أحكام جريمة التزوير الالكتروني في القانون الكويتي

تتسم جرائم التزوير بوجه عام بكونها جرائم ذات درجة عالية من الحساسية، لكونها تمثل خطراً جسيماً على أي مجتمع، حيث تضرب أسس الثقة بين أفراد المجتمع الواحد في الصميم، كما تؤثر بشكل سلبي بالغ على القيم الدينية والاجتماعية وأيضاً الاقتصادية، لاسيما وأنها تساهم بشكل كبير في نشر الفساد بجميع صوره، مما جعل شريعتنا الإسلامية الغراء تؤثم فعل التزوير وتبعها في ذلك القانون الوضعي.

وفي ظل التقدم الإلكتروني الهائل الذي نحيا فيه وما أفرزه من تطور في مجال المعاملات بشتى أنواعها، وظهرت أدوات ووسائل جديدة لإتمام تلك المعاملات منها المحرر الإلكتروني والتوقيع الإلكتروني وغيرها، فقد تطورت جريمة التزوير التي تستهدف ما تحويه تلك الوسائل والأدوات الإلكترونية من بيانات ومعلومات، لتتخذ شكلاً جديداً وهو الشكل الإلكتروني،

المحامي مسفر عايض
mesferlaw.com

وبالطبع فإن تطور جريمة التزوير من شكلها التقليدي إلى الشكل الإلكتروني واكبه تطور وتغير في مكوناتها ومقوماتها، وهو أمر منطقي خاصة وأن مكونات ومقومات جريمة التزوير التقليدية لا تصلح لقيام جريمة التزوير الإلكتروني نظراً للطبيعة الخاصة بها، لذلك كان من اللازم أن يقوم المشرع بسن قانون يمكنه من خلالها مواجهة جريمة التزوير الإلكتروني وسائر الجرائم الإلكترونية الأخرى، وهو بالفعل ما بادر إليه المشرع الكويتي بإصداره لقانون مكافحة جرائم تقنية المعلومات رقم 63 لسنة 2015 ليضع الأحكام والضابط التي تنظم هذه الطائفة من الجرائم المستحدثة.

وسوف نتناول في هذا المقال أهم الجوانب الخاصة بجريمة التزوير الإلكتروني، والأحكام التي قررها المشرع الكويتي في شأن تلك الجريمة في قانون مكافحة جرائم تقنية المعلومات آنف الذكر.

أهمية البحث :

تكتسب هذه الدراسة حول أحكام جريمة التزوير الإلكتروني في القانون الكويتي أهميتها من عدة جوانب، يمكن إجمالها فيما يلي:

أولاً: الأهمية الموضوعية :تمثل جريمة التزوير الإلكتروني أحد أخطر الجرائم المستحدثة في عصر الرقمنة، حيث تضرب أسس الثقة في المعاملات الإلكترونية في الصميم، وتؤثر بشكل سلبي بالغ على القيم الدينية والاجتماعية والاقتصادية، كما تساهم بشكل كبير في نشر الفساد بجميع صوره، مما جعل شريعتنا الإسلامية الغراء تؤثم فعل التزوير وتبعها في ذلك القانون الوضعي.

ثانياً: الأهمية التشريعية :تسلط الدراسة الضوء على النصوص القانونية المنظمة لجريمة التزوير الإلكتروني في قانون مكافحة جرائم تقنية المعلومات رقم 63 لسنة 2015، وقانون المعاملات الإلكترونية رقم 20 لسنة 2014، وتبين مدى كفاية هذه النصوص في مواجهة هذه الجريمة المستحدثة، وتحديد مواطن القوة والضعف فيها.

المحامي مسفر عايض
mesferlaw.com

ثالثاً: الأهمية العملية :تساعد الدراسة في تعريف المحققين والقضاة ورجال القانون بخصائص جريمة التزوير الإلكتروني وأركانها، مما ييسر عملية كشفها والتحقيق فيها، ويمكّن من تطبيق العقوبات المقررة لها بشكل صحيح.

رابعاً: الأهمية الأكاديمية :تسد الدراسة ثغرة في المكتبة القانونية الكويتية من خلال تقديم بحث متكامل حول جريمة التزوير الإلكتروني، مستعرضاً مختلف جوانبها القانونية والفقهية، ومحللاً النصوص القانونية ذات الصلة.

خامساً: الأهمية المجتمعية :تعمل الدراسة على نشر الوعي بأخطار جريمة التزوير الإلكتروني، وسبل الوقاية منها، وتعزيز ثقة الأفراد والمؤسسات في المعاملات الإلكترونية.

أهداف البحث

تسعى هذه الدراسة إلى تحقيق مجموعة من الأهداف، يمكن إجمالها فيما يلي:

1. **تقديم تعريف شامل لجريمة التزوير الإلكتروني**، من خلال استعراض مختلف التعاريف الفقهية، والخروج بتعريف جامع يحدد ماهيتها وطبيعتها القانونية، في ظل خلو القانونين الكويتيين (قانون مكافحة جرائم تقنية المعلومات وقانون المعاملات الإلكترونية) من تعريف نصي لها.

2. **تحليل السمات الخاصة بجريمة التزوير الإلكتروني**، والتي تميزها عن جريمة التزوير التقليدي، وفي مقدمتها: كونها جريمة عابرة للحدود، وإمكانية ارتكابها في أي مرحلة من مراحل المعالجة الإلكترونية (الإدخال، المعالجة، الإخراج)، وصعوبة الكشف عنها وإثباتها، وصعوبة الادعاء بارتكابها على سبيل الخطأ.

المحامي مسفر عايض
mesferlaw.com

3. **تحديد محل جريمة التزوير الإلكتروني**، والذي يشمل: المحرر الإلكتروني، والتوقيع الإلكتروني، والوسيط الإلكتروني (الدعامة المادية، نظام المعالجة الإلكترونية للبيانات، النظام الإلكتروني المؤتمت، نظام الحاسب الآلي، النظام الإلكتروني)، والموقع الإلكتروني، وذلك وفقاً لما ورد في المادة (2/3) من قانون مكافحة جرائم تقنية المعلومات.

4. **بيان أركان جريمة التزوير الإلكتروني**، والتي تتمثل في: الركن المفترض (أداة الجريمة - استخدام وسيلة من وسائل تقنية المعلومات)، والركن المادي (فعل الاصطناع، التغيير، أو التحوير)، والركن المعنوي (القصد الجنائي العام بعنصريه العلم والإرادة.)

5. **استعراض العقوبات المقررة لجريمة التزوير الإلكتروني**، سواء في قانون مكافحة جرائم تقنية المعلومات أو قانون المعاملات الإلكترونية، وبيان العقوبات الأصلية (الحبس والغرامة) والعقوبات التكميلية (المصادرة والإغلاق والنشر)، وظروف تشديد العقوبة.

6. **تقديم توصيات للجهات التشريعية والقضائية**، تهدف إلى تطوير النصوص القانونية المنظمة لجريمة التزوير الإلكتروني، وتعزيز آليات كشفها والتحقيق فيها، ونشر الوعي بأخطارها وسبل الوقاية منها.

أولاً: المقصود بجريمة التزوير الإلكتروني

تنتمي جريمة التزوير بوجه عام سواء في صورتها التقليدية أو الإلكترونية إلى طائفة الجرائم التي تستلزم دقة فائقة من قبل الجاني عند ارتكابها، لاسيما وأن الأدوات التي تستخدم في ارتكابها تقتضي أن يكون الجاني على درجة كبيرة من المهارة والقدرة على استخدامها، وخاصة جريمة التزوير الإلكتروني التي تقتضي المزيد من تلك الدقة والمهارة لارتباطها بتقنية المعلومات.

المحامي مصفر عارض
mesferlaw.com

والتزوير بوجه عام عرفه الفقه القانوني بأنه التغيير الواقع على الحقيقة بغرض الغش في مستند أو وثيقة أو أي محرر آخر، على أن يكون هذا التغيير بوسيلة من الوسائل التي يقررها القانون، وأن يكون من شأن هذا التغيير في الحقيقة أن يترتب عليه ضرر بمصلحة عامة أو خاصة، وقد ربطها البعض بنية استخدام الجاني للمحرر المزور في الغرض الذي أعد من أجله[1].

