيم اقتطاع قيمة القرض بداية كل شهر آليا بإدخال اسم الموظف تحت عبارة (نعم)، حيث يمكن إعفاء أحد الموظفين بإدراجه تحت عبارة (لا) .

فالموظف العام القائم على تحرير هذه الوثائق الرسمية الإدارية عندما يقوم بمعالجتها آليا بإدخال البيانات اللازمة لجهاز الحاسب الآلي، قد يقوم في مرحلة الإدخال بالتلاعب في البيانات حيث يقوم بتغييرها، كما في المثال السابق أو بتغيير بيانات فاتورة الهاتف أو بيانات معاملة بنكية عند إنشاء الوثيقة المتعلقة بها عن طريق الحاسب الآلي، باعتبار هذا الجهاز أصبح يمثل عصب الحياة في حياتنا اليومية في المحاكم والوزارات والمدارس والجامعات والمواصلات وغيرها<sup>2</sup> .

إن الصلة وثيقة بين التزوير المعنوي والجريمة المعلوماتية، لأن النظام المعلوماتي التي

---

1 : عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت ، مرجع سابق ، ص 223 .

2 : نفس المرجع ، ص 209 .

ترتكب الجريمة من خلاله عبارة عن معلومة تتدفق بطريقة غير مرئية وهذه المعلومة والتي تعكس معنى معين يمكن التحكم في دلالتها عن طريق البرمجة<sup>1</sup> .

إن هذه الفروض في التزوير المعنوي تخالف الرأي الذي يعتبر أن تزوير الوثيقة المعلوماتية لا يتم إلا بالطرق المادية عن طريق الحذف أو الإضافة أو التعديل، أو الإصطناع، أو تزوير التوقيع أو الصورة ، فالتزوير بالطرق المعنوية في هذه الوثيقة وارد باعتبار أن إنشاءها من طرف الموظف العام المكلف قانونا بذلك قد يمنحه فرصة تغيير المعطيات التي تلاقاها من ذوي الشأن خلال مرحلة الإدخال، تماما مثلما قد يفعل عندما يحررها على ورقة ، حيث يقوم النظام المعلوماتي بمعالجتها وتخزينها، أو إخراجها عن طريق مخرجات الجهاز بذلك المضمون المزور .

إن إمكانية وقوع التزوير المعلوماتي بالطرق المعنوية وارد بصورة أكبر من التزوير المادي والسبب في ذلك جوهر أو حقيقة التزوير المعنوي والذي يتحقق بتشويه المعاني التي كان يجب أن يعبر المحرر عنها، فهو تزوير يؤدي إلى تغيير مضمون أو دلالة المحرر ذاته، فضلا عن أنه لا يتضمن آثار مادية تشير بجلاء إلى العبث بالمحرر ولذلك لا يستدل عليه إلا إذا تم التوصل إلى حقيقة ما كان يجب إثباته وذلك للوصول إلى أن ما تم مخالف للحقيقة ، هذا فضلا عن أن التزوير المعنوي مصاحب لإنشاء المحرر المزور ذاته<sup>2</sup> .

---

1 : عبد الفتاح بيومي حجازي ، مرجع سابق، ص 222 .

2 : نفس المرجع ، ص 222 .

### ثالثا : بيان الأدلة في عدم حصر طرق التزوير في الوثيقة المعلوماتية

إن الطرق المذكورة في التزوير ليست على سبيل الحصر في جريمة التزوير المعلوماتية، لأن هذه التكنولوجيا متطورة ، وأشكالها متغيرة بشكل سريع ، ولذلك لا يناسب الصيغة التشريعية في تجريم تزوير الوثيقة المعلوماتية أن تكون دالة على حصر طرق التزوير فيها .

فالتزوير لم يعد مجرد حك في مضمون السند وتعديل لبعض كلماته أو تحشيه له بعبارات إضافية أو حذف لبعض العبارات أو صنع سند أو تدوين أقوال غير التي صدرت عن المتعاقدين أو إثبات وقائع كاذبة على أنها صحيحة أو تحريف وقائع . هكذا يتجاوز التزوير الإلكتروني التزوير الورقي ، وإن كان هو نفسه في المفهوم الوظيفي لناحية تحريف الحقائق أو البيانات، لكنه في الجانب التقني لا يقتصر فقط على معالجة الدعامة الورقية الملموسة المقروءة، بل يتطلب التعامل مع تقنيات المعلوماتية والشرائح الإلكترونية ومختلف العناصر الجزئية الإلكترونية أو المكملة لها<sup>1</sup> .

إن طرق التزوير حتى وإن اتصلت بوثيقة ورقية لم تكن واردة على سبيل الحصر في الصيغ التشريعية الجنائية الغربية والعربية في نظر بعض الفقهاء<sup>2</sup> ، رغم أن أغلب الفقه يرى أن فعل تغيير الحقيقة لا يدخل في دائرة التجريم، إلا إذا تم باحدى الطرق المنصوص عليها قانونا، باعتبار أن التزوير يعتبر كذب مكتوب، وحظر مطلق الكذب قاعدة خلقية لا قانونية،

---

1 : وسيم شفيق الحجار، الإثبات الإلكتروني. مكتبة صادر ناشرون ، د . م ، 2002 ، ص . ص 98 ، 99 .

2 : من بين هؤلاء : عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص

فالكذب ولو ترتب عليه ضررا بالغير، عملا مباحا في نظر القانون الجنائي متى كان بسيطا مجردا يفتن إليه كل شخص عادي في ادراكه لكن الأمر ليس كذلك حين يكون الكذب جسيما بحيث يعد احتيالا على الناس كما في النصب، أو يؤكد ذلك الإحتيال بمستند يظهر فيه الكذب وتغيير الحقيقة كما في التزوير<sup>1</sup>.

إلا أن الناظر في منهج التشريعات الجنائية المعاصرة يجد أن بعضها\* قد تخطى عن صيغة تحديد طرق التزوير عند تجريم الفعل في قانون العقوبات، خاصة بعد استيعابها فعل تغيير الحقيقة في وثيقة معلوماتية، وبالتالي لم يعد حصر طرق التزوير ذو دلالة أو أثر في تقرير وقوع التزوير من عدمه، ذلك أن العلة من تجريم هذا الفعل هو المساس بالثقة في الوثائق ذات القيمة القانونية، ومتى اهتزت هذه الثقة بأي طريقة كانت بتغيير الحقيقة فيها، وبالتالي عدم الإطمئنان إليها خاصة إذا كانت وثائق رسمية، اعتبر الفعل تزويرا مهما كانت الطريقة التي ارتكب بها.

وهذا الاتجاه له ما يقابله في الفقه<sup>2</sup> والقضاء، ففي مصر اعتبر التقليد والاصطناع من طرق التزوير في اجتهاد الفقه والقضاء رغم عدم ذكرهما في النصوص المتعلقة بالتزوير، ولو كان صحيحا أن طرق التزوير قد جاءت على سبيل الحصر لكان موقفهما بالغ الحرج، لأن مبدأ

---

1 : عبد الرحمن عبد الله حميد آل علي، مرجع سابق، ص 89 .

\* : قانون العقوبات الفرنسي المعدل عام 1993 (المادة 1/441)

2 : - عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 230. عوض محمد، مرجع سابق، ص 194 .

الشرعية والذي يعني أنه لا جريمة ولا عقوبة إلا بنص، لا يسوغ لأحد أن يضيف إلى طرق التزوير التي جرمها المشرع طرقاً أخرى لم ينص عليها ، والقاعدة أن الأصل في الأشياء الإباحة<sup>1</sup> .

كما اعتبر القضاء أن طرق التزوير التي نص عليها القانون تندرج جميعها تحت مطلق التغيير بتغيير الحقيقة التي يعاقب عليها القانون ، ولم يميز المشرع بين طريقة وأخرى من هذه الطرق بل سوى بينها جميعاً<sup>2</sup> .

### الفرع الثاني : الضرر

الضرر في جريمة التزوير هو من العناصر اللازمة لقيام الركن المادي، بل إن بعض الفقه<sup>3</sup> يرى بأنه ركن مستقل في هذه الجريمة نظراً لتلك الأهمية، حيث إن هذه الجريمة لا تقوم بدون حصول الضرر، وسواء كان الضرر عنصر من عناصر الركن المادي أو ركناً مستقلاً لدى القائلين بذلك، فإن له مدلول معيناً في هذه الجريمة .

### أولاً : مدلول الضرر

إن الركن المادي لجريمة التزوير لا يكتمل إلا إذا أصاب تغيير الحقيقة أمراً يحدث التغيير

---

1 : عبد الفتاح بيومي حجازي ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت ، مرجع سابق ، ص 230 .

2 : أحمد خليفة الملط ، مرجع سابق ، ص 436 .

3 : محمود نجيب حسني ، مرجع سابق ، ص 282 - علي جبار الحسيناوي، جرائم الحاسوب والإنترنت . دار اليازوري، عمان ، الأردن ، 2009 ، ص 70 .

فيه لو استعمل المستند ، ضرارا فعليا أو محتملا بمن يحتج بالمستند عليه . ذلك لأن القانون لا يكثرث بمجرد الكذب الذي لا يضر أحد منه <sup>1</sup>.

ولذلك فإن قيام الركن المادي مرتبط بتحقق ضرر معين أو مجرد احتمالية و قوعه، والضرر المحقق هو الضرر الواقع فعلا، وهو لا يكون له محل إلا باستعمال المحرر المزور، جاعلا من هذا الاستعمال جريمة قائمة بذاتها<sup>2</sup>، ويكون الضرر مجتملا متى كان يمكن تحققه في المستقبل أمرا منتظرا وفقا لمجرى الأمور العادي<sup>3</sup>.

ومجرد تغيير الحقيقة في الورقة الرسمية يتحقق بها ركن الضرر فإن كل عبث بها ينال من الثقة والاحترام الواجبين بها<sup>4</sup>. ولذلك فإن تاريخ تقدير توافر الضرر هو وقت حصول تغيير الحقيقة ، فلو حدث هذا التغيير دون وقوع الضرر رغم أنه كان محتمل الوقوع وقت تمامه ، فإن جريمة التزوير قائمة<sup>5</sup>، بل حتى لو قام سبب ينفي كل احتمال للضرر بعد حدوث التغيير كإعدام المحرر، أو موافقة صاحب الامضاء بعد التزوير، أو تنازله عن الورقة المزورة<sup>6</sup>.

ولذلك يكفي في بيان الضرر في جريمة التزوير أن تكون الورقة المزورة من الأوراق الرسمية، فالضرر في تزوير هذه الاوراق ينتج بالضرورة من الاعتداء الواقع على الثقة العامة<sup>7</sup>.

---

1 : أحمد محمود خليل ، مرجع سابق ، ص 111 .

2 : عمر السعيد رمضان ، مرجع سابق ، ص 163 .

3 : إيهاب فوزي السقا ، مرجع سابق ، ص 57 .

4 : فتوح الشاذلي ، عفيفي كامل عفيفي ، مرجع سابق ، ص 256 .

5 : عبد الرحمن عبد الله حميد آل علي ، مرجع سابق ، ص 161 .

6 : إيهاب فوزي السقا ، مرجع سابق ، ص 57 .

7 : Cour de Cassation ,Chambre Criminelle, 24 mai 2000 .

هذا يعني أن مدلول الضرر في جريمة تزوير الوثيقة الرسمية قائم على أساس قانوني وهو الانتقاص من الثقة العامة التي تتمتع بها وبالتالي الإخلال بقيمتها القانونية، باعتبار أن الضرر هو كل إخلال أو احتمال الإخلال بمصلحة يحميها القانون، وتلك المصلحة في جريمة التزوير هي حماية الثقة العامة في الوثائق التي لها قيمة قانونية .

وعندما ينجم عن هذا الإخلال مساس بالذمة المالية للمضرور على نحو يؤدي لإنقاص عناصرها الإيجابية أي الحقوق ، وتحصيلها بالالتزامات أي يزيد عناصرها السلبية يكون الضرر مادياً<sup>1</sup> ، وهو نفس مدلول الضرر المادي الذي يقترن بعمل غير مشروع مدنيا ، والذي يعرف بأنه الإخلال بمصلحة للمضرور ذات قيمة مالية<sup>2</sup> .

أما الضرر المعنوي فهو الذي يصيب المضرور في شعوره أو عاطفته أو كرامته أو شرفه أو أي معنى آخر من المعاني التي يحرص الناس عليها<sup>3</sup> ، وفي معناه الواسع هو مجموع الإعتداءات التي لا تؤثر مباشرة في الذمة المالية<sup>4</sup> .

ويعتبر ضرراً خاصاً ذلك الإخلال بمصلحة خاصة لشخص أو أشخاص معينين ، أما

الضرر العام فهو الإخلال بمصلحة من مصالح المجتمع ككل .

---

1 : عبد الرحمن عبد الله حميد آل علي ، جرائم تزوير المعلوماتية - دراسة تحليلية تأصيلية، مرجع سابق ، ص 161 .

2 : عبد الرزاق أحمد السنهوري ، الوسيط في شرح القانون المدني الجديد، المجلد الثاني . منشورات حلبي الحقوقية، ط3، بيروت ، 1998 ، ص 965 .

3 : نفس المرجع ، ص 976 .

4 : Philippe pierre, "L'indemnisation du préjudice moral en Droit Français ", S , D, ([www.fondation-droit-centimental.org/préjudice-moral-étude-fr](http://www.fondation-droit-centimental.org/préjudice-moral-étude-fr)).

ومهما كان نوع الضرر فإن قيامه لازم عن طبيعة التزوير في المحرر الرسمي لأن تغيير الحقيقة فيه بطريق الغش بالوسائل التي نص عليها القانون، ينتج حتما حصول ضرر بالمصلحة العامة لما يترتب على العبث بالورقة الرسمية من تقليل لقيمتها في نظر الجمهور لحسابها ذات حجية<sup>1</sup> .

ولذلك فإن التزوير قائم حتى إذا تم تغيير الحقيقة في ورقة رسمية باطلة شكلا لإحتمال حصول الضرر للغير أو المجتمع، إذ المحرر الباطل وإن جرده القانون من كل أثر له فإنه قد تتعلق به ثقة الغير ممن لا يتضح أمامهم ما يشوبه من عيوب ويصح أن ينخدع فيه كثير من الناس الذين يفوتهم ملاحظة ما فيه من نقص ، وهذا وحده كاف لتوقيع حصول الضرر بالغير بسبب هذا المحرر<sup>2</sup> .

### ثانيا : مدى خصوصية الضرر في جريمة تزوير الوثيقة المعلوماتية

لقد اختلف في تحديد مدلول الضرر في جريمة تزوير الوثيقة المعلوماتية، حيث انقسم الفقه إلى اتجاهين أحدهما يربط مدلول الضرر بالوصف القانوني للوثيقة المعلوماتية، وبالتالي يضيق من مدلوله، أما الرأي الثاني فيربط مدلول الضرر بما هو واقع وهو الخسارة الناتجة عن التزوير .

---

1 : أحمد خليفة الملط ، مرجع سابق ، ص 445 .

2 : نفس المرجع ، ص 445 .



## 1- المدلول القانوني للضرر :

يربط هذا الإتجاه الفقهي قيام الضرر بمدى وقوع التزوير في وثيقة معلوماتية لها قيمة قانونية في الإثبات، وقد أعدت لذلك منذ نشوئها، وهو ما يتفق مع نظرية "جارو" حول الضرر كعنصر من عناصر الركن المادي في تزوير الوثيقة الورقية، حيث يرى الفقيه "جارو" أن الضرر لا يقوم إلا إذا وقع التزوير في محرر أعد أساسا كأداة لإثبات الحقوق والمراكز القانونية. وهذا الجوهر في نظرية "جارو" يتفق مع أنصار التضييق في التزوير المعلوماتي، الذين يرون تحري النصوص وعدم الخروج عليها <sup>1</sup> .

فالتزوير المعلوماتي مرتبط بتزوير معطيات لإستخدامها في انتاج آثار قانونية، فإن تخلف ذلك المضمون فإن الأمر يتعلق بإتلاف معطيات معلوماتية، أو بتعطيل سير النظام المعلوماتي. ولذلك فالضرر في جريمة التزوير المعلوماتي لا يبدو كأمر جلي، ولكن كعنصر ضمني، حيث تزوير تلك المعطيات التي لها قيمة قانونية يرتب ضررا، بحسب طبائع الأشياء<sup>2</sup>. وينتمي لهذا الإتجاه الفقيه "جاسن" الذي قسم الإتجاهات الفقهية في تحديد مدلول الضرر إلى اتجاهين ، حيث يتبنى الإتجاه الأول مفهوما ضيقا للضرر وهو أن تكون الوثيقة الذي وقع تغيير الحقيقة فيها ذات بعد قانوني، أي أن يكون لها قيمة في الإثبات وفقا للقواعد التي تحكم تزوير المحررات ، وهو الإتجاه الذي يميل إليه هذا الفقيه<sup>3</sup>، في مقابل الإتجاه الثاني الذي يأخذ

---

1 : عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 248 .

2 : Nadina Velicu, Marcel Podasca, Le combat contre la criminalité informatique dans le contexte Europeen, S.D, ([www.proceeding.univ-danubius.ro](http://www.proceeding.univ-danubius.ro)), p 233 .

3 : بلال أمين زين الدين، مرجع سابق ، ص 360 .

بالمفهوم الواسع للضرر، والذي يقوم على الخسارة الناتجة عن تغيير الحقيقة في الوثيقة دون النظر إلى قيمتها في الإثبات .

## 2- المدلول الواقعي للضرر :

رغم أن أساس نظرية جارو هو مدى المساس بالقيمة القانونية للوثيقة كدليل إثبات، حيث لاوجود للضرر إلا إذا أصاب القيمة الثبوتية للوثيقة، وذلك لعدة تجريم تزوير الوثيقة الرسمية وهي قيمتها في إثبات العلاقات القانونية، إلا أن هذه النظرية تضمنت ما يسمى بحالة الدليل العارض إحتياطاً، حيث إن الضرر يتحقق في حال تزوير وثيقة ليست معدة ابتداء كدليل إثبات ولكن يمكن اتخاذها كذلك في ظروف معينة، وهو ما يتفق مع المدلول الواقعي للضرر الذي أخذ به الإتجاه الفقهي الثاني، حيث ربط الضرر بالخسارة المترتبة عن التزوير .

ولذلك فالضرر قائم كلما كان هناك خسارة، حتى ولو لم يكن المحرر قد أعد أصلاً للإثبات، بمعنى أنه لا يشترط أن يكون المحرر المزور أصلاً أداة للإثبات ولكن يكفي أن يصلح كذلك في ظروف معينة، والرأي الذي حاول التوسع في فكرة التزوير المعلوماتي وربط الضرر بحصول خسارة مترتبة عليه، هو في الوقت ذاته يتفق مع الفقيه " جارو " الذي تحوط حين قال بنظريته عن الضرر فأخذ بفكرة " الدليل الطارئ " وكان هدفه المصلحة العامة، فهو لا يرغب في أن يترك تقدير الضرر مطلقاً بيد القاضي حفاظاً على المصلحة العامة، وفي الوقت ذاته يرغب في ألا يفلت مزور بدعوى أن تزويره لم يترتب عليه ضرر<sup>1</sup>.

---

1 : عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 249 .

إلا أننا نأخذ في جريمة تزوير الوثيقة الرسمية الإدارية المعلوماتية بالمدلول القانوني للضرر، على اعتبار أن هذه الوثيقة تتمتع بقيمة قانونية في الإثبات ابتداءً أي منذ نشوئها، والضرر في هذه الحالة مفترض من الناحية القانونية باعتبار أن هذه الوثيقة تنبعث منها ثقة عامة عند الأفراد.

### المطلب الثاني : الركن المعنوي

لا تكتمل جريمة التزوير في وثيقة معلوماتية إلا إذا توافر الركن المعنوي إلى جانب الركن المادي على غرار باقي الجرائم، وتعتبر هذه الجريمة من الجرائم العمدية حيث لا بد من توافر القصد الجنائي، غير أنه لا يكفي وجود القصد العام فقط، وإنما لا بد من توافر قصد خاص، وهو ما سنبينه في الفرعين الموالين :

#### الفرع الأول : القصد العام

يقوم القصد الجنائي في جريمة التزوير إذا انصرفت إرادة الجاني إلى تغيير الحقيقة في المحرر باحدى الطرق التي بينها القانون مع توقعه احتمال حدوث ضرر مادي أو أدبي نتيجة لهذا الفعل<sup>1</sup>.

فالقصد العام يقوم على عنصري العلم والإرادة، وعنصر العلم يرتبط بعلم الجاني أنه يغير الحقيقة في محرر يحظى بحماية القانون، يستوي في ذلك أن يكون المحرر ورقيا أو وثيقة معلوماتية، ولذلك فإن عدم علم الجاني أنه يغير الحقيقة في محرر يتمتع بحماية القانون ينفي

---

1 : عمر السعيد رمضان، مرجع سابق، ص 294.

القصد الجنائي لديه<sup>1</sup> ، وهذا العلم مفترض فلا يدفع مسؤوليته عن ذلك بجهله<sup>2</sup> . إذ يفترض علم الجاني أن ما حصل من تغيير الحقيقة فيه يعتبر محررا في نظر القانون، وإن هذا التغيير قد حصل بطريقة من الطرق المنصوص عليها في القانون<sup>3</sup> .

كما يجب أن يدرك الجاني أنه يغير الحقيقة في محرر<sup>4</sup> .

وفي جريمة تزوير الوثيقة الرسمية الإدارية المعلوماتية يتوافر القصد العام بانصراف إرادة الجاني إلى تغيير الحقيقة في وثيقة رسمية إدارية معلوماتية، مهما كانت الطريقة التي استخدمها لإيقاع التغيير حيث لم تعد هذه الطرق محصورة كما هي في جريمة التزوير في وثيقة ورقية، وهذا هو الإتجاه الحديث للتشريعات المقارنة من أجل تحقيق المرونة في الصيغة التشريعية لتجريم التزوير، بما ينسجم مع التعدد التقني لأشكال الوثيقة المعلوماتية ووسائل تغيير الحقيقة فيها، وكذا التطور المستمر في ذلك .

ولكن يجب أن يرتبط علم الجاني بأنه يغير الحقيقة في وثيقة لها قيمة قانونية، ولذلك هي تتمتع بالحماية القانونية ضد هذا التغيير. ويفترض علم الجاني أن ما قام به من تغيير للحقيقة قد تم فيما يعتبر وثيقة من الناحية القانونية، حيث لا أثر لطبيعتها المعلوماتية في اعتبارها كذلك قانونا، ولا أثر لطبيعة الوسيلة أو الطريقة التي تم بها التغيير\* .

---

1 : عبد الفتاح بيومي حجازي، الحكومة الإلكترونية، الكتاب الثاني ، مرجع سابق ، ص 249 .

2 : فتوح الشاذلي، عفيفي كامل عفيفي ، مرجع سابق ، ص 258 .

3 : أحمد خليفة الملط، مرجع سابق ، ص 475 .

4 : Robert Louis Garron, op . cit , p 9 .

\* : Cour de Cassation , Chambre Criminelle, 3 mai 1995 .

فالقصد الجنائي العام بعنصره العلم والإرادة يجب توافره لدى الجاني حتى يمكن نسبة جريمة التزوير المعلوماتي إليه<sup>1</sup> ، حيث يجب أن يكون عالما بأن إدخال المعلومات والبيانات إلى مضمون المحررات أو نحو تلك المعلومات أو تحويلها و إتلافها أو القيام بأية أفعال أخرى من شأنها أن تؤدي إلى التأثير على المجرى الطبيعي لمعالجة البيانات. فإذا كان جاهلا بأن الفعل الذي يرتكبه غير مشروع فلا يتحقق القصد<sup>2</sup>.

### الفرع الثاني : القصد الخاص

لا يكفي لقيام الركن المعنوي توافر القصد العام، إذ لا يكفي توافر الإرادة والعلم بمكونات الجريمة، بل لابد أن تكون نية الجاني قد اتجهت وقت ارتكاب هذا الفعل إلى استعمال المحرر المزور فيما زور من أجله، أي إلى الإحتجاج به على اعتبار أنه صحيح<sup>3</sup>.

وتعتبر صيغة النص الجنائي الفرنسي في تجريم التزوير من الصيغ الواضحة في تطلب هذا القصد، حيث يشير النص إلى ضرورة وقوع التزوير بنية الغش، أي أن تكون نية الجاني من التزوير التأثير في إثبات حق أو واقعة لها آثار قانونية، ويعني ذلك أن المشرع الفرنسي يتطلب في الجريمة توافر قصد عام لدى الجاني ، كما تطلب أيضا توافر قصد خاص قوامه غرض الجاني التأثير في إثبات حق أو واقعة قانونية<sup>4</sup> ، ولذلك نصت المادة 1/441 من قانون العقوبات الفرنسي على :

---

1 : خالد محمد كدفور المهيري، مرجع سابق ، ص 685 .

2 : نزيه عبد اللطيف ، " التزوير المعلوماتي " ، 9 يوليو 2011 ، ( <http://nazihabdellatif.blogspot.com / 2011/> ) ، (blog - spot-09 html

3 : إيهاب فوزي السقا ، جريمة التزوير في المحررات الإلكترونية، مرجع سابق ، ص 59 .

4 : أشرف توفيق شمس الدين، مرجع سابق ، ص 114 .

"Constitue un faux toute altération frauduleuse de la vérité, de nature a causer un préjudice et accomplie par quelque moyen que ce soit , dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques " .

