جريمة التزوير الإلكتروني كجريمة مستحدثة في التشريع الكويتي

الدكتور/ بدر أحمد الجاسر الراجحي
أستاذ مساعد - قسم القانون الجزائي
كلية الحقوق - جامعة الكويت

ملخص

إن هذه الدراسة تبحث بيان ماهية جريمة التزوير الإلكتروني وبيان محل هذه الجريمة التي تتمثل في المحرر الإلكتروني، وكذلك بيان أركان جريمة التزوير الإلكتروني التي تقوم على ركنين أساسيين وهما الركن المادي والركن المعنوي. وفي السياق ذاته تبحث هذه الدراسة جريمة تزوير التوقيع الإلكتروني باعتبارها أهم صور التزوير الإلكتروني، وذلك من خلال تحليل هذه الجريمة، وتعريف تزوير التوقيع الالكتروني، وبيان وظائفه وخصائصه وصوره وعيوبه، ثم قمنا ببحث آليات حماية التوقيع الإلكتروني من مغبّة تزويرها، كما بحثنا في المبحث الثالث مسألة القواعد القانونية الخاصة بمواجهة جريمة التزوير الإلكتروني، وذلك من خلال مناقشة قواعد الاختصاص الجنائي بشأن جريمة التزوير الإلكتروني من حيث المبادئ المتعلقة بتحديد الاختصاص بالنسبة لجرائم التزوير الإلكتروني، وكذلك من حيث المحاكم المختصة بجرائم التزوير الإلكتروني، كما بحثنا قواعد تحصيل وتقييم الأدلة الخاصة بإثبات جريمة التزوير الإلكتروني، وذلك من خلال مناقشة دور رجال الضبط القضائي في مواجهة جرائم الكمبيوتر (المعلوماتية) وكذلك دور القاضي في تقييم وتقدير الأدلة الخاصة بهذه الجرائم خاصة جرائم التزوير الإلكتروني، ثم أنهينا دراستنا ببيان النتائج والتوصيات التي توصلنا إليها من خلال هذه الدراسة.

مقدمة

تعد جرائم التزوير من أهم الموضوعات في نظام العقوبات المعاصرة، وذلك لخطورتها التي تخل بالثقة الواجب توافرها بين أفراد المجتمع، حيث إن هناك ارتباطاً وثيق الصلة بين جرائم التزوير وما يترتب عليها من آثار دينية واجتماعية واقتصادية، وقد احتلت جريمة التزوير بشكل عام أهمية بالغة في التشريعات القانونية المقارنة (مثل المشرع الفرنسي،

والمصري)، خاصة التشريعات الجزائية التي حددت أركانها وصورها والعقوبات المقررة على ارتكابها، وقد سبق أن جرّم المشرّع الكويتي هذا الفعل في قانون الجزاء الكويتي رقم ١٦ لسنة ١٩٦٠ في المواد (٢٥٧ – ٢٦٢) والتي تتكون من ركن مادي وركن معنوي، حيث يجب توافرهما معاً قبل البحث في مدى تحقق أي نوع من جرائم التزوير المختلفة.

وحيث إن موضوع بحثنا هو التزوير الإلكتروني فإنه يقوم على ما يسمى بالمحرر الإلكتروني الذي يكون عبارة عن مجموعة من العلامات والرموز التي تعبّر اصطلاحاً عن مجموعة مترابطة من الأفكار والمعاني الصادرة عن شخص أو أشخاص معينين وهو في جوهره كتابة مركبة من حروف وعلامات تعبر عن معنى أو فكرة معينة.

وقد تنبهت العديد من التشريعات الجزائية الحديثة المقارنة إلى السلوكيات المستحدثة في جرائم التزوير الإلكتروني والتي عكستها تقنية المعلومات واستطاعت أن تتخطى المفهوم التقليدي للتزوير، وقد تبنّاها المشرّع الكويتي في القانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي (قانون مكافحة جرائم تقنية المعلومات)، وكذلك القانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية الكويتي (قانون المعاملات الإلكتروني).

مشكلة الدراسة:

تعد جريمة التزوير الإلكتروني من الجرائم المستحدثة، والتشريعات الجنائية عادة ما يثار بصددها العديد من الإشكاليات القانونية، والتي تكون عرضة لانتقاد الباحثين والتي نحن بصددها، ويأتي على رأسها عدم وضوح تعريف جريمة التزوير الإلكتروني الوارد في كل من قانون مكافحة جرائم تقنية المعلومات وقانون المعاملات الإلكترونية، وكذلك عدم وضوح القصد الجنائي الوارد في قانون الجزاء، وكذلك قانون مكافحة جرائم تقنية المعلومات، كما أنه لم ترد في قانون مكافحة جرائم تقنية المعلومات أي إشارة للقواعد الإجرائية الجزائية المتعلقة بالجرائم الإلكترونية، وبذلك يتم اللجوء إلى القواعد العامة في قانون الإجراءات والمحاكمات الجزائية والتي تعد تقليدية بطبيعتها، الأمر الذي يثير العديد من الصعوبات، وبالتالي فهذه الدراسة تبحث مدى كفاية النصوص التقليدية والإلكترونية في محاربة الجرائم الإلكترونية.

أهداف الدراسة:

عنت هذه الدراسة بتحقيق العديد من الأهداف التي يمكن إيجازها بما يلي:

- بيان ماهية التزوير الإلكتروني وأركانه.

- دراسة جريمة تزوير التوقيع الإلكتروني كنموذج لجرائم التزوير الإلكتروني لما لها من أهمية بالغة في التعامل الإلكتروني.
- مدى إمكانية تطبيق النصوص التقليدية على جريمة التزوير الإلكتروني من عدمه.
- كيفية مكافحة هذه الجريمة ووضع الآليات اللازمة لحماية محل هذه الجريمة.

أهمية الدراسة:

تكمن الأهمية في تناول الدراسة لظاهرة من أهم الظواهر المستحدثة وهي الجرائم الإلكترونية وبصفة خاصة جريمة التزوير الإلكتروني، فالتطور التقني رغم إيجابياته إلا أن له العديد من السلبيات التي تهدد أمن واستقرار المجتمع خاصة حال ارتكاب هذه الجريمة التي تؤدي إلى الإخلال بالثقة العامة ليس في دولة الكويت فقط بل في العالم كله. ومن ثم كان البحث في التشريعات الخاصة بالجرائم المعلوماتية ومنها جريمة التزوير الإلكتروني في الكويت والتشريعات المقارنة لمواجهة مثل هذه الجريمة.

منهج الدراسة:

اعتمد الباحث في هذه الدراسة على المنهج التحليلي المقارن، فمن خلال المنهج التحليلي سوف يقوم الباحث بتحليل النصوص القانونية وبيان مدى كفايتها من عدمه، وذلك بتحليل الآراء الفقهية والتوفيق بينها وإعطاء الحلول المناسبة، بالإضافة إلى جمع المعلومات المتعلقة بالدراسة وتحليلها، أما من خلال المنهج المقارن، فسوف يقوم الباحث بمقارنة القانون الكويتي بالقوانين الأخرى فيما يخص موضوع البحث واستخراج أوجه التشابه وأوجه الاختلاف فيما بينها.

خطة الدراسة:

سوف نتناول الدراسة وفقاً للخطة التالية:

- مقدمة
- المبحث الأول: ماهية جريمة التزوير الإلكتروني
- المطلب الأول: تعريف جريمة التزوير الإلكتروني.
- المطلب الثاني: محل جريمة التزوير الإلكتروني.
- المطلب الثالث: أركان جريمة التزوير الإلكتروني.

- المبحث الثاني: تزوير التوقيع الإلكتروني.
- المطلب الأول: ماهية التوقيع الإلكتروني.
- المطلب الثاني: آليات حماية التوقيع الإلكتروني من تزويره إلكترونياً
- المبحث الثالث: القواعد القانونية الخاصة بمواجهة جريمة التزوير الإلكتروني.
- المطلب الأول: قواعد الاختصاص الجنائي بشأن جريمة التزوير الإلكتروني.
- المطلب الثاني: قواعد تحصيل وتقييم الأدلة الخاصة بإثبات جريمة التزوير الإلكتروني.

المبحث الأول
ماهية جريمة التزوير الإلكتروني

إن التزوير يعد من الجرائم الدقيقة التي تحتاج للقيام بها عناية خاصة بسبب اختلاف طرق التزوير وتطورها، حيث لم تقتصر جريمة التزوير بمفهومها التقليدي، بل بفضل الوسائل الإلكترونية وسرعة تطورها ظهرت جرائم التزوير الإلكترونية، وهذا الأمر هو ما دعا الدول المتقدمة إلى تناول جريمة التزوير في شكلها الجديد في قوانينها الجزائية لإضفاء الحماية الجزائية على المعلومات أو البيانات الموجودة في الشبكة الإلكترونية التي تتعلق بإثبات حقوق أو مراكز قانونية معينة، وبذلك سنقوم بتقسيم هذا المبحث إلى ثلاثة مطالب، نخصص الأول لتعريف جريمة التزوير الإلكتروني، والثاني لبيان محل جريمة التزوير الإلكتروني، وفي المطلب الثالث: أركان جريمة التزوير الإلكتروني، وذلك على التفصيل الآتي:

المطلب الأول
تعريف جريمة التزوير الإلكتروني

التزوير لغة: هو إصلاح الكلام وتهيئته، وكلمة تزوير مشتقة من أصل زور، والزور هو الكذب والباطل[١]. أما التزوير في الفقه عموماً: هو كل وسيلة يستعملها شخص ليغش بها آخر[٢]. وقد ذهب الفقه الجنائي إلى تعريف التزوير بأنه تغيير الحقيقة بقصد الغش في سند أو وثيقة أو أي محرر آخر بإحدى الطرق التي نص عليها القانون، تغييراً من شأنه إحداث ضرر بالمصلحة العامة أو مصلحة شخص من الأشخاص، ومقترن بنيّة استعمال المحرر المزور فيما أعد له[٣]. وبتضييق النطاق أكثر عرّف البعض التزوير الإلكتروني بأنه أي تغيير للحقيقة يرد على التوقيع أو المحرر أو الوسيط الإلكتروني[٤]. وقد ذهب البعض الآخر إلى أنه تغيير الحقيقة في المستندات المعلوماتية وذلك بقصد استعمالها[٥].

---

(١) أبو بكر عبد القادر الرازي، مختار الصحاح، دار الفكر للطباعة والنشر والتوزيع، ١٩٨١م، ج١، ص٢٨٠.

(٢) محمد عقاد، جريمة التزوير في محررات الحاسب، دراسة مقارنة، المؤتمر السادس، الجمعية المصرية للقانون الجنائي ٢٥-١٩٩٣/١٠/٢٨، دار النهضة العربية، ص٣٩٢.

(٣) د. أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم الخاص، ط٤، دار النهضة العربية، ١٩٩١م، ص٤٠٢.

(٤) د. غنام محمد، مكافحة جرائم الكمبيوتر، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مؤتمر القانون والكمبيوتر والإنترنت، ص٣٣.

(٥) د. علي القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات، ١-٢٠٠٠/٥/٣، ص٦٣.

وقانوناً نصت المادة (٢٥٧) من قانون الجزاء الكويتي على أنه: «يعد تزويراً كل تغيير للحقيقة في محرر بقصد استعماله على نحو يوهم بأنه مطابق للحقيقة، إذا كان المحرر بعد تغييره صالحاً لأن يستعمل على هذا النحو، ويقع التزوير إذا اصطنع الفاعل محرراً ونسبه إلى شخص لم يصدر منه، أو أدخل تغييراً على محرر موجود سواء بحذف بعض ألفاظه أو بإضافة ألفاظ لم تكن موجودة، أو بتغيير بعض الألفاظ، أو وضع إمضاء أو خاتم أو بصمة شخص آخر عليه دون تفويض من هذا الشخص، أو حمل ذلك الشخص عن طريق التدليس على وضع إمضائه أو خاتمه أو بصمته على المحرر دون علم بمحتوياته أو دون رضاء صحيح بها، ويقع التزوير أيضاً إذا غير الشخص المكلف بكتابة المحرر معناه أثناء تحريره بإثباته واقعة غير صحيحة على أنها واقعة صحيحة، ويقع التزوير ممن استغل حسن نية المكلف بكتابة المحرر فأملى عليه بيانات كاذبة موهماً أنها بيانات صحيحة».

كما نص المشرع في قانون المعاملات الإلكترونية الكويتي، في المادة (٣٧) منه على أنه: «مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون آخر، يعاقب بالحبس مدة لا تزيد عن ثلاث سنوات وبغرامة لا تقل عن خمسة آلاف دينار ولا تزيد على عشرين ألف دينار أو بإحدى هاتين العقوبتين كل من: ..... ج) أتلف أو عيب توقيعاً أو نظاماً أو أداة توقيع أو مستنداً أو سجلاً إلكترونياً أو زور شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحوير بأي طريقة أخرى. د) استعمل توقيعاً أو نظاماً أو أداة توقيع أو مستنداً أو سجلاً إلكترونياً معيباً أو مزوراً مع علمه بذلك».

وكذلك نص المشرع الكويتي في قانون مكافحة جرائم تقنية المعلومات في المادة (٣) على أنه: «يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من: ... ٢- زور أو أتلف مستنداً أو سجلاً أو توقيعاً إلكترونياً أو نظام معالجة إلكترونية للبيانات أو نظاماً إلكترونياً مؤتمتاً أو موقعاً أو نظام حاسب آلي أو نظاماً إلكترونياً بطريق الاصطناع أو التغيير أو التحوير أو بأي طريقة أخرى، وذلك باستخدام وسيلة من وسائل تقنية المعلومات، فإذا وقع التزوير على مستند رسمي أو بنكي أو بيانات حكومية أو بنكية إلكترونية تكون العقوبة الحبس مدة لا تجاوز سبع سنوات وبغرامة لا تقل عن خمسة آلاف دينار ولا تجاوز ثلاثين ألف دينار أو بإحدى هاتين العقوبتين».

ومما سبق، من الممكن ملاحظة أن المواد الثلاث السابقة لم تتعرض لتعريف ماهية التزوير، سوى المادة رقم ٢٥٧ من قانون الجزاء الكويتي والتي عرفت التزوير التقليدي

ولم تتعرض للتزوير الإلكتروني، حيث إن هذه الجريمة لم تكن قد ظهرت وقت وضع التشريع من جانب، ومن جانب آخر لم تشر المادة (٣٧) من قانون المعاملات الإلكترونية الكويتي والمادة (٣) من قانون مكافحة جرائم تقنية المعلومات لم تشيرا صراحة أو ضمناً إلى تعريف جريمة التزوير الإلكتروني، حيث إنهما اقتصرا على بيان طرق التزوير الإلكتروني والعقاب المحدد له، ونظراً لحداثة جريمة التزوير الإلكتروني، كان يتعين على المشرع عند سنه التشريعات التي تتناول الجريمة الإلكترونية، النص على تعريف جريمة التزوير الإلكتروني حتى لا يترك الأمر فريسة للتضارب بين الفقهاء.

أما في فرنسا فقد جرّم القانون رقم ١٩ لسنة ١٩٨٨ صورتين من التزوير: الأولى تزوير المستندات الإلكترونية أياً كان شكلها إذا كان من شأنها الإضرار بالغير وهو ما نصت عليه المادة ٥/٤٦٢ من هذا القانون، والثانية تتعلّق باستعمال المستندات المزورة سالفة الذكر وهو ما نصت عليه المادة ٦/٤٦٢[٦]. حيث نصت المادة ٥/٤٦٢ على أن «كل شخص قام بتزوير مستندات آلية أياً كان شكلها ويؤدي إلى حدوث ضرر للغير يعاقب بالحبس مدة تتراوح بين سنة وخمس سنوات وغرامة تتراوح ما بين ٢٠٠٠٠ – ٢٠٠٠٠٠٠ فرنك»[٧].

وبعد مرور ست سنوات، أصدر المشرع الفرنسي قانون العقوبات الجديد الذي ألغى نص المادتين سالفتي الذكر، وذلك بتعديل نص المادة ١/٤٤١ من قانون العقوبات الفرنسي الذي تبنى تجريم التزوير في الوثائق المعلوماتية الإلكترونية، وقد عرفت المادة ١/٤٤١ التزوير بأنه: «كل تغيير بطريق الغش في الحقيقة يكون من شأنه إحداث ضرر ويرتكب بأي طريقة كانت، سواء أكان ذلك في محرر أو أي سند آخر للتعبير عن الفكر، والذي يكون الغرض منه أو كنتيجة له شأناً في إثبات حق أو واقعة لها آثار قانونية»[٨].

ومن الأهمية بمكان الذهاب إلى أن الصياغة الجديدة لنص المادة ١/٤٤١ من قانون العقوبات الفرنسي الجديد لسنة ١٩٩٤، وسَّعت نطاق النص كي يتضمن كل صور

(٦) د. عمر الفاروق، الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دراسة تحليلية نقدية لنصوص التشريع المصري مقارناً بالتشريع الفرنسي، ط٢، ١٩٩٥م، ص٤٨٦.

(٧) د. هشام رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤م، ص٣٣٣.

(٨) Article 441-1: Constititue un faux toute altération frauduleuse de la verité, de nature à causer un prejudice et accomplice par quelque moyen que co soit, dans un écrit ou tout autre support d'expression de la pensee qui a pour objet ou qui peut avoir pour effet d'etablir la prevue d'un faux et l'usage de faux sont punis de trios ans d'emprisonnement et de 45000 euros d'amende".

التعبير عن الفكر والتي تكون في شكل إلكتروني، متى كان لها شأن في إثبات حق أو واقعة لها نتائج قانونية، كما أن المشرع الفرنسي بهذا النص لم يقصر طرق التغيير في الحقيقة (التزوير) على طرق معينة محددة على سبيل الحصر، وإنما أطلق النص من كل قيد يحدد كيفية وقوع التزوير ليستوعب أي شكل يستحدث ويؤدي إلى التزوير، وهذا يؤدي إلى القول بأن المشرع الفرنسي طوّر منهجه وساهم في هذا التعديل بإضفاء التجريم على حالات التزوير الإلكتروني بصفة خاصة لما للتقنية من سرعة وتطور هائل في استحداث وسائل جديدة ومتعددة في مجال الجرائم المعلوماتية بصفة عامة وجريمة التزوير بصفة خاصة؛ ولذا ينبغي على المشرع الكويتي أن يحذو حذو نظيره الفرنسي فيما أقدم عليه في هذا الصدد.

المطلب الثاني

محل جريمة التزوير الإلكتروني

أولاً: عناصر محل جريمة التزوير الإلكتروني

باستقراء نص المادة ٢/٣ من قانون مكافحة جرائم تقنية المعلومات الكويتي، والمادة (٣٧) من قانون المعاملات الإلكترونية نجد أن المشرع في كلا النصين قد نص على ثلاثة عناصر كمحل لجريمة التزوير الإلكتروني وهي التوقيع الإلكتروني، الوسيط الإلكتروني، المحرر الإلكتروني، ويمكن عرضها وفقاً للنحو التالي:

التوقيع الإلكتروني

هو وسيلة إلكترونية يمكن بمقتضاها تحديد هوية الشخص المنسوب التوقيع إليه، مع توافر النية لديه في أن ينتج آثاره القانونية على نحو يماثل التوقيع بخط اليد[٩]. وقد عرفه جانب من الفقه بأنه: «كل إشارات أو رموز أو حروف مرخص بها من الجهة المختصة

(٩) حيث تنص المادة (١) من القانون ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية الكويتي على أنه: «التوقيع الإلكتروني: البيانات التي تتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها، وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مماثلة في مستند أو سجل إلكتروني أو مضافة عليها أو مرتبطة بها بالضرورة ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره».
انظر في تعريف التوقيع الإلكتروني كذلك: نص المادة الأولى من القانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي، وهو ذات التعريف المنصوص عليه في المادة الأولى من القانون رقم ٢٠ لسنة ٢٠١٤.