وقد تصدى المشرع الكويتي لفعل التزوير بالتعريف في قانون الجزاء الكويتي رقم 16 لسنة 1960، حيث جاء في نص المادة رقم (257) منه أنه "كل تغيير للحقيقة في محرر بقصد استعماله على نحو يوهم بأنه مطابق للحقيقة إذا كان المحرر بعد تغييره صالحاً لأن يستعمل على هذا النحو"، كما أسهب المشرع في ذات المادة المذكورة آنفاً في ذكر الطرق التي يقر القانون تحقق فعل التزوير من خلالها، والتي منها على سبيل المثال الاصطناع والتعديل والتغيير وغيرها من الطرق الأخرى.

وبالرجوع إلى القوانين ذات العلاقة وهي قانون مكافحة جرائم تقنية المعلومات، والقانون رقم 20 لسنة 2014 بشأن المعاملات الإلكترونية، وذلك باعتبارهما قد تناولا في أحكامهما جريمة التزوير الإلكتروني، سيتبين لنا أن أياً من هذين القانونين لم يتعرضا إلى جريمة التزوير الإلكتروني بالتعريف، حيث اقتصرا على عرض للطرق التي تتم من خلالها هذه الجريمة، وبيان العقوبات المقررة لمرتكبي جرائم التزوير الإلكتروني، وهو ما يُستدل منه أن المشرع لم

[1] - د/ أحمد فتحي سرور – الوسيط في قانون العقوبات: القسم الخاص – ط4 – دار النهضة العربية – مصر – 1991 – ص402.

يرغب في حصر مفهوم جريمة التزوير الإلكتروني في تعريف محدد وجامد، لاسيما وأنها جريمة مستحدثة وتتعلق بتقنية المعلومات التي تتطور يوماً بعد يوم، وبالتالي سيكون من اللازم تطوير تعريفها بشكل دوري ومستمر، وإلا سيكون ذلك بمثابة ثغرة يمكن من خلالها لمرتكبي جريمة التزوير من التملص من العقاب بزعم عدم انطباق التعريف القانوني لها على جرائمهم، وبالتالي ترك المشرع مهمة تعريف تلك الجريمة للفقه القانوني، والذي لم يتوانى عن القيام بمهمته وقام بتعريف جريمة التزوير الإلكتروني بأكثر من تعريف، ويمكننا أن نذكر أهمها على النحو الآتي بيانه:

- عرف جانب من الفقه القانوني التزوير الإلكتروني بأنه إدخال تعديل أو تغيير على الحقيقة في توقيع إلكتروني أو محرر إلكتروني.
- اتجه جانب آخر إلى تعريفه بأنه التغيير في الحقائق الواردة بوثائق او محررات إلكترونية بغرض استخدامها بعد إدخال هذا التغيير عليها.
- بينما عرفه البعض من الفقه بأنه تعديل أو تغيير أو تحوير في المعلومات والبيانات الموجودة في وثيقة أو محرر الكتروني، وذلك بغرض إدخال الغش والتضليل على الغير[2].
- وعرفه البعض الآخر بأنه استخدام لأي برنامج معالجة إلكترونية أو برامج اختراق بغرض تعديل أو تغيير البيانات أو المعلومات الأصلية أو التلاعب فيها بأي صورة كانت، وذلك بغرض ونية استعمالها[3].
- واتجه البعض إلى تعريف التزوير الإلكتروني بأنه تغيير للحقيقة الواردة في محل التزوير سواء كان محرر أو وثيقة أو دعامة أو سند، طالما كان محل التزوير له أثر في إنشاء حق أو في ترتيب أثر قانوني محدد.

المحامي مسفر عايض
mesferlaw.com

ومن مجمل التعريفات آنفة الذكر والتي وضعها الفقه القانوني لبيان مفهوم جريمة التزوير الإلكتروني يمكننا أن نستخلص تعريفاً متوازناً لها، وهي أنها الجريمة التي يقع فيها فعل التزوير المتمثل في تغيير أو تعديل أو تحوير الحقيقة على مستند إلكتروني، أو اصطناع مستند إلكتروني لا وجود له، وذلك لإدخال الغش والتضليل باستخدامه في الغرض الذي تم تزويره من أجله، لما يتحقق معه ضرراً للغير.

ثانياً: السمات الخاصة بجريمة التزوير الإلكتروني

[2] - عمر عبد السلام الجبوري – جريمة التزوير الإلكتروني في التشريع الأردني: دراسة مقارنة – رسالة ماجستير غير منشورة – كلية الحقوق – جامعة الشرق الأوسط – الأردن – 2017 – ص17.

[3] - عباس حفظي – جرائم التزوير الإلكتروني – رسالة ماجستير غير منشورة – جامعة وهران – الجزائر – 2015 - ص2.

تعد جريمة التزوير الإلكتروني جريمة ذات طابع خاص، حيث تتسم بخطورتها الجسيمة نظراً للأضرار التي ترتبها جريمة التزوير في حد ذاتها، كما أنها جريمة من الجرائم الإلكترونية مما يُكسبها طبيعة خاصة تجعلها أكثر خطورة من جرائم التزوير التقليدية، ونظراً لتلك الخطورة المزدوجة التي تتصف بها تلك الجريمة فإنها تتسم بمجموعة من السمات التي يمكننا أن نوجز أبرزها في النقاط الآتي بيانها:

(1) القدرة على أن تكون جريمة عابرة للحدود

تتسم جريمة التزوير الإلكتروني بأنها من الجرائم القادرة على أن تكون جريمة عابرة للحدود، وترجع تلك السمة إلى الطبيعة الخاصة التي تتسم بها تلك الجريمة كونها يمكن أن تُرتكب عبر شبكة الإنترنت، والجرائم التي تتم بتلك الصورة لا تتقيد بحدود جغرافية ولا يُشترط فيها أن تتم داخل إقليم الدولة الواحدة، كما لا تتطلب وجود الجاني والمجني عليه أو المحرر محل التزوير وجوداً مادياً في ذات المكان عند ارتكابها.

المحامي مسفر عايض
mesferlaw.com

ولعل تلك السمة تمثل أهمية كبيرة عند التعرض لجريمة التزوير الإلكتروني، خاصة وأنها تؤثر بشكل كبير على تحديد القضاء المختص بنظرها، لاسيما إذا كان الجاني في دولة والمجني عليه في دولة أخرى، وكان المحرر الذي تم التزوير فيه موجوداً على شبكة الإنترنت، ففي تلك الحالة تثور إشكالية القضاء صاحب الاختصاص بنظرها، كما تثير أيضاً إشكالية تحديد القانون واجب التطبيق على تلك الجريمة، ويرجع ذلك جميعه إلى طبيعة جرائم التزوير الإلكتروني والتي قد تجعلها في كثيراً من الحالات جريمة عالمية.

(2) يتم ارتكابها في أياً من مراحل تشغيل نظام المعالجة الإلكترونية

تتسم جرائم التزوير الإلكتروني أيضاً بأنها جرائم تقنية، ويُقصد بذلك أنها لا تُرتكب إلا من خلال استخدام وسيلة من وسائل تقنية المعلومات كالحواسب الآلية وشبكة الإنترنت وشبكات المعلومات، وهو ما يتيح ارتكاب تلك الجريمة في أي مرحلة من المراحل التي يتم اتباعها في تشغيل نظام المعالجة الإلكترونية، حيث أنه من المتعارف عليه أن مراحل المعالجة الإلكترونية لأي نظام هي ثلاث مراحل أساسية، ونوضح تلك المراحل وكيفية ارتكاب جريمة التزوير الإلكتروني خلال كل مرحلة منها على النحو التالي:

- **المرحلة الأولى: مرحلة الإدخال:** وهذه المرحلة هي المرحلة التي يتم فيها ترجمة المعلومات والبيانات من اللغة المفهومة التي حررت بها إلى لغة لا يتم فهمها إلا من قبل النظام الإلكتروني وتغذيته بها، وهو ما يتيح خلال تلك المرحلة ارتكاب جريمة

التزوير الإلكتروني عن طريق تغذية النظام ببيانات غير صحيحة باعتبارها هي البيانات الصحيحة، أو ترجمة ما تتضمنه الوثائق الأصلية بشكل مخالف للحقيقة الواردة فيها، وهو ما يعرفه الفقه في تلك الحالة بالتزوير المعنوي.