أما المشرع المصري فلم يحدد نوع القصد الذي يتطلبه لدى الجاني، وما إذا كان يكفي بالقصد العام أم أنه يتطلب إضافة إليه القصد الخاص ، وقد خلت نصوص التجريم من فكرة سوء النية أو الخداع أو الغش<sup>1</sup> .

ويتضح ذلك بالرجوع إلى المادة 23 من قانون التوقيع الإلكتروني في الفقرة ب ، حيث جرم المشرع المصري الإعتداء على المحرر الإلكتروني بالتزوير، لكنه لم يبين نية الغش، إذ نصت هذه المادة على "أُتلف أو عيب توقيعاً أو وسيطاً أو محرر الكترونياً، أو زور شيئاً من ذلك بطريقاً لإصطناع أو التعديل أو التحويل و بأي طريق آخر " .

ويستدل على ضرورة توافر القصد الخاص في جريمة التزوير، أن التزوير وإن كان يعاقب عليه على حدة مستقلاً عن الإستعمال إلا أنه لا خطر منه لو جرد من نية الإستعمال<sup>2</sup> .

أما على المستوى الدولي فقد أشارت المادة السابعة من اتفاقية بودابست حول الإجرام المعلوماتي إلى هذه النية الإجرامية .

---

1 : أشرف توفيق شمس الدين، مرجع سابق ، ص 115 .

2 : عبد الرحمن عبد الله حميد آل علي ، مرجع سابق ، ص 175 .

وقد أتاحت الإتفاقية للدول الأطراف فيها أن يشترطوا في قوانينهم الداخلية نية الغش في تغيير الحقيقة أو نية الإضرار بالغير أو أي نية إجرامية أخرى لازمة لتقرير المسؤولية الجنائية عن أفعال التزوير<sup>1</sup> .

## **المبحث الثاني : العقوبات المقررة لجريمة تزوير الوثيقة الرسمية الإدارية**

### **المعلوماتية**

إن بيان العقوبات المقررة في جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية يقتضي الرجوع إلى الصيغ التشريعية المجرمة لفعل التزوير في هذه الوثيقة، سواء كان هذا الفعل مجرماً بنصوص خاصة ، أو من خلال نصوص قانون العقوبات . كما يقتضي الأمر أحياناً لتحديد العقوبة المناسبة، ربط النصوص الخاصة بنصوص قانون العقوبات في حال وجود عقوبات أشد منصوص عليها في هذا القانون .

### **المطلب الأول : العقوبات المقررة بنصوص خاصة**

إنتهج المشرع الإماراتي والمصري منهجاً معيناً في تجريم التزوير المعلوماتي ، حيث جرماً هذا الفعل في قوانين منفصلة عن قانون العقوبات كما بينا في الفصل الأول ، ولذلك فإن بيان العقوبات المقررة لهذه الجريمة سيكون من خلال النصوص الواردة في تلك القوانين، مع الرجوع إلى صيغة العقاب في قوانين العقوبات المتعلقة بجريمة التزوير إذا تطلب الأمر ذلك .

---

1 : بلال أمين زين الدين ، مرجع سابق ، ص . ص 363 ، 364 .

## الفرع الأول : العقوبات المقررة في قانون التوقيع الإلكتروني المصري

عاقب المشرع المصري على فعل تزوير الوثيقة المعلوماتية بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو باحدى هاتين العقوبتين، وذلك في المادة 23 من قانون التوقيع الإلكتروني، إلا أنه يجب مراعاة تطبيق العقوبة الأشد المنصوص عليها في قانون العقوبات أو أي قانون آخر .

ولذلك نصت هذه المادة على : "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 باحدى هاتين العقوبتين كل من : - أتلف أو عيب توقيعاً أو وسيطاً أو محرراً الكترونياً أو زور شيئاً من ذلك بطريق الإصطناع أو التعديل أو التحويل أو بأي طريق آخر ."

ولذلك يستنتج من هذا النص أن عقوبة تزوير المستند الإلكتروني في مصر تختلف بحسب نوع المستند الإلكتروني المزور<sup>1</sup> .

فالتزوير في الوثيقة المعلوماتية الرسمية الإدارية يعاقب عليه بعقوبة أشد ، ومن ذلك التزوير الواقع في وثيقة من وثائق الأحوال المدنية والتي لها طبيعة معلوماتية، حيث اعتبرها المشرع المصري وثائق رسمية من خلال ما نص عليه في قانون الأحوال المدنية في المادة 72

---

1 : محمد أمين الرومي، المستند الإلكتروني، مرجع سابق ، ص 87 .



منه، التي نصت على : " في تطبيق أحكام هذا القانون وقانون العقوبات تعتبر البيانات المسجلة بالحاسبات الآلية وملحقاتها بمراكز معلومات الأحوال المدنية ومحطات الإصدار الخاصة بها المستخدمة في إصدار الوثائق وبطاقات تحقيق الشخصية بيانات واردة في محررات رسمية .

228 فإذا وقع تزوير في المحررات السابقة أو غيرها من المحررات الرسمية تكون العقوبة الأشغال الشاقة المؤقتة أو السجن لمدة لا تقل عن خمس سنوات" .

ولذلك فإن عقوبة التزوير في مستند الكتروني قد تكون هي العقوبة المنصوص عليها في المادة 23 من قانون التوقيع الإلكتروني، وقد تكون عقوبة أشد من الحبس والغرامة في حالات أخرى، وذلك إذا كان قانون العقوبات أو أي قانون آخر من قوانين الدولة يشدد العقوبة على تزوير مستند<sup>1</sup> . وهو مقتضى المادة 72 سابقة الذكر، حيث شددت العقوبة فيها إلى الأشغال الشاقة المؤقتة أو السجن لمدة لا تقل عن خمس سنوات، تبعا لطبيعة الوثيقة المزورة .

غير أن الملاحظ أن المشرع الجنائي المصري لم يكن موفقا في تحديد العقوبة المناسبة لجريمة تزوير الوثيقة المعلوماتية باتخاذها منها معينا في العقاب، من خلال تلك النصوص المنفرقة بين قانون التوقيع الإلكتروني، وقانون العقوبات، وقوانين أخرى، مما جعل صيغة العقاب مجتزأة، فليس هناك نصا جنائيا واحدا يبين تدرج العقوبة حسب طبيعة الوثيقة المعلوماتية المزورة .

---

1 : محمد أمين الرومي، مرجع سابق، ص 88 .

## الفرع الثاني : العقوبات المقررة في قانون مكافحة جرائم تقنية المعلومات الإماراتي

نصت المادة 04 من القانون 2006/02 المتعلق بمكافحة جرائم تقنية المعلومات على:

"يعاقب بالسجن المؤقت كل من زور مستندا من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية معترفاً به قانوناً في نظام معلوماتي .

وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين إذا وقع التزوير فيما عدا ذلك من المستندات إذا كان من شأن ذلك إحداث ضرر " .

لقد قرر المشرع الإماراتي لجريمة تزوير الوثيقة الرسمية المعلوماتية عقوبة السجن المؤقت كعقوبة أصلية ، سواء تعلق الأمر بوثيقة صادرة عن الحكومة الاتحادية أو المحلية باعتبارها تتمتع بقيمة قانونية ، وذلك عندما استخدم عبارة " معترفاً به قانوناً " .

ويرى المؤلف "أحمد عبد الواحد" أنه وفقاً للقاعدة العامة فإنه ينحسر مع هذه المادة إمكانية تطبيق المواد 217 و 217 مكرر، 222 من قانون العقوبات الاتحادي لوجود قانون خاص يعاقب على الفعل ذاته، إلا أن قانون مكافحة جرائم تقنية المعلومات قد نص في المادة 26 على: " لا يخل تطبيق العقوبات المنصوص عليها في هذا القانون بأية عقوبة أشد ينص عليها في قانون العقوبات أو أي قانون آخر "، وبذلك يكون القانون رقم 02 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات قد أحال إلى قانون العقوبات الاتحادي في تطبيق العقوبة متى كانت أشد من تلك الواردة فيه، ليكون القاضي في جريمة التزوير الإلكتروني واستعماله ممسكاً بالقانون رقم 02 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات في يد ويقانون العقوبات

الإتحادي في يد أخرى في معرض حكمه متحريا العقوبة الأشد الواردة في أي منهما ليقوم بتطبيقها على واقعة التزوير الإلكتروني<sup>1</sup> .

وتعتبر عقوبة السجن المؤقت كعقوبة سالبة للحرية من العقوبات الملائمة بطبيعة وجسامة جريمة التزوير، باعتبار أن هذه العقوبات هي من العقوبات المقررة للجرائم المخلة بالثقة العامة<sup>2</sup> .

أما بالنسبة للغرامة كعقوبة مالية فهي منصوص عليها في هذا القانون باعتبارها عقوبة اختيارية حيث يمكن الحكم بها مع عقوبة الحبس إذا تعلق الأمر بتزوير وثيقة معلوماتية غير رسمية ، وقد لا يحكم بها .

كما نصت المادة 24 من نفس القانون على عقوبة المصادرة حيث نصت على : " مع عدم الإخلال بحقوق الغير حسن النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها ، كما يحكم بإغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم إذا كانت الجريمة قد ارتكبت بعلم مالكة ، وذلك إغلاقا كلياً أو للمدة التي تقدرها المحكمة " .

---

1 : أحمد عبد الواحد أحمد آل علي ، مرجع سابق ، ص 143 .

2 : نزيه عبد اللطيف ، مرجع سابق ،

## المطلب الثاني : العقوبات المقررة في قانون العقوبات الفرنسي

صنف المشرع الفرنسي العقوبات المقررة لجريمة التزوير إلى أصناف تتناسب طردا مع طبيعة الوثيقة المزورة، ولذلك نظم المادة 441 من قانون العقوبات في عدة فقرات، حيث تختلف العقوبة فيما إذا كانت الوثيقة محل التزوير وثيقة رسمية إدارية، أو وثيقة عرفية، كما تختلف حسب صفة الشخص مرتكب التزوير .

### الفرع الأول : اختلاف العقوبة حسب طبيعة الوثيقة محل التزوير

إن فعل التزوير لا يعد جريمة إلا إذا انصب على وثيقة لها قيمة قانونية، ويتحقق ذلك دائما في حال كانت الكتابة عامة<sup>1</sup> .

وقد اعتبرت محكمة النقض الفرنسية فعل التزوير قائم في حال حذف واستبدال عبارات في سجل الحالة المدنية<sup>2</sup> .

هذه الوثائق لها حماية خاصة باعتبارها صادرة عن جهة إدارية عامة ، ولذلك تتفاوت العقوبات المقررة في حال تزويرها بحسب خطورة الآثار المترتبة على ذلك، باعتبار أن ذلك يؤدي إلى إضعاف الثقة العامة في مثل هذه الوثائق، وهي نتيجة خطيرة يجب مواجهتها بالعقوبة المناسبة على خلاف التزوير في الوثيقة العرفية، ولذلك شدد المشرع الجنائي الفرنسي العقوبة كلما اشتدت خطورة الفعل وذلك تبعا لنوع الوثيقة محل التزوير .

<sup>1</sup> : Philippe blueau, " le faux en ecriture publique ", courrier des maires , n° 249 , (Septembre 2011).

<sup>2</sup> : Cour de cassation, chambre criminelle, 18 octobre 2000 .

## أ- العقوبة المقررة في حال تزوير وثيقة صادرة عن إدارة عامة :

إن التزوير المرتكب في وثيقة صادرة عن إدارة عامة معاقب عليه طبقا للمادة 441-2  
فقرة 1 من قانون العقوبات الفرنسي بخمس سنوات سجن، وغرامة قدرها 75000 أورو، وهي  
العقوبة الأصلية المقررة، حيث تنص المادة المذكورة أعلاه على ما يلي :

" le faux commis dans un document délivré par une administration publique aux  
fins de constater un droit , une identité ou une qualité ou d'accorder une  
autorisation est puni de cinq ans d'emprisonnement et de 75000 euros d'amende" .

إن التزوير في هذه الحالة يتعلق بالوثيقة تثبت حقا أو واقعة، أو تمنح ترخيصا ، وهي  
صادرة عن جهة إدارية عامة، حيث يقع التغيير في الحقيقة بنية الغش ، أيا كان شكل الوثيقة،  
سواء كانت ورقية، أو بأشكال مستحدثة لإنشاء دليل يثبت حقا أو واقعة لها آثار قانونية .

ولما كانت الوثيقة محررة من إدارة عامة ، فإن ذلك يستتبع أن تكون العقوبة مرتفعة وهي  
خمس سنوات سجن، و75 ألف أورو غرامة، لحماية الثقة العامة التي تتمتع بها هذه الوثيقة .

في هذه الحالة يتعلق الأمر بتزويد الغير - بنية الغش - بوثيقة إدارية بهدف إثبات حق  
أو واقعة، كما هو الحال في تزوير التصاريح والرخص ، والشهادات .

وتعتبر هذه العقوبات أصلية، يمكن أن تلحق بها عقوبات تكميلية مثل المنع من ممارسة  
الحقوق المدنية، والأسرية، وكذا المنع من شغل الوظائف العامة .

## ب- العقوبة المقررة في حال تزوير وثيقة عامة أو رسمية :

يعاقب المشرع الجنائي الفرنسي على التزوير في وثيقة عامة أو رسمية طبقا للمادة 441-

4 فقرة 1 من قانون العقوبات، حيث تنص هذه المادة على ما يلي :

" Le faux commis dans une écriture publique ou authentique ou dans un enregistrement ordonné par l'autorité publique est puni de dix ans d'emprisonnement et de 150 000 € d'amende " .

يقصد في هذا النص بالوثائق العامة تلك الصادرة عن جهات حكومية ، وكذا الوثائق القضائية بمعنى الأحكام والقرارات .

إن التزوير في هذه الوثائق يأخذ أشكالا متعددة كتزوير وثائق ضريبية، أو محاضر شرطة، أو محاضر رسمية محررة من طرف موظف عام بمناسبة تأدية مهامه 1 .

أما الوثائق الرسمية فتشمل الوثائق الصادرة عن موظفين عامين مكلفين بتحرير مثل هذه الوثائق مثل الموثق باعتباره ضابط عمومي، أو المحضر وغيرهم .

## الفرع الثاني : اختلاف العقوبة حسب صفة المزور

إذا نظرنا إلى فعل التزوير بحسب صفة فاعله، فإننا نجد المشرع الجنائي الفرنسي قد رفع العقوبة في حال ارتكب جرم التزوير من طرف شخص يملك سلطة عامة، أو مكلف بتأدية خدمة عامة، في إطار آدائه لوظائفه أو مهامه، وذلك بمقتضى المادة 4/441 فقرة 3 من القانون الجنائي التي تنص على ما يلي :

---

1 : Cour de cassation, chambre criminelle, 28 Octobre 2003 .

" Les peines sont portées à quinze ans de réclusion criminelle et à 225 000€ d'amende lorsque le faux ou l'usage de faux est commis par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public agissant dans l'exercice de ses fonctions ou de sa mission".

إن العقوبة المقررة في حال تزوير وثيقة رسمية إدارية معلوماتية من طرف موظف عام أو مكلف بخدمة عامة ترتفع إلى 15 سنة سجن، كما ترتفع الغرامة إلى 225 ألف أورو، بحسب خطورة الفعل في هذه الحالة، ذلك أن تلك السلطة التي يملكها هذا الشخص، والتي حولها إياه القانون لتحرير مثل هذه الوثائق، تمكنه من ارتكاب التزوير، ويكون الأمر أيسر عندما تكون هذه الوثائق معلوماتية، حيث سيكون بالضرورة هذا الشخص من الأشخاص المرخص لهم أو المسموح لهم قانونا بالدخول إلى النظام المعلوماتي، لمعالجتها أليا\* .

تمتد عبارة "الأشخاص المخول لهم سلطة عامة" لتشمل كل من يملك سلطة اتخاذ القرار، وكذا الموظفين الممثلين للدولة، وكذا رؤساء المجالس البلدية ومساعدتهم<sup>1</sup> .  
ويختلف الأمر في هذه الحالة عن حكم المادة 441-6 التي تنص على :

" le fait de se faire délivrer indûment par une administration publique ou par un organisme chargé d'une mission de service public , par quelque moyen frauduleux que se soit , un document destiné à constater un droit, une identité ou une qualité ou à accorder une autorisation est puni de deux ans d'emprisonnement et de 30 000 euros d'amende" .

---

\* : وهو ما يحصل كثيرا في سجلات الحالة المدنية من طرف الضابط العمومي المكلف بها، حيث يرتكب التزوير في وثائق الحالة المدنية مثل شهادات الميلاد، والزواج، وشهادات الوفاة .

1 : Cour de Cassation, Chambre Criminelle , 27 février 1984 .

ففي هذه الحالة أحد الخواص هو الذي استخدم وسائل احتيالية من أجل الحصول على وثائق إدارية مزورة<sup>1</sup> .

## الفصل الثالث : صور خاصة لجريمة تزوير المعلومات

إن الوثيقة الرسمية الإدارية المعلوماتية تتخذ أشكالاً عديدة، فقد تكون عقداً، أو وثيقة هوية أو سفر، أو شهادة ميلاد أو وفاة، كما قد تأخذ شكل بطاقة الكترونية مثل بطاقات التأمين الصحي، بطاقات التعريف ، البطاقات الإئتمانية وغيرها .

وهذه الوثائق تقترب بتوقيع الكتروني يثبت صحتها ، ونسبتها إلى صاحبها ، ولذلك فإن هذا التوقيع على قدر من الأهمية مما يقتضي حمايته جنائياً من الإعتداءات التي قد تقع عليه، ومن أخطر هذه الإعتداءات تزوير هذا التوقيع .

كما أن حماية الوثيقة المعلوماتية ضد التزوير إذا كانت في شكل بطاقة الكترونية يقتضي بيان هذه الجريمة وتحديد عناصرها .

### المبحث الأول : جريمة تزوير التوقيع الإلكتروني

جرمت بعض التشريعات فعل تزوير التوقيع الإلكتروني في نصوص خاصة، وذلك بعد أن أصبح له نفس القيمة القانونية التي يتمتع بها التوقيع العادي، مثلما هو الحال في التشريع المصري .

---

<sup>1</sup> : Marie helene, " le faux et la preuve " , 09/03/2011, (www.blog avocat.fr/space/marie-helene.isern-real) .



## المطلب الأول : جريمة تزوير التوقيع الإلكتروني في التشريع المصري

جرم المشرع المصري فعل تزوير التوقيع الإلكتروني من خلال نصوص قانون التوقيع

الإلكتروني ، حيث نص في المادة 23/ب على معاقبة كل من : " أتلف أو عيب توقيعاً أو وسيطاً أو محرراً الكترونياً أو زور شيئاً من ذلك بطريق الإصطناع أو التعديل أو التحوير أو بأي طريق آخر " .

من خلال هذا النص سنحاول بيان أركان هذه الجريمة ، خصائصها ، وعلاقتها ببعض الجرائم المعلوماتية الأخرى .

### الفرع الأول : صيغة النص المجرم

يتضح من صيغة النص السابق أن المشرع المصري جمع عدة أنماط للسلوك الإجرامي الذي قد ينال التوقيع الإلكتروني إلى جانب التزوير في نص واحد ، مثل الإتلاف والتعيب ، رغم أنه أشار إلى طرق الإصطناع والتعديل والتحويل وهي من طرق التزوير . كما أنه جمع بين الإعتداء الواقع على التوقيع الإلكتروني ، وكذا المحرر الإلكتروني (الوثيقة المعلوماتية)، ولذلك سنبين عناصر الركن المادي لهذه الجريمة من خلال تحليل هذا النص .

### أولاً : شرح الركن المادي من خلال صيغة النص المجرم

يقوم الركن المادي بإتيان فعل من أفعال التزوير عن طريق الإصطناع أو التعديل أو

التحوير ، كإنشاء منظومة التوقيع الإلكتروني ونسبتها إلى شخص من الأشخاص<sup>1</sup> .

إن طرق الإصطناع أو التعديل أو التحوير كطرق يتم بها تزوير المعلوماتي بالنسبة للتوقيع الإلكتروني أو المحرر الإلكتروني لم ترد على سبيل الحصر لأن المشرع أضاف - أو بأي طريق آخر - ولذلك يقوم التزوير المعلوماتي، ومناطه تغيير الحقيقة في محرر أو غيره بطريقة معلوماتية أو الكترونية على نحو يحقق الإضرار بالغير<sup>2</sup> .

أما بالنسبة لطريقة التقليد فيرى "منير محمد الجنبهي" و "ممدوح محمد الجنبهي" أن التوقيع الإلكتروني لا يمكن تقليده، وإنما يمكن استعماله دون علم مالكة باعتباره يتم بواسطة منظومة الكترونية تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، فيما يتم تزوير التوقيع التقليدي بتقليد توقيع شخص آخر مما يعني أن التوقيع ذاته مختلف عن التوقيع الخاص بصاحبه، وذلك لأن التوقيع المقلد لا يمكن أن يكون بذات خواص التوقيع الأصلي وبالتالي لا يمكن أن يكون متماثل معه<sup>3</sup> .

أما في جريمة تزوير التوقيع الإلكتروني فإنه يتم الحصول على منظومة التوقيع الإلكتروني الخاصة بشخص آخر ، وبالتالي التوقيع الإلكتروني في حد ذاته صحيح لم يطرأ عليه تعديل أو تغيير، بل تم استخدامه دون رضا مالكة، حيث يكون الجاني قد تحصل على منظومة التوقيع الإلكتروني بطريق غير مشروع بنية استخدامها في توقيع وثائق معلوماتية .

---

1 : عبد الفتاح بيومي حجازي ، الوقيع الإلكتروني في النظم القانونية المقارنة، مرجع سابق ، ص 543 .

2 : نفس المرجع ، ص 544 .

3 : منير محمد الجنبهي ، ممدوح محمد الجنبهي، مرجع سابق ، ص 54.

ولذلك ف جريمة تزوير التوقيع التقليدي تختلف عن جريمة تزوير التوقيع الإلكتروني سواء في طريقة التزوير أو في أسلوب اكتشاف هذا التزوير، فطريقة الكشف عن التوقيع التقليدي المزور تكون عن طريق مضاهاة التوقيع المزيف بتوقيع الشخص المنسوب إليه هذا التوقيع، بينما في حالة تزوير التوقيع الإلكتروني لا يمكن استخدام تلك الطريقة لاكتشاف تزوير التوقيع، إذا أن التوقيع سليم لكنه ليس صادرا من الشخص مالك منظومة التوقيع الإلكتروني<sup>1</sup> .

إن الحصول على منظومة التوقيع الإلكتروني، والتوقيع بها كما لو كان التوقيع صادرا من صاحبه كثير الحدوث عندما يتعلق الأمر ببطاقات الإئتمان<sup>2</sup>، خاصة عندما يتعلق الأمر بالتعامل عبر شبكة الأنترنت، نظرا لحساسية البيانات عبر هذه الشبكة (من بينها رقم بطاقة الإئتمان) والتي قد تقع في أيدي القراصنة أو المتطفلين، وهو ما يضر بالثقة في التعامل<sup>3</sup>.

فالتوقيع السري المرتبط بالبطاقة الممغنطة يعتبر من صور التوقيع الإلكتروني، وهو استخدام مجموعة من الأرقام أو الحروف أو كليهما لتحديد هوية الموقع وشخصيته، ويتم تركيبها في شكل كودي معين بحيث لا يعلمها إلا صاحب التوقيع ومن يبلغه بها<sup>4</sup> .

---

1 : منير محمد الجنبهي ، ممدوح محمد الجنبهي ، مرجع سابق ، ص . ص 54 ، 55 .

2 : أعتبر أن أولى تطبيقات التوقيع الإلكتروني كانت معاصرة لإستعمال بطاقة الإئتمان في عمليات سحب النقود أو إجراء المشريات أو الحصول على الخدمات، ثم اتسعت لتشمل عمليات الشراء عن بعد، لتمتد إلى القيام بالإجراءات الإدارية (ثروت عبد الحميد ، مرجع سابق، ص 82 ) .

3 : ثروت عبد الحميد ، مرجع سابق ، ص 90 .

4 : حسين بن سعيد بن سيف الغافري، " الجرائم الواقعة على التجارة الإلكترونية " 2010/07/09، ( www.Mohamoon.com/ montada/ Default .asp

أما التوقيع الرقمي وهو أكثر أنواع التوقيعات الإلكترونية انتشاراً فإنه يرتبط بنظام التشفير، ولذلك فإنه قد يتعرض لكسر الشفرة والوصول إلى الأرقام الخاصة به، والقيام بنسخها وإعادة استخدامها بعد ذلك، وهي من أشهر الوسائل التي يمكن الإعتماد عليها في تزوير التوقيع الإلكتروني<sup>1</sup>.