باعتماد التوقيع ومرتبطة بالتصرف القانوني ارتباطاً وثيقاً تسمح بتمييز شخص صاحبها وتحديد هويته، وتنم دون غموض عن رضائه بهذا التصرف»، فالتوقيع الإلكتروني يقوم بالوظائف التي يقوم بها التوقيع التقليدي وهي تمييز هوية الشخص والتعبير عن رضائه للارتباط بالعمل القانوني، ولا يغفل إجراءات إصدار القانون الإلكتروني وتوثيقه(١٠). وقد عرفه جانب آخر من الفقه بأنه «مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية مَنْ تصدر عنه هذه الإجراءات، وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته»(١١). وهذا التعريف لم يحدد صور التوقيع الإلكتروني بل ذكر أنه مجموعة من الإجراءات التقنية، ومن ثم فإنه يشمل جميع صور التوقيع الموجودة حالياً، وتلك التي ستظهر لاحقاً بفعل التطور التقني، كما أن هذا التعريف قد أبرز وظائف التوقيع الإلكتروني وهي تحديد هوية الموقع والتعبير عن إرادته بالموافقة على مضمون السند الذي تم وضع التوقيع عليه. ونحن من جانبنا نؤيد التعريف الأخير لشموليته، حيث يحتوي على جميع أنواع التوقيع الإلكتروني الحالية وما يمكن أن يظهر مستقبلاً.

الوسيط الإلكتروني

هو ما يسمى بالنظام الإلكتروني المؤتمت والذي عبر عنه قانون المعاملات الإلكتروني بأنه «برنامج أو نظام إلكتروني لحاسب آلي تم إعداده ليتصرف أو يستجيب لتصرف بشكل مستقل كلياً أو جزئياً، دون تدخل أو إشراف أي شخص طبيعي في الوقت الذي يتم فيه التصرف أو الاستجابة له»(١٢).

وفي قانون التوقيع الإلكتروني المصري رقم ١٥ لسنة ٢٠٠٤، فإن الوسيط الإلكتروني حسب نص المادة الأولى منه هو أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكتروني، ومؤدى ذلك أن الوسيط الإلكتروني هو نظام معلوماتي، أي أجهزة وبرامج يساعد في إنشاء التوقيع الإلكتروني وإصدار المحررات الإلكترونية(١٣). وبذلك يكون المشرع المصري في هذا النص قد ساوى بين التزوير الإلكتروني الذي يقع في المحررات

(١٠) د. ثروت عبد الحميد، التوقيع الإلكتروني، مخاطره وكيفية مواجهتها، مدى حجيته في الإثبات، مكتبة الجلاء الجديدة، المنصورة، ٢٠٠١م، ص٤٩.

(١١) د. حسن جميعي، إثبات التصرفات القانونية عن طريق الإنترنت، دار النهضة العربية، ٢٠٠٠م، ص٣٤.

(١٢) انظر في تحديد الوسيط الإلكتروني كذلك: نص المادة الأولى من القانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية.

(١٣) د. عبد الفتاح حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية، ط١، ٢٠٠٥م، ص٥٥٦ وما بعدها.

الإلكترونية أو التوقيع الإلكتروني والذي يقع على المكونات المنطقية من برامج وأنظمة (الوسيط) التي تخص إنشاء التوقيع الإلكتروني.

وهذا ما سار عليه المشرع الكويتي حين نص على توقيع عقوبة الحبس والغرامة أو إحدى هاتين العقوبتين على كل من «زوّر أو أتلف مستنداً أو سجلاً أو توقيعاً إلكترونياً أو نظام معالجة إلكترونية للبيانات أو نظاماً إلكترونياً مؤتمتاً أو موقعاً أو نظام حاسب آلي أو نظاماً إلكترونياً بطريق....». وبذلك يكون المشرع الكويتي قد ساوى بين تزوير المستند أو السجل الإلكتروني والتوقيع الإلكتروني وبين تزوير نظام المعالجة الإلكترونية للبيانات أو نظام إلكتروني مؤتمت أو موقع أو نظام حاسبا آلي أو نظام إلكتروني وهو ما يسمى بالوسائط الإلكترونية وكلها تعد محل جريمة التزوير الإلكتروني.

المحرر الإلكتروني

لم يرد تعريف محدد في القوانين العربية بشأن المحرر الإلكتروني، خاصة قانون مكافحة جرائم تقنية المعلومات الكويتي، وقانون المعاملات الإلكترونية الكويتي، ولكن وردت تعريفات متشابهة مرتكزة في غالبيتها على التعريف الذي ورد في القانون النموذجي للأونسيترال والذي نصت عليه المادة ٢/ج حيث عرفت رسالة البيانات الإلكترونية وهي بمثابة المحرر الإلكتروني والتي صار على نهجها الكثير من تشريعات الدول العربية بأنها «المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكتروني أو البريد الإلكتروني أو البرق أو التلكس أو النسخ البرقي»[١٤]، ومن ثم فقوام السند الإلكتروني باعتباره رسالة معلومات إلكترونية هو إثباته على دعامة إلكترونية وأياً ما كان شكل هذا الإثبات (صورة أو صوت أو كتابة) فهذا يعد إعداد المستند إلكترونياً.

وقد جاء تعريف المستند أو السجل الإلكتروني في قانون المعاملات الإلكتروني على أنه «مجموعة بيانات أو معلومات يتم إنشاؤها أو تخزينها أو استخراجها أو نسخها أو إرسالها أو إبلاغها أو استقبالها كلياً أو جزئياً بوسيلة إلكترونية على وسيط ملموس أو على وسيط إلكتروني آخر، وتكون قابلة للاسترجاع بشكل يمكن فهمه»[١٥]. ويبدو أن

(١٤) د. منير الجنبيهي، د. ممدوح الجنبيهي، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م، ص١١٥-١١٦.

(١٥) انظر كذلك: نص المادة الأولى من القانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية الكويتي وهي مناظرة تماماً للمادة الأولى من القانون ٦٣ لسنة ٢٠١٥.

المشرع الكويتي قد تبنى أيضاً تعريف قانون الأونسيترال النموذجي مثله في ذلك مثل التشريع المصري وغيره من التشريعات العربية المقارنة.

ثانياً: المعلومات التي يمكن أن تكون محلاً لجريمة التزوير الإلكتروني

يتمثل موضوع جريمة التزوير من الناحية التقليدية ومحلها في «المحرر»، فلا وجود للتزوير إذا لم ينصب على تغيير الحقيقة في المحرر، أما من الناحية الإلكترونية فيتمثل في المحرر الإلكتروني والذي يعرّف «بمجموعة من العلامات والرموز التي تعبّر اصطلاحاً عن مجموعة مترابطة من الأفكار والمعاني الصادرة عن شخص أو أشخاص معينين»[١٦]، وهو في جوهره كتابة مركبة من حروف وعلامات تعبّر عن معنى أو فكرة معينة، وحسب الاتجاه التشريعي والفقهي الراجح يفترض إمكانية إدراك مادة المحرر بالقراءة البصرية[١٧]، وأن ينتقل معنى الرموز والعلامات عن طريق المطالعة والنظر، فالفقه متفق على أن فكرة المحرر تفترض إمكانية استشفاف دلالة رموز المحرر بالنظر إليها، لذلك لا يعتبر من قبيل المحررات، الأسطوانة أو شريط التسجيل (الفيلم) الذي سجلت عليه عبارات أياً كانت أهميتها القانونية، وكذلك لا يعد تزويراً ما يدخل على الصوت الذي يحمله من تشويه[١٨].

والعنصر الآخر من عناصر المحرر لمحل التزوير هو أن فكرة المحرر توجب أن يكشف عن شخصية محرره، ومن المستقر عليه فقهاً كذلك أن يكون المحرر معبراً عن فكرة بشرية[١٩]. وإزاء ما تقدم تبرز أهمية تحديد المحررات التي يمكن أن تكون محلاً لجريمة التزوير المعلوماتي، وتحديد مدلول محدد للمستند الإلكتروني وذلك حتى يتسنى تحديد نطاقه ومعالمه، وذلك لاختلاف خطة التشريعات في النص على المستند الإلكتروني ومدى انطباق الحماية المقررة له، فغالبية التشريعات لا تفرد نظرية عامة للمستند الإلكتروني ولا تحدد قواعد عامة تسري على أي مستند تتوافر له الصفة الإلكترونية، وإنما تقتصر هذه التشريعات على النص على أهم تطبيقات فكرة المستند الإلكتروني مثل التوقيع والسجلات الإلكترونية[٢٠].

---

(١٦) د. حسنين عبيد، دروس في قانون العقوبات القسم الخاص، دار النهضة العربية، ١٩٨٢م، ص١٤٣.

(١٧) د. هشام رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤م، ص٢٢٦.

(١٨) د. محمود نجيب حسني، الموجز في شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، ١٩٩٤م، ص٢٤٧.

(١٩) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، ١٩٩٤م، ص١٥٥-١٥٦.

(٢٠) د. أشرف شمس الدين، الحماية الجنائية للمستند الإلكتروني، دراسة مقارنة، المؤتمر العلمي =

وقد ثار خلاف فقهي حول المعلومات التي يمكن أن تكون محلاً لجريمة التزوير الإلكتروني، فمنهم من يرى أن المعلومات التي تصلح أن تكون الوعاء المعلوماتي الجدير بالحماية القانونية هي تلك المعلومات والبيانات التي لها قيمة مادية بوصفها نشاطاً إنسانياً، وضرورة أن يتحقق فيها عنصران: هما التجديد والابتكار من جهة، والسرية، والاستئثار من جهة أخرى، فالتجديد والابتكار ميزة أساسية تفرض نفسها قبل كل شيء، وبانعدامها تزول حقيقة المعلومات(٢١).

فالمعلومة قبل كل شيء تعبير وصياغة مخصصة من أجل تبليغ رسالة، أو يمكن تبليغها عن طريق علامات أو إشارات مختارة لكي تحمل الرسالة إلى الغير، والمعلومة بوصفها رسالة مخصصة للتبليغ يجب أن تكون مادية بحيث تحسها عن الإنسان، وأن تكون مبتكرة، فالمعلومة وإن كانت مادية ومحددة إذا كان الوصول إليها شائعاً من قبل الكافة، فمن السهولة أن يقع الاعتداء عليها، وبالنسبة للسرية فهي صفة ملازمة للمعلومة حيث تحصرها في نطاق محدد من الأشخاص، ومن ثم فالمعلومة الشائعة وغير السرية لا تعد من قبيل المعلومات بمعناها الحقيقي، كما أن الاستئثار كذلك يعد أمراً ضرورياً للمعلومة، لأنه في جميع جرائم المعلوماتية يستأثر الجاني بسلطات تخص غيره على المال المعلوماتي المعتدى عليه بشكل مطلق(٢٢).

ويستند أنصار هذا الاتجاه على أن معظم القوانين التي عالجت جرائم تقنية المعلومات، لاسيما القوانين والتشريعات العربية (ومن بينها القوانين والتشريعات الكويتية)، لم تقم بأي تعديل يبين طبيعة المعلومات التي تصلح لأن تكون محلاً للحماية الجنائية، حيث

= الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، المدة من ٢٦-٢٠٠٤/٣/٢٨، منشور على wwwlarabwinfo.com ص٩. انظر في ذلك: تعريف المستند أو السجل الإلكتروني، حيث تنص المادة (١) من القانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي على: «المستند أو السجل الإلكتروني: مجموعة بيانات أو معلومات يتم إنشاؤها أو تخزينها أو استخراجها أو نسخها أو إرسالها أو إبلاغها أو استقبالها كلياً أو جزئياً بوسيلة إلكترونية، على وسيط ملموس أو على وسيط إلكتروني آخر، وتكون قابلة للاسترجاع بشكل يمكن فهمه» والتوقيع الإلكتروني «البيانات التي تتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها، وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي، أو أي وسيلة أخرى مماثلة في مستند أو سجل إلكتروني أو مضافة عليها أو مرتبطة بها بالضرورة ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره».

(٢١) د. شيماء عبد الغني محمد عطا الله، التزوير المعلوماتي منشور علىwww.shalmaatalla.com

(٢٢) د. محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، موسوعة جرائم المعلوماتية، منشأة المعارف، الإسكندرية، ٢٠٠٦م، ص٨٨.

لم تسوّي بين المعلومة ذات القيمة المادية والمعلومة ذات القيمة المعنوية، كالمساواة بين التزوير في الوثيقة المعلوماتية (المستند المعلوماتي)، والتزوير في المحرر العادي[٢٣].

ويرى جانب آخر من الفقه الجنائي أن المعلومات التي يتم إخراجها في مخرجات ورقية من الحاسب تنطبق عليها نصوص التزوير التقليدية في المحررات، أما البيانات المعالجة فتنطبق عليها نصوص التزوير الإلكتروني الواردة في التشريعات التي عالجت جرائم تقنية المعلومات ومنها جرائم التزوير[٢٤]، وقد استند أنصار هذا الاتجاه إلى أن التزوير يستلزم لوقوعه الكتابة سواء أكانت مرئية أم مؤلفة من علامات أو رموز مرئية، بوصفها متطلباً تقليدياً لجريمة التزوير في المحررات، وهو ما لا يتحقق في جريمة التزوير الإلكتروني، حيث إن تحريف أو تغيير البيانات المسجلة على دعامات معلوماتية كالأشرطة الممغنطة، فإنه يشكل جريمة اعتداء على البيانات وليس تزويراً إلا إذا أخرجت في صورة محرر مكتوب بعد المعالجة الآلية للمعلومات الموجودة في الداخل والتي تم الاعتداء عليها[٢٥].

والكثير من التشريعات لم تضع نصوصاً تحدد بموجبها فكرة المستند الإلكتروني وتحدد قوته في الإثبات وتعاقب على المساس به، ومن ثم ثار خلاف في الفقه عن سريان النصوص العقابية التي تحمي المحررات الورقية على المستند الإلكتروني، فذهب رأي في الفقه إلى وجوب تفسير تعبير «المستند» الوارد في النصوص السارية تفسيراً واسعاً بحيث تشمل معه المستند الإلكتروني – وهذا ما كان يأخذ به القضاء الكويتي في السابق قبل صدور كل من قانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات، والقانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية – حيث استند هذا الجانب من الفقه والقضاء على أنه لا يلزم في المحرر أن يكون مكتوباً على مادة معينة كالأوراق؛ وذلك لأن النص جاء عاماً والمطلق يؤخذ على إطلاقه ما لم يقيد[٢٦]، بينما لا يؤيد الرأي الآخر هذا الاتجاه ويرى الأخذ بالتفسير الضيق لفكرة المستند، فالتفسير الواسع يذهب

(٢٣) د. عمر عيسى الفقي، الجرائم المعلوماتية، دار النهضة العربية، ٢٠٠٥م، ص٦٧.

(٢٤) د. حسام راضي، حماية المعلومات وتشريعات تقنية المعلومات، منشور على شبكة الإنترنت .www arablae.com

(٢٥) د. أحمد تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، الحماية الجنائية، دراسة مقارنة، دار النهضة العربية، ٢٠٠٠م، ص٣٩١.

(٢٦) تمييز ١٥ /١١/ ٢٠٠٥، طعن ٧٧ لسنة ٢٠٠٥ جزائي. انظر كذلك: تمييز ٤/١/ ٢٠١٣، طعن ٣٠٤ لسنة ٢٠١٢ جزائي.

إلى أن تعبير المستند يمكن أن يمتد ليشمل المستند الورقي والإلكتروني[٢٧]. أما التفسير الضيق لفكرة المستند والذي يؤيده الفقه الغالب بأن فكرة المستند لا يمكن أن تسري على المستند الإلكتروني وأنه لابد من صدور تنظيم تشريعي للمستند الإلكتروني يراعى فيه الضمانات التي يجب أن تتوافر في هذا المستند حتى يكفل له الفاعلية في التعامل والقبول في التعاملات[٢٨]، فجريمة التزوير ترتبط بفكرة المحرر، ويترتب على انتفائه انتفاء الجريمة ذاتها، فلا يعد المستند الإلكتروني في نظر هذا الاتجاه الضيق من قبيل المحرر، ومن ثم تنحسر عنه جريمة التزوير.

وفي تقديرنا نرى أن الرأي الموسّع لمدلول المستند الذي يشمل المستند الورقي والمستند الإلكتروني هو رأي منتقد؛ حيث إنه لا يجوز التوسّع في تفسير النصوص الجزائية، وذلك بتطبيق فكرة المحرر والكتابة والتوقيع إذا تحققت بوسيلة إلكترونية؛ والسبب في ذلك أن فكرة المستند الإلكتروني بمعناه الواسع لا تزال حتى الآن عرضة للتطور التقني، ولا يجوز التضحية باستقرار التعاملات قبل التأكد من أداء المستند الإلكتروني لدوره الذي يرسمه له القانون، كما أن التشريعات المقارنة التي أقرت فكرة المستند الإلكتروني قد لجأت إلى إصدار تشريعات خاصة تنظم تطبيقات هذا المستند مثل السجلات والتوقيع الإلكتروني، وإذا كان هذا الرأي صحيحاً لكانت هذه التشريعات قد ساوت في التطبيق بين فكرتي المستند دون حاجة إلى نصوص خاصة، وهو ما لم يحدث، مما يدل على عدم جواز إجراء هذه المساواة من خلال التوسع في التفسير.

أما الرأي الضيق لمدلول المستند فهو الأقرب إلى اتفاقه مع النصوص التشريعية، وأن دليل ذلك هو أن المشرع الكويتي قد جعلها جريمة مستقلة عن جريمة التزوير التقليدية، حيث وضع نصاً خاصاً في قانون مكافحة جرائم تقنية المعلومات وأفرد عقوبة جنائية لكل من زور أو أتلف مستنداً أو سجلاً أو توقيعاً إلكترونياً أو نظام معالجة إلكترونية للبيانات أو نظاماً إلكترونياً مؤتمتاً أو موقعاً أو نظام حاسب آلي أو نظاماً إلكترونياً بطريق الاصطناع أو التغيير أو التحوير أو بأي طريقة أخرى، وذلك باستخدام وسيلة من وسائل تقنية المعلومات وذلك في المادة ٢/٣ من هذا القانون، وهو بهذا قد ساوى بين المستندات الورقية والمستندات الإلكترونية، فإن كانت هذه المساواة من الممكن

(٢٧) د. حسام الدين محمود لطفي، استخدام وسائل الاتصال الحديثة في التفاوض على العقود وإبرامها، دراسة مقدمة إلى ندوة وسائل حسم المنازعات في العمليات المصرفية، مركز القاهرة الإقليمي للتحكيم التجاري الدولي، يونيه ١٩٩٨م، ص٨ وما بعدها.

(٢٨) د. عمر الفاروق، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دراسة تحليلية نقدية لنصوص التشريع المصري مقارناً بالتشريع الفرنسي، ط٢، ١٩٩٥م، ص٧٩.

التوصل إليها عن طريق تفسير النصوص القائمة في قانون الجزاء الكويتي، لما كان المشرع الكويتي بحاجة إلى إفراد هذا النص، ويسري ذات الأمر على نص المادة (٣) من قانون المعاملات الإلكترونية الكويتي، إذ ساوى المشرع الكويتي بين السجلات الورقية وبين السجلات الإلكترونية والمستندات والرسائل والمعاملات والتوقيعات الإلكترونية.

المطلب الثالث

أركان جريمة التزوير الإلكتروني

لجريمة التزوير الإلكتروني ركنان: الركن المادي والركن المعنوي، وهذا ما سوف نبحثه في الفرعين التاليين.

الفرع الأول

الركن المادي لجريمة التزوير الإلكتروني

يقوم الركن المادي لجريمة التزوير الإلكتروني على عناصر ثلاثة وهي: الأول تغيير الحقيقة، والثاني أن يتم تغيير الحقيقة بإحدى طرق التزوير الإلكتروني المنصوص عليها قانوناً، أما الثالث فهو إلحاق الضرر بالمجني عليه، وهذا ما سوف نتناوله كالآتي:

أولاً: تغيير الحقيقة

تغيير الحقيقة هو إبدالها بما يخالفها، وهذا يعد السلوك الإجرامي الذي تقع به جريمة التزوير، فإن انتفى هذا العنصر لا نكون بصدد جريمة تزوير على الإطلاق[٢٩]. ويتم ذلك في التزوير الإلكتروني بأي طريقة يقرها القانون الذي يقرر هذه الجريمة، وذلك بإدخال بعض البيانات أو المعلومات إلى البرنامج من خلال استغلال الأخطاء والعيوب المنطقية التي يحتويها هذا البرنامج، وهي في الحقيقة عبارة عن مجموعة من الممرات الخالية والمتروكة في البرنامج، ويمكن استغلال هذه المحررات المعيبة فنياً بإضافة أية معلومات إليها[٣٠].