- **المرحلة الثانية: مرحلة المعالجة:** ويُقصد بها المرحلة التي يتم من خلالها استقبال النظام الإلكتروني للبيانات التي تم إدخالها وإخضاعها للعديد من العمليات الحسابية والاستنتاجية، تمهيداً لاتخاذ الإجراء المحدد بشأنها من قبل المبرمج سواء كان التخزين أو التصنيف أو الترتيب أو غيرها من الإجراءات الأخرى، ويمكن ارتكاب جريمة التزوير الإلكتروني في تلك المرحلة بأكثر من وسيلة، منها على سبيل المثال لا الحصر التلاعب في إعدادات برامج الحاسب ونظم المعلومات ليتم معالجة البيانات بصورة مغايرة للصورة المطلوب معالجتها عليها، وبالتالي الخروج بنتائج مخالفة للحقيقة.
- **المرحلة الثالثة: الإخراج:** وهي المرحلة الأخيرة من مراحل المعالجة الإلكترونية، والتي يتم خلالها إظهار النتائج المتحصلة من مرحلة المعالجة، ويمكن ارتكاب جريمة التزوير الإلكتروني في تلك المرحلة عن طريق برامج إلكترونية يمكنها الوصول إلى المخرجات الموجودة على الدعامة التي يتم استقبال المخرجات عليها والتلاعب في محتواها بالتعديل أو التغيير.

المحامي مسفر عايض
mesferlaw.com

(3) صعوبة الكشف عنها أو إثباتها

جرائم التزوير الإلكتروني تختلف عن جرائم التزوير التقليدية من حيث درجة صعوبة اكتشافها أو الوقوف على آثارها، حيث يسهل اكتشاف جرائم التزوير التقليدية باعتبارها تتم عن طريق الكشط أو الشطب أو التغيير أو غيرها من الطرق التي تستهدف المحرر، وهي طرق يسهل اكتشافها والانتباه إلى آثارها، بينما جرائم التزوير الإلكتروني يصعب اكتشافها أو الانتباه إلى آثارها إن كانت تترك آثاراً من حيث الأصل، حيث أن طرق التزوير الإلكتروني لا تخلف آثار مادية يمكن اكتشافها، وذلك باعتبارها تستهدف الوصول إلى البيانات والمعلومات والتلاعب في مضمونها وتغييره، وذلك بطرق فنية غير ملموسة تستخدم فيها تقنيات مختلفة يصعب أن يفطن إليها أو إلى آثارها أحد، خاصة وأن التحقيق في تلك الجرائم والبحث عن خيوطها الأولية تستلزم نوع خاص من المحققين لديهم إلمام تقنيات الحاسب ونظم المعلومات، وهو ما لا يتحقق لدى المحققين التقليديين.

كما أن تلك الجرائم – وفقاً لرأي الفقه القانوني – تعد جرائم خفية، حيث أن المجني عليه لا يمكنه اكتشاف وقوع جريمة التزوير الإلكتروني عند ارتكابها، بل قد لا يكتشفها إلا بعد مرور فترة زمنية غير قصيرة على ارتكابها، وقد يكون اكتشافه لها عن طريق المصادفة.

ويمكننا أن نعزي صعوبة إثبات جريمة التزوير الإلكتروني إلى عدة عوامل أهمها:

- الصعوبة البالغة في الحفاظ على الدليل الخاص بارتكابها، لاسيما وأن الجاني فيها يتمتع بقدرات فنية عالية تجعله قادراً على محو أي دليل قد يتخلف عن جريمته بكل سهولة.
- عدم قيام غالبية المجني عليهم بالإبلاغ عن الجريمة خاصة في الحالات التي يكون فيها المجني عليه هو شركة أو مؤسسة لها سمعتها في مجال عملها، وبالتالي يكون انتشار خبر وقوعها ضحية لتلك الجريمة بمثابة ضربة قوية لسمعتها أمام عملائها.
- نظراً لكون تلك الجريمة يتم ارتكابها من قبل الجاني في وسط إلكتروني باختلاف صوره، فإنها لا تترك ثمة آثار مادية يمكن التقاطها وتتبعها.

(4) صعوبة الادعاء بارتكابها على سبيل الخطأ

تتسم أيضاً جرائم التزوير الإلكتروني بصعوبة شديدة في ادعاء الجاني بأنه قد ارتكبها بشكل غير متعمد أو على سبيل الخطأ، ولا يخلي من ذلك ما تضمنه القانون من اشتراط تحقق الركن المعنوي (القصد الجنائي) لدى مرتكبها، حيث أن تلك السمة لا تنفي كون تلك الجريمة من الجرائم العمدية، إلا أن إثبات عدم توافر القصد الجنائي يمثل صعوبة بالغة للجاني الذي ارتكبها، وذلك لكون ارتكاب جريمة التزوير الإلكتروني يتطلب إعداد وتجهيز العديد من المعارف والفنيات والمهارات الخاصة، مما يستلزم تخطيط مسبق لارتكابها، ولا يُتصور أن ترتكب على سبيل المصادفة أو الخطأ.

المحامي مسفر عايض
mesferlaw.com

ثالثاً: المحل الذي تنصب عليه جرائم التزوير الإلكتروني

محل الجريمة هو العنصر الذي تستهدفه الجريمة بالفعل المادي الذي يشكل السلوك الإجرامي للجاني، فعلى سبيل المثال في جريمة السرقة يكون المحل هو المال الذي يستهدف الجاني سرقته، وجرائم الضرب والجرح يكون محلها جسد المجني عليه، أما في جرائم التزوير الإلكتروني فإن المشرع الكويتي قد حدد محل الجريمة في جريمة التزوير الإلكتروني بموجب نص المادة رقم (2/3) من قانون مكافحة جرائم تقنية المعلومات، والتي نصت على أن "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: ... 2- زور أو أتلف مستنداً أو سجلاً أو أو توقيعاً إلكترونياً أو نظام معالجة إلكترونية للبيانات أو نظام إلكتروني مؤتمت أو موقعاً أو نظام حاسب آلي أو نظام إلكتروني ...".

وبالتالي فإن محل الجريمة لا يقتصر على محل وحيد بل يتمثل في أكثر من محل يمكن أن تستهدف جريمة التزوير الإلكتروني أياً منها، وتتمثل تلك المحال في المحرر الإلكتروني، والتوقيع الإلكتروني، والوسيط الإلكتروني، ونظام المعالجة المعالجة الإلكترونية للبيانات، والنظام الإلكتروني المؤتمت، والموقع الإلكتروني، ونظام الحاسب الآلي، والنظام الإلكتروني، وسوف نتعرض لكل محل منهم بشكل مفصل في النقاط الآتي بيانها.

(1) المحرر الإلكتروني

تناول الفقه القانوني التعريف بالمحرر الإلكتروني بأكثر من تعريف، ومن أهم وأبرز تلك التعاريف يمكننا أن نذكر التعريف القائل بأن المحرر الإلكتروني هو المحرر الذي يشتمل على بيانات تم معالجتها إلكترونياً، ومكتوبة وموقع عليها توقيعاً إلكترونياً، ويتم وضعه على دعامة مادية تتناسب مع طبيعته، ويقبل التحول إلى محرر ورقي عن طريق استخدام مخرج من مخرجات الحاسب الآلي كالطابعات[4].

المحامي مسفر عايض
mesferlaw.com

وقد تناول المشرع الكويتي المحرر الإلكتروني في قانون مكافحة جرائم تقنية المعلومات رقم 63 لسنة 2015 تحت مسمى المستند أو السجل الإلكتروني وذلك في المادة رقم (1) منه، حيث عرفه بأنه "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".

كما تناوله أيضاً في قانون المعاملات الإلكترونية رقم 20 لسنة 2014 ولكن تحت مسميين، المسمى الأول هو المستند أو السجل الإلكتروني والذي يتفق في تعريفه له مع التعريف الوارد بقانون مكافحة جرائم تقنية المعلومات، والمسمى الثاني هو مسمى الرسالة الإلكترونية، والتي عرفها قانون المعاملات الإلكترونية في مادته الأولى على أنها "بيانات إلكترونية ترسل أو تستلم بوسائل إلكترونية أياً كانت وسيلة استخراجها في المكان المستلمة فيه".