إن التوقيع الرقمي يستخدم نظام التشفير بأسلوب المفتاح العام المزدوج وفق التالي<sup>2</sup>:

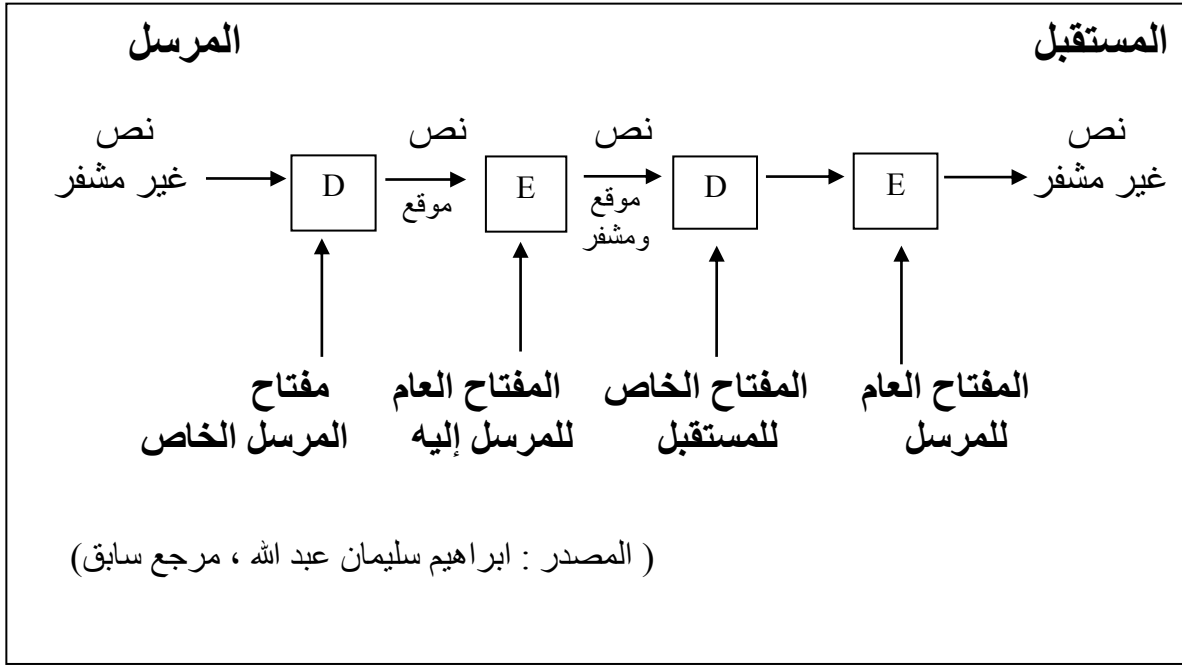
1. يقوم المرسل بوضع بصمة (علامة خاصة) ويتم تشفير هذه البصمة أو العلامة الخاصة باستخدام المفتاح الخاص للمرسل.
  2. يقوم المرسل بتشفير الرسالة باستخدام المفتاح العام للمرسل إليه.
  3. إرسال الرسالة باستخدام الشبكة.
  4. يستقبل المرسل إليه الرسالة ويقوم بفك شفرة الرسالة باستخدام المفتاح الخاص به وبالتالي يتمكن من قراءة الرسالة.
  5. يقوم المستقبل بفك بصمة المرسل باستخدام المفتاح العام للمرسل والتأكد من شخصيته.
- (أنظر الشكل رقم 11).

---

1 : حسين بن سعيد بن سيف الغافري، "الجرائم الواقعة على التجارة الإلكترونية"، مرجع سابق .

2 : ابراهيم سليمان عبد الله، "التجارة الإلكترونية أمن المعلومات"، ب.ت، (files/002379/ecom72www.kau.edu.sa).

شكل رقم (11) التوقيع الرقمي باستخدام نظام التشفير بأسلوب المفتاح العام المزدوج



لأن التوقيع الإلكتروني على رسالة ما، عبارة عن بيانات مجتزأة من الرسالة ذاتها يجري تشفيره وإرساله معها، بحيث يتم التثبت من صحتها من الشخص عند فك التشفير وانطباق محتوى التوقيع على الرسالة، وهكذا يرتبط التوقيع الإلكتروني بالتشفير ارتباطاً عضوياً، والتشفير عملية تغيير في البيانات، بحيث لا يتمكن من قراءتها سوى الشخص المستقبل وحده باستخدام مفتاح فك التشفير، وفي تقنية المفتاح العام يتوفر ذاته لدى المرسل والمستقبل ويستخدم في عمليتي التشفير وفك التشفير<sup>1</sup>.

1 : عماد محمد علي البلوي، جريمة تزوير التوقيع الإلكتروني دراسة وصفية لأساليب الكشف والتحقيق والتجريم، (مذكرة ماجستير في العلوم الشرطية)، قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009/10/28، ص 26 .

ولذلك فإن عملية التشفير بالمفتاح العام المستخدمة كتوقيع رقمي تعتمد على الخطوات

التالية<sup>1</sup> :

- 1- يولد كل مستخدم زوج من المفاتيح لإستخدامها في التشفير وفتح شفرة الرسائل .
  - 2- يضع كل مستخدم واحد من المفاتيح في سجل عام أو ملف آخر يمكن الوصول إليه وهذا يسمى المفتاح العام ، حيث يتم حفظ المفتاح الثاني بشكل سري ويسمى المفتاح الخاص.
  - 3- إذا رغب المستخدم (A) بإرسال رسالة خاصة إلى المستخدم (B) عند ذلك يقوم المستخدم (A) بتشفير الرسالة باستخدام المفتاح العام لـ (B) .
  - 4- عندما يستلم المستفيد (B) الرسالة فسيفتح الشفرة باستخدام مفتاحه الخاص. لا يستطيع أي شخص آخر أن يفتح الشفرة لأن المستخدم (B) هو الوحيد الذي يمتلك المفتاح الخاص .
- إن المفتاح السري يعتبر كمدخل لخوارزمية التشفير ، فهو قيمة منفصلة عن النص الأصلي المفهوم والواضح للرسالة وبناء عليه تنتج الخوارزمية مخرجات مختلفة اعتمادا على المفتاح السري المحدد الذي تم استخدامه في معادلة التشفير في وقت معين<sup>2</sup>. ولذلك فإن تزوير التوقيع الرقمي يقتضي الحصول على المفتاح السري، مما يجب معه لمقتضيات الأمان المحافظة على سرية هذا المفتاح من طرف مالكه .

---

1 : خضر مصباح اسماعيل الطيبي، أساسيات أمن المعلومات والحاسوب. دار الحامد، ط1، عمان، الأردن ، 2010 ، ص 242 .

2 : نفس المرجع ، ص 179 .

## ثانيا : طبيعة التوقيع الإلكتروني محل التزوير

لا يمكن القول بوقوع التزوير في توقيع الكتروني لا يتمتع بالحجية القانونية، فهو شرط جوهري وخاصية أساسية في هذا التوقيع ليكون مشمولا بالحماية القانونية ضد التزوير، ولذلك لا بد من الإعراف بهذه الحجية قانونا، وتوفير الشروط الفنية والتقنية ليؤدي التوقيع الإلكتروني الوظائف المنوطة به .

### 1- تمتع التوقيع الإلكتروني بالحجية القانونية

أعطى المشرع المصري للتوقيع الإلكتروني حجية في الإثبات عند استخدامه في المعاملات التجارية والمدنية والإدارية، حيث نص في المادة 14 من قانون التوقيع الإلكتروني على أنه في نطاق المعاملات المدنية والتجارية والإدارية يتمتع التوقيع الإلكتروني بذات الحجية المقررة للتوقيع التقليدي في قانون الإثبات، على أنه يجب مراعاة الضوابط الفنية والتقنية التي حددتها اللائحة التنفيذية لهذا القانون، وكذا الشروط التي نص عليها هذا القانون.

وقد نصت المادة 18 من قانون التوقيع الإلكتروني على شرط الموثوقية، إذ أن التوقيع

الإلكتروني لن يكون له أي قيمة بدون هذا الشرط ، والذي يتحقق بتوافر العناصر التالية :

1. إرتباط التوقيع الإلكتروني بالموقع وحده دون غيره .
2. سيطرة الموقع وحده دون غيره على الوسيط الإلكتروني .
3. إمكانية كشف أي تعديل أو تبديل في بيانات التوقيع الإلكتروني .

ويعتبر هذا النص إستجابة لمتطلبات المعاملات الإلكترونية التي تعتمد على الوثائق المعلوماتية الموقعة الكترونياً، وهو تجسيد للمادة 3/06 من قانون الأونسترال النموذجي للتوقيع الإلكتروني التي تنص على :

" يعتبر التوقيع الإلكتروني موثقاً به لغرض الوفاء بالإشترط المشار إليه في الفقرة (1) إذا: أ- كانت بيانات إنشاء التوقيع مرتبطة في السياق الذي تستخدم فيه بالموقع دون أي شخص آخر .

ب- كانت بيانات إنشاء التوقيع خاضعة وقت التوقيع لسيطرة الموقع دون أي شخص آخر .  
ج- كان أي تغيير في التوقيع الإلكتروني يجري بعد حدوث التوقيع قابلاً للاكتشاف .  
د- إذا كان الغرض من إشترط التوقيع قانوناً هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع، وكان أي تغيير يجري في تلك المعلومات بعد وقت التوقيع قابلاً للاكتشاف ."  
إن تفرد الموقع بالتوقيع الإلكتروني يقتضي ألا يستطيع أي شخص فك رموز التوقيع الخاص به أو الدخول عليه سواء عند استعماله لهذا التوقيع أو عند إنشائه<sup>1</sup> .

وتتحقق من الناحية الفنية سيطرة وتحكم الموقع وحده دون غيره على الوسيط الإلكتروني المستخدم في تثبيت التوقيع الإلكتروني عن طريق حيازة الموقع لأداة حفظ المفتاح الشفري الخاص المتضمن في البطاقة الذكية المؤمنة والرقم السري المقترن بها<sup>2</sup> .

---

1 : أسامة بن غانم العبيدي، " حجية التوقيع الإلكتروني "، المجلة العربية للدراسات الأمنية والتدريب ، العدد 56، ب.ت ، ص 165.

2 : محمد حسين منصور ، مرجع سابق ، ص 284 .



## 2- أداء التوقيع الإلكتروني لوظائفه :

يجب أن يؤدي التوقيع الإلكتروني وظائف أساسية وهي :

1. السرية .

2. التوثق من الهوية

3. سلامة البيانات

4. عدم القدرة على إنكاره .

ولتحقيق الخاصية الأولى لابد من حماية التوقيع الإلكتروني ضد الإستخدام غير المشروع،... وتتم هذه العملية بكون التوقيع الإلكتروني موجود على بطاقة ذكية ومحمي بكود سري ، بواسطة التشفير أثناء إرسال البيانات، وعدم إمكانية نسخ التوقيع الإلكتروني<sup>1</sup>.

ولذلك يرى " هشام محمد عبد الوهاب " مدير إدارة تراخيص التوقيع الإلكتروني في هيئة تنمية صناعة تكنولوجيا المعلومات أن هذا التوقيع ذو الحجية في القانون المصري ليس مجرد صورة للتوقيع العادي بواسطة الماسح الضوئي، أو بواسطة القلم الإلكتروني على أجهزة الحاسب<sup>2</sup> .

وقد ذكرنا أن التوقيع الإلكتروني يرتبط بنظام التشفير لحمايته من خلال المفتاح العام والخاص المثبتان على بطاقة الكترونية يحتفظ بها صاحب التوقيع، وتضمن شهادة التصديق

---

1 : هشام محمد عبد الوهاب، "الضوابط الفنية والتقنية لإضفاء ذات الحجية القانونية للتوقيعات الإلكترونية في القانون المصري"، 2008/12/31 ، ( signature.gov.egwww.electronic ) .

2 : نفس المرجع .

الإلكتروني التوثق من هوية الشخص الموقع بهذه المفاتيح، حيث تصدر هذه الشهادة من جهة تصديق الكتروني مرخص لها من هيئة تنمية صناعة تكنولوجيا المعلومات في مصر، كما تثبت هذه الجهة - كطرف ثالث محايد - صدور الوثيقة المعلوماتية من الشخص الموقع .

أما وظيفة المحافظة على سلامة البيانات فهي عملية حماية البيانات ضد التغيير، وتتم هذه العملية باستخدام تقنية تشفير البيانات ومقارنة بصمة الرسالة الأصلية ببصمة الرسالة التي تم إرسالها وتوقيعها الكترونياً، وفي حالة تطابق البصمتين فإن الرسالة المرسله والموقعة الكترونياً لم يتم التغيير في محتوياتها<sup>1</sup> .

ذلك أنه بعد توقيع الرسالة باستخدام المفتاح الخاص يتم تمريرها من خلال برنامج خاص بالتشفير في الحاسب الآلي حيث يقوم هذا البرنامج بتشفير المعاملة بعمليات حسابية معقدة تتحول بمقتضاها الرسالة المكتوبة إلى رسالة رقمية ، ولكي يتمكن مستلم الرسالة من قراءتها يتعين عليه أولاً فك شفرتها باستخدام المفتاح العام الذي يمكن إرساله إلى مستلم الرسالة وذلك من خلال جهة محايدة موثوق بها تقوم بدور الوسيط بين المرسل والمرسل إليه<sup>2</sup>. وهي سلطة التصديق التي تقوم بالتحقق من هوية الشخص الذي يستخدم شهادة رقمية تستطيع التعرف على الشخص وهويته من خلال ما تحويه من معلومات مهمة عن ذلك الشخص<sup>3</sup> .

---

1 : هشام محمد عبد الوهاب، مرجع سابق .

2 : أسامة عبيد، " التوقيع الإلكتروني "، 2009/09/02، (<http://knol.google.com/k/dressam-eibeed/-/228no>)

3 : غازي أبو عرابي، فياض القضاة، " حجية التوقيع الإلكتروني "، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، العدد الأول، (2004)، ص 185 .

وفي مجال المعاملات الحكومية التي يمكن إنجازها عن طريق الوسائل الإلكترونية، لابد لصحتها أن يتم استخدام التوقيع الإلكتروني المدعوم بشهادة توثيق معتمدة من إحدى جهات الإعتماد، حتى تستطيع الدائرة الحكومية أو المؤسسة التحقق من شخصية الشخص المتعامل معها <sup>1</sup> .

ويصبح هذا التوقيع مرتبط بوثيقة رسمية إدارية معلوماتية عندما يتم التوقيع به على مثل هذه الوثائق، مثل قيام مدير في مؤسسة بإرسال إعلان لموظفيه، حيث يقوم المدير عن طريق جهاز الحاسوب بإجراء العملية الحسابية التي تضمن سلامة المحتوى وتشفير المختصر الحسابي باستخدام مفتاح المدير الخاص وإرفاقه مع الإعلان، وإرسال الملف إلى جميع الموظفين. وعند استلام أحد الموظفين للإعلان يقوم بالتأكد من صحة التوقيع باستخدام المفتاح العام للمدير لفك التشفير واستخراج المختصر الحسابي الأصلي التي تم إرساله من قبل المدير مما يؤكد أن المرسل هو المدير <sup>2</sup> .

ولذلك فإن التوقيع الإلكتروني يتعرض للتزوير ممن لديهم خبرة باستخدام الحاسب الآلي، ومعرفة تقنية بالبرامج واستخداماتها، إذ قد يستطيعون الدخول إلى منظومات التوقيع الإلكترونية باستخدام برامج خاصة والإحتيال على تلك النظم وفك شفرات التوقيع الإلكتروني ومن ثم استخدامها في أغراض احتيالية عن طريق نسخها أو تزويرها ووضعها على محرر مزور <sup>3</sup> .

---

1 : غازي أبو عربي، فياض القضاة، مرجع سابق، ص 191 .

2 : أسامة عبيد ، مرجع سابق .

3 : محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت دراسة مقارنة. دار النهضة العربية، القاهرة ، ب ت ، ص . 240 . نقلا عن : أسامة بن غانم العبيدي ، مرجع سابق ، ص 151 .

الفرع الثاني : علاقة جريمة تزوير التوقيع الإلكتروني ببعض الجرائم المعلوماتية في قانون

### التوقيع الإلكتروني

إن التوقيع الإلكتروني كما ذكرنا يرتبط بشهادات التصديق الإلكتروني لتأكيد صحته، والوثوق به عند التوقيع على الوثائق المعلوماتية ، ولذلك لا بد من حمايته ضد فعل التزوير، أو أي من الأفعال التي قد تشكل اعتداء عليه ، والتي قد تكون لها علاقة بارتكاب التزوير في التوقيع .

ولذلك فقد جرم المشرع المصري مجموعة من الأفعال في قانون التوقيع الإلكتروني، وهي إصدار شهادة تصديق دون ترخيص ، إفشاء سرية البيانات ، اختراق الوسيط الإلكتروني أو الحصول على توقيع الكتروني بطريق غير مشروع .

### أولاً : جريمة إصدار شهادة تصديق الكتروني بدون ترخيص

لقد جرم المشرع المصري إصدار شهادة تصديق الكتروني دون الحصول على ترخيص بمزاولة النشاط من هيئة تنمية صناعة تكنولوجيا المعلومات، وهي الهيئة المخولة بذلك في مصر، وقد نص على تجريم هذا الفعل في المادة 23/أ كالتالي: "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" .

إن السبب في تجريم هذا الفعل هو الآثار الخطيرة التي تترتب على شهادة التصديق

الإلكتروني في حق الغير، حيث يكون مضمونها التسليم بصحة بيانات التوقيع الإلكتروني،...ومما لا شك فيه أن هذا السلوك يقضي على الثقة التي يجب توافرها في المعاملات الإلكترونية<sup>1</sup>، ومن ثم يتم التلاعب في بيانات التوقيع الإلكتروني التي تضمن صحتها هذه الشهادة .

غير أن المشرع المصري لم يكن دقيقا في حصر الأفعال التي قد تمس بالثقة في المعاملات الموقعة الكترونيا، وذلك بالنظر لمنهج التشريعات العربية المقارنة منها قانون التجارة الإلكترونية الإماراتي الذي جرم تزوير شهادة التصديق حماية للتوقيع الإلكتروني من خلال إنشاء شهادة تتضمن بيانات غير صحيحة مع العلم بذلك أو نشرها أو تقديمها، لأي غرض غير مشروع ، وقد ورد النص على هذه الجريمة في المادة 29 من هذا القانون .

ويتحقق فعل الإنشاء باختلاق الشهادة التي لا وجود لها، أما النشر فيكون بإنشاء شهادات غير صحيحة ثم استعمالها، والصورة الثالثة تتمثل في الحصول على شهادة منشأة لدى الغير، ثم مد الآخرين بها للإستعمال أو يستعملها الجاني لنفسه<sup>2</sup> .

وفي كل هذه الصور يكون الغرض غير مشروع أو إحتيالي ، حيث يتم التسليم بصحة بيانات التوقيع الإلكتروني .

---

1 : عبد الفتاح بيومي حجازي ، التوقيع الالكتروني في النظم القانونية المقارنة ، مرجع سابق ، ص 540 .

2 : نفس المرجع ، ص 320 .

كما جرم المشرع الإماراتي فعل تقديم بيانات مزورة لمزود خدمات التصديق ، وذلك في المادة 30 من القانون السابق الذكر، وهو ما لم ينص عليه المشرع المصري .

ويرى " د. عبد الفتاح بيومي حجازي " أن هذه الجريمة تقترب إلى حد ما من التزوير التقليدي، فقد ينتحل الجاني هوية غيره أو يبدل شخصيته<sup>1</sup> ، لإنشاء شهادة تصديق إلكتروني غير صحيحة .

### ثانيا : جريمة إنشاء سرية البيانات الإلكترونية

جرم المشرع المصري إنشاء سرية البيانات الإلكترونية في المادة 23/د بنصه على ما يلي: "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 :

د- خالف أيًا من أحكام المادتين (19) ، (21) من هذا القانون " .

وبالرجوع إلى المادة 21 المشار إليها نجدتها تنص على: "بيانات التوقيع الإلكتروني والوسائط الإلكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الإلكتروني سرية، ولا يجوز لمن قدمت إليه أو اتصل بها بحكم عمله إفشاؤها للغير أو استخدامها في غير الغرض الذي قدمت من أجله" .

إن إنشاء بيانات التوقيع الإلكتروني من طرف موظفي الجهة المرخص لها بإصدار

---

1 : عبد الفتاح بيومي حجازي ، التوقيع الإلكتروني في النظم القانونية المقارنة ، مرجع سابق ، ص 323 .

شهادات التصديق الإلكتروني بحكم عملهم الذي يمكنهم من الإطلاع على هذه البيانات، قد يؤدي إلى استخدام هذه البيانات دون رضا صاحبها، والتوقيع باسمه مما يشكل تزويراً، أو قد يستخدمها هذا الموظف استخداماً غير مشروع .

كما قد يؤدي ذلك إلى فض مفاتيح التشفير، خاصة ما يتعلق ببيانات المفتاح الخاص إذا قام هذا الموظف بكشف مفاتيح التشفير المودعة لدى جهة التصديق الإلكتروني، ذلك أن التشفير يلعب دوراً مهماً في المحافظة على سرية البيانات، كما يحمي التوقيع الإلكتروني ضد التزوير .

ولذلك فالجاني في هذه الجريمة شخص له صفة في تدوين البيانات التي تمت معالجتها وله علاقة مشروعة بالمعلومات، وقام بإفشائها للغير في غير الغرض المخصصة له، وإفشاء هذه المعلومات يعني إذاعتها أو نقلها وإطلاع الغير عليها، وإعلانها للكثير من الناس وخروجها من حيز الكتمان أو السرية بعد أن كان العلم بها قاصراً على أصحابها أو الذين ائتمنوا عليها بحكم وظيفتهم، وهم في هذه الجريمة، مزودي خدمة المصادقة الإلكترونية ومعاونيهم، والذين يقومون بدون علم ورضاء صاحبها بإفشاء سرها<sup>1</sup> .

### ثالثاً : جريمة الحصول على توقيع الكتروني بطريق غير مشروع

جرم المشرع المصري الحصول على توقيع الكتروني بطريق غير مشروع وذلك في المادة 23/هـ التي تنص على: "مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات

---

1 : عبد الفتاح بيومي حجازي ، التوقيع الإلكتروني في النظم القانونية المقارنة ، مرجع سابق ، ص 551 .

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 :

هـ- توصل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر الكتروني، أو اخترق هذا الوسيط أو اعترضه أو عطله عن أداء وظيفته ."

إن الحصول على التوقيع الإلكتروني بطريق غير مشروع قد يتم بصور مختلفة، فقد يقع عن طريق الإحتيال أو السرقة، كما قد يتم اختراق الوسيط الإلكتروني عن طريق الدخول إلى النظام المعلوماتي بأي وسيلة تقنية والحصول على بيانات التوقيع الإلكتروني بغير حق، ولذلك ترتبط هذه الجريمة بتزوير التوقيع الإلكتروني عند وجود نية استعمال منظومة التوقيع الإلكتروني - المتحصل عليها بطريق غير مشروع - في التوقيع على وثيقة رسمية إدارية دون علم ورضاء مالكيها .

### المطلب الثاني: خصائص جريمة تزوير التوقيع الإلكتروني

تتميز جريمة تزوير التوقيع الإلكتروني بخصائص تجعلها مختلفة عن جريمة تزوير التوقيع العادي بحكم البيئة الافتراضية التي تتم فيها، والوسائل التي ترتكب بها، مما يجعل هذه الجريمة تتميز بطبيعة مختلفة عن جريمة تزوير التوقيع العادي .

إن هذه الخصائص تتمثل في ارتباط جريمة تزوير التوقيع الإلكتروني بجريمة السرقة وجريمة الإختراق، وصعوبة الكشف عن التزوير، لإستخدام أساليب تقنية دقيقة مقارنة بالتزوير العادي.



## الفرع الأول : ارتباط جريمة تزوير التوقيع الإلكتروني بجريمة السرقة وجريمة الإختراق

إن التوقيع الإلكتروني هو منظومة مكونة من رموز وأرقام تميز صاحبها وتحدد هويته، ومن بين صور هذا التوقيع المعتمدة على فكرة الرموز نجد التوقيع الكودي أو السري الذي يرتبط غالبا بالبطاقات الممغنطة وغيرها من البطاقات الحديثة المشابهة والمزودة بذاكرة الكترونية ، ويتم تزويره بعد تعرضه للسرقة ، ثم استخدام الرقم والبطاقة في السحب <sup>1</sup> .

أما صورة التوقيع البيومتري فتعتمد على الخواص الذاتية للشخص كقزحية العين، بصمة الأصبع ، نبرة الصوت وغيرها ، حيث يتم التقاط صورة دقيقة لعين المستخدم أو بصمة يده أو صوته ثم تخزين بطريقة مشفرة في ذاكرة الحاسب الآلي والذي يقوم بمطابقة صفات المستخدم مع هذه الصفات المخزنة ولا يسمح له بالتعامل إلا في حال المطابقة ، لكن قد تتعرض هذه الصورة من التوقيع للإختراق بفك تشفير هذه البيانات ونسخها <sup>2</sup> .

كما يمكن التقاط أرقام البطاقات عبر شبكة الإنترنت بعد عملية اختراق واستخدامها باسم مالك البطاقة ، ففي عام 2004 أعلن مكتب التحقيقات الفيدرالي (FBI) أنه يحقق في حادث اختراق أجهزة كمبيوتر تم خلاله سرقة أرقام ثمانية ملايين بطاقة وفاء من شركة " Data processors international " ، وقد تستخدم تقنية تفجير الموقع التي تعتمد على ضخ مئات الآلاف من الرسائل الإلكترونية من جهاز القرصان إلى الجهاز المستهدف للتأثير على السعة

---

1: أمجد حمدان الجهني، "جرائم بطاقة الدفع الإلكتروني عبر شبكة الانترنت"، ب.ت، (<http://www.cojss.com/>)  
(replay.php?a=219

2: نفس المرجع .

التخزينية مما يشكل ضغطا يؤدي إلى تفجير الموقع وتشتيت البيانات المخزنة فيه، لنتقل بعد ذلك إلى جهاز القرصان ، ليتجول في الموقع بسهولة ، ويحصل على كل ما يحتاجه من أرقام وبيانات خاصة ببطاقات الوفاء<sup>1</sup> .