ويتم تغيير الحقيقة بتغيير بعض أو كل البيانات الواردة في البرنامج، ومن ثم يعد مرتكباً لجريمة تزوير إلكتروني ذلك الشخص الذي يدخل في برنامج لسجلات الشرطة ويقوم بتغيير أو حذف بعض أسماء المجرمين المطلوبين للعدالة، وعلى العكس لا يعد تزويراً

(٢٩) أ. أحمد أمين، شرح قانون العقوبات الأهلي، القسم الخاص، لجنة التأليف والترجمة والنشر، القاهرة، ١٩٢٣م، ص٤٨٥، د. محمود مصطفى، شرح قانون العقوبات، القسم الخاص، ط/ جامعة القاهرة، ١٩٨٥م، ص١٠٤.

(٣٠) انظر الموقع: WWW.STARTIMES.COM 1F.ASPX? i=1909009

إلكترونياً وقوع الإتلاف على هذا البرنامج الذي تحويه تلك البيانات أو المعلومات، لأننا في هذه الحالة نكون بصدد جريمة إتلاف معلوماتي وليس جريمة تزوير إلكتروني[٣١].

كما يتم تغيير الحقيقة بتحوير المعطيات والبيانات التي تمت معالجتها باتباع إجراءات إلكترونية معينة، وذلك من خلال استخدام الحاسب الآلي لطبع فواتير مصطنعة أو ذات قيمة كبيرة، ومن ثم يقوم العملاء بتسديدها وهم واقعون تحت تأثير الثقة التي يعتقدونها في هذه الحاسبات[٣٢].

والتزوير الإلكتروني لا يتم من قبل مشغل الحاسب فحسب، حيث يمكن أن يتم ذلك التزوير من جانب شخص عادي ليس له أي دراية فنية بتشغيل الحاسب الآلي، ورغم ذلك فإنه يرتكب هذه الجريمة، كما هو الحال بالنسبة للشخص الذي يقوم بالإدلاء بمعلومات أو بيانات إلى مبرمج الحاسب وتكون غير صحيحة ويعلم بأنها مزورة[٣٣].

ومن حيث إمكانية تطبيق نصوص التزوير التقليدية على أنشطة تغيير الحقيقة المعلوماتية، فرغم أن غالبية الدول قد حسمت هذا الأمر لحساب عدم انطباق النصوص التقليدية في جرائم التزوير التقليدية على جرائم التزوير الإلكترونية، واتخذت تدابير تشريعية لتجريم التزوير الإلكتروني وتوفير أداة قانونية لمكافحتها، إلا أن هناك دولاً أخرى لم تسرِ في هذا الاتجاه، وما زال الخلاف في ذلك قائماً كما سبق وذكرنا.

وقد حسم المشرع في العديد من الدول هذا الخلاف بالتدخل التشريعي إما بنصوص خاصة أو بتعديل النصوص التي تحكم التزوير التقليدي، حيث قام المشرع الفرنسي بتعديل نص جريمة التزوير التقليدية حتى يستوعب بهذا التعديل المستندات الإلكترونية (أي التزوير الإلكتروني)، وذلك بتعديل نص المادة ١/٤٤١ من قانون العقوبات الفرنسي، والنص على جرائم التزوير في الوثائق المعلوماتية الإلكترونية أو استخدامها فيما زورت من أجله في الفقرتين ١ و٢ من المادة ٤٤١ [٣٤].

(٣١) د. عبد الفتاح حجازي، الدليل الإلكتروني والتزوير في الجرائم الإلكترونية والإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٤م، ص٢٩٦.

(٣٢) د. محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والإنترنت، المرجع السابق، ص١٣٧.

(٣٣) د. يونس عرب، صور الجرائم الإلكترونية واتجاهات تبويبها، ورشة عمل عن تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، المدة من ٢-٢٠٠٦/٤/٤، ص٢٣-٢٤.

(٣٤) M. Cabrillac et B. Teyssie, Carte de prelevement aupres d'un distributeur automatique, ibid, p.75.

كما تضمن قانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي هذه الجريمة (جريمة التزوير الإلكتروني) في المادة ٢/٣ منه والتي تنص على أنه: «يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من:

١ - ...

٢ - زور أو أتلف مستنداً أو سجلاً أو توقيعاً إلكترونياً أو نظام معالجة إلكترونية للبيانات أو نظاماً إلكترونياً مؤتمتاً أو موقعاً أو نظام حاسب آلي أو نظاماً إلكترونياً بطريق الاصطناع أو التغيير أو التحوير أو بأي طريقة أخرى وذلك باستخدام وسيلة من وسائل تقنية المعلومات.

فإذا وقع التزوير على مستند رسمي أو بنكي أو بيانات حكومية أو بنكية إلكترونية تكون العقوبة الحبس مدة لا تجاوز سبع سنوات وبغرامة لا تقل عن خمسة آلاف دينار ولا تجاوز ثلاثين ألف دينار أو إحدى هاتين العقوبتين»[٣٥].

وبذلك يكون المشرع الكويتي قد أخذ بتجريم التزوير الإلكتروني في نصوص خاصة وذلك في القانون رقم ٦٣ لسنة ٢٠١٥، والقانون رقم ٢٠ لسنة ٢٠١٤ وهي قوانين خاصة وإن كانت قد استقت نصوصها من نصوص قانون الجزاء الكويتي رقم ١٦ لسنة ١٩٦٠، في المواد ٢٥٧، ٢٥٨، ٢٥٩.

ثانياً: إتمام تغيير الحقيقة بإحدى الطرق المنصوص عليها قانوناً

ليس كافياً أن يتم التزوير بتغيير الحقيقة وحدها، وإنما يلزم أن يتم هذا التغيير بإحدى الطرق المنصوص عليها قانوناً، وقد نص على ذلك في قانون مكافحة جرائم تقنية المعلومات في المادة ٢/٣ حيث نص على أنه: «٢- زور أو أتلف... بطريق الاصطناع أو التغيير أو التحوير أو بأي طريقة أخرى، وذلك باستخدام وسيلة من وسائل تقنية المعلومات»، ومن ثم يكون المشرع الكويتي قد حدد صور التزوير الإلكتروني في الاصطناع أو التغيير أو التحوير أو بأي طريقة أخرى، ويلاحظ أن المشرع الكويتي وجد

(٣٥) انظر في ذلك: أيضاً نص المادة ٣٧ فقرة (ج) من القانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية الكويتي على أنه: «مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون آخر يعاقب بالحبس لمدة لا تزيد على ثلاث سنوات وبغرامة لا تقل عن خمسة آلاف دينار ولا تزيد على عشرين ألف دينار أو بإحدى هاتين العقوبتين كل من: ..... ج- أتلف أو عيب توقيعاً أو نظاماً أو أداة توقيع أو مستنداً أو سجلاً إلكترونياً أو زور شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحوير بأي طريقة أخرى».

أن محاولة حصر طرق التزوير الإلكتروني أمر غير ممكن، لذلك استشعر عدم قدرته على هذا الحصر فنص في الفقرة الثانية على عبارة «أو بأي طريقة أخرى» ليمكنه بذلك استيعاب أية صورة من صور التزوير الإلكتروني نظراً لسرعة التطور المعلوماتي في هذا الصدد. أما في قانون المعاملات الإلكترونية فقد عدّد بعضاً من صور التزوير الإلكتروني في المادة ٣٧/ج وهي الاصطناع أو التعديل أو التحوير أو بأي طريقة أخرى ليستجيب النص لأي صورة قد تستجد في هذا الشأن، وهو أمر وارد في ظل تقنية المعلومات التي تتطور بشكل متسارع.

وحسناً فعل المشرع صنعاً حينما نص في قانون مكافحة جرائم تقنية المعلومات وقانون المعاملات الإلكتروني على بيان طرق التزوير الإلكتروني دون حصر لها وذلك بإضافة عبارة «أو بأي طريقة أخرى»، وهذا ما لم يقم به المشرع الكويتي في قانون الجزاء في المادة ٢٥٧ حيث ذكرت طرق التزوير على سبيل الحصر، ولذا ينبغي على المشرع الكويتي أن يعدل قانون الجزاء في نص المادة ٢٥٧ من قانون الجزاء الكويتي رقم ١٦ لسنة ١٩٦٠ ويساير ما قام به في القانونين سالفي الذكر.

وهذا ما تبناه المشرع الفرنسي في قانون عام ١٩٩٤، حيث لم يشترط ضرورة أن يحدث تغيير الحقيقة بوسيلة معينة، حيث إنه أجاز في نص المادة ١/٤٤١ أن يحدث تغيير للحقيقة بأي وسيلة كانت، ويستوي أن يحدث تغيير الحقيقة على محرر أو دعامة أو سند، طالما أن هذه الدعامة من الممكن أن يكون لها أثر في إنشاء حق أو كل ما من شأنه إحداث نتائج قانونية معينة[٣٦].

ومما سبق يتضح لنا أن ما نص عليه المشرع من طرق التزوير هو ما يطلق عليه بطرق التزوير المادية، كما نص على أن التزوير الإلكتروني ممكن أن يقع بأي طريقة أخرى سواء أكانت مادية أم معنوية، ونعطي فيما يلي أمثلة لبعض طرق التزوير المادية والمعنوية:

(أ) الطرق المادية للتزوير الإلكتروني

- **وضع إمضاءات أو أختام أو بصمات مزورة**، وذلك بإدخال صورة توقيع الشخص المنسوب إليه التزوير عن طريق جهاز الماسح الضوئي المرتبط بالحاسب، ويضاف التوقيع للورقة التي انطوت على البيان المزور، ومن ثم تكتسب صفتها الرسمية بعد أن تم تدوين بيانات غير صحيحة فيها على غير إرادة صاحبها،

(٣٦) د. عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دراسة تحليلية نقدية لنصوص التشريع المصري مقارناً بالتشريع الفرنسي، ط٢، ١٩٩٥م، ص٨٨.

وما يصدق على التوقيع يصدق على البصمة وكذلك الختم الشخصي[٣٧]، وبذلك نحصل على مستند صحيح من الناحية الشكلية لكنه مزور لأنه نسب إلى شخص بعد أن حمل إمضاءه أو بصمته أو ختمه على غير إرادته.

- **تغيير المحررات أو الأختام أو الإمضاءات أو زيادة كلمات:** وذلك بعد تلقي الحاسب الآلي للبيانات والمعلومات ومعالجتها في ضوء طلبات وحاجات الجهة العامة أو الخاصة التي استخدمت الحاسب الآلي، وذات الأمر يقوم به الحاسب حتى ولو تلقى النص المكتوب من شبكة الإنترنت، فتتم المعالجة بمعرفة الحاسب بناء على طلب ذوي الشأن والتي تظهر بعد ذلك مادياً في صورة مخرجات لهذا الحاسب، وخلال مرحلة المعالجة يتم التزوير وذلك بالتغيير في النص المعالج بالإضافة أو الحذف أو التعديل في صلب المحرر المعلوماتي أو الإمضاء أو الختم الموضوع عليه، وذلك بإزالة كلمة أو رقم أو رمز معين[٣٨].
- **وضع أسماء أو صور أشخاص آخرين مزورة:** وذلك عن طريق رسم الصورة ضوئياً ونقلها لجهاز الحاسب الآلي واستخراجها ورقياً عن طريق الطابعة، أو إدخالها على بيانات مخزنة في ذاكرة الحاسب نفسه وعرضها على الشاشة دون طباعة ورقية، حيث إن التزوير المعلوماتي والإلكتروني لا يتطلب المستند الورقي أو المطبوع[٣٩].
- **التقليد:** ويقصد به المحاكاة وهو إنشاء محرر على مثال محرر آخر[٤٠]. فيمكن استخراج محرر طبق الأصل لمحرر موجود، وهذا هو التزوير بطريق التقليد حيث يسهل وقوعه بطريقة التزوير الإلكتروني، ولا يشترط في التقليد أن يبلغ حداً من الإتقان، بل يكفي أن ينخدع الناس إلى حد وهمهم بصحة المحرر[٤١]، كما في أوراق العملة مثلاً.

---

(٣٧) د. جميل الصغير، الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، ٢٠٠١م، ص٣٥ وما بعدها.

(٣٨) د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، ١٩٩٩م، ص٢٣٤.

(٣٩) القاضي/ وليد عكوم، مفهوم وظاهرة الإجرام المعلوماتي، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات، ١-٢٠٠٠/٥/٣، ص٥.

(٤٠) د. عوض محمد عوض، الجرائم المضرة بالمصلحة العامة، دار المطبوعات الجامعية، الإسكندرية، ١٩٨٥م، ص١٧٤.

(٤١) نقض ١٩٧٢/٦/١٩، المجموعة، س٣٢، رقم ٢١٠، ص٩٤٠، نقض ١٩٧٩/٤/٢٩، المجموعة، س٣٠، رقم ٢١٠٧، ص ٥٠٦.

- **الاصطناع**: وهو خلق محرر بأكمله ونسبته إلى غير محرره[٤٢]، وفي ذلك قالت محكمة التمييز الكويتية أنه إنشاء محرر على غرار المحرر الرسمي بحيث يعطي المحرر المصطنع شكل المحرر الرسمي ومظهره، وينسب إنشاؤه إلى موظف مختص بتحريره للإيهام برسميته ولو أنه لم يصدر في الحقيقة عنه[٤٣]، وكذلك قالت محكمة النقض المصرية بأنه إنشاء محرر بكامل أجزائه على غرار أصل موجود، أو خلق محرر على غير مثال سابق[٤٤]، والفرق بينه وبين التقليد هو أنه في الاصطناع لا يهم الجاني مدى التشابه بين خطه وخط الغير، عكس التقليد لأنه يضع محرراً جديداً بكامله، بينما التقليد يعالج جزءاً من المحرر، وليس هنا تلازم بين الطريقتين فكلتيهما طريقة مستقلة للتزوير[٤٥]؛ ولذلك فتزوير النقود الورقية عن طريق الحاسب الآلي هي من طرق الاصطناع، كما هي من طرق التقليد[٤٦].

(ب) الطرق المعنوية للتزوير الإلكتروني:

- تغيير إقرارات ذوي الشأن وهي إحدى طرق التزوير المعنوي، وتتحقق حين يقوم كاتب المحرر بتغيير البيانات التي طلب منه كتابتها وذلك عند تدوينها[٤٧]، وهذه الطريقة من الصعوبة إثباتها، كما أنها لا تتيسر إلا عند إنشاء المحرر، ولا صعوبة في ذلك في التزوير الإلكتروني وذلك في حالة الترجمة[٤٨].
- جعل واقعة مزورة في صورة واقعة صحيحة: وهي كل إثبات لواقعة على غير حقيقتها[٤٩]، فكل تشويه أو تحريف يدخله كاتب المحرر على الوقائع التي يثبتها

(٤٢) د. نجيب حسني، شرح قانون العقوبات، المرجع السابق، ص٢٣٩.
(٤٣) تمييز ٢٠٠٥/١/٤، طعن ١٧٥ لسنة ٢٠٠٤ جزائي؛ تمييز ٢٠٠٩/٤/٢١، طعن ٣٣٥ لسنة ٢٠٠٨ جزائي.
(٤٤) نقض ١٩٦٨/٥/٦، المجموعة، س١٩، رقم ١٠٥، ص٥٣٦، نقض ١٩٧١/١٢/٢٧، المجموعة، س٢٢، رقم ٢٠٠، ص٨٣٣.
(٤٥) د. جميل الصغير، المرجع السابق، ص١٤٤.
(٤٦) د. عبد الفتاح حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الكتب القانونية، القاهرة، ٢٠٠٧م، ص٢٦١-٢٦٢.
(٤٧) د. رمسيس بهنام، الجرائم المضرة بالمصلحة العامة، منشأة المعارف، الإسكندرية، ١٩٨٦م، ص١٨٦.
(٤٨) د. أحمد تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، المرجع السابق، ص٣٩٤.
(٤٩) تمييز ٢٠٠٣/٦/١٧، طعن ١/٢٠٠٢ جزائي.

فيه عند تدوينه المحرر يعد تزويراً معنوياً بهذه الطريقة[٥٠]. وتعد هذه الطريقة أكثر طرق التزوير المعنوي اتساعاً، إذ تشمل صورتي تغيير إقرارات أولي الشأن، وجعل واقعة غير معترف بها في صورة واقعة معترف بها، طالما أن هذه الطريقة للتزوير المعنوي تعني كل إثبات لواقعة في محرر يغاير حقيقتها[٥١].

- جعل واقعة غير معترف بها في صورة واقعة معترف بها: حيث يذهب الفقه إلى أن هذه الصورة ليست مستقلة، وإنما تدخل ضمن طريقة «جعل واقعة مزورة في صورة واقعة صحيحة» ومثالها أن يثبت مأمور الضبط القضائي واقعة اعتراف المتهم على حين أنه لم يعترف أو يثبت الموثق أن البائع قد أقر بقبض الثمن، على حين أنه لم يقر بذلك، فالثابت في هذين المثالين أن الواقعة المدعى حدوثها هي واقعة مزورة وغير معترف بها، وأن هذا التزوير جعلها في صورة واقعة صحيحة ومعترف بها[٥٢]، ومن المقصود وقوع التزوير الإلكتروني بهذه الطريقة، فيمكن قيام الموثق الذي يدخل البيانات التي يدلي بها الخصوم للحاسب الآلي بالتعمد بتغيير الحقيقة لهذه الأقوال، أو يثبت عكسها على نحو يجعل واقعة غير معترف بها في صورة واقعة معترف بها؛ مما يؤدي لتغيير مضمون ذلك السند، وتلك الوثيقة مما يقوم به التزوير الإلكتروني[٥٣].

ونلفت الانتباه إلى أن طرق التزوير المادية والمعنوية السابق بيانها إنما هي مجرد أمثلة لطرق التزوير الإلكتروني، إذ يمكن أن يكون هذا التزوير بأي طريقة من الطرق السابقة والتي يكشفها التطور في الواقع العملي.

ثالثاً: إضرار المجني عليه (حال أو محتمل)

بالإضافة إلى العنصرين السابقين يجب أن يترتب على تغيير الحقيقة بالطرق سالفة الذكر ضرر بالمجني عليه (حال أو محتمل) وهو يعني إهدار حق أو إخلال لمصلحة مشروعة يعترف بها القانون ويكفل لها حمايته[٥٤]، وبانتفاء الضرر ينتفي التزوير فهو

(٥٠) د. نجيب حسني، المرجع السابق، ص٢٤٣.

(٥١) د. أحمد صبحي العطار، جرائم الاعتداء على المصلحة العامة: دراسة في القسم الخاص من قانون العقوبات المصري، الهيئة المصرية العامة للكتاب، ١٩٩٣، ص٢٦٨.

(٥٢) د. رمسيس بهنام، الجرائم المضرة بالمصلحة العامة، المرجع السابق، ص١٩٠.

(٥٣) د. حسني عبد السميع، الجرائم المستحدثة عن طريق الإنترنت، دراسة مقارنة بين الشريعة والقانون، دار النهضة العربية، ٢٠١١م، ص٤٧٣-٤٧٤.

(٥٤) د. نجيب حسني، المرجع السابق، ص٢٥١.

عنصر جوهري في جريمة التزوير لا تقوم بدونه[٥٥]، ومن اللازم على المحكمة أن تظهر في حكمها توافر عنصر الضرر وإلا يكون حكمها معيباً، إلا إذا كان توافر عنصر الضرر مستفاداً من مجموع عبارات الحكم[٥٦].

ونظراً لعدم كفاية النصوص المتعلقة بالتزوير في المحررات لمواجهة التزوير الذي يقع في مجال المعالجة الآلية للمعلومات، فقد عاقب المشرع الفرنسي على التزوير الذي يقع في المحررات المعالجة آلياً سواء أكانت داخل الجهاز أم خارجه، فقرر في المادة ٤٦٢/٥ من القانون الصادر سنة ١٩٨٨م معاقبة «كل من زور أية مستندات معالجة آلياً – أياً كان شكلها – إذا سبب ذلك ضرراً للغير»[٥٧].

كما لم يحدد قانون العقوبات الفرنسي الجديد في المادة ٤٤١/١ أي ضوابط للضرر في جريمة التزوير الإلكتروني، حيث نصت تلك المادة على وجوب حصول الضرر من ذلك التزوير حتى يتم العقاب عليه، بما فيها التزوير الإلكتروني، وأن تكون هناك علاقة سببية بين تغيير الحقيقة وعنصر الضرر الذي تحقق، فقد استقر الفقه على أن الضرر كركن في جريمة التزوير لن يختلف الأمر في تطلبه في التزوير الإلكتروني[٥٨].