وهو ما يمكننا معه أن نعرف المحرر الإلكتروني بأنه بيانات أو معلومات إلكترونية قابلة لوضعها على وسيط مادي ملموس أو دعامة إلكترونية، وتكون قابلة للاستعادة والاسترجاع في صورة يمكن فهمها.

(2) التوقيع الإلكتروني

---

[4] - إيهاب السقا – جريمة التزوير في المحررات الإلكترونية – دار الجامعة الجديدة – مصر – 2008 – ص16.

يُعرف التوقيع الإلكتروني لدى الفقه القانوني بعدة تعاريف أبرزها أنه جملة من الحروف أو الأرقام أو الرموز أو الإشارات التي تتمتع بطابع منفرد ومتميز، بما يسمح لها بأن تكون محددة لشخص صاحب التوقيع وتميزه عن غيره من الأشخاص، ويعد هو الوسيلة الرئيسية في إتمام وتنفيذ المعاملات الإلكترونية.

ولم يترك المشرع الكويتي مسألة التعريف بالتوقيع الإلكتروني للفقه القانوني، حيث تصدى له بالتعريف بموجب نص المادة رقم (1) من قانون مكافحة جرائم تقنية المعلومات، وأيضاً بنص المادة الأولى من قانون المعاملات الإلكترونية، واللتان اتفقتا على ذات التعريف للتوقيع الإلكتروني بأنه "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".

المحامي مسفر عايض
mesferlaw.com

وهو ما نستخلص منه أن التوقيع الإلكتروني وإن كان يختلف في تكوينه وطبيعته عن التوقيع التقليدي، إلا أنه يتفق معه في وظيفته التي يؤديها، والتي تتمثل في تحديد هوية صاحبه وتمييزه عن غيره من الأشخاص، ويستدل منه على ارتضائه بالالتزام الذي يتضمنه المحرر الذي يتم تذييله به.

وللتوقيع الإلكتروني أكثر من صورة، وتتمثل أهم تلك الأشكال وأكثرها شيوعاً في الاستخدام الأشكال التالية:

- هناك التوقيع بالقلم الإلكتروني كأحد أبرز أشكال التوقيع الإلكتروني، وهو شكل يتم فيه التوقيع الإلكتروني باستخدام قلم إلكتروني مسجل عليه هذا التوقيع، وهذا القلم يتم بموجبه الكتابة على شاشة الكمبيوتر لوضع هذا التوقيع على أي وثيقة إلكترونية، ويساعد في إتمام ذلك برنامج يقوم بوظيفة التقاط التوقيع ووظيفة التحقق من صحته وصحة نسبته إلى صاحبه القائم بالتوقيع[5].
- وهناك أيضاً التوقيع الإلكتروني من خلال استخدام الماسح الضوئي، حيث يتم نسخ التوقيع الخطي الخاص بصاحب التوقيع من خلال الماسح الضوئي، ووضعه كما هو على الوثيقة الإلكترونية المراد تذييل التوقيع بها، ويمكن لصاحب التوقيع أن يحتفظ بنسخة من توقيعه المنسوخ على الماسح الضوئي ليقوم باستخدامه وقتما شاء للتوقيع على أي وثيقة إلكترونية أو أي محتوى يوجد على دعامة إلكترونية.

[5] - سعيد قنديل – التوقيع الإلكتروني – دار الجامعة الجديدة – مصر – 2006 – ص26,

- ويوجد شكل آخر للتوقيع الإلكتروني وهو التوقيع الرقمي، وهذا التوقيع يتشكل من مفاتيح ورموز سرية يتم تكوينها عبر مجموعة من اللوغاريتمات والمعادلات الرياضية التي تتسم بالتعقيد، وذلك لتوفير ضمانات لأمان هذا التوقيع والحفاظ عليه.

(3) الوسيط الإلكتروني

يدخل في نطاق الوسيط الإلكتروني أكثر من وسيط، وتتمثل تلك الوسائط الإلكترونية في:

- **الدعامة المادية** التي يتم تدوين المعلومات والبيانات الإلكترونية عليها، بحيث يسهل قراءتها وفهمها من قبل أي شخص سواء بشكل مباشر أو عن طريق استخدام وسبلة من وسائل تقنية المعلومات المخصصة لذلك، ومن الصور المختلفة لتلك الدعامة المادية نذكر الوثائق الإلكترونية، والأقراص الضوئية، والذاكرة الضوئية، وغيرها من الأشكال الحديثة للدعامة المادية.
- **نظام المعالجة الإلكترونية للبيانات** والذي عرفه المشرع الكويتي كمحل لجريمة التزوير الإلكتروني، وذلك في نص المادة رقم (1) من قانون مكافحة جرائم تقنية المعلومات، والتي عرفته بأنه النظام الإلكتروني الذي تكون وظيفته إنشاء البيانات أو الرسائل أو إدخالها أو استرجاعها أو إرسالها أو استخراجها أو تخزينها أو عرضها أو معالجتها بشكل إلكتروني.
- **النظام الإلكتروني المؤتمت** والذي ورد أيضاً التعريف به في قانون مكافحة جرائم تقنية المعلومات بالمادة رقم (1) منه، وتمثل تعريفه في أنه ""برنامج أو نظام إلكتروني لحاسب آلي تم إعداده ليتصرف أو يستجيب لتصرف بشكل مستقل كلياً أو جزئياً، دون تدخل أو إشراف اي شخص طبيعي في الوقت الذي يتم فيه التصرف أو الاستجابة له"، ومن التطبيقات العملية للنظام الإلكتروني المؤتمت الروبوتات والذكاء الاصطناعي.
- **نظام الحاسب الآلي** والذي يتمثل في مجموعة من البرامج والأنظمة المعلوماتية والتي يمكنها أن تؤدي مهمتها التي أعدت من أجلها بتحليل وبرمجة وإظهار وحفظ وإرسال واستلام المعلومات والبيانات والأوامر، سواء كان ذلك بشكل منفرد ومستقل أو بالاتصال مع غيرها من الأنظمة المعلوماتية الأخرى.
- **النظام الإلكتروني** والذي لم يتصدى المشرع الكويتي له بالتعريف في أي قانون، لذلك فإنه وبالعودة إلى أدبيات الفقه القانوني في هذا الشأن تبين أن الفقه قد تناوله بالتعريف، حيث عرفه بأنه مجموعة مترابطة من الوسائل التقنية والشبكات والبرامج التي تعمل كوحدة واحدة بهدف خلق أو تخزين أو إرسال أو استقبال أو معالجة المعلومات والرسائل بصورة إلكترونية.

المحامي مسفر عايض
mesferlaw.com

(4) الموقع الإلكتروني

يُقصد بالموقع الإلكتروني أي مكان متاح على الشبكة المعلوماتية يمكن من خلاله الحصول على أي معلومات، وذلك عن طريق استخدام عنوان معين للوصول إليه.

رابعاً: أركان جريمة التزوير الإلكتروني

تناول الفقه القانوني أركان جريمة التزوير الإلكتروني وحددها في ركنين أساسيين وهما الركن المادي والركن المعنوي، إلا أننا ومن خلال مقارنة تلك الجريمة ببعض الجرائم الأخرى ذات الطبيعة الخاصة وقفنا على أنها لا تقوم على هذين الركنين فقط، ولكن هناك ركن ثالث هام لا يجوز إغفاله وهو الركن المفترض/ وسوف نوضح ذلك عند التصدي لهذه الأركان الثلاث على النحو التالي.

(1) الركن المفترض (أداة الجريمة)

المحامي مسفر عايض
mesferlaw.com

يقصد بالركن المفترض في بعض الجرائم الركن الذي يفترض القانون قيامه وتحققه في جرائم محددة، بحيث لا يتم الانتقال لبحث توافر باقي أركان الجريمة من عدمه إلا بعد تحقق هذا الركن، والذي بانتفائه لا تتحقق الجريمة حتى وإن تحققت باقي أركانها، حيث يتحول تكييفها ووصفها القانوني من الجريمة التي كان يلزم توافر الركن المفترض فيها إلى جريمة أخرى لا تتطلب الركن المفترض، كما هو الحال في جرائم الوظيفة العامة، حيث يستلزم القانون توافر ركناً مفترضاً فيها يتمثل في ثبوت صفة الموظف العام أو المكلف بخدمة عامة في الجاني، وحال انتفاء هذه الصفة بنتفي الركن المفترض وتخرج الجريمة عن إطار جرائم الوظيفة العامة وتصبح جريمة عادية.