## الفرع الثاني : إستخدام أساليب تقنية في تزوير التوقيع الإلكتروني وصعوبة الكشف عنها

لقد أصبح للتوقيع الإلكتروني دورا واسعا في مجال المعاملات والتوقيع على الوثائق نتيجة الثورة التكنولوجية والإعتماد على المعلوماتية في إنجاز هذه المعاملات، ومنها تلك التي تتم في القطاع الحكومي، حيث اتجه الواقع إلى البحث عن بديل للتوقيع التقليدي يستطيع أن يؤدي ذات الوظيفة من ناحية ويتكيف مع وسائل الإدارة الحديثة من ناحية أخرى ، وهذا البديل يمكن أن يكون رقما سريا أو رمزا محددًا وهو ما يسمى بالتوقيع الإلكتروني أي التوقيع الناتج عن اتباع اجراءات محددة تكنولوجيا تؤدي في النهاية إلى نتيجة معينة معروفة مقدما فيكون مجموع هذه الإجراءات هو البديل الحديث للتوقيع بمفهومه التقليدي وهو ما نسميه بالتوقيع الإجرائي<sup>2</sup>.

إن هذا الإختلاف في طبيعة التوقيع يجعل تزويره مختلفا، ويصبح اكتشافه صعبا بالنظر لسهولة اكتشاف تزوير التوقيع الخطي بمضاهاة الخطوط ، فيما لا يترك تزوير التوقيع الإلكتروني أثرا ظاهرا باعتبار أن التوقيع الإلكتروني هو ختم الكتروني مشفر يملك مفاتحه

---

1 : أمجد حمدان الجهني، مرجع سابق .

2 : أحمد السيد كردي ، " التوقيع الإلكتروني مفهومه التكنولوجي وحمايته " ، 30 سبتمبر 2011 ،

<http://kenanaonline.com/users/ahmedkordy/posts/323677>

صاحب التوقيع<sup>1</sup>، ويتم تزويره باعتماد التوقيع نفسه عن طريق الحصول عليه ، بينما تزوير التوقيع العادي يكون من خلال تقليد التوقيع بطريقة تشبه التوقيع الأصلي<sup>2</sup> .

إن تزوير التوقيع الإلكتروني أمر صعب بالمقارنة مع تزوير التوقيع العادي، باعتبار أن التوقيع الإلكتروني عبارة عن منظومة رقمية مرتبطة بأنظمة أمان تقنية، حيث يعتمد التوقيع الرقمي- وهو أهم صور التوقيع الإلكتروني- على الدوال الرياضية واللوغاريتمات، كما أنه يعتمد على نظام المفاتيح العامة والخاصة، كما يؤمنه نظام التشفير .

ولذلك يعرف التوقيع الإلكتروني بأنه نظام تشفير الكتروني يعتمد على مفتاح خاص ومفتاح عام، وتنشأ المفاتيح بواسطة عمليات حسابية خاصة تضمن السرية<sup>3</sup>، حيث يستخدم المفتاح الخاص في وضع التوقيع الإلكتروني على المحررات الإلكترونية ويتم الإحتفاظ به على بطاقة ذكية مؤمنة، أما المفتاح العام فيوضع لدى شخص مستقبل الرسالة، ويستخدم في التحقق من شخصية الموقع على المحرر الإلكتروني والتأكد من صحة وسلامة محتوى المحرر الإلكتروني الأصلي<sup>4</sup> .

إن التوقيع الإلكتروني يعد من قبيل البيانات الإلكترونية في صورها المختلفة التي تستخدم الرموز والحروف والتشفير، وهو غير الإمضاء الذي يعد كتابة يقوم بها الشخص تتخذ شكلا

---

1 : ياسر العدل ، " التوقيع الإلكتروني"، 2009/09/29، (<http://www.ahewar.org/debat/show.art.asp>، aid=186248 ?)

2 : محمد محروك،"خصوصيات التوقيع الإلكتروني وحجيته في الإثبات"،4 فيفري 2013،(<http://www.marocdroit.com>)

3 : ياسر العدل ، مرجع سابق .

4 : نفس المرجع .

معينا مميزا يعتمد على الشخص في التعبير عن إلتزامه بوثيقة ما، كما أنه ليس من قبيل البصمة لأن هذا التوقيع يقوم على تقنيات لا تعد جزء من جسم الإنسان باستثناء التوقيع البيومتري<sup>1</sup> .  
ولذلك فإن تزوير التوقيع العادي يعتمد على تقليد الإمضاء أو الختم، مما يتطلب من الجاني معرفة فنية، بخلاف تزوير التوقيع الإلكتروني الذي يتطلب خبرة علمية في مجال الحاسوب والبرامج لأن طبيعة هذا التوقيع مختلفة تماما عن الأول .

### **المبحث الثاني : جريمة تزوير البطاقة الائتمانية \***

يتطلب تكيف فعل الإعتداء على البطاقة الائتمانية بالتلاعب في محتواها بوصفه تزويرا، أن يتم أولا تحديد طبيعتها القانونية لإمكانية إدراجها ضمن مفهوم الوثيقة المعلوماتية، واعتبارها وثيقة رسمية إذا كانت صادرة عن بنك أو مصرف تابع للحكومة.  
ولتحديد الطبيعة القانونية للبطاقة الائتمانية لابد من تعريفها، ثم محاولة ربط ذلك بأساليب التلاعب فيها .

### **المطلب الأول : تعريف بطاقة الائتمان**

تباينت التعاريف المتعلقة ببطاقات الائتمان، وتتنوع ضيقا واتساعا حسب الزاوية التي ينظر منها إلى هذه البطاقة ، مما انعكس على تحديد وصفها القانوني .

---

1 : غازي أبو عرابي، فياض القضاة ، مرجع سابق ، ص 182 .

\* : نقصد ببطاقة الائتمان ما يصدر عن البنوك أو المصارف والمؤسسات المالية من بطاقات ذات طبيعة معلوماتية مهما كانت الوظيفة التي تؤديها ، حيث يميز الفقه بين هذه البطاقات حسب وظيفتها، ويعتبر بطاقة الائتمان واحدة منها.

## الفرع الأول : تعريف بطاقة الإئتمان من الناحية المادية

قد تتفق التعاريف التي نظرت إلى بطاقة الإئتمان من حيث شكلها وتكوينها المادي بدل النظر إلى وظائفها، فقد التقت عند تعريفها بأنها "بطاقة مستطيلة من البلاستيك تحمل إسم المؤسسة المصدرة لها وشعارها وتوقيع حاملها ورقمها واسم حاملها ورقم حسابه وتاريخ صلاحيتها"<sup>1</sup> ، أو هي " بطاقة معدنية أو بلاستيكية ممغنطة، عليها اسم حاملها، وتاريخ إصدارها ، وتاريخ نهاية صلاحيتها ، ورقم سري لا يعرفه إلا حاملها " <sup>2</sup> .

كما عرفت بأنها " بطاقة بلاستيكية صغيرة الحجم شخصية تصدرها البنوك أو منشآت التمويل الدولية تمنح لأشخاص لهم حسابات مصرفية مستمرة وهي من أشهر الخدمات المصرفية الحديثة "<sup>3</sup> . أو هي "بطاقة بلاستيكية مزودة بشريط ممغنط ضيق، والذي قد يستخدم كوسيلة للتحكم في الدخول أو للتفويض ببدء المعاملة، وفي العادة يجري تشفير البيانات في ثلاث قنوات أفقية على امتداد الشريط"<sup>4</sup> .

كما توصف بأنها " بطاقة بلاستيكية مصنوعة من مادة خاصة مستطيلة الشكل طبع على أحد وجهتيها الأمامي بشكل بارز رقمها وتاريخ صلاحيتها وإسم حاملها واسم الشركة العالمية

---

1 : معادي أسعد صوالحة، بطاقات الإئتمان النظام القانوني وآليات الحماية الجنائية والأمنية دراسة مقارنة. المؤسسة الحديثة للكتاب، ط1 ، طرابلس، لبنان ، 2011 ، ص 39 .

2 : بكر بن عبد الله أبو زيد ، بطاقة الإئتمان. مؤسسة الرسالة، د.م، 1996، ص 17 .

3 : محمود سحنون ، " النظام المصرفي والبطاقات البلاستيكية " ، بحث مقدم لمؤتمر تشريعات عمليات البنوك بين النظرية والتطبيق، جامعة اليرموك، 2002 ، ص 02 .

4 : رياض فتح الله بصله، جرائم بطاقة الإئتمان. دار الشروق، ط1، القاهرة، 1995، ص 122 .

للبطاقة وشعارها والمصرف المصدر لها أحيانا. وعلى الوجه الخلفي شريط معلومات الكتروني مغناطيسي أسود اللون، يليه شريط ورقي أبيض اللون مخصص لتوقيع حاملها<sup>1</sup>.

يجمع التعريفات السابقة مجموعة من العناصر المتعلقة بشكل البطاقة وهي المادة المكونة لها، حجم البطاقة وأبعادها ، الشريط الممغنط، شريط التوقيع ، المعلومات الخاصة بالجهة مصدرة البطاقة ، المعلومات الشخصية لصاحب البطاقة .

يمكن توضيح شكل البطاقة من خلال العناصر السابقة كالتالي :

### 1- المادة المكونة للبطاقة وحجمها :

تدخل مادة البلاستيك كمكون أساسي لجسم البطاقة بصفة عامة ، ويتم التحكم بتشكيل هذه المادة عن طريق عملية التسخين إلى درجة الإنصهار ثم إجراء عملية الحقن للمصهور، ليتم تشكيله على هيئة قطع بلاستيكية مستطيلة الشكل ذات أطراف شبه دائرية يتراوح عرضها ما بين (5-05.5 سم) وطولها (8-8.5 سم)، وسمكها (0.8 مم)، ويتم تغليف جسم البطاقة بمواد كيميائية أخرى تشكل غطاء البطاقة ، والتي تختلف عن المركب الأساسي المكون لجسم البطاقة تمهيدا لصياغة وتثبيت البيانات والمعلومات والأشكال عليه<sup>2</sup> ، حيث يتم تصنيع البطاقة من عديد كلوريد الفينيل غير المرن<sup>3</sup> .

---

1 : كميث طالب البغدادي، الإستخدام غير المشروع لبطاقة الإنتمان. دار الثقافة ، ط1، عمان ، الأردن، 2008، ص 65.

2 : عماد علي الخليل، مرجع سابق ، ص.ص 19 ، 20 .

3 : محمد أحمد وقيع ، مرجع سابق ، ص 160 .

## 2- بيانات ومعلومات البطاقة :

تتوزع البيانات المتعلقة بالبطاقة بين الجهة مصدرة البطاقة على وجه هذه البطاقة وقد تكون مرئية أو غير مرئية ، ومعلومات صاحب البطاقة ، ولتوضيح ذلك نأخذ نموذج ( visa card ) حيث تضم البيانات التالية :

### أ- شعار الجهة :

هو علامة أو رسم يخص الجهة مصدرة البطاقة ، حيث تتخذ منظمة فيزا العالمية شعار " اليمامة " وهي صورة مجسمة ثلاثية الأبعاد تظهر بأجنحة متغيرة الألوان عند تحريك البطاقة تبعا لإنعكاس الضوء عليها<sup>1</sup> .

### ب- اسم البنك مصدر البطاقة :

يظهر اسم البنك المصرح له من قبل الهيئات الدولية بإصدار البطاقات ويظهر رقمه المحدد من قبل الهيئات الدولية واسمه وشعاره على البطاقات التي يصدرها<sup>2</sup> .

### ج- الرقم المكون من أربع خانات :

توجد أربع أرقام مطبوعة على البطاقة أعلى رقم البطاقة يجب أن تطابق الأرقام الأربعة الأولى من رقم البطاقة<sup>3</sup> ، ففي بطاقة " فيزا " يجب أن يبدأ كل من الرقم المطبوع ورقم

---

1 : عماد علي الخليل، مرجع سابق ، ص . ص 20 ، 21 .

2 : نجاح محمد فوزي ، وعي المواطن تجاه جرائم الإحتيال " بطاقات الدفع الإلكتروني نموذجا " ، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007 ، ص 64 .

3 : عمر الشيخ الأصم، " مرجع سابق ، ص 18 .

الحساب البارز برقم (4) ، كما يجب أن تتوافق الخانات الأربع الأولى من رقم الحساب البارز مع أول أربع خانات للرقم المطبوع <sup>1</sup> .

#### د- حرف بارز خاص بالجهة :

هذا الحرف هو حرف (V) ويكون موقعه عادة على يمين تاريخ الإنتهاء ، كما أن بعض بطاقات منظمة فيزا قد يظهر فيها هذا الحرف بأشكال متعددة منها : (CV) أو (BV) أو (PV)، وبدون هذه الأحرف فإن البطاقة تكون مقلدة أو مزورة حتما <sup>2</sup> ، لذلك فإن الحرف (V) والحرف الذي يظهر أمامه خط واحد مع تاريخ الصلاحية يعتبر العلاقة السرية وفيرة الضمان لبطاقات فيزا <sup>3</sup> .

#### هـ - طباعة مجهرية لإسم الجهة :

يتم طباعة اسم الجهة طباعة دقيقة بخطوط متوازية ، وتتميز الحروف والأرقام الغائرة على البطاقة بالتجانس في الحجم والمسافة البينية <sup>4</sup> .

#### و- تاريخ الإصدار والإنتهاء :

يبين هذا التاريخ مدة صلاحية البطاقة .

أما المعلومات المتعلقة بصاحب البطاقة فهي الإسم واللقب ، رقم الحاسب ، صورة الشخص أحيانا .

---

1 : عماد علي الخليل، مرجع سابق ، ص 20 .

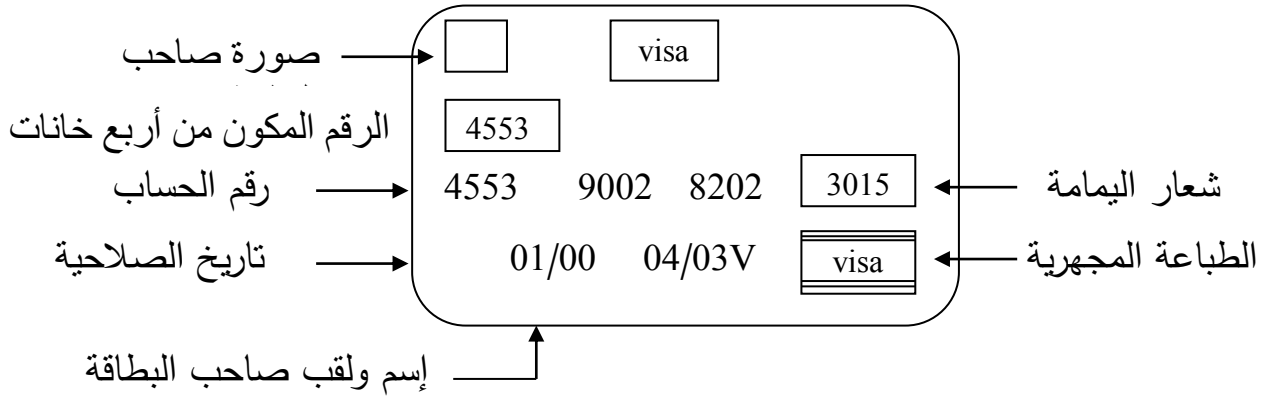
2 : نفس المرجع ، ص 21 .

3 : عمر الشيخ الأصم ، مرجع سابق ، ص 18 .

4 : نفس المرجع ، ص 18 .



### الشكل رقم (12) : وجه بطاقة فيزا



### 3- الشريط الممغنت :

هو المكان المخصص على البطاقة لتخزين البيانات الإلكترونية الخاصة<sup>1</sup> ، حيث لا يمكن قراءتها إلا بأجهزة مخصصة لذلك، وهي بيانات خاصة بصاحب البطاقة والتي يحتاجها الحاسب الآلي للتعرف عليه مثل الإسم، رقم البطاقة وسقفها ، تاريخ الصلاحية<sup>2</sup> .

يتم تخزين هذه البيانات على شكل مسارات أو أسطر، بحيث يتضمن كل سطر منها مجموعة خاصة من تلك البيانات والتي لا يمكن قراءتها إلا من خلال جهاز قارئ والذي يرتبط بنفس الوقت بجهاز حاسوب مزود ببرنامج خاص مهمته ترجمة هذه البيانات إلى بيانات أخرى يفهمها حاسوب البنك على أنها البيانات الخاصة بعمل معين ويقوم بمطابقتها مع البيانات الخاصة بهذا العميل والمخزنة سلفا على الجهاز<sup>3</sup> .

1 : نجاح محمد فوزي ، مرجع سابق ، ص 65 .  
2 : محمد أحمد وقيع ، مرجع سابق ، ص 174 .  
3 : عماد علي الخليل ، مرجع سابق ، ص 22 .

#### 4- شريط التوقيع :

يقع أسفل الشريط الممغنط وبمسافة أمنية محددة ، بحيث يثبت على هذه المساحة توقيع حامل البطاقة المعتمد لدى البنك ،.... وفي معظم البطاقات المصرفية الممغنطة يتركب شريط التوقيع بطريقة كيميائية خاصة ، بحيث إذا وقع عليه خدش أو تأكل أو تلاعب بالتوقيع تظهر مباشرة على الشريط وبخطوط متقطعة كلمة لاغي وهذه إشارة أمنية هامة وضعت لمصلحة التاجر الذي يقبل الوفاء بالبطاقة حتى لا يقع ضحية احتيال أو تزوير من شخص لا يملك البطاقة<sup>1</sup> .

#### 5- الرقم السري :

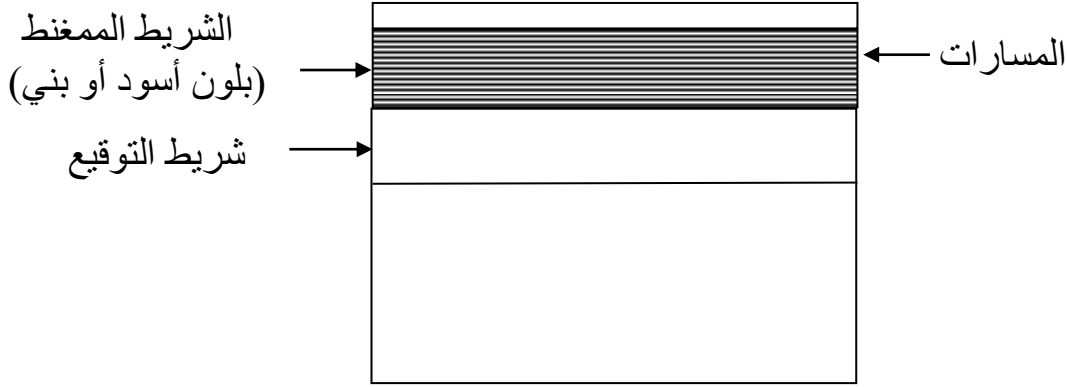
يسلم هذا الرقم للعميل بمظروف مغلق عند استلامه للبطاقة ، ويستخدمه حامل البطاقة عند الصرف النقدي من ماكينات الصرف الآلي ATM ، والذي من خلاله تتعرف الماكينة على صاحب البطاقة وتسمح له بالصرف في حالة إدخاله للرقم السري الصحيح<sup>2</sup> .

---

1 : عماد علي الخليل ، مرجع سابق ، ص . ص 21 ، 22 .

2 : نجاح محمد فوزي ، مرجع سابق ، ص 66 .

### الشكل رقم (13) : ظهر بطاقة فيزا



لقد تطورت بطاقات الإئتمان وأخذت أشكالاً مختلفة منها البطاقة الرقائعية وهي "بطاقة بلاستيكية بذات أبعاد ومواصفات البطاقة الممغنطة، إلا أنها تحتوى على شريحة من الدوائر المتكاملة مدمجة بها، تعمل كذاكرة إلكترونية ذات سعات تخزينية مختلفة، تستخدم في العديد من التطبيقات، وتعد التطبيقات المصرفية أحد أهم استخدامات هذا النوع من البطاقات"<sup>1</sup> .

ويدخل في هذه البطاقة ثلاثة أنواع فرعية هي بطاقة الذاكرة وهي التي تتضمن ذاكرة لتخزين البيانات والمعلومات، البطاقة الذكية وهي التي تحتوي معالجا آليا للبيانات والمعطيات بحيث تشمل مواصفات أمان عالية، والبطاقة حادة الذكاء والتي تتضمن معالجا صغيرا للبيانات وذاكرة وشريط ممغنط وشاشات عرض ومفاتيح إدخال بيانات والتي تتيح بمجملها عملية تخزين المعلومات الشخصية والبيانات المالية لحاملها<sup>2</sup>، وتعتمد على خوارزمية برمجية هي خوارزمية المفتاح العام التي تسمح بإنشاء مباشر للتوقيعات الرقمية<sup>3</sup> .

1 : نجاح محمد فوزي ، مرجع سابق ، ص 70.

2 : معادي أسعد صوالحة ، مرجع سابق ، ص . ص 53 ، 54 .

3 : رياض فتح الله بصله ، مرجع سابق ، ص 127 .

## الفرع الثاني : تعريف بطاقة الائتمان من الناحية الموضوعية

عرفت بطاقة الائتمان بأنها: "بطاقة تتضمن معلومات معينة من اسم حاملها ورقم حسابه تصدرها جهات معينة عادة تكون بنكا أو مؤسسة مالية، حيث تمكن حاملها من سداد قيمة مشترياته عن طريقها بحيث تقوم الجهة المصدرة بتعجيل وفاء قيمة المشتريات للتاجر على أن تستردها لاحقا من الحامل على دفعات مضافا لها عمولة أو فائدة متفق عليها"<sup>1</sup> .

كما اعتبرت "بطاقات تصدر بوساطة مؤسسة مالية بإسم أحد الأشخاص وتقوم تلك البطاقة بوظيفتي الوفاء والائتمان، أي أن حاملها يملك امكانية تتابع سداد المبالغ التي استخدمها من الاعتماد المفتوح من جانب مصدر البطاقة"<sup>2</sup> .

وهي أيضا " مستند تصدره مؤسسة مالية تلتزم بموجبه بدفع قيمة مشتريات حاملها إلى التاجر الذي يقبل التعامل بالبطاقة بناء على اتفاق مسبق معه، ثم رجوع المصدر للبطاقة على حاملها لإستيفاء المبلغ خلال فترة الائتمان المسموح بها للعميل"<sup>3</sup>.

كما نظر إليها على أنها " عبارة عن مجموعة من الأفكار والمعاني صادرة عن البنك أو المؤسسة المالية"<sup>4</sup> .

هذه التعاريف تشير إلى مجموعة من العناصر وهي :

- 
- 1 : فداء يحيى أحمد الحمود ، مرجع سابق ، ص 15 .
  - 2 : فايز رضوان، بطاقات الوفاء، المطبعة العربية ، القاهرة ، 1990، ص 71 . نقلا عن : نفس المرجع ، ص 14 .
  - 3 : محمد توفيق سعودي، بطاقات الائتمان والأسس القانونية للعلاقات الناشئة عن استخدامها. دار الأمين للنشر ، ط1، القاهرة، 2001 ، ص 21 نقلا عن : معادي أسعد صوالحة ، مرجع سابق ، ص 45 .
  - 4 : جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة. دارالنهضة، القاهرة، 2003، ص 120

1- بطاقة الائتمان تعتبر وعاء لمعلومات معينة ذات أثر قانوني مثل المركز المالي لصاحب البطاقة .

2- تشكل المعلومات الموجودة على البطاقة مجموعة من الأفكار والمعاني سواء كانت مرئية أو غير مرئية ، مفهومة أو غير مفهومة بمجرد النظر إليها .

3- تعتبر هذه البطاقة مستند من الناحية القانونية سواء كانت صادرة عن بنك أو مؤسسة مالية أو مصرف حكومي .

هذه النتائج لها دلالات من حيث تحديد مدى وقوع التزوير إذا تعلق الأمر بالتلاعب في المعلومات الموجودة على البطاقة ، خاصة تلك المعلومات المشفرة . فقد ركزت التعريفات السابقة على زاوية نظر معينة جمعت بينها ابتداء وهي النظر إلى هذه البطاقة باعتبارها مستند أو وثيقة، وهو محور العلاقة التي نبحت عنها بين بطاقة الائتمان - كشكل من أشكال البطاقات الإلكترونية - وجريمة التزوير، ولذلك لن أتعرض لوظائف هذه البطاقة من الناحية المصرفية أو المالية، وهي الزاوية التي تهتم الباحث في النظام القانوني للبطاقات الائتمانية بصفة عامة .

إذن ما يهمنا أن هناك ثلاثة عناصر كل منها يمثل ضلعا من مثلث متساوي الأضلاع، الضلع الأول هو البطاقة، والضلع الثاني هو المعلومات، والضلع الثالث هو النظام، ومن هذه العناصر الثلاثة يتكون النظام الكلي لبطاقة الائتمان<sup>1</sup> ، ولذلك فإن البحث عن مدى وقوع التزوير في بطاقة الائتمان يقتضي الربط بين الأضلع الثلاث لإيجاد نظرية متكاملة في ذلك .

---

1 : رياض فتح الله بصله، مرجع سابق ، ص 106 .