الفرع الثاني

الركن المعنوي لجريمة التزوير الإلكتروني

يتخذ الركن المعنوي في جريمة التزوير الإلكتروني صورة القصد الجنائي، فهي جريمة عمدية، ويكفي فيها القصد العام الذي يقوم على علم المتهم بأركان الجريمة، واتجاه إرادته إلى الفعل المكون لها، وتحقيق النتيجة، دون أن تتطلب هذه الجريمة توافر قصد جنائي خاص يتمثل في نية استعمال المحرر المزور فيما زور من أجله.

(٥٥) نقض ١٩٦٨/٥/٢٧، المجموعة، س١٩، رقم ١٢٣، ص٦١٥.

(٥٦) أ. د. غنام محمد غنام، د. فيصل عبدالله الكندري، شرح قانون الجزاء الكويتي: القسم الخاص، دولة الكويت، ط٤، ٢٠١٥ – ٢٠١٤ ، ص١٤٨. أنظر كذلك: نقض ١٩٧٤/٢/١٦، المجموعة، س٢٥، رقم ١٨٨، ص٨٦٦. انظر كذلك: تمييز ٥/٧/١٩٨٢، طعن ٩٦/٨٢ جزائي؛ تمييز ٢٠٠٩/٥/١٢، طعن ٢٧٢ لسنة ٢٠٠٨ جزائي.

(٥٧) د. أحمد خليفة الملط، الجرائم المعلوماتية (دراسة مقارنة)، ط٢، دار الفكر العربي، الإسكندرية، ٢٠٠٦م، ص٥٧٦.

(٥٨) د. عبدالفتاح حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، بدون ناشر، ٢٠٠٩م، ص٢٤٧.

أولاً: القصد العام

التزوير الإلكتروني جريمة عمدية يشترط لقيامها توافر القصد العام والذي يتوافر بإدراك الجاني بأنه يغير الحقيقة في محرر إلكتروني بإحدى الطرق المنصوص عليها في القانون، وأن من شأن هذا التغيير إحداث ضرر للغير أو احتمال حدوثه، مع انصراف إرادته إلى ذلك كله[٥٩]، وفي ذلك قالت محكمة التمييز الكويتية أنه يتعين على المحكمة عند الدفع بانتفاء هذا القصد أو المنازعة في توافره أن تعرض لذلك في حكمها وتقول كلمتها فيه بأسباب سائغة[٦٠].

ولا يكفي ذلك، بل لابد من أن تكون إرادته متجهة إلى تغيير الحقيقة من جراء سلوكه غير المشروع والتي من شأنها الإضرار بالغير، وعليه إذا كان جاهلاً بأن الفعل الذي يرتكبه غير مشروع فلا يتحقق لديه القصد الجنائي، ولو كان جهله الحقيقة راجعاً إلى إهماله في تحريها[٦١]. وعلم الجاني بأن تغيير الحقيقة يقع فيما يعتبر في نظر القانون محرراً إلكترونياً، وبأن هذا التغيير يتم بإحدى طرق التزوير علم مفترض، فلا يفيد في دفع مسئوليته جهله في هذا الصدد[٦٢].

وإذا انتفى علم الجاني بأي ركن من أركان الجريمة فلا يترتب عليه توافر القصد الجنائي، لأنه يفترض بالفاعل أن يكون عالماً بكافة أركان الجريمة، كما ينتفي القصد إذا أهمل المبرمج القائم بتحرير المحرر وقام بتغيير بيانات معينة دون قصد فإن الإهمال لا يحقق العلم في القصد، ويستوجب قيام القصد في التزوير المعلوماتي أن تكون إرادة الجاني متجهة إلى تغيير الحقيقة التي من شأنها الإضرار بالغير حتى وإن كان هذا الإضرار محتمل الوقوع[٦٣].

ثانياً: القصد الجنائي الخاص

كما سبق وأن ذكرنا أن كلاً من قانون مكافحة جرائم تقنية المعلومات وقانون المعاملات الإلكترونية لم يتطرقا صراحة أو ضمناً إلى ماهية التزوير الإلكتروني حيث

(٥٩) د. أيمن رمضان محمد أحمد، الحماية الجنائية للتوقيع الإلكتروني، رسالة دكتوراه، دار النهضة العربية، القاهرة، ٢٠١١م، ص٢١٤.

(٦٠) تمييز ٢٠٠٢/٥/٢١، طعن ٣٢٦/٢٠٠١ جزائي.

(٦١) نقض ١٩٦٨/٢/٢٦، المجموعة، س١٩، رقم ٥١، ص٢٨٠، نقض ١٩٧٨/١٠/١، المجموعة، س٢٩، رقم ١٢٤، ص٦٤١.

(٦٢) د. عفيفي كامل عفيفي، المرجع السابق، ص٢٤٠.

(٦٣) نقض ١٩٦٢/٥/٢٢، المجموعة، س١٣، رقم ١٢٥، ص٤٨٩.

أنهما اقتصرا على بيان طرق التزوير الإلكتروني، ولم يتطرق إلى ماهية التزوير إلا المادة ٢٥٧ من قانون الجزاء الكويتي والتي عرفت التزوير التقليدي، فبالرجوع إلى المادة ٢٥٧ من قانون الجزاء رقم ١٦ لسنة ١٩٦٠ نجد أنها نصت على أنه: «يعد تزويراً كل تغيير للحقيقة في محرر بقصد استعماله على نحو يوهم بأنه مطابق للحقيقة، إذا كان المحرر بعد تغييره صالحاً لأن يستعمل على هذا النحو».

فقوله «بقصد استعماله» هذا ما يعني القصد الخاص، فالمقصود بالقصد الخاص في جريمة التزوير التقليدي، اتجاه نية الجاني وقت ارتكاب الفعل إلى استعمال المحرر المزور فيما زور من أجله، أي الاحتجاج به على اعتبار أنه صحيح، فإذا تخلفت هذه النية انتفى القصد الجنائي، ولا أهمية لكون المحرر قد استعمل فعلاً أو لم يستعمل[٦٤]، ولا يفيد المتهم أن ينفي هذه النية عنه وذلك بقوله إنه لم يحصل على فائدة ما من التزوير الذي ارتكبه[٦٥]، ومتى توافر للقصد عناصره فلا عبرة بالبواعث أو الغاية التي تدفع الجاني إلى ارتكاب التزوير[٦٦].

وهذا ما لا نجده في جريمة التزوير الإلكتروني حيث اكتفى المشرع بتوافر القصد العام حين نص في المادة ٢/٣ من قانون مكافحة جرائم تقنية المعلومات، والمادة ٣٧ من قانون المعاملات الإلكترونية الكويتي على أن: «كل من ... زور» فمجرد التزوير تقع الجريمة بغض النظر عن توافر «نية الاستعمال» من عدمه.

(٦٤) د. أحمد خليفة الملط، المرجع السابق، ص٠٤٧.

(٦٥) نقض ١٩٤٤/٤/١٠، مجموعة القواعد، ج٦، رقم ٣٣٣، ص٤٥٥.

(٦٦) نقض ١٩٥٨/٦/١٦، المجموعة، س٩، رقم ١٦٨، ص٦٦٧. انظر كذلك: تمييز ٢٠٠٩/٢/١٠، طعن ٤٤٥ لسنة ٢٠٠٨ جزائي.

المبحث الثاني
تزوير التوقيع الإلكتروني

تمهيد وتقسيم:

للتزوير الإلكتروني العديد من الصور، ومنها تزوير التوقيع الإلكتروني، وهو بلا شك من أهم صور التزوير الإلكتروني، الأمر الذي دعانا إلى تخصيص مبحث في هذه الدراسة لبحث هذه الجريمة من خلال بيان مفهومها وصورها وعيوبها ووظائفها، وآليات حمياتها.

المطلب الأول
ماهية التوقيع الإلكتروني

تمهيد وتقسيم:

تعد جريمة تزوير التوقيع الإلكتروني من الجرائم المستحدثة المرتبطة بجريمة التزوير الإلكتروني؛ حيث تعتبر من أهم صور هذه الجريمة والتي سنتناولها بالشرح والتحليل من خلال خمسة فروع.

الفرع الأول
مفهوم التوقيع الإلكتروني

إن للتوقيع الإلكتروني أهمية بالغة في مجال التعاملات الإلكترونية سواء على الصعيد المحلي أو الدولي، ويعتبر من أهم الأدوات التي تقوم عليها التجارة الإلكترونية والتبادل التجاري الدولي، وهذا كله يرجع إلى انتشار التعاملات وإنجازها باستخدام التقنية الحديثة.

ونظراً لتلك الأهمية عمدت التشريعات الحديثة على وضع تعريف خاص به سواء على مستوى التشريعات الوطنية أو على المستوى الدولي، فقد عرّفه القانون المدني الفرنسي بأن «التوقيع الضروري لإتمام التصرف القانوني الذي يميز هوية من وقعه ويعبر عن رضائه بالالتزامات التي تنشأ عن هذا التصرف، وعندما يكون إلكترونياً فيجب أن يتم باستخدام وسيلة آمنة لتحديد هوية الموقّع وضمان صلته بالتصرف الذي وقع عليه»[٦٧]. كما عرفه المشرع الكويتي في قانون المعاملات الإلكترونية بأنه: «البيانات التي تتخذ هيئة حروف أو أرقام أو

(٦٧) انظر: نص المادة ٤/١٣١٦ من القانون المدني الفرنسي والمعدل في عام ٢٠٠٦ والمعدلة والمضافة بقانون التوقيع الإلكتروني رقم ٢٣٠ لسنة ٢٠٠٠م.

رموز أو إشارات أو غيرها، وتكون مدرجة بشكل إلكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مماثلة في مستند أو سجل إلكتروني أو مضافة عليها أو مرتبطة بها بالضرورة ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره»[٦٨].

كما نصت المادة الثانية (أ) من قانون الأونسيترال النموذجي على تعريف التوقيع الإلكتروني بأنه: «بيانات في شكل إلكتروني مدرجة في رسالة بيانات، أو مضافة إليها أو مرتبطة بها منطقياً، يجوز أن تُستخدم لتعيين هوية الموقّع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقّع على المعلومات الواردة في رسالة البيانات»[٦٩].

في حين عرفه التوجيه الأوروبي رقم ٩٣ لسنة ١٩٩٩م والذي أصدره المجلس الأوروبي بالمادة ٢٠ منه بأنه: «بيان يأخذ الشكل الإلكتروني ويرتبط أو ينفصل بشكل منطقي بمعطيات إلكترونية أخرى، والذي يمكن أن يخرج بشكل موثق»[٧٠] وهو التعريف الذي يرى فيه البعض بأنه ينظر للتوقيع الإلكتروني بنظرة فنية باعتباره وسيلة تكنولوجية للأمان والسرية[٧١].

ويلاحظ بأن تعريف التوقيع الإلكتروني في كافة القوانين المنظمة متفق عليه تقريباً، فرغم اختلاف الألفاظ، توجد وحدة في مضمون التعاريف، كما لم ينص على شكل معين للتوقيع الإلكتروني، حيث إنه يأخذ عدة أشكال وذلك كله بهدف أداء وظيفة أو عدد من الوظائف التي تؤديها التوقيعات الخطية التقليدية.

الفرع الثاني

خصائص التوقيع الإلكتروني[٧٢]

يتكون التوقيع الإلكتروني من عناصر متفردة وسمات خاصة بالموقع تتخذ شكل أرقام أو حروف أو إشارات أو رموز أو غيرها، وكذلك يحدد شخصية الموقع ويميزه. كما أنه يعبّر عن رضاء الموقع بمضمون المحرر[٧٣]. والتوقيع الإلكتروني يتصل برسالة

(٦٨) انظر: نص المادة (١) من القانون ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي.

(٦٩) انظر في ذلك: قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية (٢٠٠١)، متوفر في http://www.uncitral.org/pdf/arabic/texts/electcom/ml-elecsig-a.pdf

(٧٠) DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999L0093&from=FR

(٧١) د. أيمن عبدالله فكري، الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الرياض، ٢٠١٤، ص٣٩١ وما بعدها.

(٧٢) انظر: نص المادة (١٩) من قانون المعاملات الإلكترونية الكويتي رقم ٢٠ لسنة ٢٠١٤.

(٧٣) د. سعيد السيد قنديل، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٦م، ص٥١ وما بعدها.

إلكترونية، وهي عبارة عن معلومات يتم إنشاؤها أو إرسالها أو تسليمها أو تخزينها بوسيلة إلكترونية، وكذلك يحقق أغراض ووظائف التوقيع التقليدي متى كان صحيحاً وأمكن إثبات نسبته إلى موقعه، وأخيراً يحقق التوقيع الإلكتروني الأمان والخصوصية والسرية في نسبته للموقع، بالنسبة للمتعاملين مع أنواعه وخاصة مستخدمي شبكة الإنترنت وعقود التجارة الدولية، ويتم ذلك عن طريق إمكانية تحديد هوية الموقع، ومن ثم حماية المؤسسات من عمليات تزوير التوقيعات(٧٤).

الفرع الثالث

صور التوقيع الإلكتروني

أولاً: التوقيع بالقلم الإلكتروني

هو عبارة عن قلم إلكتروني حسابي يمكن عن طريقه الكتابة على شاشة الحاسب الآلي الخاص بالموقع، ويتم ذلك باستخدام برنامج هو المسيطر والمحرك لهذه العملية، وهذا البرنامج يؤدي مهمتين وهما التقاط التوقيع والتحقق من صحة هذا التوقيع(٧٥). فيتلقى البرنامج أولاً بيانات العميل عن طريق بطاقته الخاصة التي يتم وضعها في الآلة ثم تظهر التعليمات على الشاشة، ثم تظهر بعد ذلك رسالة إلكترونية تطلب توقيعه باستخدام قلم على مكان محدد داخل شاشة الحاسب الآلي(٧٦)، ويطلب البرنامج من الشخص الضغط على مفاتيح معينة تظهر له على الشاشة تفيد بالموافقة أو عدم الموافقة على التوقيع، ومتى تمت الموافقة، يتم التشفير للبيانات الخاصة بالتوقيع ويتم تخزينها باستخدام البرنامج، وبعد ذلك تأتي مرحلة التحقق من صحة التوقيع بمقارنة المعلومات مع التوقيع المخزن، ومن ثم يتم تحديد ما إذا كان التوقيع مزوراً أم صحيحاً(٧٧).

ويؤخذ على هذه الصورة بأنها لا تتمتع بالأمان الذي يمكن أن يحقق الثقة في التوقيع الإلكتروني، ويعود ذلك إلى أن المرسل إليه يستطيع الاحتفاظ بنسخة من صورة التوقيع، ويعيد نسخها ولصقها على أي وثيقة من الوثائق المحررة على الوسائط

(٧٤) د. ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧م، ص٣٥ وما بعدها.

(٧٥) د. أحمد شرف الدين، التوقيع الإلكتروني وقواعد الإثبات ومقتضيات الأمان في التجارة الإلكترونية، المرجع السابق، ص٥.

(٧٦) د. ثروت عبد الحميد، المرجع السابق، ص٥١ وما بعدها.

(٧٧) د. منير الجنبيهي، د. ممدوح الجنبيهي، التوقيع الإلكترون وحجيته في الإثبات، دار الفكر الجامعي، الإسكندرية، ٢٠٠٤م، ص١٠ وما بعدها.

الإلكترونية ويدعي أن واضعها هو صاحب التوقيع الفعلي، الأمر الذي يحتاج إلى إثبات الصلة بين التوقيع بهذه الصورة والمحرر، ولهذا السبب فإن هذا النوع من التوقيع الإلكتروني لا يعتد به في استكمال عناصر الدليل الكتابي المعد للإثبات(٧٨).

ثانياً: التوقيع الرقمي

هو بيانات أو معلومات متصلة بمنظومة بيانات أخرى أو صياغة منظومة في صورة شفرة، يسمح للمرسل إليه إثبات مصدرها، والتأكد من سلامة مضمونها وتأمينها ضد أي تحريف أو تعديل(٧٩)، ويتم ذلك باستخراج مفاتيح سرية وطرق حسابية معقدة ومعادلات رياضية تتحول بواسطتها المعاملة من رسالة ذات كتابة عادية مقروءة ومفهومة إلى معادلة رياضية أو رسالة رقمية غير مقروءة وغير مفهومة ما لم يتم فك تشفيرها ممن يملك مفتاح فك الشفرة والمعادلات الخاصة بذلك(٨٠).

وعند رغبة الموقع بإرسال رسالة بيانات عبر البريد الإلكتروني مثلاً فإنه يعد ملخصاً للرسالة باستخدام برنامج تشفير وباستخدام المفتاح الخاص وإرسالها للشخص المرسل إليه والذي يستخدم مفتاح عام للتحقق من صحة التوقيع الإلكتروني الرقمي، ثم ينشئ المرسل إليه ملخص رسالة باستخدام ذات برنامج التشفير ويقارن بين ملخص الرسالتين، فإن كانتا متطابقتين، فهذا دليل على أن الرسالة قد وصلت سليمة دون تحريف أو تعديل، أما عند حدوث التعديل أو التحريف في الرسالة فسيكون ملخص الرسالة التي أنشأها المستلم مختلفة عن تلك التي أنشأها المرسل (الموقع)(٨١)، وهذه الطريقة تحقق أعلى درجات الثقة والأمان للمحرر الإلكتروني، ولكن يعيبها إمكانية سرقة هذه الأرقام أو معرفتها من قبل الغير والتصرف فيها بشكل غير مشروع، خاصة في ظل التقدم والتطور التقني وازدياد حالات الاحتيال والقرصنة(٨٢).

---

(٧٨) د. عيسى غسان ربضي، القواعد الخاصة بالتوقيع الإلكتروني، المرجع السابق، ص١٦١ وما بعدها.

(٧٩) د. ثروت عبد الحميد، المرجع السابق، ص٦١.

(٨٠) د. ثروت عبد الحميد، المرجع السابق، ص٦١.

(٨١) حيث يوجد نوعان من المفاتيح أحدهما عام وهو ما يسمح لكل شخص مهتم، القيام بقراءة رسالة البيانات عبر الإنترنت دون تعديل عليها لعدم امتلاكه المفتاح الخاص، فإذا وافق على مضمونها وملخصها ورغب في الالتزام بها، وضع توقيعه عليها عن طريق المفتاح الخاص به، ويعيد الإرسال مرة أخرى لمصدر الرسالة مرفقاً بها توقيعه في ملفه، ولا يستطيع إجراء أي تعديل به لأنه لا يمتلك المفتاح الخاص بالموقع، انظر في ذلك: د. خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨م، ص٢١٤.

(٨٢) د. ممدوح محمد مبروك، المرجع السابق، ص١٥ وما بعدها.

ثالثاً: التوقيع البيومتري

تقوم هذه الصورة على اعتماد الصفات والخواص الفيزيائية والطبيعية والسلوكية للأفراد والتي تختلف من شخص لآخر، ومن هذه الخواص البصمة الشخصية وبصمة قرنية العين وخواص اليد البشرية وبصمة نبرة الصوت والتعرف على الوجه البشري وغيرها من الصفات الجسدية والسلوكية(٨٣). وهذه البيانات الذاتية يتم تشفيرها حتى لا يتمكن أي شخص من الوصول إليها ومحاولة تعديلها أو العبث بها مع السماح للمصرح لهم باستخدامها(٨٤).

وبذلك يعد التوقيع البيومتري وسيلة يمكن الوثوق بها والاعتماد عليها في تمييز الشخص وتحديد هويته، وهو ما يتيح استخدامها في إبرام التصرفات القانونية التي تتم بالوسائل الإلكترونية(٨٥)، ولكن يعيبها إمكانية مهاجمتها وفك شفرتها بواسطة قراصنة الحاسب الآلي، ولذا يجب لتأمين الثقة في التوقيع البيومتري أن يتم استخدام منظومة بيانات مؤمنة للتوقيع الإلكتروني بحيث تضمن انتقاله دون إمكانية التلاعب فيه(٨٦).