وبالرجوع إلى المؤلفات السابقة والأدبيات والآراء الفقهية التي وضعت بشأن أركان جريمة التزوير الإلكتروني، تبين لنا أنها لم تأت على ذكر هذا الركن، وإن كان هذا الركن في رأينا الشخصي هو ركناً منطقياً، لاسيما وأن بانتفائه تنتفي الصفة الإلكترونية عن جريمة التزوير، وتصبح جريمة تزوير تقليدية، حيث يتمثل هذا الركن في شرط لازم وأساسي لتوافر الصفة الإلكترونية للجريمة، وهو الشرط الذي يضع الحد الفاصل بين جريمة التزوير الإلكترونية ونظيرتها التقليدية، ألا وهو شرط أداة الجريمة أو الوسيلة التي يستخدمها الجاني في ارتكاب جريمته.

وقد ربط المشرع الكويتي تحقق صفة الجريمة الإلكترونية لجريمة التزوير بأن يتم ارتكابها عن طريق استخدام أداة محددة، وتتمثل تلك الأداة في أي وسيلة من وسائل تقنية المعلومات،

ويتضح ذلك جلياً من خلال تعريفه للجريمة المعلوماتية بوجه عام على أنها "كل فعل يرتكب من خلال **استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات** بالمخالفة لأحكام هذا القانون".

بجانب ذلك نجد أن المشرع الكويتي قد أكد على أهمية الركن المفترض وضرورة تحققه في جريمة التزوير الإلكتروني كركن مفترض خاص بها، وذلك لما ذكره في نص مادة تجريم التزوير الإلكتروني وهي المادة رقم (2/3) من قانون مكافحة جرائم تقنية المعلومات، حيث ورد بها أن ".. 2- كل من زور أو أتلف مستنداً أو سجلاً أو توقيعاً إلكترونياً أو نظام معالجة إلكترونية للبيانات أو نظام إلكتروني مؤتمت ..... **وذلك باستخدام وسيلة من وسائل تقنية المعلومات** ..."، وهو ما يؤكد أن المشرع قد أخذ بشرط تحقق الركن المفترض في جريمة التزوير، حيث تطلب لتوافر صفة الإلكترونية لجريمة التزوير أن يتم ارتكابها بواسطة وسيلة من وسائل تقنية المعلومات، وفي حال عدم تحقق تلك الصفة فإننا – عند تحقق الركنين المادي والمعنوي – نكون أمام جريمة تزوير تقليدية.

المحامي مسفر عايض
mesferlaw.com

(2) الركن المادي

يقصد بالركن المادي للجريمة النشاط والسلوك الإجرامي الذي يقوم الجاني بمباشرته وارتكابه، حيث يمثل هذا الركن المظهر المادي الملموس الذي تتخذه الجريمة والذي يقرر القانون تجريمه ومعاقبة فاعله، ويتمثل النشاط والسلوك الإجرامي في جرائم التزوير الإلكتروني في فعل محدد وهو فعل تغيير الحقيقة، ويُقصد به إحلال أمراً غير حقيقي محل الأمر الحقيقي في محل الجريمة، وقد حدد المشرع الكويتي في نص المادة رقم (2/3) من قانون مكافحة جرائم تقنية المعلومات الصور المختلفة التي يتم من خلالها ارتكاب فعل تغيير الحقيقة، وتتمثل تلك الطرق في:

- فعل الاصطناع: ويُقصد بالاصطناع إنشاء محرر إلكتروني أو توقيع إلكتروني أو أي محل آخر من المحال التي يمكن أن تقع عليها جريمة التزوير، يكون غير موجود من قبل القيام بفعل الاصطناع، ومن النماذج الشائعة لفعل الاصطناع إنشاء محرر إلكتروني ليس له وجود من الأصل، أو اختلاق توقيع إلكتروني ليس له وجود وتذييل محرر إلكتروني به، أو أن يكون المحرر أو التوقيع المصطنع هو تقليد لمحرر أو توقيع إلكتروني موجود بالفعل.
- فعل التغيير: يختلف فعل التغيير عن فعل الاصطناع في أن الأخير ينشئ ويخلق محرر أو توقيع إلكتروني أو غيره لم يكن له وجود من قبل، في حين أن فعل التغيير يرد على

توقيع إلكتروني أو محرر إلكتروني له وجود فعلي، ولكنه ينصب على محتواه لتغيير حقيقة هذا المحتوى بصورة مادية، وعلى سبيل المثال لذلك إضافة رقم لتغيير حقيقة الرقم الموجود بالمحرر، أو إضافة اسم إلى الأسماء الموجودة به، أو حذف اسم موجود بالفعل.

- فعل التحوير: التحوير يختلف عن التغيير في أن التغيير يمثل تغيير مادي ملموس في الحقيقة الواردة بالمحرر، بينما نجد أن التحوير يمثل تغيير معنوي غير ملموس على مضمون هذا المحرر دون المساس المادي بهذا المضمون، ومن الأمثلة على فعل التحوير أن يقوم الجاني بإدخال معلومات غير صحيحة للحاسب الآلي للحصول على مخرجات مخالفة للحقيقة، بحيث تظهر المخرجات سليمة ظاهرياً ولكنها تكون مزورة في حقيقتها.

ويثور تساؤل هام بشأن الجريمة التزوير الإلكتروني فيما يخص مدى اشتراط ترتب الضرر للمجني عليه كنتيجة وأثر لارتكاب الجاني لفعل التزوير الإلكتروني من عدمه، وهل هو شرط لازم لتحقق تلك الجريمة أم لا؟

المحامي مسفر عايض
mesferlaw.com

وللإجابة على هذا التساؤل ينبغي الرجوع إلى مادة التجريم رقم (2/3) من قانون مكافحة جرائم تقنية المعلومات، والتي سنجد أنها لم تتضمن اشتراط تحقق ضرر للمجني عليه كنتيجة لفعل التزوير، ولا يعني ذلك عدم اشتراط المشرع لشرط تحقق الضرر للمجني عليه لتحقق جريمة التزوير الإلكتروني، لاسيما وأنه إذا انتفى الضرر – أياً كان نوعه – عن الفعل فعلى أي أساس يتم تصنيف هذا الفعل على أنه جريمة؟

ونرى أن المشرع الكويتي لم يغفل ذكر شرط تحقق الضرر، ولكنه أغفل ذكر تحقق الضرر الحال واكتفى في تجريم التزوير الإلكتروني بالضرر المحتمل[6]، ويُقصد بالضرر المحتمل الضرر الذي لا يقع بشكل حال وبمجرد ارتكاب الجريمة بشكل فعلي، ولكنه يحتمل تحققه ووقوعه مستقبلاً، وبالتالي فإن مجرد تحقق فعل التزوير وتهديده لمصلحة مشروعة تخص المجني عليه، فإن مجرد هذا التهديد يعد خطراً محتملاً يضع فعل التزوير الإلكتروني محلاً للتجريم.

(3) الركن المعنوي

[6] - د/ بدر أحمد الجاسر – جريمة التزوير الإلكتروني كجريمة مستحدثة في التشريع الكويتي – مجلة الحقوق – ع (1) – جامعة الكويت – 2020 - ص182.

الركن المعنوي لأي جريمة من الجرائم العمدية يتمثل في القصد الجاني، والقصد الجنائي نوعان وهما القصد الجنائي العام والذي يتمثل في علم الجاني بأن ما يرتكبه من فعل يمثل جريمة يقرر القانون عقوبة لمرتكبها، وأن تتجه إرادته الحرة على الرغم من علمه بذلك إلى ارتكابها وتحقيق أركانها، وهناك القصد الجنائي الخاص والذي يتطلبه القانون – إضافة إلى القصد الجنائي العام - في بعض الجرائم لتحقق الركن المعنوي لها، ويُقصد بالقصد الجنائي الخاص الباعث أو الغاية التي يقوم الجاني بارتكاب جريمته من أجل تحقيقه، أي أن يكون في نية الجاني تحقيق هدف معين من جريمته.