## المطلب الثاني : مدى وقوع التزوير بالتلاعب في البطاقة الائتمانية

من خلال التعريفات السابقة والأشكال الموضحة يتبين أن بطاقة الائتمان تتكون من معلومات مقروءة مثبتة على كيانها المادي ، ومعلومات غير مقروءة موجودة على الشريط الممغنط أو المغناطيسي، وهذه الطبيعة هي التي أثارت ذلك الجدل الفقهي حول تزويرها .

### الفرع الأول : التزوير في المعلومات المقروءة لبطاقة الائتمان

ارتبطت الوثيقة بالورق لمدة طويلة ، لكن رغم ذلك يمكن أن تكون مادتها مصنوعة من الخشب أو النحاس أو الجلد أو أية مادة أخرى يتصور أن تستعمل لذلك<sup>1</sup>، وإن ما يترتب على ذلك من حيث المبدأ ألا يوجد مانع قانوني أو حتى فني من أن تكون المادة التي يتم تثبيت البيانات والمعلومات عليها مصنوعة من البلاستيك أو الورق المقوى أو الصلب،... وجسم البطاقة المصنوع من مادة بلاستيكية أو حتى من الورق الصلب المصقول تصلح من حيث المبدأ لأن تكون وعاء للمحرر شأنها شأن أية مادة أخرى<sup>2</sup> .

أما من ناحية المعلومات الموجودة على البطاقة والتي تعبر عن فكرة يمكن ادراكها بالنظر إليها مباشرة فإن التغيير فيها يكون الركن المادي لجريمة التزوير<sup>3</sup> ، لأنها تتعلق بحامل البطاقة والجهة التي أصدرتها، وتاريخ الصلاحية، وهي في مجملها تجعل البطاقة مستندا يمكن استخدامه فيما أعد له<sup>4</sup> .

1 : محمود نجيب حسني ، مرجع سابق ، ص 248 .

2 : محمد عماد مرهج الهيتمي، الحماية الجنائية لبطاقات الائتمان الممغنطة. دار الكتب القانونية، القاهرة، 2009، ص 273.

3 : فداء يحي أحمد ، مرجع سابق ، ص 109 .

4 : محمد حماد مرهج الهيتمي ، مرجع سابق ، ص 275 .

ولذلك فإن التغيير الذي ينال هذه المعلومات لا يثير إشكالا ، حيث لتوافر صفة الوثيقة يجب أن تتضمن كتابة أو ما يقوم مقامها من رموز يمكن أن تنقل المعنى بمجرد النظر إليها، وبطاقة الإئتمان يمكن اعتبارها كذلك حيث إنها تحتوي على بيانات واضحة<sup>1</sup> .

أما المعلومات غير المرئية والتي يتضمنها الشريط الممغنط وهي معلومات مشفرة فلا ينطبق عليها الوصف السابق، باعتبار أن التزوير يفترض تغييرا في علامات أو رموز مرئية، لأن حاسة البصر هي التي تكشف الفكرة التي يعبر عنها المحرر ، كما أنه يعتبر أداة لتبادل الأفكار مما يستوجب أن يكون مقروء بمجرد الإطلاع عليه بالعين المجردة أو ما يقوم محلها مثل حاسة اللمس<sup>2</sup> . كما أن الفقه عرف الوثيقة بأنها كل مسطور يتضمن علامات ينتقل بها الفكر لدى النظر إليها من شخص إلى آخر<sup>3</sup> .

هذا الإتجاه الفقهي\* لايعتد بالتزوير إلا إذا انصب على أحد بيانات البطاقة المقروءة، أما البيانات المشفرة فلا ينطبق عليها الوصف السابق، فثمة صعوبة قانونية تواجه تطبيق نصوص جريمة التزوير وهي عدم تحقق وصف الوثيقة بالنسبة للمعلومات المثبتة على أوعية الكترونية،

---

1 : كميث طالب البغدادي ، مرجع سابق ، ص 197

2 : جميل عبد الباقي الصغير ، مرجع سابق ، ص 121 .

3 : نفس المرجع ، ص 121 .

\* : محمود نجيب حسني ، مرجع سابق ، ص 347، جميل عبد الباقي الصغير ، مرجع سابق ، ص 125، عماد علي الخليل ، مرجع سابق ، ص 68 .

أيا كانت أهمية هذه المعلومات المثبتة بهذا الشكل من وجهة نظر من ثبتها أو من وجهة نظر المجتمع<sup>1</sup> . ومن ثم يحيلنا هذا الإتجاه الفقهي مجددا إلى حسم المسألة بإتجاه عدم تطبيق نص التزوير التقليدي على تزوير المعلومات الموجودة على أوعية الكترونية ، باعتبارها لا تعتبر وثيقة من الناحية القانونية ، وفي هذا الفرض توجد هذه المعلومات على بطاقة ائتمانية سواء على شريط ممغنط أو ذاكرة أو شريحة الكترونية معتمدة على خوارزميات لإنشاء التوقيعات الرقمية .

ولذلك يقع التغيير في بطاقة الإئتمان بإحدى الطرق التي بينها القانون على سبيل الحصر<sup>2</sup>، حيث يقع بطرق التزوير المادي عن طريق تزوير الإمضاء كما في حال قيام السارق أو من عثر على البطاقة المفقودة بالتوقيع على البطاقة إذا كانت خالية من توقيع حاملها الشرعي، ثم يقوم فيما بعد بنسخ هذا التوقيع على فواتير الشراء لدى التجار، أو بوضع أسماء أو صور أشخاص آخرين مزورة كقيام الجاني بوضع اسمه مكان اسم الحامل الشرعي للبطاقة، أو تزوير صورته إذا كانت البطاقة تحوى صورة صاحبها، أو عن طريق التقليد أو الإصطناع<sup>3</sup>.

### الفرع الثاني : التزوير في المعلومات المشفرة لبطاقة الإئتمان

إن المعلومات المشفرة الموجودة على بطاقة الإئتمان لها أهميتها مثل بقية المعلومات

---

1 : محمد حماد مرهج الهيتي ، مرجع سابق ، ص 283 .

2 : جميل عبد الباقي الصغير ، مرجع سابق ، ص 124 .

3 : نفس المرجع ، ص.ص 124 ، 127 .



الموجودة عليها، وهو ما جعل اتجاهها فقهيًا آخر\* يرى بأن التغيير الذي يمس هذه المعلومات يكون جريمة التزوير، فبطاقة الائتمان تعتبر وثيقة تقع عليها جريمة التزوير، حيث إنها تحتوي على بيانات واضحة مثل الإسم والتوقيع وتاريخ الصلاحية وعلى بيانات أخرى قد تكون أهم لكنها تثبت على الشريط المغناطيسي للبطاقة بصورة غير مرئية، كما أنها تمثل حق صاحبها في المبلغ الذي تمثله تلك البطاقة وحقه في الشراء من التاجر الذي يقبل التعامل بهذه البطاقات، هذا من ناحية ومن ناحية أخرى فهي تعبر عن عقد وعلاقة قانونية قائمة بين حاملها والبنك المصدر لها وتثبت قيام هذه العلاقة بما تشمل من حقوق والتزامات متبادلة بين الطرفين<sup>1</sup>.

كما أن التزوير الكلي أو الجزئي للبطاقة لا يمكن أن يتم في أهم صور التغيير إلا بنسخ المعلومات من بطاقة صحيحة ونافاذة.... فالتغيير الذي يصيب الكيان المعنوي للبطاقة بما تتضمنه الأشرطة المغنطة من بيانات ومعلومات هو الأكثر إثارة للمشاكل مما لو انصب التغيير على كيان البطاقة المادي<sup>2</sup>.

ويعتبر هذا الإتجاه أن وصف الوثيقة متوافر بالنسبة للمعلومات المشفرة أيضا وإن كانت لا تدركها العين المجردة، والقول بعدم توافر هذه الصفة في هذه الحالات على أساس عدم رؤية

---

\* : فداء يحي أحمد، مرجع سابق، ص 11، كميت طالب البغدادي، مرجع سابق، ص 199. حنان ربحان مبارك المضحكي، الحماية الجنائية لبطاقات الائتمان المغنطة (دراسة مقارنة). المكتب الجامعي الحديث، دم، 2012، ص 179.

1 : كميت طالب البغدادي، مرجع سابق، ص 197.

2 : محمد حماد مرهج الهيتي، مرجع سابق، ص 278.

مدلول العبارات فيه خلط بين ضرورة معرفة مدلولها بحاسة البصر ومدى قراءتها عن طريق الحاسب الآلي<sup>1</sup> ، كما أن وصف الوثيقة لا يمكن أن يستقل عن البيانات والمعلومات غير المقروءة ولا سيما أن التغيير في البطاقة يرتكز على الجانب الأخير مع عدم أهمية التغيير الذي تتعرض له المعلومات المقروءة، مما يمكن على ضوءه القول بانتفاء أهمية التغيير الذي تتعرض له البيانات المقروءة بالقياس للتغيير الذي تتعرض له البيانات غير المقروءة<sup>2</sup> .

وهو الإتجاه الذي نؤيده ذلك أن المعلومات المشفرة الموجودة على بطاقة الإئتمان لها قيمتها من الناحية القانونية مثل المعلومات الظاهرة، فهي تتعلق بحق أو مركز قانوني لصاحبها، ولا ينفي عنها هذه القيمة لمجرد أنها غير مقروءة نظرا لطبيعتها .

بل إن التغيير في هذه المعلومات أشد خطورة من التغيير الواقع على المعلومات الظاهرة، باعتباره لا يترك أثر ظاهرا على البطاقة وقد يصعب اكتشافه ، والقول بوقوع التزوير في المعلومات المقروءة فقط لا يحقق مقصد المشرع من تجريم التزوير وهو حماية تلك الثقة التي تتمتع بها مثل هذه الوثائق، لا سيما عندما يتعلق الأمر ببطاقات مصرفية حكومية .

### **المطلب الثالث : طرق التزوير في بطاقة الإئتمان**

قد يتم تزوير بطاقات الإئتمان بالتلاعب في محتوياتها بطرق مختلفة سواء تعلق الأمر بالمعلومات المرئية الموجودة عليها، أو بالمعلومات المشفرة الموجودة على الشريط الممغنط،

---

1 : محمد حماد مرهج الهيتي ، مرجع سابق ، ص 287 .

2 : نفس المرجع ، ص 302 .

حيث لكل نوع من هذه المعلومات أهميته فهو مرتبط بحق أو مركز قانوني ذو طابع مالي ، وأي تغيير في أي منها يقع به التزوير سواء كان تزويرا كليا أو جزئيا ، كما يمكن الحصول على بطاقة ائتمانية عن طريق تزوير الوثائق المطلوبة لإستخراجها ، وفي هذه الحالة تعتبر البطاقة صحيحة، إلا أن واقعة الحصول عليها ينطبق عليها وصف التزوير.

### الفرع الأول : التزوير الكلي لبطاقة الإئتمان

يقع التزوير الكلي لبطاقة الإئتمان على جميع عناصرها ، يقول في ذلك الأستاذ " رياض فتح الله بصله " أننا إذا رجعنا إلى مخطط المثلث المتساوي الأضلاع (البطاقة، المعلومات، النظام)، سوف نجد أنه جرى إنتاج البطاقة بتجهيزات مادية، وجرى تلقين البطاقة المصطنعة ببيانات صحيحة مسروقة، الأمر الذي أدى إلى اختراق النظام عن طريق تداول واستخدام البطاقة<sup>1</sup> .

إن الجاني في هذه الحالة سيقوم بتقليد بطاقة ائتمانية بالتلاعب في مكوناتها الأساسية<sup>2</sup>، وهي:

#### 1- المادة المكونة للبطاقة :

تصنع بطاقة الإئتمان بمواصفات معينة ، وتتكون عادة من ثلاث طبقات بلاستيكية مضغوطة مصنوعة من مادة بولي كلوريد الفينيل " PVC " ، أما مادة الطبقة الوسطى فتحتوي على مادة " PVC " ومادة أوكسيد التيتانيوم وهي المادة التي تجعل البلاستيك باللون الأبيض<sup>3</sup>.

1 : رياض فتح الله بصله ، مرجع سابق ، ص . ص 158 ، 159 .

2 : عمر الشيخ الأصم ، مرجع سابق ، ص . ص 15 ، 16 .

3 : محمد عبد الرسول خياط ، مرجع سابق ، ص 49 .

إن من السهل الحصول على هذه المواد ، وقد يفتتها البعض وهو ما يعرف بالبلاستيك الأبيض وهي عبارة عن بطاقة من حيث الحجم والأبعاد إلا أنها لا تحمل أي بيانات ويمكن نقل هذه البيانات إلى البلاستيك الأبيض واستخدامه بالطريقة التي يرغبون في تطبيقها<sup>1</sup> ، فهذه التجهيزات المادية متوفرة في الأسواق دون ما ضرورة لوضع ضوابط أمنية على شرائها<sup>2</sup> .

## 2- المعلومات :

المعلومات الموجودة على البطاقة قد تكون ظاهرة، أو موجودة على الشريط المغنط.

### أ- المعلومات الظاهرة :

يتم تزوير البيانات لتوضع على جسم البطاقة، وهي البيانات المطبوعة السطحية، الغائرة أو البارزة، ومما يسهل عملية الطباعة هو تلك المادة المستعملة في جسم البطاقة لتوضع عليها المعلومات، حيث توضع الطباعة الجرافيكية عادة في الطبقة الوسطى من البطاقة ، وسمكها ما بين 0.020 بوصة إلى 0.025 بوصة وهي محمية من الأسفل والأعلى بمادة " PVC " الشفافة، وتغطي بطبقة بلاستيكية لحماية البيانات المعلومات من العوامل البيئية المحيطة والحرارة ، وهذه المواد وطريقة الطباعة تسهل عملية الطباعة المكبوسة لرقم الحساب وتاريخ الإنتهاء والبيانات الأخرى المطلوبة لحاملها<sup>3</sup> .

---

1 : عمر الشيخ الأصم ، مرجع سابق ، ص 15 .

2 : رياض فتح الله بصله ، مرجع سابق ، ص.ص 108 ، 109 .

3 : محمد عبد الرسول خياط ، مرجع سابق ، ص 50 .

## ب- المعلومات الموجودة على الشريط الممغنط :

إن تزوير المعلومات الموجودة على الشريط الممغنط يتم إما بالنسخ<sup>1</sup> لإستعمالها في إنشاء بطاقات، أو بالتشفير<sup>2</sup> حيث إن عملية ترقيم البطاقات الصحيحة التي يتم إصدارها داخل مركز البطاقات في أي بنك أو مؤسسة مالية تخضع لمعادلات رياضية معقدة يحكمها شفرة خاصة بكل بنك (Algorithm)<sup>3</sup> .

وقد أصبح الحصول على هذه الأرقام ممكنا من خلال برامج حاسوبية يتم تسويقها عبر شبكة الإنترنت ، حيث يكفي الحصول على برنامج من تلك البرامج بالدخول إلى أحد تلك المواقع، ثم انزال البرنامج ، وفي المرحلة الثانية تشغيله وإدخال رقم بطاقة ائتمانية صحيحة ، ليتولى البرنامج بعد ذلك عملية التخليق لأرقام بطاقات ائتمانية تصل إلى مائة رقم بطاقة صحيحة منسوبة لذات البنك ثم استخدام تلك الأرقام بعد ذلك في أية عمليات سواء بدمجها مع بطاقات مقلدة أو تلقينها لأشرطة ممغنطة لبعض البطاقات منتهية الصلاحية واستخدامها في إجراء المعاملات<sup>4</sup> .

أما طريقة نسخ الشريط الممغنط فيتم من خلال وحدة الكترونية لنسخ وتخزين البيانات الملقنة عليه ، حيث استخدمت تلك الوحدة بمعرفة عاملين في بعض المطاعم والفنادق والمحال

---

1 : Guy Weber, "La Fin de la Bande Magnétique" , décembre 2011, ([www.six-telekurs.com/fr/dl-tkicch-clearit](http://www.six-telekurs.com/fr/dl-tkicch-clearit) 50 fraud).

2 : رياض فتح الله بصله ، مرجع سابق ، ص 109 .

3 : نجاح محمد فوزي ، مرجع سابق ، ص 107 .

4 : نفس المرجع ، ص . ص 107 ، 108 .

العامة في نسخ البيانات الملقنة للأشرطة الممغنطة لبطاقات الإئتمان بعد مغافلة أصحابها وحال شروعهم في سداد قيمة مشترياتهم<sup>1</sup> . ثم تأتي بعد ذلك مرحلة تفريغ محتوى هذه الوحدة إلى أحد الملفات على جهاز حاسب آلي ليتم إعادة تلقينها بعد ذلك بواسطة على أشرطة ممغنطة لبطاقات بلاستيكية خام أو مقلدة أو صحيحة منتهية الصلاحية ، باستخدام وحدة تكويد الأشرطة الممغنطة<sup>2</sup> ، وكذلك الأمر بالنسبة لسرقة هذه البيانات من خلال أجهزة الصرف الآلي، أو القرصنة عبر شبكة الإنترنت .

كما يمكن الإحتيال على حامل البطاقة عبر الشبكة حيث تعتمد هذه الطريقة على اصطياد البيانات المصرفية عن طريق البريد الإلكتروني ، حيث يتلقى المستفيد رسالة الكترونية تبدو كأنها من بنك أو مؤسسة حكومية تريد التأكد من بياناته لديها لتحديثها ، وعندما يتم إرسال تلك البيانات يتم تحويل المستخدم إلى موقع آخر يشبه الموقع الأصلي<sup>3</sup> ، وتسمى هذه الطريقة بطريقة التصيد وهي تقنية للحصول على المعلومات الخاصة بالمستعمل الذي يكون ضحية بريد مضلل يؤدي به إلى موقع مزور<sup>4</sup> ، والغرض من وراء الحصول على هذه المعلومات هو إعادة استعمالها<sup>5</sup> .

---

1 : نجاح محمد فوزي ، مرجع سابق ، ص 109 .

2 : نفس المرجع ، ص 110 .

3 : نفس المرجع ، ص 113 .

4 : François Paget, "Fraude Financière et Opérations Bancaires en ligne : Menaces et contre-mesures", 2009, ([www.bulletin-numismatique.fr/bn/bn069/images/mcafee](http://www.bulletin-numismatique.fr/bn/bn069/images/mcafee)), p 8 .

5 : Abderrahmane Nitaj, "la Cryptographie et la confiance Numérique", 23 mars 2013([www.math.unicaen.fr](http://www.math.unicaen.fr)), p 6

## الفرع الثاني : التزوير الجزئي لبطاقة الائتمان

يعتمد التزوير الجزئي لبطاقة الائتمان على وجود بطاقة صحيحة ابتداء في يد المزور  
ليتمكن من التلاعب في مكوناتها المرئية وغير المرئية بالأساليب المناسبة، حيث سيستثمر  
المزور في هذه الحالة الجسم الحقيقي للبطاقة وما عليه من هولو جرام ونقوش وطباعة وكتابة  
أمنية<sup>1</sup> .

هذا يعني أن التزوير في هذه الحالة له ثلاثة فروض إما سرقة المعلومات الخاصة  
بالبطاقة، أو تقليد الشريط الممغنط، أو تزوير التواقيع على بطاقات ائتمان مسروقة والصورة  
أحيانا إذا كانت موجودة .

### أولا : سرقة المعلومات الخاصة بالبطاقة

يقوم الجاني في هذا الفرض بالحصول على بطاقة ائتمان صحيحة بطريقة غير مشروعة  
قد تكون منتهية فترة الصلاحية أو ملغاة، حيث يتم العبث في بياناتها أو أحد البيانات التأمينية  
بطريقة لا تلاحظ بسهولة<sup>2</sup> . وتتم العملية بالتخلص من البيانات المطبوعة طباعة نافرة عن  
طريق تسخينها بواسطة التسخين في الماء لدرجة الغليان وضغط الحروف النافرة حتى تختفي،  
ثم وضع أرقام بيانات جديدة مطبوعة طباعة نافرة بواسطة آلة طباعة نافرة<sup>3</sup> . ثم يتم تلقينها  
بأرقام حسابات تمت سرقة المعلومات الخاصة بها ، أو الحصول عليها بطريقة غير مشروعة ،

---

1 : رياض فتح الله بصللة، مرجع سابق ، ص 111 .

2 : محمد عبد الرسول خياط ، مرجع سابق ، ص 40 .

3 : رياض فتح الله بصللة، مرجع سابق ، ص 111 .

وكثيرا ما تتم هذه الاعتداءات عند التعامل عبر شبكة الإنترنت، مثل عمليات الشراء والإنتفاع بالخدمات التي تتيحها التجارة الإلكترونية، حيث تتطلب من المستخدم ملء النموذج الإلكتروني ببيانات بطاقته الائتمانية ومنها الرقم السري<sup>1</sup> .

كما يمكن الحصول على هذه المعلومات من الأماكن الأكثر تداولاً لها مثل الفنادق والمطاعم والمتاجر الكبرى، وذلك باقناع أي موظف فيها بتسجيل أو بيع أرقام بطاقات الائتمان للزبائن، حيث يلقي هذا النوع من السرقات زواجا كبيرا نظرا لإعتقاد صاحب البطاقة أنها لديه ولا علم له بسرقة أرقام البطاقة<sup>2</sup> .

### ثانيا : تزوير التوقيع على بطاقات ائتمان مسروقة

في هذا الفرض يقوم الجاني بسرقة بطاقة ائتمان صحيحة ، ثم كشط ما عليها من توقيع ولصق آخر مكانه ، والتوقيع عليه ، أو المحو الآلي أو الكيميائي للتوقيع الأصلي أو لأجزاء من هذا التوقيع<sup>3</sup> . (أنظر الشكل الموالي)

---

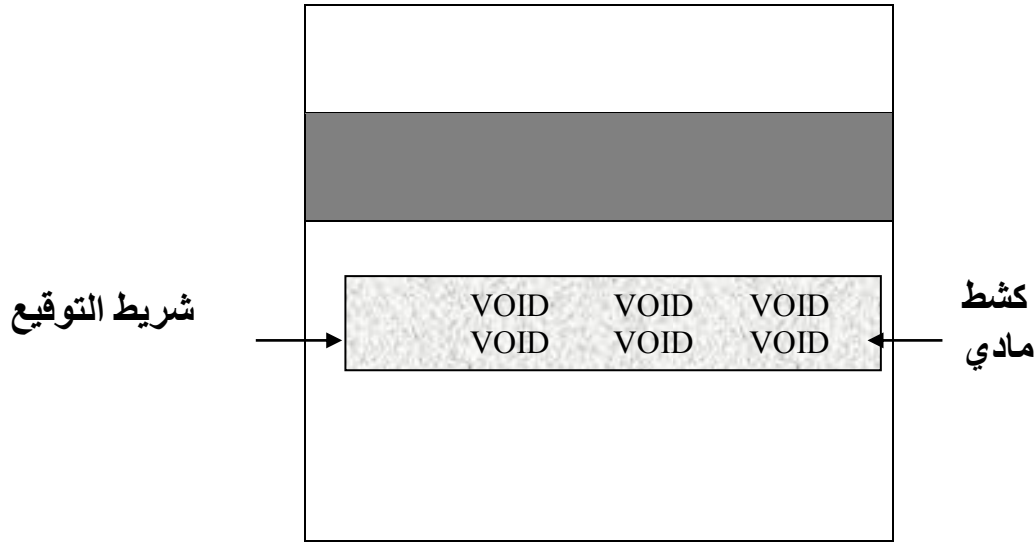
1 : محمد أمين أحمد الشوابكة، مرجع سابق ، ص 199 .

2 : محمد عبد الرسول خياط ، مرجع سابق ، ص 39 .

3 : رياض فتح الله بصله ، مرجع سابق ، ص 115 .



## شكل رقم (14) يوضح كشط شريط التوقيع



( المصدر : رياض فتح الله بصله ، مرجع سابق ، ص 112 . )

### ثالثا : تزوير الشريط الممغنط

ذكرنا سابقا أن الشريط الممغنط يحتوي على المعلومات المشفرة ، لذلك على الجاني في هذه الحالة تقليد الشريط الممغنط عن طريق محو ما عليه من بيانات وإعادة تشفير : بمعلومات جديدة وصحيحة ومسروقة بواسطة جهاز تشفير<sup>1</sup> .

ومن المعلومات التي يحتاجها الجاني في ذلك رقم بطاقة الإئتمان، حيث إن هذا الرقم يتم إصداره داخل مركز البطاقات التابع للبنك أو المؤسسات المالية طبقا للوغاريتم خاص بكل بنك، مما يصعب معه استنتاج رقم بطاقة صحيحة صادرة عن هذه الجهات استنادا إلى أرقام صحيحة لبطاقات صادرة عن ذات البنك<sup>2</sup> .

1 : رياض فتح الله بصله ، مرجع سابق ، ص . ص 111 ، 112 .

2 : نجاح محمد فوزي ، مرجع سابق ، ص 107 .

لكن النشاط الإجرامي لا يتوقف أمام التطور التكنولوجي والمعلوماتي، حيث تم تطوير برامج للحاسب الآلي تعمل على تخليق أرقام بطاقات ائتمانية صحيحة لنفس البنك بعد تزويده برقم بطاقة ائتمانية صحيحة، ثم يتولى الجاني تزويد الشريط الممغنط للبطاقة المنتهية الصلاحية أو المفقودة أو المسروقة بهذا الرقم . كما يمكن الحصول على البيانات الشخصية والمصرفية لصاحب البطاقة من خلال طريقة التصيد كما ذكرنا سابقا، لتلقينها على الشريط الممغنط، وقد يتم بيع هذه البيانات أو تبادلها مع منافع غير مشروعة أخرى من خلال بعض غرف الدردشة على شبكة الإنترنت<sup>1</sup> .