ويؤخذ على نصوص قانون المعاملات الإلكترونية، أنه لم يعدّد صور التوقيع الإلكتروني، وكان يتعين على المشرّع أن يفرد لها نصاً يبين هذه الصور ويوضح مفهومها حتى لا تكون هناك صعوبة عند تناولها بالشرح والتعليق بدلاً من تكراره للنصوص في ذات الأمر بين قانون مكافحة تقنية المعلومات، وقانون المعاملات الإلكترونية، ولذا ينبغي على المشرع الكويتي أن ينص في تشريع المعاملات الإلكترونية على ما يفيد ذلك.

الفرع الرابع
وظائف التوقيع الإلكتروني

للتوقيع الإلكتروني وظيفتان رئيسيتان هما تحديد هوية الموقّع والتعبير عن رضاه.

أولا: تحديد هوية الموقّع

التوقيع الإلكتروني هو علامة شخصية تكشف هوية صاحب هذا التوقيع، من خلال استخدام وسائل وإجراءات موثوق بها تتمثل في استخدام أنظمة مختلفة

(٨٣) د. إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية، مجلس النشر العلمي، جامعة الكويت، الكويت، ٢٠٠٣م، ص١٥٩.
(٨٤) د. إبراهيم الدسوقي أبو الليل، المرجع السابق، ص١٥٩.
(٨٥) د. ثروت عبد الحميد، المرجع السابق، ص٦٠ وما بعدها.
(٨٦) د. سعيد السيد قنديل، المرجع السابق، ص٧٠ وما بعدها.

مثل التوقيع باستخدام القلم الإلكتروني أو البصمة الإلكترونية أو استخدام نظام التشفير بأنواعه، فهذه الوسائل تسمح بتحديد هوية الشخص الذي أوجد هذه الوثائق من خلال الربط بين هوية هذا الشخص والنصوص والرسائل التي يتبادلها مع غيره(٨٧). والتوقيع الإلكتروني يقوم بهذا الدور، بشكل رموز أو أرقام أو حروف أو إشارات تدل على شخصية الموقع وتميزه عن غيره(٨٨). والتوقيع الإلكتروني بهذا الشكل يميز شخصية صاحبه ويعبر عنه وعن هويته وإرادته في الالتزام بمضمون المحرر الإلكتروني(٨٩).

ثانياً: التعبير عن رضا الموقع

التوقيع التقليدي وكذلك الإلكتروني يدل كل منهما على رضا الموقّع بما هو مدون في المحرر وقبوله بما جاء فيه(٩٠)،، فيستفاد برضاء الموقع وقبوله الالتزام بمجرد وضع توقيعه إلكترونياً على البيانات التي تحتويها المحررات الإلكترونية(٩١)، ويعتبر الرضا صحيحاً بتوافر الأهلية وهي قدرة الشخص على إبرام التصرفات القانونية، وأن يخلو الرضا من عيوب الإرادة وهي الغلط والتدليس والإكراه والغبن أو الاستغلال وإلا كانت الإرادة معيبة لمصلحته ومن ثم قابلية التصرف للبطلان(٩٢).

الفرع الخامس
عيوب التوقيع الإلكتروني

على الرغم من إيجابيات التوقيع الإلكتروني والتي سهّلت العديد من العمليات التجارية والشخصية، إلا أن هناك بعض الجوانب السلبية التي يتعرض لها التوقيع الإلكتروني ويمكن إجمالها في أمرين:

(٨٧) لورانس محمد عبيدات، إثبات المحرر الإلكتروني، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٩م، ص١٥٠ وما بعدها.

(٨٨) د. عادل الأبيوكي، المرجع السابق، ص٢٦.

(٨٩) د. فيصل الغريب، التوقيع الإلكتروني وحجيته في الإثبات، بحوث ودراسات المنظمة العربية للتنمية الإدارية، القاهرة، ٢٠٠٥م، ص١٠٩ وما بعدها.

(٩٠) د. لورانس عبيدات، إثبات المحرر الإلكتروني، المرجع السابق، ص١٤٢ وما بعدها.

(٩١) د. لورانس عبيدات، المرجع السابق، ص١٥٣.

(٩٢) د. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، بدون تاريخ، ص٢٤٢.

أولاً: إساءة استعمال التوقيع الإلكتروني

مما لا شك فيه أن من صور التوقيع الإلكتروني التوقيع الرقمي، وهو التوقيع الذي يمكن من خلاله وضع التوقيع من خلال الرموز أو الأرقام، ومثال ذلك استعمال التوقيع الرقمي الخاص بالبطاقة البنكية، حيث قد يستعمل الغير هذه البطاقة لسحب مبالغ مالية لا يحق له الحصول عليها، كأن يحصل شخص ما على بطاقة بنكية عن طريق السرقة أو النصب ويقوم باستخدامها في سحب مبالغ مالية أو دفع فواتير مستحقة عليه(٩٣)، كما أن التوقيع الإلكتروني معرض للتزوير وخاصة من الأشخاص الذين يتوافر لديهم معرفة جيدة باستخدامات الحاسب الآلي(٩٤).

ثانياً: ارتفاع تكلفة التوقيع الإلكتروني

بعض صور التوقيع الإلكتروني وتطبيقاتها عالية التكلفة مما يشكّل عقبة أمام انتشار استخدام التوقيع الإلكتروني نظراً لاستخدامها تقنيات حديثة مكلّفة لا يستطيع الشخص العادي وحتى بعض المؤسسات تحملها؛ مما يحد من انتشار استخدام التوقيع الإلكتروني(٩٥).

(٩٣) د. محمد عبيد الكعبي، المرجع السابق، ص٢٤٠.

(٩٤) د. عادل الأبيوكي، المرجع السابق، ص٣٧.

(٩٥) د. ممدوح محمد مبروك، مدى حجية التوقيع الإلكتروني في الإثبات، دار النهضة العربية، القاهرة، ٢٠٠٩م، ص١٤.

المطلب الثاني
آليات حماية التوقيع الإلكتروني من تزويره إلكترونياً

تمهيد:

إن بيئة المعاملات الإلكترونية، على الرغم من الإيجابيات التي حملتها وساهمت في تطور هذه الآلية، لا تخلو من بعض السلبيات التي قد تقوّض جهود الأطراف المعنية وتحول دون خلق بيئة آمنة وموثوقة لكافة المتعاملين، خاصة مع تنامي ظاهرة التزوير الإلكتروني، وهو ما استدعى تدخل المشرعين لسن القوانين الكفيلة بوضع آليات ووسائل للحماية الجنائية للتوقيع الإلكتروني الذي يرتكب بصدده العديد من الجرائم الإلكترونية، ومن هذه الجرائم جريمة الدخول غير المصرح به على قاعدة بيانات تتعلق بالتوقيع الإلكتروني، وجريمة الحصول على التوقيع الإلكتروني بالوسائل الاحتيالية، وجريمة تزوير التوقيع الإلكتروني، وأخيراً جريمة إتلاف وتعييب التوقيع الإلكتروني.

وحيث إننا نناقش جريمة التزوير الإلكتروني فسوف يكون موضوع الحماية الجزائية الذي نحن بصدده منصباً على حماية التوقيع الإلكتروني من تزويره إلكترونياً. وبذلك سوف نتناول هذا المطلب من خلال ثلاثة فروع:

الفرع الأول: النصوص القانونية التي تحمي التوقيع الإلكتروني

الفرع الثاني: تشفير التوقيع الإلكتروني

الفرع الثالث: التصديق على التوقيع الإلكتروني

الفرع الأول
النصوص القانونية التي تحمي التوقيع الإلكتروني

نص المشرع الكويتي في المادة ٢/٣ من قانون مكافحة جرائم تقنية المعلومات على أنه: «يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من: ١-..... ٢- زور أو أتلف مستنداً أو سجلاً أو توقيعاً إلكترونياً أو نظام معالجة إلكترونية للبيانات أو نظاماً إلكترونياً مؤتمتاً أو موقعاً أو نظام حاسب آلي أو نظاماً إلكترونياً بطريق الاصطناع أو التغيير أو التحوير أو بأي طريقة أخرى، وذلك باستخدام وسيلة من وسائل تقنية المعلومات، فإذا وقع التزوير على مستند رسمي أو بنكي أو بيانات حكومية أو بنكية

إلكترونية تكون العقوبة الحبس مدة لا تجاوز سبع سنوات وبغرامة لا تقل عن خمسة آلاف دينار ولا تجاوز ثلاثين ألف دينار أو بإحدى هاتين العقوبتين، ويعاقب بذات العقوبة بحسب الأحوال، كل من استعمل أياً مما ذكر مع علمه بتزويره أو فقده لقوته القانونية».

كما تنص كذلك المادة (٣٧) من قانون المعاملات الإلكترونية الكويتي على أنه: «مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون آخر، يعاقب بالحبس مدة لا تزيد على ثلاث سنوات وبغرامة لا تقل عن خمسة آلاف دينار ولا تزيد على عشرين ألف دينار أو بإحدى هاتين العقوبتين كل من: أ- ..... ب- .... ج- أتلف أو عيب توقيعاً أو نظاماً أو أداة توقيع أو مستنداً أو سجلاً إلكترونياً أو زور شيئاً من ذلك بطريق الاصطناع أو التعديل أو التحوير بأي طريقة أخرى. د- استعمل توقيعاً أو نظاماً أو أداة توقيع أو مستنداً أو سجلاً إلكترونياً معيباً أو مزوراً مع علمه بذلك».

ويتضح من صيغة النصين السابقين أن المشرع الكويتي قد جمع عدة أنماط للسلوك الإجرامي الذي قد يقع على التوقيع الإلكتروني إلى جانب التزوير وذلك في كل نص من النصين سالفي الذكر مثل الإتلاف والتعييب، وفعل الإتلاف يتحقق بإفقاد البرنامج الإلكتروني الخاص بالتوقيع الإلكتروني قدرته على العمل عن طريق نشر فيروس إلكتروني، أو سكب سائل على الوسيط الإلكتروني أو التوقيع الإلكتروني مما يفقد التوقيع الإلكتروني القدرة أو الصلاحية بصورة جزئية كأن يصدر التوقيع مشوهاً أو غير واضح، أما التعييب فإنه يتحقق بأي سلوك إجرامي يؤدي إلى إفقاد المحرر الإلكتروني وظيفة من وظائفه مثل طمس التوقيع الإلكتروني المدون عليه وطمس بعض الأسطر المكتوبة بطريقة إلكترونية فيه[٩٦]. وإلى جانب الإتلاف والتعييب فقد عاقب المشرّع الكويتي كذلك على تزوير التوقيع الإلكتروني والذي يتحقق عن طريق الاصطناع أو التقليد أو التحوير أو التعديل.

ولم يقف عند هذا الحد، بل عاقب كل من استعمل توقيعاً أو نظاماً أو أداة توقيع أو مستنداً أو سجلاً إلكترونياً معيباً أو مزوراً مع علمه بذلك، فلم يقصر المشرّع الكويتي العقوبة على التزوير فقط، بل ذكر التقليد والتعييب حتى لا يترك مجالاً للشخص الذي استخدم التوقيع الإلكتروني استخداماً غير مشروع وعاقبه بذات عقوبة التزوير.

(٩٦) د. عبد الفتاح حجازي، النظام القانوني للتوقيع الإلكتروني، المرجع السابق، ص٥٤٢.

الفرع الثاني
تشفير التوقيع الإلكتروني

كلما كان الإجراء المتّبع يحقق الثقة بين المتعاملين زادت كمية المعاملات الإلكترونية والتجارة الإلكترونية، فيجب على القائم على الموقع الإلكتروني التوثق من صحة الطلب والذي يتطلب التحقق من أن من يخاطبه هو فعلاً من سجل اسمه أو عنوانه الإلكتروني أو غير ذلك من البيانات والمعلومات التي تتطلبها المواقع على شبكة الإنترنت، ويكتسب هذا الأمر أهمية كبيرة في ضوء الزيادة الكبيرة في حجم جرائم الاختراق والاحتيال الإلكتروني المرتكبة باستخدام شبكة الإنترنت، ومن هنا جاءت أهمية التشفير لمنع مرتكبي جرائم الاختراق والاحتيال الإلكتروني من ارتكاب جرائمهم ضد هذه التعاملات الإلكترونية(٩٧).

والذي دفع بعض الجهات لإيجاد تقنيات لحماية أمن المعلومات بصفة عامة وأمن التجارة الإلكترونية بصفة خاصة من خلال استخدام تقنية التشفير لضمان خصوصية تعاملات الأطراف ومنع أية تعديات عليها(٩٨).

فقد نص المشرع الكويتي في المادة الأولى من قانون المعاملات الإلكترونية على أن «التشفير: عملية تحويل نص بسيط أو وثيقة نصية أو رسالة إلكترونية إلى رموز غير معروفة أو مبعثرة يستحيل قراءتها بدون إعادتها إلى هيئتها الأصلية»، ولم يتطرق له المشرع الكويتي ضمن المصطلحات التي أوردها في قانون مكافحة جرائم تقنية المعلومات، وبذلك يكون المشرع الكويتي قد تطرق إلى تقنية التشفير بشكل غير مباشر من خلال تطرقه إلى التوقيع الإلكتروني الذي يعتمد بشكل أساسي على عملية التشفير.

وقد عرفه البعض من الفقه بأنه تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو من تعديلها أو تغييرها(٩٩). وبذلك نجد أن التشفير يعتمد على عمليات رياضية يتم بها تحويل النص المراد إرساله إلى رموز وإشارات لا يمكن فهم محتواها إلا بواسطة فك الشفرة وتحويل الرموز والإشارات إلى نصوص مقروءة ومفهومه باستخدام مفاتيح التشفير العامة

(٩٧) د. خالد مصطفى فهمي، النظام القانوني للتوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧م، ص١٠٠ وما بعدها.

(٩٨) Donn B. Parker, Fighting Computer Crime: A New Framework for Protecting Information, 1998 Wiley computer Publishing, United States of America, P.12.

(٩٩) د. عبد الفتاح حجازي، المرجع السابق، ص٢٠٣.

والخاصة، فهذه العملية لا تتم إلا إذا كان مستقبل الرسالة يملك مفتاح التشفير الذي يحول الإشارات والرموز إلى النص الأصلي(١٠٠).

والتشفير حتى يمكنه القيام بدوره كآلية من آليات حماية التوقيع الإلكتروني فلابد من وجود عدة ضوابط وهي:

- إباحة تشفير البيانات والمعلومات التي يتم كتابتها أو التعامل فيها باستخدام الوسائل الإلكترونية(١٠١).
- الحق في المحافظة على سرية البيانات والمعلومات المشفرة وذلك بالاعتراف لأصحابها بالحق في سرية تلك البيانات والمعلومات وتجريم الاعتداء عليها(١٠٢).
- اعتبار استخدام التشفير وسيلة يعتد بها قانوناً في تحرير البيانات والمعلومات من جانب الجهات المختصة، كأثر لإقرار المشرع للنص المشفر وحجيته في إثبات التصرفات القانونية، فإنه يعتبر من المحررات الإلكترونية حيث يمكن تحويل الإشارات والرموز إلى نصوص مقروءة ومفهومة تكون حجة على من قام بمخالفة الاتفاق المبرم بين الطرفين(١٠٣).

وتبرز أهمية التشفير في منع الغير من مستخدمي شبكة الإنترنت من الوصول إلى البيانات والمعلومات والمحافظة على سريتها وخصوصيتها للأطراف باستخدام وسائل إلكترونية رقمية أو رموز معينة عوضاً عن الكتابة التقليدية التي لا يعرفها إلا أطراف التعامل التجاري بما لا يسمح باستخدامها من قبل الغير، فاستخدام التشفير يحقق أكبر درجة من الأمن والحماية لمستخدمي شبكة الإنترنت نتيجة لاستعمال أفضل طرق التشفير التي يصعب فكها(١٠٤).

ويؤدي فك الشفرة إلى إفشاء البيانات وانتشارها ومن ثم الإضرار بأصحابها وبالغير، ويجب من ثم على المشرع الكويتي بصفة خاصة وباقي المشرعين الذين لم ينصوا في تشريعاتهم على عقاب من يقوم بفك الشفرة وفض المعلومات المشفرة نظراً للأضرار الكبيرة التي تترتب على هذا الفعل(١٠٥).

---

(١٠٠) د. عبد الفتاح حجازي، المرجع السابق، ص٢٠٣.

(١٠١) د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، ٢٠٠١م، ص٣١ وما بعدها.

(١٠٢) د. عبد الفتاح حجازي، المرجع السابق، ص٢٠٤.

(١٠٣) د. عبد الفتاح حجازي، المرجع السابق، ص٢٠٤.

(١٠٤) د. خالد مصطفى فهمي، المرجع السابق، ص١٠١ وما بعدها.

(١٠٥) د. لورانس محمد عبيدات، المرجع السابق، ص١٣٩ وما بعدها.

الفرع الثالث
التصديق على التوقيع الإلكتروني

إن هناك جهات رسمية تقوم بالتصديق على التوقيع الإلكتروني، وهي وسيلة فنية آمنة للتحقق من صحة التوقيع أو المحرر، حيث يتم نسبته إلى شخص معين أو جهة معينة أو طرف محايد يطلق عليه مقدم خدمات التصديق أو مورد خدمات التوثيق أو جهة التوثيق، وهي هيئة عامة أو خاصة تعمل تحت إشراف السلطة التنفيذية، وقد نص المشرع الكويتي في القانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية في المادة الأولى منه على تعريف ما يسمى بمزود خدمات التصديق وهو «الشخص الطبيعي أو المعنوي المعتمد والمرخص له من الجهة المختصة بإصدار شهادات تصديق إلكترونية أو أية خدمات أو مهمات متعلقة بها وبالتوقيعات الإلكترونية والمنظمة بموجب أحكام القانون»، كما عرف المشرع في ذات المادة «شهادة التصديق الإلكتروني: الشهادة التي تصدر من الجهة المرخص لها، والتي تصادق على إثبات نسبة التوقيع الإلكتروني إلى شخص معين وتثبيت الارتباط بين الموقع وبيانات إنشاء التوقيع استناداً إلى إجراءات توثيق معتمدة».

كما أن المشرع نص في المادة (٣٧) من القانون ٢٠ لسنة ٢٠١٤ على: «مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون آخر، يعاقب بالحبس لمدة لا تزيد على ثلاث سنوات وبغرامة لا تقل عن خمسة آلاف دينار ولا تزيد على عشرين ألف دينار أو بإحدى هاتين العقوبتين كل من:

أ - ...

ب - أصدر شهادة تصديق إلكترونية أو زاول أي من خدمات التصديق الإلكتروني دون الحصول على ترخيص بذلك من الجهة المختصة».

كما تنص المادة (٣٨) من ذات القانون على أنه: «يعاقب بالحبس مدة لا تزيد على سنة والغرامة التي لا تقل عن ثلاثة آلاف دينار ولا تزيد على عشرة آلاف دينار، أو بإحدى هاتين العقوبتين كل من رخص له بإصدار خدمات التصديق الإلكترونية إذا قام بتقديم بيانات غير صحيحة في طلب التسجيل الذي يقدم إلى الجهة المختصة أو خالف شروط الترخيص».

كما تنص المادة (٣٩) كذلك على أنه: «مع عدم الإخلال بالمسئولية الجزائية الشخصية لمرتكب الجريمة، يعاقب المسئول عن الإدارة الفعلية للشخص المعنوي بذات

العقوبات المقررة عن الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون إذا كان إهماله وإخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة مع علمه بذلك.

ويكون الشخص المعنوي مسئولاً بالتضامن عما يحكم به من عقوبات مالية وتعويضات إذا كانت المخالفة قد ارتكبت من أحد العاملين باسم الشخص المعنوي أو لصالحه».

وحسناً فعل المشرع الكويتي وذلك بهدف حماية التوقيع الإلكتروني كمفرد أساسي وهام في تكوين المحرر الإلكتروني، حيث احتاط للتوقيع الإلكتروني من جميع الجوانب بدءاً من تعريف مفهوم الشفرة وبيان ماهيته وكيفية تطبيقه؛ وذلك لحماية التوقيع الإلكتروني من الاختراق والإتلاف والتزوير، ولم يقف عند هذا الحد بل اهتم أيضاً بالجهات التي تقوم بالتصديق على التوقيع الإلكتروني، وعرف ما يسمى بمزوّد خدمات التصديق وهو الشخص الطبيعي أو المعنوي المعتمد والمرخص له من الجهة المختصة، كما عرّف المشرّع كذلك ماهية شهادة التصديق الإلكتروني وهي التي تصدر من الجهة المرخص لها والتي تصادق على إثبات نسبة التوقيع الإلكتروني إلى شخص معين، وتثبيت الارتباط بين الموقع وبيانات إنشاء التوقيع استناداً إلى إجراءات توثيق معتمدة، وكل هذا بهدف حماية التوقيع الإلكتروني من تعرضه للتزوير والإتلاف والتعييب.