وبالنسبة لجريمة التزوير الإلكتروني فإنها من طائفة الجرائم العمدية التي يستلزم فيها المشرع تحقق الركن المعنوي، والركن المعنوي لها يتكون من القصد الجنائي العام فقط، وذلك بأن يتحقق لدى الجاني عنصر العلم بأنه يرتكب فعلاً يمثل تغييراً للحقيقة ويشكل جريمة التزوير الإلكتروني التي يعاقب عليها القانون، وعنصر الإدارة الحرة وذلك بأن تتجه إرادته – الخالية من أي ضغط أو إكراه أو تهديد أو أي عيب من العيوب التي تعيب الإرادة – إلى القيام بهذا الفعل الذي يعلم بتجريمه، فإذا انتفى أياً من عنصري العلم أو الإرادة، كما لو كان الجاني يجهل بأن الفعل الذي يقوم به يمثل تغييراً للحقيقة وأن القانون يضعه موضع التجريم، أو كان على علم بذلك ولكنه كان مكرهاً على ارتكابه لكونه تحت تهديد حياته أو حياة شخص عزيز عليه كزوجته أو أحد أبنائه، فإن الركن المعنوي للجريمة – القصد الجنائي – ينتفي في حقه.

المحامي مسفر عايض
mesferlaw.com

وقد خلا نص التجريم من أي ذكر لاستلزام تحقق نية خاصة لدى الجاني عند ارتكابه لجريمة التزوير الإلكتروني، أو حتى غرض استخدام المحرر الإلكتروني المزور فيما تم إعداده من أجله، وذلك كما فعل في مادة تجريم التزوير التقليدي رقم (257) من قانون الجزاء الكويتي رقم 16 لسنة 1960، حيث لم يضع المشرع ضمن صياغة نص التجريم عبارة (بقصد استخدامه) وإلا كان الأمر مختلفاً، ولكان الركن المعنوي لجريمة التزوير الإلكتروني عندئذ سيتشكل من القصد الجنائي العام والقصد الجنائي الخاص معاً، إلا أنه لم يفعل فأصبح الركن المعنوي لتلك الجريمة قائماً على القصد الجنائي العام فقط، وذلك بغض النظر عن السبب أو الغرض الذي ارتكب لجاني جريمته من أجله.

خامساً: العقوبة القانونية لجريمة التزوير الإلكتروني

واجه المشرع الكويتي جريمة التزوير الإلكتروني بعقوبات صارمة بغية الحد من ارتكابها من جهة ومعاقبة من يرتكبها من جهة أخرى، إلا أنه في هذا السياق لم يقرر تلك العقوبة بموجب نص قانوني واحد، بل قام بتجريم التزوير الإلكتروني في موضعين الموضع الأول بقانون

مكافحة جرائم تقنية المعلومات، والموضع الثاني بقانون المعاملات الإلكترونية، وسوف نوضح ذلك على النحو الآتي بيانه:

(1) العقوبة المقررة بقانون مكافحة جرائم تقنية المعلومات

قرر المشرع الكويتي لجريمة التزوير الإلكتروني في ظل قانون مكافحة تقنية المعلومات عقوبات أصلية وأخرى تكميلية، وبيان ذلك على النحو التالي:

- **العقوبات الأصلية:** ورد في صدر نص تجريم فعل التزوير الإلكتروني والمتمثل في المادة رقم (2/3) من قانون مكافحة جرائم تقنية المعلومات رقم 63 لسنة 2015 العقوبة المقررة لمرتكب هذه الجريمة، والتي تمثلت في عقوبة الحبس لمدة لا تزيد عن ثلاث سنوات مع الغرامة التي تتراوح قيمتها من ثلاثة آلاف دينار كحد أدنى وحتى عشرة آلاف دينار كحد أقصى، أو توقيع إحدى هاتين العقوبتين فقط دون الأخرى، وذلك وفقاً لما يتراءى للمحكمة الموضوع التي تنظر الجريمة، وتبعاً لجسامة الجريمة وظروفها والتي تختلف من حالة إلى أخرى.

المحامي مسفر عايض
mesferlaw.com

وقد حدد المشرع في المادة رقم (11) من ذات القانون الظروف المشددة للعقوبة الأصلية، والتي حال تحقق احدها لا يجوز الحكم بعقوبة تقل عن نصف الحد الأقصى للعقوبة، أي لا تقل بالنسبة لجريمة التزوير الإلكتروني عن الحبس سنة ونصف (باعتبار الحد الأقصى هو الحبس ثلاث سنوات)، والغرامة التي لا تقل عن خمسة آلاف دينار (باعتبار أن الحد الأقصى هو عشرة آلاف دينار)، أو بإحدى هاتين العقوبتين فقط، وتتمثل تلك الظروف المشددة في:

1- أن ترتكب جريمة التزوير الإلكتروني من خلال عصابة منظمة.
2- أن يكون الجاني من شاغلي الوظائف العامة، وأن يستغل سلطته ونفوذه التي يستمدها من تلك الوظيفة في ارتكاب جريمته.
3- أن يتم ارتكابها من خلال الاستغلال أو التغرير بالقصر أو من في حكمهم من ناقصي الأهلية.
4- أن تكون هناك أحكام سابقة بإدانة الجاني في جرائم مماثلة، وذلك سواء كانت تلك الأحكام صادرة من القضاء الوطني أو من قضاء أجنبي.

- **العقوبات التكميلية:** وتتمثل تلك العقوبات في عقوبات جوازية للمحكمة التي تنظر الجريمة، فلها أن توقعها على الجاني أو تكتفي بالعقوبة الأصلية فقط، وتتمثل تلك العقوبات في:

- عقوبة المصادرة والتي بموجبها يتم مصادرة الأدوات المستخدمة في الجريمة كالبرامج والأجهزة الإلكترونية والوسائل التقنية وغيرها من أدوات أخرى، بجانب مصادرة الأموال التي تحصل عليها الجاني من خلال ارتكاب جريمته.
- عقوبة الإغلاق والتي بموجبها يتم إغلاق المحل أو الموقع الذي ارتكب فيه أو من خلاله الجاني جريمته، ويكون الإغلاق لمدة سنة متى كان مالك هذا المحل أو الموقع على علم بأن الجاني يستخدمه لارتكاب الجريمة، وإن كان تكرار ارتكاب تلك الجريمة من ذات المحل أو الموقع يجعل من عقوبة الغلق عقوبة أصلية يجب على المحكمة أن تقضي بها.

(2) العقوبة المقررة بقانون المعاملات الإلكترونية

المحامي مسفر عليض
mesferlaw.com

ثاني القوانين التي تجرم التزوير الإلكتروني وتعاقب مرتكبه هو قانون المعاملات الإلكترونية رقم 20 لسنة 2014، وبعد أن ننوه بداية وقبل التعرض لمضمون تلك العقوبة أن المشرع الكويتي وعند معرض حديثه عن العقوبة المقررة لجريمة التزوير الإلكتروني في مادة التجريم رقم (37) من قانون المعاملات التجارية الكويتي، فقد استهل ذلك بعبارة **"مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون آخر"**، وهي عبارة يستدل منها على أن العقوبة الواردة بهذا القانون لا يتم اللجوء إلى تطبيقها إلا في حالة عدم وجود عقوبة أشد لنفس الجريمة في قانون آخر.

وقد قرر المشرع الكويتي في نص المادة آنفة الذكر على عقوبات أصلية توقع على مرتكب جريمة التزوير الإلكتروني، وهذه العقوبات قوامها عقوبة الحبس لمدة لا تتجاوز ثلاث سنوات، والغرامة التي تتراوح قيمتها من خمسة آلاف دينار كحد أدنى إلى عشرين ألف دينار كحد أقصى، أو القضاء بإحدى هاتين العقوبتين فقط دون الأخرى.