### الفرع الثالث : استخراج بطاقة ائتمان صحيحة بوثائق مزورة

إن عملية استخراج بطاقة الائتمان تبدأ بتقديم بيانات معينة يحددها البنك وذلك من خلال وثائق تثبت ذلك ، ليتم إدخال هذه البيانات على الحاسب الآلي . يقوم البنك بتجميع البيانات التي قدمت وأدخلت على الحاسب خلال فترة زمنية معينة ، لتسجل على الشريط الممغنط الخاص بكل بطاقة ، ثم يرسل هذا الشريط الذي يحوي البيانات الخاصة إلى قسم آخر يتولى إصدار البطاقة وإرسالها إلى الفرع الذي يتعامل معه العميل<sup>2</sup>. والغرض في هذه الحالة هو إصدار هذه البطاقة البنكية بناء على وثائق قدمها العميل مغيرا في

---

1 : نجاح محمد فوزي ، مرجع سابق ، ص 188 .

2 : ضياء أمين مشيمش، التوقيع الإلكتروني دراسة مقارنة ، صادر للمنشورات الحقوقية، ط1، د.م، 2003، ص.ص 98 ،

حقيقتها ، ومما لاشك فيه أن هذا الفعل يعد تزويرا ، مما يقتضي وصف " التزوير " في الحصول على بطاقة الإئتمان باستعمال ورقة مزورة<sup>1</sup> .

وقد انتشر هذا الفعل خلال عقد التسعينات حيث دأب بعض المحتالين إلى التقدم إلى أفرع بعض البنوك بمستندات إثبات شخصية مزورة للحصول على بطاقات إئتمان بأسماء منتحلة وعناوين وهمية، ويتم استخدام تلك البطاقات بمبالغ مالية كبيرة في عمليات سريعة ومتتالية<sup>2</sup> . وقد يحترف الجاني هذا النوع من الجرائم ، حيث يستهدف أكثر من بنك لإستصدار عدة بطاقات بذات الأسلوب وبأسماء وبيانات منتحلة لتحقيق أكبر عائد ممكن خلال فترة زمنية قصيرة وقبل اكتشاف تلك الوقائع مستغلا ضعف خبرة بعض موظفي البنوك في كشف تزوير الوثائق .

وقد يرتبط هذا النوع من الجرائم بتزوير وثائق رسمية إدارية مثل بطاقة التعريف وجواز السفر، أو شهادات الحالة المدنية التي يطلبها البنك لإثبات معلومات معينة عن طالب البطاقة، حيث يزور الجاني هذه الوثائق ويستعملها وهو على علم بذلك من أجل الحصول على بطاقة إئتمانية ببيانات مزورة لإستخدامها لتحقيق عائد مالي .

---

1 : إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الإئتمان. دار الجامعة الجديدة للنشر، الإسكندرية، 2007 ، ص 233 .

2 : نجاح محمد فوزي ، مرجع سابق ، ص 97 .

## الخاتمة :

ساهمت المعلوماتية في تحول الوثيقة الورقية إلى وثيقة ذات طبيعة معلوماتية ، وقد امتد ذلك إلى الوثيقة الرسمية الإدارية باعتبارها الوسيلة الأساسية في اتمام المعاملات الإدارية خاصة باعتماد أسلوب الإدارة الإلكترونية، والدخول للحكومة الإلكترونية ، وتأثير التجارة الإلكترونية والإنترنت .

هذا التحول في طبيعة الوثيقة كان له متطلباته القانونية من خلال المجهودات التشريعية لوضع الإطار القانوني للمعاملات الإلكترونية ، وتحديد المصطلحات التقنية والقانونية المرتبطة بها ، وكذلك من حيث انسجام النصوص الجنائية مع الشكل الجديد للجرائم المعتمدة على المعلوماتية .

كما اقتضى هذا التحول مجموعة من المتطلبات التقنية التي تعتبر الأساس لإستكمال الإطار القانوني للمعاملات الإلكترونية، والتي ترتبط في شق مهم منها بتوفير الأمن المعلوماتي.

إن هذا التزاوج بين القانون والمعلوماتية أصبح ضروريا لمواجهة أشكال الإعتداءات على المعلومة الموجودة في وعاء الكتروني ، خاصة عندما تتحول هذه الإعتداءات إلى أفعال إجرامية وبصور مختلفة ، قد تمس بسرية وتكامل وموثوقية المعلومة المعالجة آليا، وكثيرا ما ترتبط هذه الجرائم أو تتداخل مع جريمة التزوير في الوثيقة الرسمية الإدارية المعلوماتية، من خلال جريمة الدخول غير المشروع للنظام التي قد تقترن بها جريمة تعطيل نظام المعالجة الآلية ، بما تنطوي عليه من تغيير للحقيقة في المعلومات، أو من خلال الإعتداءات العمدية

على سلامة المعطيات، وجرائم الإلتلاف والإحتيال، إلا أن جريمة التزوير المعلوماتي ترتبط بوجود وثيقة بالمفهوم القانوني ، حيث تتأرجح هذه الجريمة بين الوجود والعدم بوجود هذه الوثيقة أو إنعدامها، فإذا كانت هذه الوثيقة رسمية صادرة عن جهات إدارية، فإنها تتمتع بثقة عامة لدى تداولها ، مما يجعل حمايتها ضد التزوير أشد .

إن هذه الصلة الوطيدة بين قيام جريمة التزوير ووجود الوثيقة ابتداء جعل الفقه والتشريع يتجه نحو تحديد مفهوم الوثيقة المعلوماتية ومن أصنافها الوثيقة الرسمية الإدارية، ثم تحديد قيمتها الثبوتية التي تعتبر أساس وعلّة تجريم التزوير فيها، مما أدى إلى ظهور اتجاهات عديدة في ذلك .

لقد تعددت الإتجاهات التشريعية من خلال النماذج والصيغ التشريعية على المستوى الدولي والوطني، حيث كان قانون الأونسترال النموذجي للتجارة الإلكترونية بمثابة الدليل الإرشادي في كيفية تنظيم التعامل بالوثيقة المعلوماتية في مختلف المعاملات حتى تلك المعاملات الرسمية التي تخص الجهات الحكومية، وذلك من خلال إعمال مبدأ النظر الوظيفي لمواجهة هذه الطبيعة المستجدة للوثيقة، وقد تم صياغة العديد من النماذج التشريعية الوطنية وفق هذا الدليل لإزالة العقبات القانونية أمام التحول إلى المعاملات اللاورقية، لكن هذه النماذج تباينت من حيث منهجها في تنظيم هذه المعاملات، حيث تقاربت بعض النماذج التشريعية العربية من خلال وضع نصوص خاصة تضطلع بتحديد المفاهيم والمصطلحات المستحدثة في هذا المجال، وتبين القيمة القانونية للوثيقة المعلوماتية كدليل إثبات مدني ، ومن التشريعات السبّاقة في ذلك عرضنا ثلاث نماذج على التوالي وهي قانون المعاملات الإلكترونية الأردني،

قانون المعاملات والتجارة الإلكترونية الإماراتي، قانون التوقيع الإلكتروني في مصر ، مع بعض الاختلاف بين هذه التشريعات من حيث النصوص القانونية في تحديد مفهوم الوثيقة المعلوماتية، وشروط تمتعها بالحماية القانونية لا سيما الشروط التقنية، وما يرتبط بذلك من تحديد قيمتها كدليل إثبات، أما التشريع الفرنسي فهو نموذج له خصوصيته من حيث أنه اعتمد منهاجا مغايرا في تنظيم التعامل بالوثيقة المعلوماتية وتحديد قيمتها الثبوتية، حيث وسع مفهوم الوثيقة ضمن صيغة النص القائم المتعلق بالإثبات، معتمدا مبدأ النظر الوظيفي للمساواة بين الدليل المدني الورقي ونظيره المعلوماتي.

إن تلك الإتجاهات التشريعية كانت لها امتداداتها الفقهية أيضا، فقد ظهرت اتجاهات فقهية في تحديد مفهوم الوثيقة المعلوماتية بصفة عامة، انقسمت بين اتجاه مادي وآخر موضوعي كانت لها انعكاساتها على تحديد مفهوم التزوير في هذا النوع من الوثائق، مما انعكس أيضا على الصيغ التشريعية الجنائية في تجريم التزوير، غير أن هذه الإتجاهات تنطلق جميعها من ضرورة توافر مجموعة من الشروط التقنية في الوثيقة المعلوماتية لمساواتها وظيفيا بالوثيقة الورقية، ومن ثم معادلتها بها في مجال الإثبات، وإضافة الحماية القانونية عليها، حيث تتعلق هذه الشروط بالكتابة والتوقيع ، الحفظ والثبات .

لقد تعددت الصيغ التشريعية في تجريم تزوير الوثيقة المعلوماتية، حيث نجد صيغة النص المتعلق بالتزوير في قانون العقوبات الفرنسي وهي صيغة موسعة تشمل كل تزوير في وثيقة ذات قيمة قانونية مهما كانت طبيعتها ورقية أو معلوماتية، ليتم تغطية أشكال التزوير المستجدة التي أفرزتها التكنولوجيا المعاصرة، إذ فصل المشرع الجنائي الفرنسي من خلال المادة 1/441

من قانون العقوبات المعدل الجدل القائم حول طبيعة الوثيقة محل التزوير ، كما أنه فصل في طبيعة المصلحة المحمية في جريمة تزوير الوثيقة المعلوماتية ، وبذلك انفصلت هذه الجريمة عن جرائم الإعتداء على نظم المعالجة الآلية للمعطيات لإختلاف المصلحة المحمية، بينما بقي الجدل قائماً بالنسبة لصيغة نص التزوير التقليدي في التشريعات المقارنة في مدى امتداده ليشمل التزوير في الوثيقة المعلوماتية، ولذلك حاولت بعض الدول تجريم التزوير فيها بنصوص منفصلة عن قانون العقوبات، كما هو الحال في مصر من خلال نصوص قانون التوقيع الإلكتروني وقانون الأحوال المدنية، وكذا في الإمارات العربية المتحدة من خلال القانون الإتحادي لجرائم تقنية المعلومات.

إن ضبط صيغة النص المجرم للتزوير في قانون العقوبات ، أو ضبط صيغة النص المجرم للتزوير في الوثيقة المعلوماتية في قوانين مستقلة سيحسم الجدل في هذه المسألة ، كما سيسهل تحديد الوصف القانوني المناسب عند تشابك الأفعال المكونة للسلوك المادي فيها مع جرائم معلوماتية أخرى .

فمن خلال الصيغ التشريعية الجنائية في التزوير يتبين أن الركن المادي في جريمة تزوير الوثيقة الرسمية الإدارية المعلوماتية يقوم بأفعال مختلفة عن التزوير التقليدي ، وذلك بالتلاعب في محتوى الوثيقة داخل النظام الذي يخص أحد الجهات الإدارية الحكومية، أو بخلق وثيقة معلوماتية غير صحيحة، دون حصر للطرق التي يقع بها التزوير ، وهي الصيغة المستحدثة في التشريعات الجنائية المقارنة في تجريم التزوير.

لكن الجدل استمر في تقرير وقوع التزوير من عدمه بحسب ما إذا كان منصبا على مخرجات الحاسب الآلي ، أم على المعلومات المخزنة فيه، غير أن هذه التفرقة لم تكن منطقية، وهي تخالف مقصد المشرع من وراء تجريم التزوير، لذلك فإن التزوير يقع على مخرجات الحاسب الآلي، كما يقع على المعلومات المخزنة فيه، ولذلك أصبحت صيغة النص المجرم للتزوير تجمع بين جانبيين أحدهما موضوعي والآخر تقني.

إن اختلاف الصيغ التشريعية في تجريم التزوير في الوثيقة المعلوماتية ينعكس بالضرورة على صيغة العقاب، حيث نجد هذه الصيغة لدى المشرع الجنائي المصري والإماراتي الذين جرما التزوير في هذه الوثيقة في نصوص مستقلة تحيل إلى قانون العقوبات في حال كانت العقوبة المقررة فيه أشد في باب التزوير، أما المشرع الجنائي الفرنسي فقد خصص مجموعة من الفقرات الواردة ضمن المادة 441 من قانون العقوبات لتصنيف العقوبات المقررة لجريمة التزوير بالتناسب مع طبيعة الوثيقة المزورة وصفة الجاني .

كما أن تنوع صور جريمة تزوير الوثيقة الرسمية الإدارية المعلوماتية، وأهمها تزوير التوقيع الإلكتروني، والبطاقة الإئتمانية أدى إلى إتباع بعض التشريعات المقارنة منها معينا، حيث تم تجريم تزوير التوقيع الإلكتروني بنص مستقل مثلما فعل المشرع المصري من خلال نصوص قانون التوقيع الإلكتروني، ذلك أن هذه الجريمة مختلفة عن جريمة تزوير التوقيع العادي، كما تم تجريم تزوير البطاقة الإئتمانية، الفصل الجدل الفقهي حول طبيعتها القانونية من حيث كونها وثيقة من الناحية القانونية من عدمه لتقرير مدى وقوع التزوير فيها .

بناء على ما سبق يمكننا حصر نتائج البحث فيما يلي :



1- ترتبط جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية بوجود هذه الوثيقة بالمعنى القانوني، حيث لا بد من تمتعها بقيمة قانونية كدليل إثبات مدني يساوي الدليل الرسمي الورقي .

2- اعتمد قانون الأونسترال النموذجي للتجارة الإلكترونية مبدأ النظير الوظيفي لتحقيق المساواة بين الكتابة ورسالة البيانات (الوثيقة المعلوماتية)، واستيعاب أي وسيلة مستجدة تفضي إليها التكنولوجيا المتطورة، ومن أجل ذلك استوجب مجموعة من الإشتراطات التقنية والقانونية .

3- اتبعت العديد من الدول نفس منهج قانون الأونسترال النموذجي للتجارة الإلكترونية لإزالة العقبات القانونية أمام التعامل بالوثيقة المعلوماتية، وهو ما سار عليه المشرع الأردني، الإماراتي، والمصري ، حيث تعتبر هذه التشريعات من النماذج العربية الأولى في تنظيم المعاملات الإلكترونية، كما سار على هذا المنهج المشرع الفرنسي أيضا، تبعا لمتطلبات هذا القانون وكذا قانون التوجيه الأوربي للتوقيعات الإلكترونية.

4- اختلفت التشريعات الوطنية في صيغها المتعلقة بتنظيم التعامل بالوثيقة المعلوماتية بصفة عامة ومساواتها بالوثيقة الورقية، لكنها اجتمعت حول مبدأ النظير الوظيفي الذي قرره قانون الأونسترال.

5- انتهج كل من المشرع الأردني، الإماراتي، والمصري منهاجا واحدا وهو تنظيم التعامل بالوثيقة المعلوماتية في قانون مستقل، وهو نفس المنهج المتبع في تجريم تزوير هذه الوثيقة.

6- لم توفق هذه التشريعات في ضبط المصطلحات من الناحية القانونية والتقنية ، حيث تباينت المصطلحات المستخدمة في التعريف بالوثيقة المعلوماتية بين مصطلح السجل الإلكتروني،

المستند الإلكتروني، رسالة المعلومات، رسالة بيانات، على خلاف قانون الأونسترال النموذجي الذي استخدم مصطلح رسالة البيانات.

7- فتحت هذه التشريعات المجال أمام استخدام الوثيقة المعلوماتية في المعاملات الرسمية، ولدى المؤسسات والدوائر الحكومية ، مما استوجب حماية الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية ضد أشكال الإعتداءات والجرائم الماسة بها ، ومن بينها التزوير .

8- لم يكن منهج هذه التشريعات واضحا، ولم تكن الصيغ التشريعية الجنائية دقيقة حيث :  
(أ) - لم يحدد المشرع المصري في نصوص قانون التوقيع الإلكتروني أركان جريمة تزوير الوثيقة المعلوماتية، سواء من حيث السلوك المادي (الذي خلط فيه بين الإلتاف والتزوير)، أو من حيث نوع القصد المطلوب. كما أنه لم يضع أحكاما خاصة بتزوير الوثيقة الرسمية الإدارية إلا من خلال نصوص متفرقة، مما جعل منهج المشرع المصري قاصرا عن استيعاب جريمة التزوير.

(ب) - أحسن المشرع الإماراتي عندما جرم تزوير المستند الإلكتروني الصادر عن مؤسسات عامة اتحادية أو محلية في نص مستقل ضمن القانون الاتحادي الخاص بجرائم تقنية المعلومات، وكذا عندما شدد العقوبة عند تزويره، لكنه لم يوفق في صيغته الجنائية التي لم تبين الركن المادي لهذه الجريمة، مع عدم وضوح نوع القصد المطلوب .

9- انتهج المشرع الفرنسي منهجا مغايرا للنماذج التشريعية السابقة ، حيث جسد مبدأ النظر الوظيفي في التعامل بالوثيقة المعلوماتية - وهو المبدأ الذي قرره قانون الأونسترال - من خلال تحقيق الإنسجام بين النصوص القانونية القائمة والمتطلبات التكنولوجية، بتوسيع

المصطلحات المتعلقة بالدليل الكتابي واشتراطاته في القانون المدني من جهة، ومفهوم التزوير في قانون العقوبات من جهة أخرى، لتحقيق المقصد من تجريم التزوير لا سيما عندما يقع هذا الفعل على الوثيقة الرسمية الإدارية ، كما حصر العقوبات المقررة لهذه الجريمة تبعا لنوع الوثيقة المعلوماتية المزورة، مشددا العقوبة في حال كانت الوثيقة رسمية أو صادرة عن إدارة عامة .

10- ساعدت الإتجاهات الفقهية في تكوين مدلول الوثيقة المعلوماتية بوجه عام، لكنها اختلفت هي الأخرى في ضبط هذا المدلول مما انعكس على طبيعة النص المجرم للتزوير، حيث اختلف فيما إذا كانت تلك الأجسام المادية الحاملة للمعلومات بالأساليب المعلوماتية، أم أنها تلك المعلومات الخاضعة للمعالجة بالأساليب السابقة .

11- لا يمكن للوثيقة المعلوماتية أن تؤدي وظيفتها مثل الوثيقة الورقية إلا إذا توافرت فيها الشروط الفنية والتقنية وهي الكتابة الإلكترونية، التوقيع الإلكتروني، سلامة المحتوى وثباته، وهو الإشتراط الوظيفي المطلوب لمساواتها بها من حيث القيمة القانونية، وبالتالي حمايتها ضد التزوير .

12- البيانات المعالجة الموجودة على دعامة الكترونية تؤدي نفس الدور الذي تؤديه الوثيقة الورقية في مجال الإثبات دون الإعتداد بنوع هذه الدعامة طالما أمكن الإحتفاظ بها والرجوع إليها كلما دعت الحاجة إلى ذلك.

13- يمكن تحديد مدلول الوثيقة المعلوماتية استنادا إلى عنصرين هما الدعامة المادية والمعلومات المعالجة بالأساليب المعلوماتية، ويجب ربط هذا المدلول بالنص المجرم للتزوير .

14- جريمة تزوير الوثيقة المعلوماتية لها علاقة بجرائم معلوماتية أخرى، قد ترتبط بها مثل جريمة الإحتيال المعلوماتي التي ترتبط بجريمة تزوير البطاقة الائتمانية، أو قد تشتهه بأخرى مثل جريمة الإتلاف .

15- تقوم جريمة تزوير الوثيقة المعلوماتية بأفعال مختلفة عن التزوير التقليدي عن طريق التلاعب في محتوى وثيقة داخل النظام، أو بخلق وثيقة معلوماتية غير صحيحة ، دون الإعتداد بطريقة التزوير .

16- تتنوع صور جريمة تزوير الوثيقة الرسمية الإدارية المعلوماتية ، وأكثرها شيوعا تزوير التوقيع الإلكتروني، وتزوير البطاقة الائتمانية .

17- تقوم جريمة تزوير التوقيع الإلكتروني بأفعال مختلفة عن تزوير التوقيع العادي من خلال الحصول على منظومة التوقيع الإلكتروني بطريقة غير مشروعة بنية استخدامها في التوقيع على هذه الوثيقة، أو من خلال كسر الشفرة الخاصة بها ونسخها وإعادة استخدامها.

18- يرتبط تزوير البطاقة الائتمانية بالتلاعب في كيانها المعلوماتي، كما هو الحال بالنسبة لكيانها المادي ، بل إن تزويرها لن يتم بشكل مستقل عن التلاعب في تلك المعلومات المشفرة الموجودة عليها .

## التوصيات :

1. توحيد المصطلحات القانونية والتقنية في مجال المعاملات الإلكترونية، خاصة ما يتعلق بمفهوم الوثيقة المعلوماتية واشتراطاتها لمعادلتها وظيفيا بالوثيقة الورقية، وكذا نوع التوقيع الإلكتروني المقترن بها الذي يسمح بأداء نفس الوظائف التي يؤديها التوقيع الخطي .
2. إعتداد مبدأ النظير الوظيفي في الصيغ التشريعية لإمكانية التعامل بالوثيقة المعلوماتية مقارنة بالوثيقة الورقية، ومساواتها بها من حيث القيمة القانونية في الإثبات ، من خلال الإسترشاد بما نص عليه قانون الأونسترال في هذا المجال خاصة ما يتعلق بتحقيق هذا المبدأ من الناحية التقنية .
3. تبني الإتجاه الموسع في صيغة النص المتعلق بالدليل الكتابي ، وكذا صيغة النص المجرم للتزوير فيه لإستيعاب الأشكال المستحدثة تكنولوجيا لتجنب الإحالة إلى نصوص مستقلة، وهو الإتجاه الأنسب لربط القانون بالمعلوماتية .
4. تحديد الشروط التقنية اللازمة في التوقيع الإلكتروني المقترن بالوثيقة المعلوماتية، كي تتمتع هذه الأخيرة بالحماية القانونية اللازمة ضد التزوير ، ولضمان الثقة عند التعامل بها، لاسيما إذا كانت هذه الوثيقة صادرة عن جهات إدارية عامة، ويعتبر التوجيه الأوربي للتوقيع الإلكتروني نموذجا في هذا المجال، حيث ميز بين التوقيع الإلكتروني البسيط، والتوقيع الإلكتروني المتقدم الذي يمنح قيمة قانونية أقوى للوثيقة المعلوماتية .

5. عدم تحميل النص الجنائي التقليدي في التزوير تأويلات تتنافى مع مبدأ الشرعية وحظر القياس، حيث لا يمكن في إطار هذا النص اعتبار تغيير الحقيقة في الوثيقة المعلوماتية بوجه عام جريمة تزوير لعدم انسجام صيغة النص مع هذا الشكل المستحدث للوثيقة .
6. تجنب الحلول المجتزئة لتطبيق النص الجنائي القائم دون ضرورة تعديله ، من خلال مد هذا النص ليشمل المعلومات المزورة بالأساليب المعلوماتية شريطة إثباتها على دعامة ورقية، لأن هذا يعني بقاء التلازم بين الوثيقة والطبيعة الورقية .
7. تجنب الصيغة التشريعية التي تصنف جريمة تزوير الوثيقة المعلوماتية ضمن جرائم المساس بالأنظمة المعلوماتية، وذلك لإختلاف المصلحة المحمية جنائياً ، حيث المصلحة المعتبرة في جريمة التزوير هي حماية الثقة العامة في الوثيقة لاسيما الوثيقة الرسمية الصادرة عن الجهات الإدارية ، بينما المصلحة المعتبرة في جرائم المساس بالأنظمة المعلوماتية هي حماية النظام .
8. ضبط الصيغ التشريعية الجنائية المتعلقة بتزوير الوثيقة الرسمية الإدارية المعلوماتية في بعض النماذج التشريعية العربية منها قانون التوقيع الإلكتروني المصري، والقانون الإتحادي لجرائم تقنية المعلومات الإماراتي، من خلال بيان الركن المادي والمعنوي لجريمة التزوير، لا سيما تزوير الوثيقة الرسمية الإدارية ببيان السلوك المادي ونوع القصد المتطلب، وضبط المصطلحات الواردة في النص منها مصطلح الوثيقة .
9. ضبط صيغة التجريم من حيث بيان النية الإجرامية المطلوبة ، وهي نية الغش في تغيير الحقيقة اضراراً بالغير ، كما أشارت إلى ذلك اتفاقية بودابست حول الإجرام المعلوماتي.

10. الفصل بين جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية وبعض الجرائم المعلوماتية التي قد تتصل بها كجريمة الدخول غير المشروع لنظام المعالجة الآلية، وجريمة تعطيل هذا النظام ، حيث المصلحة المحمية جنائيا هي سرية المعلومة ، وسلامة سير النظام، وذلك على غرار اتجاه المشرع الجنائي الفرنسي الذي فصل جريمة التزوير عن الجرائم الماسة بالأنظمة المعلوماتية بعد تعديل قانون العقوبات .

11. تجنب الصيغة التشريعية الجنائية الدالة على حصر طرق التزوير أو محاولة تعدادها لعدم ملاءمتها نتيجة التطور التكنولوجي المستمر .

12. يجب أن تكون صيغة النص المجرم دالة على طبيعة الوثيقة المعلوماتية محل التزوير من حيث قيمتها القانونية في الإثبات .

13. استخدام العبارات الدالة على مرونة النص المجرم للتزوير لإستيعاب أي أشكال محتملة للوثيقة قد تظهر مستقبلا .