ولم يكتف المشرّع بذلك، بل عاقب كل من يرتكب أفعالاً من شأنها اهتزاز الثقة بالتوقيع الإلكتروني كإتلافه أو تزويره، وغير ذلك من الأمور التي تؤدي إلى عدم قيام التوقيع الإلكتروني بمهمته الأساسية بعقوبات قاسية ردعاً له على ما ارتكبه، ليس هذا فحسب، بل تعرض المشرع في المواد ٣٧، ٣٨، ٣٩ بمعاقبة كل من يصدر شهادة تصديق إلكترونية أو يزاول أياً من خدمات التصديق الإلكتروني دون الحصول على ترخيص بذلك من الجهة المختصة وذلك في المادة (٣٧)، وهذا يعد نوعاً من التحايل على الجهات المختصة بإصدار هذه الشهادة حيث من الممكن تزوير هذه الشهادة بشكل أو بآخر دون الحصول على هذا التصديق من الجهات المختصة، هذا من جانب، ومن جانب آخر فقد نص المشرع على إصدار شهادة التصديق ببيانات في طلب التسجيل، وهذا يعد تزويراً واضحاً ومباشراً للحصول على شهادة التصديق من الجهات المختصة، فنكون هنا بصدد حالتين من التزوير التي قام بهما من يريد إنشاء توقيع إلكتروني، ففي المادة (٣٧) يكون التزوير بطريقة غير مباشرة، وفي المادة (٣٨) جاء النص مبيناً أن ما قام به صاحب التوقيع الإلكتروني هو تزوير بشكل مباشر.

ونرى أن المشرع قد عاقب من احتال على الجهات المختصة بطريق غير مباشر وحصل على شهادة تصديق إلكترونية مزورة ولكن بطريق الاحتيال على عقوبة أشد من تلك التي قررها على من قام بالتزوير بشكل مباشر، وحسناً ما فعله المشرع حيث إن الاحتيال والتزوير غير المباشر يعد من الصعب اكتشافه، أما التزوير المباشر فهو أمر سهل الاكتشاف ومن ثم كانت العقوبة على النحو الوارد في النصين.

ولم يكتف المشرع بذلك القدر من الحماية للتوقيع الإلكتروني، بل قام في المادة (٣٩) من ذات القانون ونص على معاقبة المسئول الذي أصدر هذه الشهادة وصدق عليها بالمخالفة لأحكام القانون إذا وقعت الجريمة بسبب إهماله وإخلاله بواجباته مع علمه بذلك.

المبحث الثالث
القواعد القانونية الخاصة
بمواجهة جريمة التزوير الإلكتروني

تمهيد وتقسيم:

أصبحت الجريمة الإلكترونية من الخطورة بمكان نظراً لتطورها السريع والمتزايد، وذلك على أمن وسلامة الأفراد والدول، وأصبح من يرتكب الجريمة الإلكترونية (المجرم الإلكتروني) أكثر خطورة وأكثر حركة وقوة عما كان في الماضي، وقد دخلت التقنيات الحديثة في المجال الإجرامي مما أدى إلى سهولة ارتكاب الكثير من الأنشطة الإجرامية، ومن ثم فلابد من البحث عن حماية خاصة ضد جريمة التزوير الإلكتروني، وسوف نقوم ببحثها من خلال هذا المبحث في مطلبين: الأول منهما نناقش من خلاله قواعد الاختصاص الجنائي بشأن جريمة التزوير الإلكتروني، وفي المطلب الثاني نناقش قواعد تحصيل وتقييم الأدلة الخاصة بإثبات جريمة التزوير الإلكتروني، وذلك على التفصيل الآتي:

المطلب الأول
قواعد الاختصاص الجنائي بشأن جريمة التزوير الإلكتروني

تمهيد وتقسيم:

تتكون الشبكات الإلكترونية من أجهزة الكمبيوتر المحلية المرتبطة بعضها بعضاً بالشبكات الإقليمية والعالمية، وهذا الربط مع استخدامه في الأنشطة الإجرامية الإلكترونية، ساعد على ظهور العديد من المشكلات القانونية في مواجهة هذه الأنشطة الإجرامية، ومن أبرز هذه التحديات تلك المتعلقة بالاختصاص والمعاينة والتفتيش والضبط والإثبات[١٠٦].

ويثار في هذا الصدد العديد من التساؤلات حول الآليات الواجب اتباعها في سبيل صياغة أحكام قانونية تعمل على ردع مثل تلك الجرائم والتي من خلالها يمكن للمحاكم النظر في القضايا الناشئة عن عمليات التزوير الإلكتروني، وهذا ما سنقوم بدراسته من خلال هذا المطلب وذلك بتقسيمه إلى فرعين: الأول نناقش من خلاله المبادئ

(١٠٦) د. ميساء مصطفى بركات، جرائم التعدي على المعلوماتية، الإتلاف والتزوير، رسالة ماجستير، جامعة بيروت العربية، كلية الحقوق، ٢٠٠٩م، ص٨٢.

المتعلقة بالاختصاص بالنسبة لجرائم التزوير الإلكتروني، والثاني نناقش من خلاله المحاكم المختصة بجرائم التزوير الإلكتروني، وذلك على التفصيل الآتي:

الفرع الأول

المبادئ المتعلقة بتحديد الاختصاص بالنسبة لجرائم التزوير الإلكتروني

إن القانون الجزائي بنصوصه الحالية لا يكفي لمواجهة تلك الصور المستحدثة من الجرائم الإلكترونية، وذلك على الرغم من أن الكثير من هذه المجالات لا يمكن أن توفر النصوص العقابية التقليدية الحماية الكافية لها، فكثير من التشريعات تعاني من القصور في تجريم هذا النوع من الجرائم بنصوص خاصة ومستقلة وإن كانت هنا نصوصاً خاصة في هذا الصدد فإنها تكون قاصرة ولا تستوعب كل صور التجريم الخاصة بهذه الجرائم[١٠٧].

وإذا كانت القاعدة العامة في تحديد الاختصاص هي في تطبيق مبدأ الإقليمية، فهناك استثناءات ترد على هذه القاعدة وهي متعلقة بمبدأ العينية والشخصية والعالمية، وذلك على النحو الآتي:

أولاً: مبدأ الإقليمية

يعد هذا المبدأ في تحديد الاختصاص من المبادئ المستقرة في التشريعات المقارنة جميعها؛ لأنه يرتبط ارتباطاً وثيقاً بسيادتها، ويقصد بمبدأ الإقليمية تطبيق التشريع الجزائي على كل الجرائم المرتكبة في الدولة بصرف النظر عن جنسية الجاني أو المجني عليه سواء أكان وطنياً أم أجنبياً، وقد ورد مبدأ الإقليمية في المادة (١١) من قانون الجزاء الكويتي حيث نصت على أنه: «تسري أحكام هذا القانون على كل شخص يرتكب في إقليم الكويت وتوابعها جريمة من الجرائم المنصوص عليها فيه، وتسري على كل شخص يرتكب خارج إقليم الكويت فعلاً يجعله فاعلاً أصلياً أو شريكاً في جريمة وقعت كلها أو بعضها في إقليم الكويت».

واستناداً للنص السابق ذكره، يمكن توقيع العقوبة المقررة على الجرائم الإلكترونية المرتكبة في إقليم دولة الكويت، فيمكن توقيع العقوبات المقررة في قانون مكافحة جرائم

(١٠٧) د. أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، ط١، ٢٠١٠م، دار النهضة العربية، القاهرة، ص٢٢١.

تقنية المعلومات، وقانون المعاملات الإلكترونية، قانون الجزاء الكويتي على كل من يقوم باختراق أجهزة الكمبيوتر وتزوير البيانات أو الملفات الموجودة في إقليم محدد، وتحديد مكان الكمبيوتر لا أثر له على وقوع الجريمة في الإقليم الوطني، باعتبار أن الفعل الإيجابي المستخدم هو الذي يحدد الركن المادي لجريمة التزوير في دولة الكويت، طالما أنه يمكن الاطلاع على المعلومات في الإقليم الوطني (الكويت).

وفي الغالب، تكون هناك صعوبات مادية تحول دون تحديد مكان ارتكاب الجريمة الأصلية، حيث ينعقد الاختصاص للقضاء الوطني نتيجة لتعقيد شبكة الإنترنت، وتنوّع طرق استخدامها، ولذلك لابد من تحديد مكان ارتكاب الفعل، لمعرفة ما إذا كان الفعل مجرّماً أم لا، وبغير ذلك لا يمكن محاكمة الفاعل والشريك في حال عدم التمكن من تحديد مكان ارتكاب الجريمة[١٠٨].

ثانياً: مبدأ الشخصية

هو وجوب سريان القانون الجزائي لكل دولة على رعاياها المتمتعين بجنسيتها أينما كانوا، ولمبدأ الشخصية شقين: الأول إيجابي حيث يطبق النص الجزائي على كل من يحمل الجنسية الوطنية ولو ارتكبت الجريمة خارج الدولة، أما الوجه الثاني فهو السلبي، والذي يعني سريان القانون الجزائي للدولة على الجرائم التي يكون المجني عليه فيها متمتعاً بجنسيتها ولو ارتكبت الجريمة خارج حدودها الإقليمية[١٠٩].

وقد نص على ذلك في قانون الجزاء الكويتي في المادة (١٢) على أنه: «تسري أحكام هذا القانون أيضاً على كل شخص كويتي الجنسية، يرتكب خارج الكويت فعلاً معاقباً عليه طبقاً لأحكام هذا القانون وطبقاً لأحكام القانون الساري في المكان الذي ارتكب فيه هذا الفعل، وذلك إذا عاد إلى الكويت دون أن تكون المحاكم الأجنبية قد برأته مما أسند إليه». وبذلك يتضح أن مجال تطبيق القانون الكويتي طبقاً لمبدأ الشخصية يكون على كل شخص كويتي يرتكب خارج الكويت فعلاً مجرماً في الكويت، ومجرماً كذلك طبقاً للدولة التي ارتكب فيها الفعل عند عودته إلى الكويت دون تبرئته مما أسند إليه.

مما سبق يتضح أن مجال تطبيق القانون الكويتي طبقاً لمبدأ الشخصية يقوم تطبيقه على كل شخص كويتي يرتكب خارج الكويت فعلاً مجرماً في الكويت،

(١٠٨) د. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، ٢٠٠١م، دار النهضة العربية، القاهرة، ص٥١.

(١٠٩) د. جميل عبد الباقي الصغير، المرجع السابق، ص٥٥.

ومجرماً كذلك طبقاً للدولة التي ارتكب فيها الفعل عند عودته إلى الكويت دون تبرئته مما أسند إليه.

ثالثاً: مبدأ العينية

يعبّر عن مبدأ العينية بتطبيق قانون الجزاء الوطني للدولة على الجرائم التي تعد ماسة بمصالح الدولة الجوهرية، رغم عدم وقوعها في الإقليم الوطني للدولة التي يمسها هذا الفعل، وبصرف النظر عن جنسية فاعلها، وذلك لما للدولة من سلطة بسط سلطانها التشريعي على الجرائم التي تمس المصالح الجوهرية والأساسية لها[١١٠].

ولم يرد نص في قانون الجزاء الكويتي على هذا المبدأ بشكل مباشر، ولكن نص عليه في القانون رقم ٣١ لسنة ١٩٧٠ بتعديل بعض أحكام قانون الجزاء الكويتي والتي تتناول الجرائم المضرة والمتعلقة بأمن الدولة، والاعتداء على أمير البلاد، والانقضاض على السلطات، وتحريض القوات المسلحة على التمرد، وكذلك التحريض على قلب نظام الحكم، وكل ما هو متعلق بأمن الدولة سواء من الداخل أو الخارج، وكذلك نرى أن المشرع الكويتي قد نص عليه في قانون خاص في المادة رقم (٤) من القانون رقم ١ لسنة ١٩٩٣ بشأن حماية الأموال العامة على أنه: «تسري أحكام هذا القانون على كل من يرتكب خارج إقليم الكويت جريمة من الجرائم المنصوص عليها فيه»، وهذا أمر محمود للمشرّع، ومع ذلك لا نعلم سبب تجاهل المشرّع الكويتي وعدم النص عليه صراحة في تشريعه الجزائي ضمن القواعد العامة لقانون الجزاء، ولذا ينبغي تدارك ذلك من خلال تعديل تشريعي لقانون الجزاء الكويتي.

وبتطبيق ذلك على الجرائم الإلكترونية، يمكن القول أن هناك العديد من الجرائم المتعلقة بالتزوير الإلكتروني يمكن أن تندرج ضمن هذا المبدأ، بغض النظر عن جنسية الفاعل حتى ولو ارتكب الفعل خارج إقليم الدولة، ومن ثم يجب التعاون في مجال مكافحة الجرائم الإلكترونية على المستوى الدولي.

رابعاً: مبدأ العالمية

يتمثل مبدأ العالمية في انطباق القاعدة الجنائية على كل جريمة يقبض على مرتكبها في إقليم الدولة أياً كانت جنسيته أو جنسية المجني عليه، وأياً كان مكان ارتكاب جريمته،

(١١٠) د. سمير عالية، أصول قانون العقوبات، القسم العام، ط١، ١٩٩٦م، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، ص١٢٦.

وأياً كانت المصلحة التي أهدرتها الجريمة[١١١]، ومع ذلك لم يعتد التشريع الكويتي بمبدأ العالمية، وإنما جعله قاصراً على الاختصاص الشخصي، ولذا ينبغي تبني هذا المبدأ في التشريع الجزائي الكويتي حتى يساير المجتمع الدولي في هذا الصدد.

ويمكن تبرير الأخذ بهذا المبدأ في مجال الإنترنت، استناداً إلى أن هذه الشبكة قد تخطت كل الحواجز المادية، فأصبح المجال أوسع وأسهل للمجرم الإلكتروني لارتكاب العديد من الجرائم بواسطتها والفرار من العقاب، فمهمة هذا المبدأ هو المساعدة على عدم إفلات المجرم من فعله حتى ولو لم يكن على إقليم الدولة التي يحمل جنسيتها.

الفرع الثاني

المحاكم المختصة بجرائم التزوير الإلكتروني

لقد تطورت استخدامات التقنية في كافة مجالات الحياة، خاصة بعد أن بدأ استخدامها في العالم وانتشار استخدام الحاسب الآلي في المنزل والمكتب واتصال الأجهزة بعضها بعضاً، عبر الشبكات الداخلية للمنشآت والشبكات المحلية والدولية من خلال الشبكة العنكبوتية وتناقل البيانات والمعلومات خلالها، ومع وجود هذا العالم الافتراضي فقد انتقلت إليه الجرائم التي كانت فيما مضى لا يمكن تطبيقها إلا على أرض الواقع لتتم عبر شبكة الإنترنت، فانتقال المعلومة ضمن شبكة الإنترنت بين مختلف دول العالم قد يؤدي إلى تطبيق تراكمي محتمل لجميع قوانين الدول المتصلة بهذه الشبكة دفعة واحدة[١١٢].

وهذا الأمر ترك إشكالية قانونية، تتمثل في كيفية تحديد المحكمة المختصة بالنظر في النزاع الذي قد يثار في هذه الحالة، ومن ثم تباينت المعايير التشريعية التي اعتمدت في تحديد المحاكم المختصة للنظر في الجرائم الإلكترونية، وهو الأمر الذي سيجري بحثه في هذا المطلب من خلال عدة أمور وذلك على النحو الآتي:

أولاً: معيار الاختصاص المكاني

تتبع أغلب التشريعات في تحديد الاختصاص المكاني ثلاثة ضوابط هي مكان وقوع الجريمة، أو محل إقامة المتهم، أو مكان إلقاء القبض عليه، وفي حال اجتماع أكثر

(١١١) د. محمود أحمد طه، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة، ٢٠٠٠م، دار النيل للطباعة، ص٩٩.

(١١٢) د. طوني ميشال عيسى، التنظيم القانوني لشبكة الإنترنت، ط١، ٢٠٠١م، منشورات صادر الحقوقية، بيروت، ص٤٣٣.

من ضابط تكون المحكمة المختصة مكانياً برفع الدعوى إليها، هي المحكمة التي ترفع إليها الدعوى[١١٣]. وقد اعتبر البعض أنه يجب النظر لاختصاص محل ارتكاب الجريمة كاختصاص رئيسي يقدم على غيره، ثم يليه اختصاص محل الإقامة، ثم اختصاص مكان إلقاء القبض على المتهم أو الجاني[١١٤].

وبالنسبة للجرائم الإلكترونية، فإن السلوك والنتيجة يتماثلان في الجريمة، ومن ثم فإن محاكم مكان النشاط الإجرامي ومكان النتيجة تكون مختصة أيضاً، وعلى ذلك، ففي حال إرسال الفيروس الإلكتروني إلى مكان، وتدمير المعلومات في مكان آخر، وتحقيق النتيجة في مكان ثالث، وإلقاء القبض على الجاني في مكان رابع، فإن الاختصاص ينعقد لمحاكم أحد هذه الأماكن[١١٥]. وقد اعتمدت العديد من الدول معيار الاختصاص المكاني[١١٦].

وحيث إن جرائم الإنترنت لا تحدها حدود بعكس الجرائم التقليدية المعروفة، الأمر الذي يجعلها في كثير من الأحيان تستعصى على الخضوع للنصوص القانونية التي تحكم مسألة الاختصاص المكاني، ومن ثم فإن الطبيعة الخاصة لهذا النوع من الجرائم الإلكترونية تتطلب تجاوز النصوص والمعايير التي طرحها الفقه للتغلب على مشكلة تنازع الاختصاص، والعمل على تبني حلول أكثر مرونة تأخذ في الحسبان النطاق الجغرافي لهذه الجرائم وسهولة ارتكابها وآلية اقترافها والتخلص من آثارها، وما إلى ذلك من اعتبارات يفرضها الطابع التقني المتطور لها، وقد أصدر المشرع الكويتي قوانين تعاقب على الأعمال المرتكبة عبر الإنترنت ومنها قانون مكافحة جرائم تقنية المعلومات وقانون المعاملات الإلكترونية (فيما يتعلق بالنصوص الجزائية) – وهي بطبيعتها تعتبر قوانين مكملة لقانون الجزاء – وبمطالعة نصوص مواد القانونين سالفي الذكر لم نصادف نصاً واحداً يتعرض لمسألة الاختصاص القضائي، فبالتالي إذا وقعت أي من هذه الجرائم المنصوص عليها في القوانين الصادرة في هذا الشأن انعقد الاختصاص للمحاكم الوطنية وفقاً للقواعد العامة السابق ذكرها.

(١١٣) د. عبد الفتاح الصيفي، أصول المحاكمات الجزائية، دار النهضة العربية، القاهرة، ١٩٩٠م، ص١٢٠.
(١١٤) د. عاطف النقيب، أصول المحاكمات الجزائية، دراسة مقارنة، منشورات عويدات، بيروت، ١٩٨٦م، ص١٢٤.
(١١٥) د. جميل عبد الباقي الصغير، المرجع السابق، ص٦٢.
(١١٦) د. ميساء مصطفى بركات، المرجع السابق، ص٩٠.

ثانياً: معيار القانون الأكثر ملاءمة

تسبب الجرائم الإلكترونية التي ترتكب بواسطة الإنترنت أضراراً كبيرة قد تختلف من دولة إلى أخرى، مما يفرض التوسع في تفسير قاعدة الاختصاص بالنسبة لمحكمة وقوع الفعل، ليكون الاختصاص للدولة الأكثر تعرضاً للضرر، مع التركيز على مبدأ التنازل للمحكمة أو التخلي عن الاختصاص(١١٧). وعلى العكس من ذلك فإن إعطاء الاختصاص لقانون دولة ما لمجرد إمكانية الوصول إلى معلومة من هذه الدولة أو تلك، أصبح غير كاف من الناحية القانونية لإعلان اختصاص هذه الدولة أو تلك.

والهدف من الأخذ بهذا المعيار، هو البحث عن القانون النموذجي الأكثر ملاءمة للاختصاص في نظر المنازعة المطروحة، ومن أمثلة ذلك ما أصدرته إحدى المحاكم الأمريكية التي اعتبرت فيه أنه لا يمكن الارتكاز إلى مجرد النفاذ، أو الاتصال بهذا الموقع أو المورد انطلاقاً من الأراضي الأمريكية، حتى ينعقد الاختصاص لها للنظر في النزاع المعروض أمامها(١١٨).