كما أضاف المشرع بعجز تلك المادة عقوبة أصلية يتم القضاء بها في جميع الحالات سواء تم الحكم بالحبس والغرامة معاً أو إحداهما فقط، وتتمثل تلك العقوبة في عقوبة النشر، والتي بموجبها يتم نشر الحكم النهائي الصادر بالإدانة، وذلك في صحيفتين يوميتين تصدران باللغة العربية، ويكون ذلك بنفقات تقع على عاتق المحكوم عليه، بجانب نشر الحكم أيضاً على شبكة الاتصالات الإلكترونية المفتوحة.

المحامي مسفر عايض
mesferlaw.com

النتائج

بعد إتمام هذه الدراسة وتحليل مختلف جوانب جريمة التزوير الإلكتروني في القانون الكويتي، توصلنا إلى مجموعة من النتائج يمكن إجمالها على النحو التالي:

1. **خلو القانونين الكويتيين من تعريف لجريمة التزوير الإلكتروني** :تبين أن كلاً من قانون مكافحة جرائم تقنية المعلومات رقم 63 لسنة 2015، وقانون المعاملات الإلكترونية رقم 20 لسنة 2014، لم يتعرضا لجريمة التزوير الإلكتروني بالتعريف، حيث اقتصرا على عرض الطرق التي تتم من خلالها هذه الجريمة وبيان العقوبات المقررة لمرتكبيها، وهو ما يُستدل منه أن المشرع لم يرغب في حصر مفهومها في تعريف محدد وجامد، تاركاً مهمة تعريفها للفقه القانوني، وذلك لما تتسم به من تطور مستمر يرتبط بتقنية المعلومات التي تتطور يوماً بعد يوم.

2. **اتساع نطاق محل جريمة التزوير الإلكتروني** :بينت الدراسة أن محل الجريمة لا يقتصر على المحرر الإلكتروني فقط، بل يتسع ليشمل التوقيع الإلكتروني، والوسيط الإلكتروني (الدعامة المادية، ونظام المعالجة الإلكترونية للبيانات، والنظام الإلكتروني المؤتمت، ونظام الحاسب الآلي، والنظام الإلكتروني)، والموقع الإلكتروني، وذلك وفقاً لنص المادة (2/3) من قانون مكافحة جرائم تقنية المعلومات، مما يعكس حرص المشرع على مواكبة التطورات التقنية المستمرة.

المحامي مسفر عايض
mesferlaw.com

3. **تميز جريمة التزوير الإلكتروني بسمات خاصة** :توصلت الدراسة إلى أن جريمة التزوير الإلكتروني تتسم بأربع سمات رئيسية تميزها عن جريمة التزوير التقليدي، وهي: القدرة على أن تكون جريمة عابرة للحدود، وإمكانية ارتكابها في أي مرحلة من مراحل المعالجة الإلكترونية (الإدخال، المعالجة، الإخراج)، وصعوبة الكشف عنها أو إثباتها، وصعوبة الادعاء بارتكابها على سبيل الخطأ، وهو ما يعكس الطبيعة الخاصة لهذه الجريمة ويزيد من خطورتها.

4. **تعدد أركان جريمة التزوير الإلكتروني** :أثبتت الدراسة أن جريمة التزوير الإلكتروني تقوم على ثلاثة أركان رئيسية، خلافاً لما ذهب إليه بعض الفقه الذي اقتصر على ركنين فقط، وهذه الأركان هي: الركن المفترض (أداة الجريمة - استخدام وسيلة من وسائل تقنية المعلومات) والذي يمثل الحد الفاصل بين جريمة التزوير الإلكتروني وجريمة

التزوير التقليدي، والركن المادي (فعل الاصطناع أو التغيير أو التحوير)، والركن المعنوي (القصد الجنائي العام بعنصريه العلم والإرادة.(

5. **اقتصار الركن المعنوي على القصد الجنائي العام** :تبين أن المشرع الكويتي لم يستلزم في نص تجريم التزوير الإلكتروني توافر القصد الجنائي الخاص (نية الاستخدام) لدى الجاني، على خلاف ما فعل في جريمة التزوير التقليدي في المادة (257) من قانون الجزاء، مما يجعل الركن المعنوي لجريمة التزوير الإلكتروني قائماً على القصد الجنائي العام فقط، وذلك بغض النظر عن السبب أو الغرض الذي ارتكب الجاني جريمته من أجله.

6. **اعتماد المشرع على معيار الضرر المحتمل** :كشفت الدراسة أن المشرع الكويتي لم يشترط لتحقق جريمة التزوير الإلكتروني وقوع ضرر فعلي للمجني عليه، بل اكتفى بتحقق الضرر المحتمل، وهو الضرر الذي لا يقع بالفعل حال ومجرد ارتكاب الجريمة، ولكنه يحتمل تحققه ووقوعه مستقبلاً، ومجرد تهديده لمصلحة مشروعة تخص المجني عليه يعد خطراً محتملاً يضع فعل التزوير الإلكتروني محلاً للتجريم.

المحامي مسفر عايض
mesforlaw.com

7. **تباين العقوبات بين القانونين** :بينت الدراسة وجود تباين في العقوبات المقررة لجريمة التزوير الإلكتروني بين قانون مكافحة جرائم تقنية المعلومات وقانون المعاملات الإلكترونية، حيث قرر الأول عقوبة الحبس لمدة لا تجاوز ثلاث سنوات وغرامة تتراوح بين ثلاثة آلاف وعشرة آلاف دينار، بينما قرر الثاني عقوبة الحبس لمدة لا تجاوز ثلاث سنوات وغرامة تتراوح بين خمسة آلاف وعشرين ألف دينار، مع إضافة عقوبة النشر في جميع الأحوال، مع إعمال قاعدة "مع عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون آخر" التي يستدل منها على أن العقوبة الأشد هي الواجبة التطبيق.

8. **تحديد المشرع لظروف مشددة للعقوبة** :توصلت الدراسة إلى أن المشرع الكويتي حدد في المادة (11) من قانون مكافحة جرائم تقنية المعلومات أربع ظروف مشددة للعقوبة، وهي: ارتكاب الجريمة من خلال عصابة منظمة، وأن يكون الجاني من شاغلي الوظائف العامة ويستغل سلطته، وأن يتم ارتكابها من خلال الاستغلال أو التغرير بالقصر أو ناقصي الأهلية، وأن تكون هناك أحكام سابقة بإدانة الجاني في جرائم مماثلة، وحال تحقق أي منها لا يجوز الحكم بعقوبة تقل عن نصف الحد الأقصى للعقوبة المقررة.

9. **إغفال المشرع لجانب الحماية الوقائية** :أشارت الدراسة إلى أن المشرع الكويتي ركز في تنظيمه لجريمة التزوير الإلكتروني على الجانب العقابي، متجاهلاً إلى حد كبير الجانب الوقائي، حيث لم يتضمن القانون نصوصاً كافية تحث على اتخاذ تدابير أمنية وتقنية للحد من وقوع هذه الجريمة، واكتفى بمعاقبة مرتكبيها بعد وقوعها.

10. **تعدد الجهات المختصة بالتحقيق والملاحقة** :خلصت الدراسة إلى أن تعدد القوانين المنظمة لجريمة التزوير الإلكتروني (قانون مكافحة جرائم تقنية المعلومات وقانون المعاملات الإلكترونية وقانون الجزاء) قد يؤدي إلى نوع من التضارب أو التداخل في الاختصاصات، خاصة في الحالات التي يتداخل فيها التزوير الإلكتروني مع جرائم أخرى، مما قد يؤثر على فعالية الملاحقة الجنائية.

المحامي مسفر عايض
mesferlaw.com

التوصيات

بناءً على ما توصلت إليه هذه الدراسة من نتائج، يمكن تقديم مجموعة من التوصيات التي من شأنها تطوير النصوص القانونية المنظمة لجريمة التزوير الإلكتروني، وتعزيز آليات كشفها والتحقيق فيها، ونشر الوعي بأخطارها وسبل الوقاية منها، وذلك على النحو التالي:

أولاً: التوصيات التشريعية:

1. **إدراج تعريف قانوني لجريمة التزوير الإلكتروني** :توصي الدراسة بأن يتضمن قانون مكافحة جرائم تقنية المعلومات تعريفاً واضحاً لجريمة التزوير الإلكتروني، يحدد ماهيتها وطبيعتها القانونية، وأركانها، وصورها، وذلك لضمان الوضوح القانوني وتجنب الاجتهادات المتضاربة في تفسيرها، مع ترك المجال لتطور المفهوم بما يتوافق مع التطور التقني المستمر.