14. ضبط صيغة العقاب في بعض الصيغ الجنائية العربية المجرمة لتزوير الوثيقة المعلوماتية، من حيث تدرج العقاب حسب طبيعة هذه الوثيقة .

15. على القاضي الجنائي مراعاة التشابه بين بعض الجرائم المعلوماتية الواقعة ضد سلامة المعلومة وجريمة التزوير، لأنها ليست ذات حدود قاطعة وممانعة ، وهي جريمة الإعتداء العمدي على المعطيات ، حيث يقوم الركن المادي فيها بأفعال الإلتلاف ، أو المحو ، أو التعديل، أو حذف المعطيات داخل النظام ، وهي نفس الأفعال التي قد تكون السلوك

المادي في جريمة التزوير، وكذا جريمة الإلتلاف، حيث تتم بمحو المعطيات ، أو تعديلها بالإضافة، أو الحذف ، لأن ذلك كثيرا ما أثار مسألة اختلاف التكييف الجنائي .

16. على القاضي الجنائي مراعاة خصوصية جريمة تزوير الوثيقة الرسمية الإدارية المعلوماتية باعتبارها قد تتم في أي مرحلة من مراحل تشغيل نظام المعالجة الآلية، ففي مرحلة الإدخال يمكن وقوع التزوير المعنوي بإدخال معلومات غير صحيحة للإعتداد بها على أنها صحيحة، أو ترك إدخال معلومات أساسية لتغيير الحقيقة، وفي مرحلة المعالجة تتداخل جريمة التزوير مع جريمة الإلتلاف أو جريمة الإعداء العمدي على المعطيات من خلال التلاعب في برامج النظام المعلوماتي، ولذلك لا بد من التكييف القانوني السليم للوقائع وتطبيق النص الجنائي المناسب .

17. على القاضي الجنائي مراعاة الإرتباط بين جريمة التزوير والإحتيال المعلوماتي الذي يتم عن طريق تغيير البيانات لإيهام المجني عليه بصحتها لغرض الحصول على فائدة مالية ، حيث قد يستعمل الجاني أساليب التزوير المعلوماتي لهذا الغرض، وبالتالي تقترن هذه الجريمة بجريمة الإحتيال خاصة في جرائم الإحتيال عن طريق البطاقة البنكية .

18. إن الإرتباط بين جريمة التزوير والإحتيال المعلوماتي في الفرض السابق يصعب من مهمة القاضي الجنائي في تحديد الوصف القانوني المناسب، نتيجة تعدد الأوصاف ، مما يدعو إلى توحيد الإجتهد القضائي في هذا المجال.

19. يحتاج القاضي الجنائي للحكم بوجود تزوير في الوثيقة المعلوماتية إلى خبراء متخصصين في كشف أساليب التزوير المعلوماتية ، وتتبع أثر التزوير في هذه الوثيقة .



20. مراعاة الأساليب المستخدمة في التزوير المعلوماتي باعتبارها لا تترك أثرا ظاهرا ، حيث تتم بأساليب تقنية فنية ، وبالتالي يحتاج الأمر لجهاز تقني متخصص في تتبع الدليل لكشف التزوير .

## قائمة المصادر والمراجع

أولا : القوانين

I- قوانين دولية :

1- قرار 51/162 المؤرخ في 16/12/1996 المتضمن قانون الأونسترال النموذجي بشأن التجارة الإلكترونية .

2- Directive 1999/93/Ce du parlement Européen et du conseil du 13 Decembre 1999 sur un cadre communautaire pour les signatures Eléctroniques, Journal officiel des communautés Européennes, n° L013,(19/01/2000).

3- قرار 185 صادر عن المجلس الأوروبي مؤرخ في 23/11/2001 حول الإجرام المعلوماتي.

4- قرار 80/56 المؤرخ في 12 ديسمبر 2001 المتضمن قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية .

II- قوانين وطنية :

أ- القانون الأردني :

1- قانون رقم 85/2001 المؤرخ في 11/12/2001 المتعلق بالمعاملات الإلكترونية الجريدة الرسمية ، عدد 4524 ، (2001/12/31) .

ب- القانون الإماراتي :

1- قانون رقم 02/2002 المؤرخ في 12 فبراير 2002 المتعلق بالمعاملات والتجارة الإلكترونية، الجريدة الرسمية ، عدد 277 ، (2002/02/16).

2- قانون اتحادي 2006/02 المؤرخ في 30 يناير 2006 المتعلق بمكافحة جرائم تقنية المعلومات، الجريدة الرسمية . عدد 442 ، (31 يناير 2006) .

### ج- القانون المصري :

1- قانون رقم 2004/15 المؤرخ في 21/04/2004 المتعلق بتنظيم التوقيع الإلكتروني ، الجريدة الرسمية، عدد 17 ، (2004/04/22) .

2- قانون رقم 94/143 المؤرخ في 09/06/1994 المتعلق بسجلات الحالة المدنية الجريدة الرسمية ، عدد 23 ، (1994/06/10) .

3- قرار وزاري 05/108 المتضمن اللائحة التنفيذية للقانون 04/15 المتعلق بالتوقيع الإلكتروني.

### د- القانون الفرنسي :

1- Droit pénal français modifié en 1993 .

2- Loi n 230/2000 du 13/03/2000 portant adaptation du droit de la preuve aux technologies de l'information et relative a la signature électronique .

3- Décret d'application 272/2001 du 30 Mars 2000 relatif à l'application des article modifiés du Droit civil Journal officiel, n° 77, (31 Mars 2001) .

## ثانيا : مراجع باللغة العربية

### I- الكتب :

#### • كتب عامة :

- 1- آمال عثمان، شرح قانون العقوبات، القسم الخاص .د.ن، د.م ، د.ت .
- 2- عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني الجديد، المجلد الثاني ، منشورات حلبي الحقوقية ، ط3 ، بيروت ، 1998 .
- 3- عمر السعيد رمضان ، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، 1986.
- 4- عوض محمد، الجرائم المضرة بالمصلحة العامة، دار المطبوعات الجامعية، الإسكندرية، 1985 .
- 5- محمود نجيب حسني ، شرح قانون العقوبات (القسم الخاص)، دار النهضة العربية ، القاهرة، 1987.

#### • كتب متخصصة :

- 1- ابراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية . مجلس النشر العلمي، جامعة الكويت، 2003 .
- 2- أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي (دراسة مقارنة). دار النهضة العربية، ط1، القاهرة ، 2000.
- 3- أحمد خليفة الملط، الجرائم المعلوماتية. دار الفكر الجامعي، ط2، الإسكندرية 2006

- 4- اسامة سمر حسين، الإحتيال الإلكتروني الوجه القبيح للتكنولوجيا . الجنادرية للنشر والتوزيع، ط1، عمان، الأردن، 2011.
- 5- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني. دار النهضة العربية، ط1، القاهرة، 2006
- 6- آمال قارة، الحماية الجزائرية للمعلوماتية في التشريع الجزائري. دار هومة، ط1 ، الجزائر، 2006 .
- 7- أمير فرج يوسف، عالمية التجارة الإلكترونية وعقودها . المكتب الجامعي الحديث، دم ، 2009 .
- 8- إيمان مأمون أحمد سليمان، إبرام العقد الإلكتروني وإثباته . دار الجامعة الجديدة، الإسكندرية، 2008.
- 9- إيهاب فوزي السقا، الحماية الجنائية والأمنية لبطاقات الإئتمان. دار الجامعة الجديدة للنشر، الإسكندرية، 2007.
- 10- بكر بن عبد الله أبو زيد ، بطاقة الإئتمان . مؤسسة الرسالة ، دم، 1996.
- 11- بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات. دار الفكر الجامعي، الإسكندرية، 2008 .
- 12- ثروت عبد الحميد، التوقيع الإلكتروني. دار الجامعة الجديدة ، الإسكندرية ، 2007 .
- 13- جلال محمد الزعبي، أسامة احمد المناعسة ، جرائم تقنية نظم المعلومات الإلكترونية (دراسة مقارنة) . دار الثقافة للنشر والتوزيع ، عمان ، الأردن ، 2010.

14- حازم نعيم الصمادي، المسؤولية في العمليات المصرفية الإلكترونية. دار وائل للنشر، عمان، الأردن، ب.ت.

15- حسن طاهر دواد ، جرائم نظم المعلومات . أكاديمية نايف العربية للعلوم الأمنية ، ط1، الرياض 2000.

16- حنان ربحان مبارك المضحكي، الحماية الجائبة لبطاقات الائتمان الممغنطة (دراسة مقارنة). المكتب الجامعي الحديث ، دم، 2012.

17- حسين عبد الباسط جمعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الإنترنت. دار النهضة العربية، القاهرة، 2000 .

18- حسين محمد الشبلي، مهند فايز الدويكات، الإحتيال المصرفي. دار مجدلاوي، ط1، عمان الأردن، ب.ت .

19- خالد عبد الفتاح محمد، التنظيم القانوني للتوقيع الإلكتروني. المركز القومي للإصدارات القانونية، ط1، دم، 2009 .

20- خالد محمد كدفور المهيري ، جرائم الكومبيوتر والإنترنت والتجارة الإلكترونية. معهد القانون الدولي ، ط2 ، دبي ، ب.ت .

21- خالد مصطفى فهمي، النظام القانوني للتوقيع الإلكتروني في ضوء التشريعات العربية والإتفاقيات الدولية. دار الجامعة الجديدة، الإسكندرية ، 2007 .

22- خالد ممدوح ابراهيم ، إبرام العقد الإلكتروني، دراسة مقارنة. دار الفكر الجامعي، الإسكندرية، 2005.

- 23- خالد ممدوح ابراهيم، **التقاضي الإلكتروني**. دار الفكر الجامعي، الإسكندرية، 2007 .
- 24- خالد ممدوح ابراهيم، **أمن الحكومة الإلكترونية**. الدار الجامعية، الإسكندرية، 2008 .
- 25- خضر مصباح اسماعيل الطيبي ، **أساسيات أمن المعلومات والحاسوب** ، دار الحامد، ط1، عمان ، الأردن، 2010.
- 26- داوود عبد الرزاق الباز، **الحكومة الإلكترونية وأثرها على النظام القانوني للمرفق العام** . منشأة المعارف، الإسكندرية، 2008 .
- 27- راسم سميح محمد عبد الرحيم، **التجارة الإلكترونية في خدمة التجارة والمصارف العربية**. مكتبة البنك المركزي، القاهرة ، 1997.
- 28- رحيمة الصغير، **العقد الإداري الإلكتروني** . دار الجامعة الجديدة ، الإسكندرية، 2007 .
- 29- رياض فتح الله بصله ، **جرائم بطاقة الائتمان** . دار الشروق ، ط1 ، القاهرة ، 1995.
- 30- سامح عبد الواحد التهامي، **التعاقد عبر الإنترنت**. دار الكتب القانونية، المحلة الكبرى، مصر، 2008.
- 31- سعد ياسين، **الإدارة الإلكترونية وآفاق تطبيقاتها العربية** . معهد الإدارة العامة، السعودية، 2005 .
- 32- سليم سداوي ، **عقود التجارة الإلكترونية** ، دراسة مقارنة. دار الخلدونية، ط1، الجزائر ، 2008 .
- 33- الصالحين محمد العيش، **الكتابة الرقمية طريقا للتعبير عن الإرادة ودليلا للإثبات**. منشأة المعارف ، ط1، الإسكندرية ، 2008 .

34- ضياء أمين مشيمش، التوقيع الإلكتروني دراسة مقارنة . صادر للمنشورات الحقوقية ، ط1، د.م، 2003.

35- عادل حرشوش، أحمد علي صالح، ستار البياتي، الإدارة الإلكترونية مرتكزات فكرية ومتطلبات تأسيس عملية . المنظمة العربية للتنمية الإدارية، القاهرة ، 2007 .

36- عباس العبودي، الحجية القانونية لوسائل التقدم العلمي في الإثبات المدني. الدار العلمية، ط1، عمان، الأردن ، 2002 .

37- عبد الفتاح بيومي حجازي، الحكومة الإلكترونية الكتاب الثاني. دار الكتب القانونية، د.م، 2007.

38- عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة. دار الفكر الجامعي، الإسكندرية، 2007 .

39- عبد الفتاح بيومي حجازي، الحكومة الإلكترونية. دار الفكر الجامعي، ط1، الإسكندرية ، 2008 .

40- عبد الفتاح بيومي حجازي، الحكومة الإلكترونية بين الواقع والطموح. دار الفكر الجامعي، ط1، الإسكندرية، 2008 .

41- عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة. دار الفكر الجامعي، الإسكندرية، ب.ت .



- 42- عبد الناصر محمد محمود فرغلي ، محمد عبيد سيف سعيد المسماري ، الإثبات الجنائي ، بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة . جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2007.
- 43- علي جبار الحسناوي، جرائم الحاسوب والأنترنت، دار اليازوري ،عمان، الأردن،2009.
- 44- عماد علي الخليل، الحماية الجزائية لبطاقات الوفاء دراسة تحليلية مقارنة. دار وائل للنشر، عمان ، الأردن ، د . ت .
- 45- عمر حسن المومني، التوقيع الإلكتروني وقانون التجارة الإلكترونية. دار وائل للنشر والتوزيع، ط1 ، عمان ، الأردن ، 2003 .
- 46- فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون. منشورات حلبي الحقوقية ، بيروت، لبنان ، 2003 .
- 47- فداء يحيى أحمد الحمود ، النظام القانوني لبطاقة الإئتمان. دار الثقافة، د . م ، د . ت .
- 48- فيصل سعيد الغريب، التوقيع الإلكتروني وحججه في الإثبات. المنظمة العربية للتنمية الإدارية، القاهرة ، 2005 .
- 49- محمد أمين الرومي، المستند الإلكتروني . دار الكتب القانونية ، المجلة الكبرى، مصر ، 2008 .
- 50- محمد أمين الشوابكة، جرائم الحاسوب والإنترنت. مكتبة دار الثقافة للنشر والتوزيع، ط1، عمان ، الأردن، 2004 .

51- محمد حسام محمود لطفي، الحماية القانونية لبرامج الحاسب الإلكتروني. دار الثقافة للطباعة والنشر، القاهرة ، 1987 .

52- محمد حماد مرهج الهيبي، الحماية الجنائية لبطاقة الإئتمان الممغنطة. دار الكتب القانونية، القاهرة، 2009.

53- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والقانون المقارن. دار الجامعة الجديدة، الإسكندرية ، 2007 .

54- محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات . دار النهضة العربية، القاهرة ، 2003.

55- محمد محمد السادات، خصوصية التوقيع الإلكتروني دراسة مقارنة . دار الفكر والقانون، ط1، القاهرة ، 2011 .

56- معاوي أسعد صوالحة ، بطاقات الإئتمان ، النظام القانوني وآليات الحماية الجنائية والأمنية دراسة مقارنة. المؤسسة الحديثة للكتاب ، ط1، طرابلس ،لبنان ، 2011.

57- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية. منشورات حلبي الحقوقية ، ط1، بيروت، لبنان ، 2005 .

58- نادر عبد العزيز شافي ، المصارف والنقود الإلكترونية. المؤسسة الحديثة للكتاب، ط1 ، طرابلس ، لبنان ، 2007 .

59- نادر فاحوش ، العمل المصرفي عبر الإنترنت . الدار العربية للعلوم، ط1 ، بيروت، لبنان، 2001 .

60- ناهد فتحي الحموري ، الأوراق التجارية الإلكترونية. دار الثقافة، ط1، عمان، الأردن،  
2009 .

61- نجاح محمد فوزي، وعي المواطن العربي تجاه جرائم الاحتيال. "بطاقات الدفع الإلكتروني  
نموذجاً". جامعة نايف العربية للعلوم الأمنية ، الرياض ، 2007.

62- هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن. دار النهضة  
العربية، القاهرة، 1992.

63- وسيم شفيق الحجار ، الإثبات الإلكتروني . مكتبة صادر ناشرون ، دم، 2002

64- يوسف أحمد النوافلة ، حجية المحررات الإلكترونية في الإثبات . دار وائل للنشر، ط1 ،  
عمان ، الأردن، 2007 .

\* كتب جد متخصصة :

1- أحمد محمود خليل ، جرائم تزوير المحررات . دن ، دم ، 2008 .

2- إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية . دار الجامعة الجديدة،  
الإسكندرية، 2008.

3- عبد الرحمن عبد الله حميد آل علي ، جرائم التزوير المعلوماتية. دن ، ط1، دم ،  
2009 .

4- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت. دار  
الكتب القانونية، المحلة الكبرى ، 2005 .

5- عبد الله بن سعود محمد السراني ، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني. جامعة نايف العربية للعلوم الأمنية ، ط1 ، الرياض، 2011 .

6- محمد أحمد وقيع الله ، أساليب التزييف والتزوير وطرق كشفها. أكاديمية نايف العربية للعلوم الأمنية، الرياض ، 2003 .

7- منير محمد الجنبهي، ممدوح محمد الجنبهي، تزوير التوقيع الإلكتروني . دار الفكر الجامعي، الإسكندرية، 2006 .

## II- الرسائل العلمية :

### • رسائل علمية متخصصة :

1- حماد مختار، تأثير الإدارة الإلكترونية على إدارة المرفق العام وتطبيقاتها في الدول العربية، (مذكرة ماجستير)، تخصص تنظيم سياسي وإداري ، قسم العلوم السياسية والعلاقات الدولية، كلية العلوم السياسية والإعلام، جامعة يوسف بن خدة، الجزائر، 2007 .

2- علي محمد عبد العزيز، تطبيقات الحكومة الإلكترونية، (رسالة ماجستير)، قسم العلوم الإدارية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2005./06/07

3- عمر بن محمد العتيبي، الأمن المعلوماتي، (أطروحة دكتوراه)، تخصص علوم أمنية، كلية الدراسات العليا، قسم العلوم الإدارية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010.

• رسائل علمية جد متخصصة :

1- أحمد عبد الواحد أحمد آل علي، جريمة التزوير في التوقيع الإلكتروني دراسة مقارنة، (رسالة ماجستير)، تخصص قانون جنائي، كلية القانون وعلوم الشرطة، أكاديمية شرطة دبي، 2011 .

2- عبد الرحمن عبد الله حميد آل علي، جرائم التزوير المعلوماتية دراسة تحليلية تأصيلية، (رسالة ماجستير)، تخصص علوم جنائية، أكاديمية شرطة دبي، ب . ت .

3- عماد محمد علي البلوي ، جريمة تزوير التوقيع الإلكتروني دراسة وصفية لأساليب الكشف والتحقيق والتجريم، (مذكرة ماجستير في العلوم الشرطية)، قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية ، الرياض، 2009/10/28 .

III- مننديات ومؤتمرات علمية :

1- أحمد شرف الدين ، "حجية المحررات الإلكترونية في الإثبات"، ورقة عمل مقدمة في ندوة المعاملات القانونية الإلكترونية وعقود التجارة الإلكترونية، دبي ، فيفري 2007 .

2- أسامة روبي، "حجية التوقيع الإلكتروني في الإثبات والإدعاء مدنيا بتزويره"، مؤتمر المعاملات الإلكترونية، جامعة الإمارات العربية المتحدة، د.ت.

3- إياد عبد الرزاق سعد الله، "التجارة الإلكترونية بين القانون النموذجي للأونسترال والتشريع الكويتي"، بحث مقدم لندوة الجوانب القانونية والتنظيمية للإتصال الإلكتروني، الكويت، 3-5 نوفمبر 2001 .

4- بسام الحمادي، "مفاهيم ومتطلبات الحكومة الإلكترونية"، ورقة بحثية مقدمة إلى مؤتمر الحكومة الإلكترونية، معهد الإدارة العامة، الرياض، 29 يناير 2002 .

5- طوني عيسى، "الركائز القانونية والتنظيمية للإدارة الإلكترونية"، ورشة العمل الإقليمية حول الحكومة الإلكترونية، صنعاء، 1-3 ديسمبر 2003 .

6- عبد الله بن سليمان، "الأثر الاقتصادي لتطبيق أعمال الحكومة الإلكترونية"، منتدى الأعمال الحكومية الثالث، السعودية، 18-20 سبتمبر 2006 .

7- عطا السنباطي، "الإثبات في العقود الإلكترونية دراسة فقهية مقارنة"، أعمال مؤتمر الأعمال المصرفية الإلكترونية، الإمارات العربية المتحدة، 10-12 ماي 2003 .

8- علي السيد الباز، "الحكومة الإلكترونية والإدارة المحلية"، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، مركز البحوث، الإمارات العربية المتحدة، 26 أبريل 2003 .

9- علي عبد القادر القهوجي، "الحماية الجنائية للبيانات المعالجة الكترونياً" بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، الإمارات العربية المتحدة، 1-3 مايو 2000 .

10- عمر الشيخ الأصم، "البطاقات الائتمانية المستخدمة والأكثر انتشاراً في البلاد العربية"، أعمال ندوة تزوير البطاقات الائتمانية. أكاديمية نايف العربية للعلوم الأمنية، ط1، الرياض، 2002 .

11- كمال رزيق، مسدور فارس، "التجارة الإلكترونية وضرورة اعتمادها في الألفية الثالثة"، نادي الدراسات الاقتصادية، كلية العلوم الاقتصادية وعلوم التسيير، جامعة سعد دحلب، البلدية، ب.ت.

- 12- محمد رأفت عثمان، "ماهية بطاقة الائتمان وأنواعها وطبيعتها القانونية وتمييزها عن غيرها"، بحث مقدم لمؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، جامعة الإمارات العربية، 2003 .
- 13- محمد عبد الرسول خياط، "عمليات تزوير البطاقات الائتمانية"، أعمال ندوة تزوير البطاقات الائتمانية، أكاديمية نايف العربية للعلوم الأمنية، ط1، الرياض، 2002 .
- 14- محمد عقاد، "جريمة التزوير في المحررات للحاسب الآلي دراسة مقارنة"، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون، القاهرة، 25-28/10/1993 .
- 15- محمود سحنون، "النظام المصرفي والبطاقات البلاستيكية"، بحث مقدم لمؤتمر تشريعات عمليات البنوك بين النظرية والتطبيق، جامعة اليرموك، الأردن ، 2002 .
- 16- مولود قارة، "التوثيق الإلكتروني"، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية حول بيئة المعلومات الآمنة، الرياض، 06-07 أبريل ، 2010 .
- 17- وليد العاكوم، "مفهوم وظاهرة الإجرام المعلوماتي"، بحوث مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 1-3 مايو 2000 .
- 18- يونس عرب، "جرائم الكمبيوتر والانترنت"، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للبحوث والدراسات الجنائية، أبو ظبي، الإمارات العربية المتحدة، 10-12 ديسمبر 2002.

## VI - مجلات علمية :

- 1- أسامة بن غانم العبيدي، "حجية التوقيع الإلكتروني"، المجلة العربية للدراسات الأمنية والتدريب، عدد 56، ب.ت .
- 2- سحر قدوري الرفاعي، " الحكومة الإلكترونية وسبل تطبيقها"، مجلة اقتصاديات شمال إفريقيا، عدد 07، ب.ت .
- 3- عادل يوسف عبد النبي الشكري، "الجريمة المعلوماتية وأزمة الشرعية الجزائية"، مجلة الجريمة المعلوماتية، عدد 07 ، (2008) .
- 4- عبد الجبار الحنيص، "الحماية الجزائية لبطاقات الإئتمان الممغنطة من التزوير" مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، العدد 02، (2008) .
- 5- غازي أبو عربي، فياض القضاة، "حجية التوقيع الإلكتروني"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، العدد الأول ، (2004) .
- 6- محمد علي قطب، "الجرائم لمعلوماتية وطرق مواجهتها"، الأكاديمية الملكية للشرطة، البحرين، (مارس 2010) .
- 7- نادر شافي ، "التوقيع الإلكتروني الاعتراف التشريعي به وتعريفه القانوني"، مجلة الجيش، عدد 249، (آذار 2006) .
- 8- كتب المدير ورجل الأعمال، مجلة خلاصات، عدد 19، (أكتوبر 2003) .



#### IV - مقالات إلكترونية :

- 1- ابراهيم سليمان عبد الله، "التجارة الإلكترونية أمن المعلومات"، ب.ت، ([www.kau.](http://www.kau.sa.files/0002389/ecom)) .( 72 sa.files/ 000 2389/ecom
- 2- ابراهيم العناني، "تزوير بطاقات الإئتمان"، 2011/11/07، ([www.justice-](http://www.justice-lawhome.com/vb/showthread.php?t=23500))،  
lawhome. ([com / vb/ showthread. Php ? t = 23500](http://www.justice-lawhome.com/vb/showthread.php?t=23500)).
- 3- أحمد السيد كردي، "التوقيع الإلكتروني مفهومه التكنولوجي وحمايته"، 30 سبتمبر 2011، ([kenanaonline.com/users/ahmedkordy/posts/323677](http://kenanaonline.com/users/ahmedkordy/posts/323677)).
- 4- أسامة عبيد، " التوقيع الإلكتروني " ، 2009/09/02 ، ([http://knol. gooole.](http://knol.gooole.com/k/dressam-eibeed/)) ،  
( [no com/k/ dressam-eibeed/-/8](http://knol.gooole.com/k/dressam-eibeed/)
- 5- أمجد حمدان الجهني، " جرائم بطاقة الدفع الإلكتروني عبر شبكة الإنترنت " ، ب . ت ،  
( [www.cojss.com /](http://www.cojss.com/replay.php?a=219) )
- 6- حاتم محمود عبد الرزاق ، " تعريف وخصائص التوقيع الإلكتروني" ، 11 سبتمبر 2012 ،  
( [www.ksp.gov.SD](http://www.ksp.gov.sd) ) .
- 7- حسين بن سعيد بن سيف الغافري، "الجرائم الواقعة على التجارة الإلكترونية"،  
([www.Mohamoon.com/montada/Default.aspx](http://www.Mohamoon.com/montada/Default.aspx)) ، 2010/07/09
- 8- حسني ثابت، "التجارة الإلكترونية تحول من التقليدية إلى الآلية"، 2009/08/31 ،  
([www.egynews.net](http://www.egynews.net)) .