ثالثاً: معيار الضرر المرتقب

يتمثل هذا المعيار في التأكيد على حق المضرور باللجوء حسب اختياره إلى محكمة محل ارتكاب الفعل الضار، أو محل وقوع الضرر، مع إضافة قيد هام في حالة لجوء المتضرر إلى محكمة وقوع الضرر يقتضي حجب اختصاص هذه المحكمة إذا أثبت المدعى عليه أنه لم يكن قادراً على توقع الضرر بصورة معقولة، وأن الفعل أو الامتناع كان من شأنه إحداث ضرر مماثل في دولته(١١٩).

وبما أن المحكمة المختصة في النظر في الجرائم الإلكترونية ومنها جريمة التزوير الإلكتروني تعتمد أولاً على معيار الاختصاص المكاني وحده، وبالتالي كان لابد من النظر إلى معايير أخرى وخصوصاً أن جريمة التزوير الإلكتروني لا يحدها حدود وترتكب عبر الشبكة الإلكترونية، فلهذا لابد أن ينظر إلى معيار الضرر المرتقب من أجل حل هذا النزاع الحاصل في المحكمة المختصة في مثل تلك الجرائم.

---

(١١٧) د. طوني ميشال عيسى، المرجع السابق، ص٤٤٧.

(١١٨) د. ميساء مصطفى بركات، المرجع السابق، ص٩٢.

(١١٩) انظر اتفاقية لاهاي لعام ١٩٩٩، المادة (١٠) من أجل المساهمة في الحد من حالات الإفراط في الاختصاص القضائي المحتمل للمحاكم في مجال نشر المعلومات عبر شبكة الإنترنت.

المطلب الثاني
قواعد تحصيل وتقييم الأدلة الخاصة
بإثبات جريمة التزوير الإلكتروني

بعد أن انتهينا من بحث قواعد الاختصاص الجنائي بشأن جريمة التزوير الإلكتروني سواء من حيث المبادئ المتعلقة بتحديد الاختصاص للنظر في جريمة التزوير الإلكتروني أو من حيث المحاكم المخولة في ذلك، ومن ثم يجب أن نبحث بعد ذلك الجانب العملي والتطبيقي من هذا الموضوع، وهو ما يتمثل في التطبيقات التي تقوم بها الجهات القضائية وجهات الضبط القضائي في سبيل مكافحة جريمة التزوير الإلكتروني[١٢٠].

ومن ثم سنقسم هذا المطلب إلى فرعين: نتناول في الفرع الأول منه دور رجال الضبط القضائي في مواجهة جرائم الكمبيوتر، وفي الفرع الثاني، دور القاضي في تقييم الأدلة الخاصة بالجرائم الإلكترونية خاصة التزوير الإلكتروني، وذلك على التفصيل الآتي:

الفرع الأول
دور رجال الضبط القضائي في مواجهة الجرائم الإلكترونية
وبصفة خاصة جريمة التزوير الإلكتروني

بعد أن أصبح المجتمع الإلكتروني حقيقة واقعة بسبب اعتماد المجتمعات على تسيير شئونها على التقنية الإلكترونية والمعلومات، أصبحت الحاجة ملحة لوضع قواعد جزائية شكلية/إجرائية جديدة، تستوعب هذا الكم الهائل من المعلومات، وتكفل مجابهة الأشكال المستخدمة للجرائم الناشئة عن إساءة استخدام هذه التقنية[١٢١]. فبالنسبة للقواعد الإجرائية المتبعة في دولة الكويت هي نفسها القواعد الإجرائية التقليدية المنصوص عليها في قانون الإجراءات والمحاكمات الجزائية الكويتي رقم ١٧ لسنة ١٩٦٠، حيث أتى قانون مكافحة جرائم تقنية المعلومات خالياً من أي قواعد شكلية مستحدثة إلا فيما يتعلق بتحديد الجهة المختصة في ضبط الجرائم والجهة المختصة في التحقيق والتصرف والادعاء (وهي النيابة العامة – نيابة شؤون الإعلام والمعلومات والنشر).

حيث تنص المادة (١٥) من قانون مكافحة جرائم تنقية المعلومات على أن «للموظفين الذين يصدر بتحديدهم قرار من الوزير المختص، ضبط الجرائم التي تقع بالمخالفة لأحكام

(١٢٠) د. ميساء مصطفى بركات، المرجع السابق، ص٩٤.
(١٢١) د. ميساء مصطفى بركات، المرجع السابق، ص٩٤.

هذا القانون وتحرير المخالفات عنها وإحالتها إلى النيابة العامة، وعلى جميع الجهات ذات الصلة تقديم التسهيلات اللازمة لهؤلاء الموظفين»، فقد منح المشرع الكويتي للموظفين الذين يصدر بتحديدهم قرار بذلك من الوزير المختص (قرار بمنحهم صفة الضبط القضائي)، أي مأموري الضبط القضائي، ومن ثم يكون لهم جمع الأدلة والمعلومات عن الجرائم التي ترتكب بصدد القانون السالف الذكر، فبناءً على قرار وزير العدل – الوزير المختص سابقاً[١٢٢] – أعطى لإدارة مكافحة الجرائم الإلكترونية التابعة للإدارة العامة للمباحث الجنائية في وزارة الداخلية سلطة ضبط الجرائم التي تقع بالمخالفة لأحكام قانون مكافحة جرائم تقنية المعلومات.

أولاً: إجراءات الضبط القضائي في معاينة جهاز الكمبيوتر

تعد مرحلة المعاينة من أولى وأهم المراحل الضرورية في كشف الجرائم، حيث يبرز دور رجل الضبط القضائي في معاينة المكان الذي ارتكبت فيه الجريمة، ولكن في إطار الجريمة الإلكترونية، فإن مسرح الجريمة هو جهاز الكمبيوتر[١٢٣]، الذي يتكون من مكونات مادية ومكونات معنوية، ومن ثم فالمعاينة ستشمل كلا النوعين:

- المعاينة على الجرائم الواقعة على المكونات المادية للكمبيوتر:

تعني المعاينة الرؤية أو المشاهدة بالعين لأي أمر، وتتركز غالبية تعريفات المعاينة حول كونها إجراء يهدف إلى إثبات حالة شيء أو شخص أو مكان، وذلك عن طريق الرؤية والفحص المباشر[١٢٤]. ويصفها بعض الفقه بأنها إثبات لحالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة[١٢٥]. وتعد الخطوة الأولى من مراحل ملاحقة الجاني والقبض عليه، وهي خطيرة إذا تم تنفيذها بشكل غير صحيح حيث تؤدي لنتائج خاطئة وإلى وجود هوة واسعة بين العدالة والمجرم، ويجب على رجل الضبط القضائي وضع يده على الأدلة المادية التي تفيد التحقيق، وكذلك وضع الأختام في الأماكن التي أجريت فيها المعاينة

(١٢٢) بعد قرار مجلس الوزراء رقم ٥٥١ لسنة ٢٠١٧ بتحديد الوزير المختص بتطبيق القانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات، أصبح الآن الوزير المختص بتطبيق القانون وإصدار القرارات اللازمة لتنفيذ أحكامه هو نائب رئيس مجلس الوزراء ووزير الداخلية.

(١٢٣) د. ميساء مصطفى بركات، المرجع السابق، ص٩٥.

(١٢٤) د. أحمد بن عبد الله البرادعي، معاينة الجريمة بين النظرية والتطبيق، مطابع ينبع الحديثة، المملكة العربية السعودية، ١٩٩٥م، ص١٣.

(١٢٥) د. فوزية عبد الستار، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ١٩٨٦م، ص٣٣٢.

متى وجد فيها آثار أو أشياء تفيد في كشف الحقيقة، ويجوز له تعيين حارس على هذه الأماكن وإخطار النيابة العامة بهذه الإجراءات(١٢٦).

وعن مدى صلاحية مسرح جرائم الكمبيوتر للمعاينة، فإن جرائم الاعتداء على أنشطة الكمبيوتر ومفاتيح التشغيل وشاشات العرض الخاصة به، لا تثير أدنى صعوبة للتقرير بصلاحية مسرح الجريمة الذي يحوي هذه المعدات لمعاينتها من قبل مأمور الضبط القضائي، وكشف كل الآثار والأدلة الناجمة عن تنفيذ الجريمة، ولابد من القول إن سرعة الانتقال إلى مسرح الجريمة يعد أهم إجراءات التحقيق، لما يترتب عليه من تسهيل مهمة المحقق في معاينة مسرح الجريمة، وسماع الشهود قبل أن تضيع معالم الجريمة(١٢٧).

- المعاينة على الجرائم الواقعة على المكونات المعنوية للكمبيوتر:

إذا كان رجال الضبط القضائي لا يواجهون أية صعوبة في معاينتهم لمسرح الجريمة الواقعة على المكونات المادية بجهاز الكمبيوتر إلا أن الصعوبات الحقيقية تظهر عندما تكون الجريمة واقعة على برامج الكمبيوتر وما يحتويه من بيانات، أي عندما يقوم المجرم الإلكتروني بأعمال تتعلق بالتعدي على كينونة جهاز الكمبيوتر، أي القيام بإتلاف للبرامج أو تزوير للمحررات الإلكترونية، وهذه الصعوبات تحول دون فعالية المعاينة أو فائدتها(١٢٨).

فالجرائم التي تقع على الكمبيوتر تكون مخفية في أكثر صورها، ولا يلاحظها المجني عليه أو يعلم بوقوعها، والإمعان في حجب السلوك وإخفائه عن طريق إرسال الفيروسات أو التلاعب بالبيانات ليس عسيراً، خصوصاً مع توافر الخبرة الفنية والتقنية العالية لدى مرتكبها(١٢٩)، كما أن غياب الدليل المرئي يتمثل في أن المعلومات مسجلة بصورة مرمّزة، ولا يمكن للإنسان قراءتها، وإن كانت قابلة للقراءة من قبل الكمبيوتر نفسه، إلا أن المجرم لا يترك أي أثر، مما يقطع غالباً كل صلة بين المجرم وجريمته، ويحول دون كشف شخصية مرتكبها أو ضبط المستند المزور مثلاً(١٣٠).

---

(١٢٦) إبراهيم حامد مرسي طنطاوي، سلطات مأمور الضبط القضائي، دراسة مقارنة، أطروحة لنيل درجة الدكتوراه، المكتبة القانونية، القاهرة، ١٩٩٧م، ص٢٩٣.

(١٢٧) Barbara etter, "Computer Crime", Paper Presented at the 4th National Outlook Symposium on Crime in the Australia, Convened by: The Australian Institute of Criminology, Canberra 21-22 June 2001, P.6.

(١٢٨) د. إبراهيم حامد مرسي طنطاوي، المرجع السابق، ص٢٩٥.

(١٢٩) Shrishail Math, R.C Tripathi, "Digital Forgeries: Problems and Challenges", International Journal of Computer Application, Volume 5, No 12, August 2010, P.9.

(١٣٠) د. ميساء مصطفى بركات، المرجع السابق، ص٢٩٥.

وبالإضافة لذلك، قد يصعب عملية التفتيش المتوقع عن الأدلة التي قد تدين المجرم الإلكتروني، وذلك بقيامه بالعديد من التدابير الأمنية التي يضر بها من حوله، كاستخدام كلمات السر للوصول إليها، أو منع الاطلاع على البيانات من خلال التشفير مثلاً، ومن الصعوبات الإضافية في هذا المجال سهولة محو الدليل أو تدميره في زمن قصير جداً، فضلاً عن سهولة تنصله من المسئولية(١٣١).

وللحفاظ على مسرح الجريمة نوصي بتصوير الكمبيوتر وما يتصل به من أجهزة بدقة تامة، والتقاط صور لأجزائه الخلفية وسائر ملحقاته، وكذلك عدم التسرع في نقل أي مادة إلكترونية من مكان وقوع الجريمة قبل إجراء اختبارات التأكد من خلو المحيط الخارجي لموقع الكمبيوتر من أية حالات للقوى المغناطيسية خشية إتلاف البيانات المخزنة.

ثانياً: إجراءات الضبط القضائي في التفتيش والضبط لأدلة الكمبيوتر

يشكل ظهور الأنماط الجديدة من الجرائم المعلوماتية عبئاً ثقيلاً على عاتق أجهزة الضبط القضائي، نظراً لما تتطلبه هذه الجرائم من الكفاءة والمعرفة والقدرة على كشف الغموض المحيط بها، والتعريف بمرتكبيها من خلال السرعة في التفتيش وضبط الأدلة. والتفتيش إجراء من إجراءات التحقيق يقوم به موظف مختص وفقاً للإجراءات المقررة قانوناً في محل يتمتع بالحرمة، بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها لإثبات ارتكابها أو نسبتها إلى المتهم(١٣٢).

أما الضبط فيقصد به في القانون إجراءات وضع اليد على شيء يتصل بجريمة وقعت، ويفيد في كشف الحقيقة عنها وعن مرتكبها، وهو من ناحية محله ولا يرد إلا على الأشياء المادية، أما الأشياء المعنوية فلا تصلح محلاً لوضع اليد، ويقصد بالضبط هنا الضبط القضائي الذي يهدف للحصول على الأدلة المتصلة بالتفتيش لمصلحة التحقيق لإثبات واقعة معينة(١٣٣).

والضبط لا يعني أنه لا يقع إلا نتيجة تفتيش، إذ من الممكن أن يكون الضبط نتيجة لمعاينة، كما أنه يجوز أن تضبط أشياء قدمها الشهود، أو المتهمون باختيارهم، وكذلك يجوز للمحقق أن يطالب أحد الأفراد بتسليم شيء في حوزته، ويمكنه إلزامه بذلك(١٣٤).

(١٣١) د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، مجلة الأمن والقانون، السنة السابعة، ١٩٩٩م، العدد (٢)، ص٨٧.

(١٣٢) د. إبراهيم حامد مرسي طنطاوي، المرجع السابق، ص٧٤٣.

(١٣٣) د. توفيق الشاوي، فقه الإجراءات الجنائية، دار الكتاب العربي، القاهرة، ١٩٥٤م، ص٤٩١.

(١٣٤) د. هشام محمد فريد رستم، المرجع السابق، ص٩٣.

وللمحقق أن يأمر بضبط الشيء بعد تقديمه، ذلك أن الامتناع عن تقديم الشيء في هذه الحالة يؤدي إلى فرض عقوبة الامتناع عن الشهادة، ولا يتوقف ضبط جهاز الكمبيوتر على المكونات المادية فقط، بل يمتد إلى مختلف أجزاء النظام، أي أنه يمتد إلى المعطيات والبيانات والبرامج المخزنة في داخله، أي إلى أشياء ذات صيغة معنوية معرضة بسهولة للتغيير، أما فيما يخص برامج الكمبيوتر بما يتضمنه من معلومات وبيانات، فإن الصعوبة تظهر في حال استخدام وسائل فنية في إتلافه وتغيير ما فيه من بيانات ومعلومات عن طريق اختراقه بفيروس، وتكمن الصعوبة في هذه الحالة في قلة الخبرة لدى مأمور الضبط القضائي باعتباره الجهة المختصة بالضبط، أما الصعوبة الثانية فتتمثل في أن عملية الضبط تواجه صعوبة في الحالات التي تكون فيها البيانات مخزنة في نظم معالجة مركزية في الكمبيوتر، ضمن شبكة معلومات كبيرة، في هذه الحالة، فإن صياغة شرط يعطي للمحقق إمكانية ضبط هذا النظام الشبكي بأكمله وعزله عن البيئة الإلكترونية المحيطة به، لا يعد تشريعاً حقيقياً لمبدأ التناسب لما فيه من مساس بحقوق الغير في النظام محل الضبط[١٣٥].

خصوصاً أن جريمة التزوير الإلكترونية هي من الجرائم المستحدثة التي لا تترك شهوداً يمكن استجوابهم، ولا أدلة مادية يمكن فحصها، من هنا تكمن الصعوبة في الكشف عن هذه الجرائم، لذلك فإن مواجهة الجرائم الإلكترونية يلزم اتخاذ إجراءات قد تتجاوز المفاهيم المستقرة التقليدية؛ وذلك لما تتسم به هذه الجرائم من حداثة في الأسلوب وسرعة في التنفيذ، وسهولة في إخفائها وقدرة على محو آثارها[١٣٦]. فعليه نرى ضرورة وجود تدخل تشريعي للنص صراحة على امتداد أحكام الضبط والتفتيش لمكونات الكمبيوتر المعنوية.

الفرع الثاني

دور القاضي في تقييم الأدلة الخاصة بالجرائم الإلكترونية وبصفة خاصة جريمة التزوير الإلكتروني

تزداد الصعوبة في الدور الذي يلعبه القاضي في مواجهة حالات التعدي إذا كانت تمس مصالح المجتمع والأفراد على حد سواء، ويزداد الأمر تعقيداً إذ يتوجب على

(١٣٥) د. هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، ٢٠٠٨، ص٢٠١.

(١٣٦) د. هلالي عبد الله أحمد، المرجع السابق، ص٢٠٣.

القاضي الجزائي الإلمام ببعض المعرفة الفنية للكمبيوتر وأنظمته وما يستجد في هذا المضمار، حيث تحال القضية موضوع الدعوى إلى القاضي للنظر فيها بهدف تحديد آلية عمله في القضية، واستخراج الأحكام التي تتناسب معها تقييم أدلة الجريمة، وتقدير مدى مشروعية الدليل المستمد من الإنترنت.

أولاً: نظام الأدلة القانونية

يتقيد القاضي بموجب هذا النظام في حكمه بالإدانة أو البراءة بأنواع معينة من الأدلة المحددة مسبقاً من جانب المشرع بغض النظر عن اقتناعه أو عدم اقتناعه بصحة ثبوت الواقعة أو عدم ثبوتها، إذ يقوم اقتناع المشرع بصحة الإسناد أو عدم صحته مقام اقتناع القاضي، فيقوم الاقتناع القانوني على افتراض صحة الدليل، بغض النظر عن حقيقة الواقع أو اختلاف ظروف الدعوى، ومن هنا فإن القاضي يحكم في الدعوى المطروحة أمامه طالما توافرت الشروط القانونية في الدليل المطروح في الدعوى حتى ولو كان مقتنعاً بإدانته، وإذا لم تتوافر هذه الأدلة التزم القاضي ببراءة المتهم، بصرف النظر عن اعتقاده الشخصي[١٣٧].

وبذلك يكون المشرع هو من يقوم بالدور الإيجابي في عملية الإثبات في الدعوى، أما دور القاضي فيتمثل في مجرد التحقيق من توافر الأدلة وشروطها القانونية وشرح حججه، أما عن موضوع الأدلة التي تكون مرتبطة بالجرائم الإلكترونية، وحول قبول هذه الأدلة في صورة مخرجات للكمبيوتر كأداة صالحة للإثبات أمام القضاء وذلك باعتبار أن الإنشاءات الإلكترونية والنبضات المغنطة التي تعتمد عليها أجهزة الكمبيوتر ليست مرئية بالعين المجردة وبالتالي لا يستطيع القاضي رؤية الدليل الأصلي، وما يقدم إليهم هو نسخ لأصول مما يجعله ثانوياً وليس أصلياً[١٣٨]. والقاضي ضمن هذا النظام القانوني لا يستطيع أن يحكم حسب اقتناعه الشخصي، بل يبقى مقيداً بنطق الحكم حسب الأدلة التي حددها المشرع.

ثانياً: نظام الاقتناع الذاتي للقاضي

وهو من أكثر الأنظمة شيوعاً والذي يقوم على عدم تحديد الأدلة مسبقاً التي يجب أن يستند إليها القاضي في إصدار حكمه[١٣٩]، حيث تنص المادة (١٥١) من قانون

(١٣٧) د. أحمد فتحي سرور، الشرعية الدستورية وحقوق الإنسان في الإجراءات الجنائية، ط١، ١٩٩٥م، دار النهضة العربية، القاهرة، ص٧٤٦.

(١٣٨) د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، ط٢، ٢٠٠٧م، منشورات الحلبي الحقوقية، بيروت، ص ٣٨٦ وما بعدها.

(١٣٩) د. محمد عيد الغريب، حرية القاضي الجنائي في الاقتناع اليقيني وأثره في تسبيب الأحكام الجنائية، ط١، ١٩٩٧م، النسر الذهبي للطباعة والنشر، القاهرة، ص٨.