2. **توحيد العقوبات بين القانونين** :توصي الدراسة بتوحيد العقوبات المقررة لجريمة التزوير الإلكتروني في كل من قانون مكافحة جرائم تقنية المعلومات وقانون المعاملات الإلكترونية، وذلك لتجنب التضارب والتداخل في التطبيق، مع الأخذ بالعقوبة الأشد تحقيقاً للردع العام والخاص، ويفضل أن يتم ذلك من خلال دمج النصوص في قانون واحد أو تعديل النصوص لتتسق مع بعضها البعض.

3. **إضافة نص يستلزم توافر القصد الجنائي الخاص** :توصي الدراسة بإضافة نص إلى مادة تجريم التزوير الإلكتروني يستلزم توافر القصد الجنائي الخاص (نية الاستخدام) لدى الجاني، أسوة بما ورد في جريمة التزوير التقليدي في المادة (257) من قانون الجزاء، وذلك لضمان تجريم الأفعال التي تشكل تزويراً إلكترونياً بشكل كامل، ولجعل الركن المعنوي للجريمة أكثر تحديداً وضبطاً.

4. **إدراج نصوص تعزز الجانب الوقائي** :توصي الدراسة بإدراج نصوص قانونية في قانون مكافحة جرائم تقنية المعلومات تلزم المؤسسات والجهات التي تستخدم نظم المعالجة الإلكترونية باتخاذ تدابير أمنية وتقنية للحد من وقوع جريمة التزوير الإلكتروني، مثل استخدام أنظمة التشفير، والتوقيع الإلكتروني الآمن، وأنظمة كشف التزوير، مع إلزام هذه الجهات بالإبلاغ عن أي محاولات تزوير تكتشفها.

5. **تنظيم التعاون الدولي في مواجهة الجريمة** :توصي الدراسة بإدراج نصوص قانونية تنظم التعاون الدولي في مجال مكافحة جريمة التزوير الإلكتروني، خاصة في ظل كونها جريمة عابرة للحدود، وذلك من خلال وضع آليات لتبادل المعلومات والخبرات، وتسليم المجرمين، والمساعدة القانونية المتبادلة، والتحقيق المشترك في الجرائم الإلكترونية.

المحامي مصطفى عليان
mesferlaw.com

ثانياً: التوصيات القضائية والإجرائية:

1. **تأهيل الكوادر القضائية والأمنية** :توصي الدراسة بتكثيف برامج التدريب والتأهيل للقضاة والمحققين ورجال الشرطة في مجال جرائم تقنية المعلومات بوجه عام، وجريمة التزوير الإلكتروني بوجه خاص، وذلك من خلال تنظيم دورات تدريبية متخصصة في مجال الأدلة الرقمية، وتحليل البيانات، وكشف التزوير الإلكتروني، بما يكفل سرعة وكفاءة التحقيق في هذه الجرائم.

2. **إنشاء وحدات متخصصة لمكافحة الجرائم الإلكترونية** :توصي الدراسة بإنشاء وحدات متخصصة في النيابة العامة والأجهزة الأمنية، تتولى التحقيق في جرائم التزوير الإلكتروني وسائر الجرائم الإلكترونية، على أن تضم هذه الوحدات كوادر قانونية وفنية متخصصة في مجال تقنية المعلومات، بما يضمن كفاءة التحقيق وسرعة الفصل في القضايا.

3. **سرعة الفصل في قضايا التزوير الإلكتروني** :توصي الدراسة بإعطاء أولوية خاصة لقضايا التزوير الإلكتروني، والعمل على سرعة الفصل فيها، وذلك نظراً للآثار الخطيرة التي قد تترتب على تأخير البت في هذه القضايا، والتي قد تؤدي إلى تفاقم الأضرار وانتشار الفساد، مع ضرورة مراعاة اتخاذ الإجراءات التحفظية العاجلة لحماية الأدلة الرقمية.

ثالثاً: التوصيات الأكاديمية والبحثية:

1. **تشجيع البحث العلمي في مجال جرائم تقنية المعلومات** :توصي الدراسة بتشجيع إجراء المزيد من الدراسات والأبحاث في مجال جرائم تقنية المعلومات بوجه عام، وجريمة التزوير الإلكتروني بوجه خاص، وخاصة فيما يتعلق بدراسة سبل كشفها والتحقيق فيها، وتقييم فعالية العقوبات المقررة، واقتراح تطويرات تشريعية، وذلك من خلال تخصيص منح بحثية وتنظيم مؤتمرات وندوات علمية متخصصة في هذا الموضوع.

المحامي مسفر عايض
mesferlaw.com

2. **تضمين موضوع جرائم تقنية المعلومات في المناهج التعليمية** :توصي الدراسة بتضمين موضوع جرائم تقنية المعلومات، ومن ضمنها جريمة التزوير الإلكتروني، بشكل موسع في مناهج كليات الحقوق والمعاهد الأمنية، وتخصيص جزء من المقررات الدراسية لدراسة هذا الموضوع بشكل متعمق، مع التركيز على الجوانب العملية والتطبيقية.

3. **إجراء دراسات مقارنة بين التشريعات** :توصي الدراسة بإجراء دراسات مقارنة موسعة بين التشريعات المختلفة فيما يتعلق بجريمة التزوير الإلكتروني، وذلك للوقوف على أفضل الممارسات التشريعية والقضائية، والاستفادة من التجارب الناجحة في تطوير النصوص القانونية الكويتية، مع مراعاة الخصوصية القانونية والدستورية لدولة الكويت.

رابعاً: التوصيات المجتمعية والإعلامية:

1. **نشر الوعي بأخطار التزوير الإلكتروني** :توصي الدراسة بنشر الوعي بين أوساط المجتمع بأخطار جريمة التزوير الإلكتروني، وسبل الوقاية منها، وذلك من خلال وسائل الإعلام المختلفة، والحملات التوعوية، والبرامج التعليمية، مما يسهم في ترسيخ ثقافة الأمن المعلوماتي وحماية الحقوق في الفضاء الإلكتروني.

2. **تشجيع الإبلاغ عن جرائم التزوير الإلكتروني** :توصي الدراسة بتشجيع الأفراد والمؤسسات على الإبلاغ عن جرائم التزوير الإلكتروني، وذلك من خلال توفير قنوات اتصال آمنة وسهلة للتبليغ، وضمان سرية المبلغين وحمايتهم من أي مساءلة، مع رفع الوعي بأهمية الإبلاغ في مكافحة هذه الجرائم.

3. **تعزيز التعاون بين القطاعين العام والخاص** :توصي الدراسة بتعزيز التعاون بين القطاعين العام والخاص في مجال مكافحة جريمة التزوير الإلكتروني، وذلك من خلال تبادل المعلومات والخبرات، وتطوير أنظمة الحماية الأمنية، وتنظيم حملات توعوية مشتركة، والاستفادة من خبرات القطاع الخاص في مجال الأمن المعلوماتي، وذلك بما يسهم في تعزيز الحماية من هذه الجريمة على المستوى الوطني.

المحامي مسفر عايض
mesferlaw.com

هذا وقد خلصت الدراسة إلى أن جريمة التزوير الإلكتروني تعد من أخطر الجرائم المستحدثة في عصر الرقمنة، وأن المشرع الكويتي قد بذل جهوداً مشكورة في مواجهتها من خلال إصدار قانون مكافحة جرائم تقنية المعلومات وقانون المعاملات الإلكترونية، إلا أن هذه النصوص لا تزال بحاجة إلى مزيد من التطوير والضبط لمواكبة التطور التقني المستمر ومواجهة الأساليب المتجددة لارتكاب هذه الجريمة، خاصة في ظل العصر الرقمي الذي نعيشه، حيث باتت المعاملات الإلكترونية تشكل جزءاً لا يتجزأ من الحياة اليومية للأفراد والمؤسسات، مما يستدعي تعزيز الحماية القانونية والتقنية لها، وضمان تحقيق التوازن بين حماية الحقوق والمصالح المشروعة وبين مكافحة الجريمة بفعالية.