- 9- ذاكر محي الدين، "آفاق استراتيجية : دور الحكومة الإلكترونية في التنمية المستدامة"،  
جريدة الصباح، يومية، العراق ، 19 أوت 2009، (www.alsabah.com) .
- 10- زيان سويدان، " انتحال الهوية الرقمية "، ب.ت، (-www.urdri.fdspt.mu.tn/Zied-  
Souiden-usurpation-id). (Souiden-usurpation-id).
- 11- سهيل ياسين، "الحكومة الإلكترونية"، جريدة الصباح، يومية، العراق، 20/09/2009،  
(www.Alsabah.com).
- 12- عدنان برنو، " قانون التوقيع الإلكتروني"، مجلة المعلوماتية، عدد 05، (تموز 2006)،  
(. news.syhttp://infmag).
- 13- محمد محروك، "خصوصيات التوقيع الإلكتروني وحجته في الإثبات"، 4 فيفري 2013،  
(www.marocdroit.com).
- 14- مولود قارة، "التعبير عن الإرادة في عقود التجارة الإلكترونية"،  
ب.ت، (Tadrib.hmsageria.net/ hame/pieces/iradelect).
- 15- نبيل زوين، "السندات الإلكترونية"، 29/10/2009، ([www.dahsha.com/uploads/](http://www.dahsha.com/uploads/))  
(-electronyya.pdfmuharriat).
- 16- نزيه عبد اللطيف، "التزوير المعلوماتي"، 9 يوليو 2011، (<http://nazihabdd dellatif>).  
(html [blogspot.com/2011/blog-spot-09](http://blogspot.com/2011/blog-spot-09)).
- 17- نوبي محمد حسن، "منظومة الحكومة الإلكترونية"، ب.ت، ([www.publications.ksu.edu](http://www.publications.ksu.edu)).  
(conferences sa/).

18- هشام محمد عبد الوهاب، "الضوابط الفنية والتقنية لإضفاء ذات الحجية القانونية للتوقيعات الإلكترونية في القانون المصري"، 2008/12/31، (signature. [www.electronic.gov.eg](http://www.electronic.gov.eg)) .

19- ياسر العدل ، "التوقيع الإلكتروني"، 2009/09/29 ، ([www.ahewar.org/debat/](http://www.ahewar.org/debat/)) ، (. asp?aid=186248[show.art](http://www.ahewar.org/show.art)) .

ثالثا : مراجع باللغة الفرنسية

#### I- Livres :

- 1- Beare Augère, pierre Bresse et Stéphanie Thuilier, **paiement Numérique Sur Internet** . Thonson publishing, S.L , 1997.
- 2- Geert Delrue, **Faux en Ecriture** . Maklu, S.L , 2007 .
- 3- Gilles St Amant , **Gouvernement en ligne** . ESG , Montréal, 2004.
- 4- Maximilien Amegee, **La Signature Electronique** . BEDA, S.L, 2002 .

#### II- Thèses et Mémoires :

- 1- Carine Bernard, **L'utilisation de la Signature Electronique au CNRS**, (Stage d'application), Institut Régional d'administration de lille, 2003/2004.
- 2- Hocine Boutella, **Système Biometrique de vérification de Signatures manuscrit en ligne**, (Mémoire de Magister), Systèmes Informatiques, école Nationale d'informatique , Alger , S.D.
- 3-Julien Esnault , **La Signature Electronique**, (Mémoire de Dess de droit du Multimédia et de l'informatique), Université de droit, paris, 2002/2003 .
- 4- Stéphane Caidi , **la preuve et la conservation de l'écrit dans la société de l'information**, (Mémoire présenté pour l'obtention du garde Maîtrise en droit), faculté de droit, université de montréal, decembre 2002 .
- 5- Thuy – Nam – Trân Tran, **L'acte Authentique Notarie Electronique**, (Thèse présenté a la faculté de droit), Institut de loi comparé, université de montréal, Août 2001 .

### **III- Ateliers et Centres Scientifiques :**

1- Françoise Banat – Berger et Anne Canteaut, "**Intégrité, Signature et processus d'archivage**", Direction des Archives de France, S.D.

2- Laila Zouak, "**Securité et confiance dans les réseaux et Systemes d'information**", Atelier sur la Sécurisation des réseaux et systemes d'information, Rabat , 19-20 Juin 2006.

3- Melanie Kowalski , "**Cybercriminalité**", centre canadien de la statistique juridique, decembre 2002 .

4- Steven Globberman, "**Définition et Evaluation des liens entre commerce électronique et croissance de la productivité** ", programme des publications de recherche d'industrie, canada, avril 2001 .

5- yvon Merliere, Dominique Jacomet et evelyne chaballier, "**l'impact du commerce électronique en matiere de soldes et de promotions** ", Institut Français de la mode, Avril 2011.

6- "**Virus Informatique**", Atelier Internet – Securité, Genève, 4 Juin 2004 .

### **IV- Les revues :**

1- Aminata Ball, "**Quelque réflexions sur l'administration Electronique**", Revue Française d'administration Publique, n° 110, 2004 .

2- Capirioli, "**Le Juge et la preuve Electronique**", Revue de droit des Technologies de l'information, N°10, (10 Janvier 2000).

3- Phillipe Bluteau, "**Le Faux en Ecriture Publique**", Courrier des Maires, n° 249, (Septembre 2011) .

4- Martine Boudreau, "**La Nouvelle définition de l'écrit en Matière de preuve**",Revue Experts, N°47,(06/2000) .

5- Mukadi Musuyi, "**Cybercriminalité, le Sida Informatique**", Revue Lubila, n°01, Janvier 2008 .

#### **IIV- Articles Electroniques :**

1- "Disque Dur", Fiche thématique 009, Cases, Luxembourg, S.D , ([www.Cases.public.lu/fr/publications/fiches/pdf](http://www.Cases.public.lu/fr/publications/fiches/pdf)).

2- Abderrahmane Nitaj, "**la cryptographie et la confiance Numérique**", 23 Mars 2013, ([www.math.unicaen.fr](http://www.math.unicaen.fr)).

3- Anthony Ben, "**Définition et Sanction pénales du faux**",23/08/2011, ([www.legavox.fr/blog/maitre-anthony-ben/d](http://www.legavox.fr/blog/maitre-anthony-ben/d))

4- Cedric Feretti et autres, "**Le Stockage Magnétique**", S.D, ([www.louisneel-centenaire.ingp.fr/img](http://www.louisneel-centenaire.ingp.fr/img))

5- Dominique Launay,"**Etat des Lieux et Orientation des projets concernant les cartes a puce et autre Supports d'identité**", S.D, ([www.Jres.org/paper/53.pdf](http://www.Jres.org/paper/53.pdf)).

6- Fabien Kerbouci, "**La preuve Ecrite Electronique et le Droit Français**" 21/01/2010, ([www.e-juristes.org](http://www.e-juristes.org)) .

7- François paget,"**Fraude Financière et Opérations Bancaire en Ligne: Menaces et Contre-Mesures**", 2009, ([www.bulletinnumis-matique.fr/bn/bn069/images/mcafee](http://www.bulletinnumis-matique.fr/bn/bn069/images/mcafee)) .

8- Guy Weber, "**La Fin de la Bande Magnétique**", Décembre 2011 ,( [www.six-telekurs.com/fr/dl-thich](http://www.six-telekurs.com/fr/dl-thich) clearit 50 Fraud) .

- 9- Jean – Luc Parouty, "**La Signature Électronique**". S.D , ([www.jres.actes/ 79.pdf](http://www.jres.actes/79.pdf)).
- 10- Louis Garron, "**L’incrimination du faux et du Mensonge en Droit pénal**", 20 Juin 2011, (ircgov-mu).
- 11- Lucien pauliac, "**La Face Cachée de la Signature Electronique**", 27 Septembre 2010 , ([www.megapreuve.org/cariboost Files/Signature électronique.pdf](http://www.megapreuve.org/cariboost/Files/Signature%20%C3%A9lectronique.pdf)).
- 12- Marie Helene, "**Le Faux et la preuve**" , 09/03/2011, ([www.blogavocat.fr/space/ marie - helene.isern-real](http://www.blogavocat.fr/space/marie-helene.isern-real)).
- 13- Nadina Velicu, Marcel podasca, "**Le Combat Contre la Criminalité Informatique dans le contexte Europeen**" , S.D , ( [www. proceeding univdanubius.ro](http://www.proceedingunivdanubius.ro)).
- 14- Najoua Djerad, "**Cycle de vie du Document Électronique et obligations de conservation**". S.D,([www.ebsi.umontreal.ca/rech/ebsi-enssil/pdf/Djerad.pdf](http://www.ebsi.umontreal.ca/rech/ebsi-enssil/pdf/Djerad.pdf))
- 15- N.Samarc, "**Les Actes Athentiques Électroniques**". 14 Novembre 2005, ([www.droit-ntic.com](http://www.droit-ntic.com)).
- 16- Pascal Renaud, "**Historique de l'internet du Nord au Sud**", S.D, ([www.africanti.org](http://www.africanti.org)).
- 17- Philippe pierre, "**L’indemnisation du préjudice Moral en Droit Français**", S.D, ([www.fondation-Droit continental.org/préjudice-mor étude-fr](http://www.fondation-Droit continental.org/pr%C3%A9judice-mor%C3%A9tude-fr)).
- 18- Pierre Florent, "**La Signature Électronique**",24/07/2009, ([www.telio.be/ blog/ 2009/07/24/ Signature.électronique](http://www.telio.be/blog/2009/07/24/Signature.%C3%A9lectronique)).
- 19- Thierry Blanchet, "**La Realisation du Minutier Central de Notaires de France**", 7 Decembre 2004, ([www.frili.org/spip.php? Article 60](http://www.frili.org/spip.php? Article 60)).

20- Valérie Sédallian, "**Preuve et Signature Électronique**", 09 Mai 2000, (Juriscom.net).

21- "**Disque Compact**", 11 octobre.2011,(Fr .wikipedia.org).

22- "**Document de Reflexion sur la question des cartes d'identité au Québec** ", Octobre 1996, ([www.cai.gov.qc.ca/06-documentation/01/pdf](http://www.cai.gov.qc.ca/06-documentation/01/pdf)).

23- Fiche de L'AWT (Agence wallonne de Télécommunication), "La Carte d'identité Électronique (EID)", 07/07/2005, ([www.awt.be/contenu/tel/gov/fr](http://www.awt.be/contenu/tel/gov/fr)).

24- "**Qu'est-ce qu'un disque mémoire flash U S B**", 2011,(windows microsoft.com/ fr/windows .

## **VII- La jurisprudence :**

1- La cour de cassation, chambre criminelle, 27 Février 1984.

2- La cour de cassation, chambre commerciale, 2 décembre1997 .

3- La cour de cassation, chambre criminelle, 24 Mai 2000.

4- La cour de cassation, chambre criminelle, 18 Octobre 2000.

5- La cour de cassation, chambre criminelle, 22 Octobre 2003.

6- La cour de cassation, chambre criminelle, 28 Octobre 2003.

7- La cour de cassation, chambre civile, 30 septembre 2010.

## فهرس المحتوى

1	مقدمة
10	فصل تمهيدى : تأثير المعلوماتية على الأنظمة القانونية
11	المبحث الأول : التحول من المعاملات الورقية إلى المعاملات الإلكترونية
11	المطلب الأول : أسباب ظهور المعاملات الإلكترونية
11	الفرع الأول : التجارة الإلكترونية
16	الفرع الثانى : الإنترنت
21	الفرع الثالث : الإدارة الإلكترونية
32	الفرع الرابع : الحكومة الإلكترونية
38	المطلب الثانى : متطلبات التحول إلى المعاملات الإلكترونية
38	الفرع الأول : المتطلبات القانونية للتحول إلى المعاملات الإلكترونية
41	الفرع الثانى : المتطلبات التقنية للتحول إلى المعاملات الإلكترونية
44	المبحث الثانى : ظهور الجرائم المتعلقة بالمعلوماتية
45	المطلب الأول : جرائم ضد سرية المعلومات وسير النظام
46	الفرع الأول : جريمة الدخول غير المشروع للنظام
49	الفرع الثانى : جريمة تعطيل نظم المعالجة الآلية
51	المطلب الثانى : جرائم ضد سلامة المعلومات وقيمتها الإقتصادية



- 51 الفرع الأول : جريمة الإعتداء العمدي على المعطيات
- 53 الفرع الثاني : جرائم الإلتلاف والإحتيال
- 60 الباب الأول : الوثيقة المعلوماتية محل التزوير
- 61 الفصل الأول : مفهوم الوثيقة المعلوماتية تشريعا وفقها
- 61 المبحث الأول : مفهوم الوثيقة المعلوماتية في التشريعات المقارنة
- 61 المطلب الأول : مفهوم الوثيقة المعلوماتية في القانون الدولي
- 62 الفرع الأول : عناصر الوثيقة المعلوماتية في قانون الأونسترال النموذجي
- 66 الفرع الثاني : مبدأ النظر الوظيفي لتحديد مفهوم الوثيقة المعلوماتية
- 69 المطلب الثاني : مفهوم الوثيقة المعلوماتية في التشريعات الوطنية
- 69 الفرع الأول : مفهوم الوثيقة المعلوماتية في التشريع الأردني
- 73 الفرع الثاني : مفهوم الوثيقة المعلوماتية في التشريع الإماراتي
- 78 الفرع الثالث : مفهوم الوثيقة المعلوماتية في التشريع المصري
- 81 الفرع الرابع : مفهوم الوثيقة المعلوماتية في التشريع الفرنسي
- 86 المبحث الثاني : مفهوم الوثيقة المعلوماتية فقها
- 86 المطلب الأول : الإتجاهات الفقهية في تحديد مفهوم الوثيقة المعلوماتية
- 86 الفرع الأول : مفهوم الوثيقة بوجه عام
- 91 الفرع الثاني : مفهوم الوثيقة المعلوماتية
- 96 المطلب الثاني : نماذج من الوثائق المعلوماتية

- 96 الفرع الأول : العقود الإلكترونية
- 101 الفرع الثاني : البطاقات الإلكترونية
- 110 الفصل الثاني : القيمة القانونية للوثيقة المعلوماتية
- 110 المبحث الأول : الإتجاهات التشريعية حول القيمة القانونية للوثيقة المعلوماتية
- 110 المطلب الأول: الإتجاهات التشريعية الدولية حول القيمة القانونية للوثيقة المعلوماتية
- 111 الفرع الأول : قانون الأونسترال
- 115 الفرع الثاني : التوجيه الأوربي حول التوقيع الإلكتروني
- 118 المطلب الثاني: الإتجاهات التشريعية الوطنية حول القيمة القانونية للوثيقة المعلوماتية
- 119 الفرع الأول : التشريع الفرنسي
- 122 الفرع الثاني : نماذج من التشريعات العربية
- 128 المبحث الثاني : شروط تمتع الوثيقة المعلوماتية بالحماية القانونية
- 128 المطلب الأول : الكتابة الإلكترونية
- 128 الفرع الأول : مفهوم الكتابة الإلكترونية
- 133 الفرع الثاني : شروط الكتابة الإلكترونية
- 136 المطلب الثاني : التوقيع الإلكتروني
- 136 الفرع الأول : مفهوم التوقيع الإلكتروني
- 145 الفرع الثاني : أشكال التوقيع الإلكتروني

- 154 الفرع الثالث : شروط التوقيع الإلكتروني
- 157 **المطلب الثالث : حفظ الوثيقة المعلوماتية**
- 157 الفرع الأول : وسائل حفظ الوثيقة المعلوماتية
- 160 الفرع الثاني : شروط حفظ الوثيقة المعلوماتية
- 164 **الباب الثاني: الصيغ التشريعية في تجريم تزوير الوثيقة الرسمية الإدارية المعلوماتية**
- 165 **الفصل الأول : تحديد مفهوم تزوير الوثيقة الرسمية الإدارية المعلوماتية**
- 165 **المبحث الأول : توسيع مفهوم التزوير في إطار نصوص قانون العقوبات**
- 166 **المطلب الأول : مفهوم التزوير في قانون العقوبات الفرنسي**
- 166 الفرع الأول : توسيع مفهوم الوثيقة محل التزوير
- 170 الفرع الثاني : عناصر التزوير في الوثيقة المعلوماتية
- 173 **المطلب الثاني : مدى تطبيق نص التزوير التقليدي على تزوير الوثيقة المعلوماتية**
- 173 الفرع الأول : عدم تطبيق نص التزوير التقليدي على تزوير الوثيقة المعلوماتية
- 175 الفرع الثاني : تطبيق نص التزوير التقليدي على تزوير الوثيقة المعلوماتية
- 176 **المبحث الثاني: تحديد مفهوم تزوير الوثيقة الرسمية الإدارية المعلوماتية بنصوص خاصة**
- 177 **المطلب الأول : الصيغ التشريعية العربية في تجريم تزوير الوثيقة الرسمية الإدارية المعلوماتية**
- 177 الفرع الأول : صيغة التجريم في التشريع المصري من خلال قانون التوقيع الإلكتروني والأحوال المدنية

- 181 الفرع الثاني : صيغة التجريم في التشريع الإماراتي من خلال القانون الإتحادي لجرائم  
تقنية المعلومات
- 184 المبحث الثالث : مقارنة بين جريمة التزوير التقليدي وجريمة تزوير الوثيقة المعلوماتية
- 184 المطلب الأول : جريمة التزوير التقليدية
- 184 الفرع الأول : تعريف التزوير فقها
- 186 الفرع الثاني : أركان جريمة التزوير
- 188 المطلب الثاني : جريمة تزوير الوثيقة المعلوماتية.
- 188 الفرع الأول: تعريف التزوير المعلوماتي فقها وأثره على الصيغة التشريعية المجرمة له
- 192 الفرع الثاني : خصائص جريمة تزوير الوثيقة المعلوماتية
- 196 الفرع الثالث: علاقة جريمة تزوير الوثيقة المعلوماتية ببعض الجرائم المعلوماتية
- 201 الفصل الثاني : أركان جريمة تزوير الوثيقة الرسمية الإدارية المعلوماتية والعقوبات المقررة  
لها .
- 201 المبحث الأول : أركان جريمة تزوير الوثيقة الرسمية الإدارية المعلوماتية
- 202 المطلب الأول : الركن المادي
- 202 الفرع الأول : السلوك المادي
- 218 الفرع الثاني : الضرر
- 224 المطلب الثاني : الركن المعنوي
- 224 الفرع الأول : القصد العام

- 226 الفرع الثاني : القصد الخاص
- 228 المبحث الثاني:العقوبات المقررة لجريمة تزوير الوثيقة الرسمية الإدارية المعلوماتية
- 228 **المطلب الأول : العقوبات المقررة بنصوص خاصة**
- 229 **الفرع الأول : العقوبات المقررة في قانون التوقيع الإلكتروني المصري**
- 231 **الفرع الثاني : العقوبات المقررة في قانون مكافحة جرائم تقنية المعلومات الإماراتي**
- 233 **المطلب الثاني : العقوبات المقررة في قانون العقوبات الفرنسي**
- 233 **الفرع الأول : اختلاف العقوبة حسب طبيعة الوثيقة محل التزوير**
- 235 **الفرع الثاني : اختلاف العقوبة حسب صفة المزور**
- 237 **الفصل الثالث : صور خاصة لجريمة التزوير المعلوماتي**
- 237 **المبحث الأول : جريمة تزوير التوقيع الإلكتروني**
- 238 **المطلب الأول : جريمة تزوير التوقيع الإلكتروني في التشريع المصري**
- 238 **الفرع الأول : صيغة النص المجرم**
- 249 **الفرع الثاني : علاقة جريمة تزوير التوقيع الإلكتروني ببعض الجرائم المعلوماتية في قانون التوقيع الإلكتروني**
- 253 **المطلب الثاني : خصائص جريمة تزوير التوقيع الإلكتروني**
- 254 **الفرع الأول : ارتباط جريمة تزوير التوقيع الإلكتروني بجريمة السرقة وجريمة الإختراق**
- 255 **الفرع الثاني: استخدام أساليب تقنية في تزوير التوقيع الإلكتروني وصعوبة الكشف عنها**
- 257 **المبحث الثاني : جريمة تزوير البطاقة الائتمانية**

257	المطلب الأول : تعريف بطاقة الإئتمان
258	الفرع الأول : تعريف بطاقة الإئتمان من الناحية المادية
265	الفرع الثاني : تعريف بطاقة الإئتمان من الناحية الموضوعية
267	المطلب الثاني : مدى وقوع التزوير بالتلاعب في البطاقة الائتمانية
267	الفرع الأول : التزوير في المعلومات المقروءة لبطاقة الإئتمان
269	الفرع الثاني : التزوير في المعلومات المشفرة لبطاقة الإئتمان
271	المطلب الثالث : طرق التزوير في بطاقة الإئتمان
272	الفرع الأول : التزوير الكلي لبطاقة الإئتمان
276	الفرع الثاني : التزوير الجزئي لبطاقة الإئتمان
279	الفرع الثالث : استخراج بطاقة ائتمان صحيحة بوثائق مزورة
281	الخاتمة
295	قائمة المصادر والمراجع
317	فهرس المحتوى

## ملخص

ساهمت ثورة المعلومات و التكنولوجيا الرقمية في تغيير طبيعة الوثائق الرسمية الإدارية، حيث بدأ التحول نحو النموذج الإلكتروني لإنجاز المعاملات المختلفة على مستوى الإدارات العامة، حتى أصبحت إدارات رقمية تنجز معاملاتها بوثائق ذات طبيعة معلوماتية .

إلا أن هذا التحول حمل معه أشكال جديدة من الإعتداءات استفادت من هذه التكنولوجيا بشكل غير مشروع ، بل أصبحت تشكل جرائم لمساسها بمصالح محمية جنائيا ،ولما كانت احدى هذه الإعتداءات تمس بالثقة العامة في الوثائق الرسمية و هي مصلحة محمية جنائيا ،فقد ثار الجدل حول تجريم الإعتداء على الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية بالتزوير فيها على غرار الوثيقة الورقية .

هذا الجدل أدى إلى ظهور اتجاهات فقهية و تشريعية في حل المسألة ،فقد انقسم الفقه بين عدم تطبيق النص الجنائي التقليدي لعدم توافر صفة المحرر في الوثيقة المعلوماتية،و بين امكانية تطبيقه باعتبار هذه الوثيقة محررا بتوافر عناصره و عدم ارتباطه بالشكل الورقي ،مما انعكس على الصيغ التشريعية في تجريم تزوير الوثيقة المعلوماتية بين ضرورة وضع نصوص جنائية خاصة للتجريم منفصلة عن القانون الجنائي ،أو توسيع صيغة النص الجنائي التقليدي ليشمل كل تزوير في وثيقة ذات قيمة قانونية مهما كانت طبيعتها.

إن الأخذ بأي صيغة من هذه الصيغ يقتضي مساواة الوثيقة المعلوماتية بالوثيقة الورقية ،خاصة تلك الوثيقة الرسمية الإدارية،مما يتطلب توفير مجموعة من الشروط التقنية،حيث يجب أن تتمتع الكتابة الإلكترونية بالثبات والإستمرارية ،و أن تقترن بتوقيع الكتروني يضمن السرية و الموثوقية، و سلامة الوثيقة من التعديل ،مع حفظها بالوسائل المناسبة بضمان التكاملية و سلامة المحتوى.

## Résumé

La révolution numérique a contribué à changer la nature des documents authentiques administratifs, ce qui permet le passage au format électronique pour la réalisation de diverses transactions au niveau de l'administration publique, jusqu'à qu'elle devienne une administration numérique, complète ses transactions par des documents électroniques.

Ce changement a apporté de nouvelles formes d'atteintes ont bénéficié de la technologie de l'information illégalement, et formé des crimes contre les intérêts protégés criminellement. L'un de ces crimes a touché la confiance publique dans les documents authentiques administratifs, suscitant un débat sur la nature de ce crime si le faux a eu lieu dans un écrit authentique.

Ce débat a conduit à l'émergence de tendances doctrinales et législatives pour résoudre la matière. La doctrine s'est divisée sur la question, il ya l'équipe qui voit le manque de validité de l'application du texte pénal traditionnel à cause de l'absence d'un écrit. au contraire il ya une autre équipe qui voit la possibilité de l'application du ce texte en tant que le document électronique consiste d'un écrit, et ce dernier n'est pas lié à la forme de papier.

Ces visions se sont reflétées sur les formules législatives, et ont entraîné vers l'incrimination du faux dans un écrit électronique par des articles spéciaux, ou bien par l'élargissement de l'article pénal traditionnel pour inclure tous fraude criminelle dans un document à valeur juridique qu'elle que soit son nature.

L'adoption de l'une de ces formules nécessite l'assimilation de l'écrit électronique à l'écrit papier. Cela nécessite un ensemble de conditions techniques liées à la durabilité de l'écrit électronique, l'authentification de signature électronique, l'intégrité et la conservation de document électronique.