الإجراءات والمحاكمات الجزائية الكويتي رقم ١٧ لسنة ١٩٦٠ على أن: «تعتمد المحكمة في اقتناعها على الأدلة المستمدة من التحقيق الذي أجرته في القضية أو من التحقيقات السابقة على المحاكمة، ولها الحرية المطلقة في ترجيح دليل على دليل وتكوين اقتناعها حسبما يوحيه إليه ضميرها، ولا يجوز للقاضي أن يعتمد في حكمه على معلوماته الشخصية»، وقد فتح هذا النص الباب على مصراعيه أمام القاضي الجزائي، وبالتالي أضحى يتمتع بسلطة واسعة من ناحية قبول الأدلة وهو غير مطالب بدليل معين، ففي جميع الأحوال تخضع الأدلة لسلطة القاضي التقديرية.

وفي ضوء ما سبق يتضح أنه في ظل هذا المبدأ لا وجود لأدلة يحظرها المشرع على القاضي أو يفرضها عليه، إذ لا وجود لما يحول دون قبول مخرجات الكمبيوتر أمام القاضي الجزائي كأدلة إثبات الوقائع الخاصة بالدعوة المنظورة أمامه[١٤٠].

ثالثاً: نظام الإثبات المختلط

يعتقد البعض أن هذا النظام هو مزيج بين نظامي الأدلة القانونية ونظام الإثبات المطلق في محاولة لجمع مزاياهما وتلافي عيوبهما، وهذا الرأي يطابق الحقيقة حيث إنه نظام يقوم على تحديد المشرع مسبقاً لأدلة الإثبات التي يجوز للقاضي الاستناد إليها عند إصداره حكمه في الدعوى التي ينظر فيها، مع حقه في تقييم كل دليل على حدة وتقدير مدة كفايته للحكم بالإدانة، أي أن قيمة الدليل متروكة للقاضي بكامل سلطته التقديرية دون تدخل من جانب المشرع، وهنا يتقيد القاضي بالأصول التي يفرضها القانون، ويخضع تقدير الأدلة لقاضي الموضوع دون رقابة عليه من محكمة التمييز، ومع ذلك فإن هذه السلطة غير مطلقة، فإذا خالف القاضي تقدير المنطق السليم ولم يراع الاستثناءات التي يفرضها المشرع، عندئذ يجوز له رد الدليل الذي اعتمده[١٤١].

وما سبق ذكره يعد من القواعد العامة في قوانين الجزاء وقوانين الإجراءات الجزائية في التشريعات المقارنة والتشريع الكويتي بصفة خاصة، ومن ثم فهي قابلة للتطبيق على كافة الجرائم التقليدية منها والمستحدثة وبصفة خاصة جريمة التزوير الإلكتروني موضوع الدراسة.

(١٤٠) د. هشام محمد فريد رستم، المرجع السابق، ص١٥٦.
(١٤١) د. ميساء مصطفى بركات، المرجع السابق، ص١٠٨.

الخاتمة

في ختام هذه الدراسة نأمل أن نكون قد سلطنا الضوء على جريمة من أهم الجرائم الإلكترونية وهي جريمة التزوير الإلكتروني التي تتم بوسائل إلكترونية بشكل كبير، وتزيد أهميتها كل يوم نظراً لانتشار استخدام المحررات الإلكترونية على مستوى الأفراد والمؤسسات، وقد تبين لنا من خلال دراسة هذا الموضوع أن جرائم التزوير التي تقع على المحررات الإلكترونية تهدد الثقة في التعامل بهذه المحررات وتمتد إلى تهديد الأشخاص من خلال شبكة الإنترنت دون إمكانية تعرضهم للمساءلة القانونية كونهم في بلدان لا يعاقب فيها على مثل هذه الأفعال.

والتزوير الذي يقع على المحررات الإلكترونية لا يقل أهمية عن نظيره التقليدي والذي يقع على المحررات الورقية المكتوبة، خاصة أن معظم التشريعات العربية والأجنبية قد اعترفت للمحرر الإلكتروني بذات الحجية التي للمحرر الورقي المكتوب.

وقد انتهينا من هذه الدراسة بعدة نتائج وتوصيات وذلك على النحو الآتي:

أولاً: النتائج

١ – الجرائم الإلكترونية بصفة عامة تمثل خطراً يساوي، بل ويزيد عن الجرائم التقليدية.

٢ – الجريمة الإلكترونية لها من السمات ما يميزها عن الجريمة التقليدية سواء من ناحية السلوك الإجرامي أو من حيث المحل أو النتيجة.

٣ – التزوير الإلكتروني أكثر دقة من نظيره التقليدي.

٤ – اتبع المشرع الكويتي أسلوباً ونهجاً مميزاً حيث نص على الجرائم الإلكترونية في قانونين أساسيين هما القانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات، والقانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية ولكنهما لم يحققا المأمول.

٥ – تقوم جريمة التزوير الإلكتروني وبصفة خاصة جريمة التزوير للتوقيع الإلكتروني بأفعال مختلفة عن التزوير التقليدي من خلال الحصول على منظومة التوقيع بطريقة غير شرعية بنية استخدامها في توقيع المحرر أو من خلال كسر الشفرة.

٦ – عدم ملاءمة إجراءات جمع الأدلة والتحقيق فيها – كالمعاينة والتفتيش وضبط الدليل – المنصوص عليها في التشريعات الإجرائية مع طبيعة جريمة التزوير الإلكتروني وأدلتها، ما يتطلب إيجاد حلول تشريعية تتلاءم مع طبيعة الإجراءات الخاصة بالتحقيق والضبط في جريمة التزوير الإلكتروني.

٧ – ضعف الخبرة التقنية التي يمتلكها رجال الضبط القضائي في تتبع الجريمة والكشف عن الجناة.

ثانياً: التوصيات

١ – العمل على الاقتداء بالدول المتقدمة والتعاون معها في مجال تكنولوجيا المعلومات والاستفادة من خبراتها في التشريعات التي تنظم جرائم المعلومات وبصفة خاصة التزوير الإلكتروني.

٢ – ضبط النص التشريعي بحيث يكون واضحاً من حيث بيان القصد الجنائي والذي يقوم على نية الغش في تغيير الحقيقة إضراراً بالغير.

٣ – العمل على إنشاء جهاز أمني مختص في مكافحة جرائم تقنية المعلومات وبالأخص التزوير الإلكتروني.

٤ – تدريب القضاة ورجال الضبط القضائي على كيفية التعامل مع الأدلة التي تساعد في ضبط الجناة وتوقيع العقاب عليهم.

٥ – إعادة النظر في القانون رقم ٦٣ لسنة ٢٠١٥، والقانون رقم ٢٠ لسنة ٢٠١٤ وبالأخص فيما يتعلق بالقواعد الإجرائية حتى يصير التشريع مواكباً للتقدم الهائل في تقنية المعلومات.

٦ – ضرورة إيجاد تناغم تشريعي بين التشريعات الإجرائية والموضوعية الخاصة بجريمة التزوير الإلكتروني، وذلك باستحداث تشريعات إجرائية تتلاءم وطبيعة هذه الجريمة، تعالج الإجراءات الجنائية الواجب اتباعها للتحقيق في هذه الجرائم، وتحدد قواعد المعاينة والتفتيش وضبط الأدلة الإلكترونية بمختلف أنواعها، بحيث يساعد القانون الإجرائي في تطبيق القانون العقابي الموضوعي على الجرائم المستحدثة التي يفرزها التقدم التكنولوجي، الأمر الذي يحول دون إفلات الجناة من العقاب.

قائمة المراجع

أولاً: المراجع العربية

- د. إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعاملات الإلكترونية، مجلس النشر العلمي، جامعة الكويت، الكويت، ٢٠٠٣م.
- إبراهيم حامد مرسي طنطاوي، سلطات مأمور الضبط القضائي، دراسة مقارنة، أطروحة لنيل درجة الدكتوراه، المكتبة القانونية، القاهرة، ١٩٩٧م.
- أبو بكر عبد القادر الرازي، مختار الصحاح، دار الفكر للطباعة والنشر والتوزيع، دمشق، ١٩٨١م، ج١.
- أحمد أمين، شرح قانون العقوبات الأهلي، القسم الخاص، لجنة التأليف والترجمة والنشر، القاهرة، ١٩٢٣م.
- د. أحمد بن عبد الله البرادعي، معاينة الجريمة بين النظرية والتطبيق، مطابع ينبع الحديثة، المملكة العربية السعودية، ١٩٩٥م.
- د. أحمد تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، الحماية الجنائية، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠٠م.
- د. أحمد خليفة الملط، الجرائم المعلوماتية (دراسة مقارنة)، ط٢، دار الفكر العربي، الإسكندرية، ٢٠٠٦م.
- د. أحمد شرف الدين، التوقيع الإلكتروني وقواعد الإثبات ومقتضيات الأمان في التجارة الإلكترونية، ورقة عمل مقدمة إلى مؤتمر التجارة المنعقد في جامعة الدول العربية، ٢٠٠٠م.
- د. أحمد صبحي العطار، جرائم الاعتداء على المصلحة العامة : دراسة في القسم الخاص من قانون العقوبات المصري، الهيئة المصرية العامة للكتاب، القاهرة، ١٩٩٣.
- د. أحمد فتحي سرور، الشرعية الدستورية وحقوق الإنسان في الإجراءات الجنائية، ط١، دار النهضة العربية، القاهرة، ١٩٩٥م.
- د. أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم الخاص، ط٤، دار النهضة العربية، القاهرة، ١٩٩١م.

- د. أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، ط١، دار النهضة العربية، القاهرة، ٢٠١٠م.
- د. أشرف شمس الدين، الحماية الجنائية للمستند الإلكتروني، دراسة مقارنة، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، المدة من ٢٦-٢٠٠٤/٣/٢٨، منشور على wwwlarabwinfo.com.
- د. أيمن رمضان محمد أحمد، الحماية الجنائية للتوقيع الإلكتروني، رسالة دكتوراه، دار النهضة العربية، القاهرة، ٢٠١١م.
- د. أيمن عبد الله فكري، الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الرياض، ٢٠١٤،
- د. توفيق الشاوي، فقه الإجراءات الجنائية، دار الكتاب العربي، القاهرة، ١٩٥٤م.
- د. ثروت عبد الحميد، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧م.
- د. ثروت عبد الحميد، التوقيع الإلكتروني، مخاطره وكيفية مواجهتها، مدى حجيته في الإثبات، مكتبة الجلاء الجديدة، المنصورة، ٢٠٠١م.
- د. جميل الصغير، الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠١م.
- د. جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠١م.
- د. حسام الدين محمود لطفي، استخدام وسائل الاتصال الحديثة في التفاوض على العقود وإبرامها، دراسة مقدمة إلى ندوة وسائل حسم المنازعات في العمليات المصرفية، مركز القاهرة الإقليمي للتحكيم التجاري الدولي، يونيه ١٩٩٨م.
- د. حسام راضي، حماية المعلومات وتشريعات تقنية المعلومات، منشور على شبكة الإنترنت www.arablae.com
- د. حسن جميعي، إثبات التصرفات القانونية عن طريق الإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٠م.
- د. حسني عبد السميع، الجرائم المستحدثة عن طريق الإنترنت، دراسة مقارنة بين الشريعة والقانون، دار النهضة العربية، القاهرة، ٢٠١١م.

- د. حسنين عبيد، دروس في قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة، ١٩٨٢م.
- د. خالد مصطفى فهمي، النظام القانوني للتوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧م.
- د. رمسيس بهنام، الجرائم المضرة بالمصلحة العامة، منشأة المعارف، الإسكندرية، ١٩٨٦م.
- د. سعيد السيد قنديل، التوقيع الإلكتروني، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٦م.
- د. سمير عالية، أصول قانون العقوبات، القسم العام، ط١، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، ١٩٩٦م.
- د. طوني ميشال عيسى، التنظيم القانوني لشبكة الإنترنت، ط١، منشورات صادر الحقوقية، بيروت، ٢٠٠١م.
- د. عادل رمضان الأبيوكي، التوقيع الإلكتروني في التشريعات الخليجية، دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، ٢٠٠٩م.
- د. عاطف النقيب، أصول المحاكمات الجزائية، دراسة مقارنة، منشورات عويدات، بيروت، ١٩٨٦م.
- د. عبد الفتاح الصيفي، أصول المحاكمات الجزائية، دار النهضة العربية، القاهرة، ١٩٩٠م.
- د. عبد الفتاح حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية، ط١، ٢٠٠٥م.
- د. عبد الفتاح حجازي، الدليل الإلكتروني والتزوير في الجرائم الإلكترونية والإنترنت، دار الكتب القانونية، القاهرة، ٢٠٠٤م.
- د. عبدالفتاح حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، بدون ناشر، ٢٠٠٩م.
- د. عبد الفتاح حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الكتب القانونية، القاهرة، ٢٠٠٧م.

- د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، ١٩٩٩م.
- د. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، ط٢، ٢٠٠٧م، منشورات الحلبي الحقوقية، بيروت.
- د. علي القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات، ١-٣/٥/٢٠٠٠.
- د. عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دراسة تحليلية نقدية لنصوص التشريع المصري مقارناً بالتشريع الفرنسي، ط٢، ١٩٩٥م.
- د. عمر عيسى الفقي، الجرائم المعلوماتية، دار النهضة العربية، القاهرة، ٢٠٠٥م.
- د. عوض محمد عوض، الجرائم المضرة بالمصلحة العامة، دار المطبوعات الجامعية، الإسكندرية، ١٩٨٥م.
- د. عيسى غسان ربضي، القواعد الخاصة بالتوقيع الإلكتروني، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٩م.
- د. غنام محمد، مكافحة جرائم الكمبيوتر، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مؤتمر القانون والكمبيوتر والإنترنت.
- أ. د. غنام محمد غنام، د. فيصل عبدالله الكندري، شرح قانون الجزاء الكويتي: القسم الخاص، دولة الكويت، ط٤، ٢٠١٥ - ٢٠١٤ ،
- د. فوزية عبد الستار، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، ١٩٨٦م.
- د. فيصل الغريب، التوقيع الإلكتروني وحجيته في الإثبات، بحوث ودراسات المنظمة العربية للتنمية الإدارية، القاهرة، ٢٠٠٥م.
- د. لورانس محمد عبيدات، إثبات المحرر الإلكتروني، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٩م.
- د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، ١٩٩٤م.

- د. محمد عبد الله أبو بكر، جرائم الكمبيوتر والإنترنت، موسوعة جرائم المعلوماتية، منشأة المعارف، الإسكندرية، ٢٠٠٦م.
- د. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، بدون تاريخ.
- محمد عقاد، جريمة التزوير في محررات الحاسب، دراسة مقارنة، المؤتمر السادس، الجمعية المصرية للقانون الجنائي ٢٥-١٩٩٣/١٠/٢٨، دار النهضة العربية.
- د. محمد عيد الغريب، حرية القاضي الجنائي في الاقتناع اليقيني وأثره في تسبيب الأحكام الجنائية، ط١، النسر الذهبي للطباعة والنشر، القاهرة، ١٩٩٧م.
- د. محمود أحمد طه، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة، دار النيل للطباعة، القاهرة، ٢٠٠٠م.
- د. محمود مصطفى، شرح قانون العقوبات، القسم الخاص، ط/ جامعة القاهرة، ١٩٨٥م.
- د. محمود نجيب حسني، الموجز في شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، ١٩٩٤م.
- د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، القاهرة، ٢٠٠١م.
- د. ممدوح محمد مبروك، مدى حجية التوقيع الإلكتروني في الإثبات، دار النهضة العربية، القاهرة، ٢٠٠٩م.
- د. منير الجنبيهي، د. ممدوح الجنبيهي، التوقيع الإلكتروني وحجيته في الإثبات، دار الفكر الجامعي، الإسكندرية، ٢٠٠٤م.
- د. منير الجنبيهي، د. ممدوح الجنبيهي، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦م.
- د. ميساء مصطفى بركات، جرائم التعدي على المعلوماتية، الإتلاف والتزوير، رسالة ماجستير، جامعة بيروت العربية، كلية الحقوق، ٢٠٠٩م.
- د. هشام رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤م.

- د. هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، مجلة الأمن والقانون، السنة السابعة، العدد (٢)، ١٩٩٩م.
- د. هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، ٢٠٠٨.
- القاضي/ وليد عكوم، مفهوم ظاهرة الإجرام المعلوماتي، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات، ١-٢٠٠٥/٣/٣.
- د. يونس عرب، صور الجرائم الإلكترونية واتجاهات تبويبها، ورشة عمل عن تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، المدة من ٢-٢٠٠٦/٤/٤.

ثانياً: الأحكام القضائية:

- نقض ١٩٤٤/٤/١٠، مجموعة القواعد، ج٦، رقم ٣٣٣، ص٤٥٥.
- نقض ١٩٥٨/٦/١٦، المجموعة، س٩، رقم ١٦٨، ص٦٦٧.
- نقض ١٩٦٢/٥/٢٢، المجموعة، س١٣، رقم ١٢٥، ص٤٨٩.
- نقض ١٩٦٨/٢/٢٦، المجموعة، س١٩، رقم ٥١، ص٢٨٠، نقض ١٩٧٨/١٠/١، المجموعة، س٢٩، رقم ١٢٤، ص٦٤١.
- نقض ١٩٦٨/٥/٦، المجموعة، س١٩، رقم ١٠٥، ص٥٣٦، نقض ١٩٧١/١٢/٢٧، المجموعة، س٢٢، رقم ٢٠٠، ص٨٣٣.
- نقض ١٩٦٨/٥/٢٧، المجموعة، س١٩، رقم ١٢٣، ص٦١٥.
- نقض ١٩٧٢/٦/١٩، المجموعة، س٢٣، رقم ٢١٠، ص٩٤٠، نقض ١٩٧٩/٤/٢٩، المجموعة، س٣٠، رقم ٢١٠٧، ص٥٠٦.
- نقض ١٩٧٤/٢/١٦، المجموعة، س٢٥، رقم ١٨٨، ص٨٦٦.
- تمييز ١٩٨٢/٧/٥، طعن ٩٦/٨٢ جزائي.
- تمييز ٢٠٠٢/٥/٢١، طعن ٣٢٦/٢٠٠١ جزائي.
- تمييز ٢٠٠٣/٦/١٧، طعن ١/٢٠٠٢ جزائي.

- تمييز ٢٠٠٥/١/٤، طعن ١٧٥ لسنة ٢٠٠٤ جزائي.
- تمييز ٢٠٠٥/١١/١٥، طعن ٧٧ لسنة ٢٠٠٥ جزائي.
- تمييز ٢٠٠٩/٢/١٠، طعن ٤٤٥ لسنة ٢٠٠٨ جزائي.
- تمييز ٢٠٠٩/٤/٢١، طعن ٣٣٥ لسنة ٢٠٠٨ جزائي.
- تمييز ٢٠٠٩/٥/١٢، طعن ٢٧٢ لسنة ٢٠٠٨ جزائي.
- تمييز ٢٠١٣/٤/١، طعن ٣٠٤ لسنة ٢٠١٢ جزائي.

ثالثاً: المراجع الأجنبية

- Article 1-441: Constititue un faux toute altération frauduleuse de la verité, de nature à causer un prejudice et accomplice par quelque moyen que co soit, dans un écrit ou tout autre support d'expression de la pensee qui a pour objet ou qui peut avoir pour effet d'etablir la prevue d'un faux et l'usage de faux sont punis de trios ans d'emprisonnement et de 45000 euros d'amende".
- Barbara etter, "Computer Crime", Paper Presented at the 4th National Outlook Symposium on Crime in the Australia, Convened by: The Australian Institute of Criminology, Canberra 22-21 June 2001.
- DIRECTIVE 93/1999/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures, Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999L0093&from=FR
- Donn B. Parker, Fighting Computer Crime: A New Framework for Protecting Information, 1998 Wiley computer Publishing, United States of America.
- Jonathan Clough, Principles of Cybercrime, 2 ed - Cambridge University Press 2015, United Kingdom.
- M. Cabrillac et B. Teyssie, Carte de prelevement aupres d'un distributeur automatique.

- Shrishail Math, R.C Tripathi, "Digital Forgeries: Problems and Challenges", International Journal of Computer Application, Volume 5, No 12, August 2010.