



وزارة التعليم العالي و البحث العلمي
جامعة عمار ثلجي الاغواط
كلية العلوم السياسية و الحقوق
قسم : القانون الخاص



مذكرة بعنوان :

التزوير المعلوماتي دراسة تفصيلية مقارنة بين التشريع الجزائري والمصري

مذكرة مقدمة لاستكمال لمتطلبات نيل شهادة ماستر في الحقوق

تخصص: قانون جنائي و علوم جنائية

تحت إشراف الأستاذ:

د. سي ناصر محمد

من إعداد الطلبة

بن رمادية عبد القادر

أحمدي نصر الدين

الاستاذ	الرتبة	الصفة
د. غريبي يحي	أستاذ التعليم العالي	رئيسا
د. سي ناصر محمد	أستاذ التعليم العالي	مشرفا
د. بلي بولنوار	أستاذ التعليم العالي	مقرا

السنة الجامعية 2025-2026

شكر و عرفان

نتقدّم نحنُ بخالصِ الشكرِ وعظيمِ الامتنانِ إلى الأستاذ المشرف د. سي ناصر همد ،

على ما قدّمه لنا من توجيهاتٍ قيّمة وإشرافٍ متميّز ، وعلى ما أحاطنا به من اهتمامٍ

ومتابعةٍ طوال مراحل إنجاز هذا العمل، مما كان له بالغُ الأثر في إخراجِه في أحسن

صورة.

كما نتوجّه نحنُ بجزيلِ الشكرِ والتقديرِ إلى إدارة قسم الحقوق، على ما قدّمته من دعمٍ

وتسهيلات، وعلى جهودها المبذولة في توفير الظروف الملائمة التي ساعدتنا على

إتمام هذا العمل في أفضل الظروف.

فلكم منا جميعاً أسمى عباراتِ الشكر والعرفان، مقرونةً بخالص الاحترام والتقدير.

الأهداء

﴿وَقُلْ رَبِّ ارْحَمْنَاهُمَا كَمَا رَبَّيَانِي صَغِيرًا﴾

الحمد لله الذي بنعمته تتم الصالحات، والصلاة والسلام على سيدنا محمد صلى الله عليه

وسلم.

أهدي هذا العمل المتواضع إلى أبي الغالي، الذي كان سندي وعموني، وغرس في

نفسي قيم الاجتهاد والصبر، فله مني كل الشكر والتقدير والعرفان.

وإلى أمي الحبيبة، نبع الحنان والعطاء، التي رافقتني بدعواتها الصادقة ورعايتها

الدائمة، فكان فضلها عليّ عظيماً بعد فضل الله تعالى.

وإلى إخوتي وأخواتي الأعزاء، الذين شاركوني لحظات التعب والأمل، وكانوا خير معين

وخير داعم في مسيرتي الدراسية.

كما أهدي هذا الجهد إلى كل أفراد عائلتي الكريمة، وإلى كل من مدّ لي يد

المساعدة والتشجيع من قريب أو بعيد.

وإحياً من الله تعالى أن يجعل هذا العمل خالصاً لوجهه الكريم، وأن يوفقنا جميعاً لما فيه

الخير والنجاح.

بن رمادية عبد القادر

إهداء

بكل مشاعر التقدير والوفاء، أهدي ثمرة هذا الجهد إلى من كانا سبب وجودي ومصدر قوتي وإصراري، إلى أبي العزيز وأمي الغالية، اللذين أحاطاني بالرعاية والمحبة، وغمراني بعطائهما اللامحدود، فكانا خير سند وخير معين في جميع مراحل حياتي.

إلى والديّ الكريمين، عرفانا بجميلهما الذي لا يوفيه شكر ولا تنفيه كلمات، وإقراراً بفضلهما الكبير فيما وصلت إليه اليوم.

وإلى إخوتي وأخواتي الأعزاء، الذين رافقوني بالمحبة والتشجيع، وشاركوا معي لحظات الكفاح والأمل، فكانوا مصدر دعم وسعادة.

كما أهدي هذا العمل إلى جميع أفراد عائلتي الكريمة، وإلى كل من ساندني وشجعني وساهم بكلمة طيبة أو دعوة صادقة في إنجاز هذا العمل.

أسأل الله تعالى أن يحفظهم جميعاً، وأن يجزيهم عنّي خير الجزاء، وأن يجعل هذا العمل نافعا ومباركا.

أحمدني نصر الدين

.

مقدمة

مقدمة.....

هد العالم خلال العقود الأخيرة تطوراً تكنولوجياً متسارعاً شمل مختلف مجالات الحياة، حيث أصبحت تكنولوجيا المعلومات والاتصال من أهم الركائز التي تقوم عليها الأنشطة الاقتصادية والإدارية والمالية والقضائية. وقد أدى هذا التطور إلى انتقال جانب كبير من المعاملات من الشكل التقليدي الورقي إلى الشكل الإلكتروني، فأصبحت البيانات والمعلومات الإلكترونية تمثل أساساً للعديد من التصرفات القانونية والمعاملات اليومية. ورغم ما حققته الرقمنة من مزايا كبيرة تمثلت في السرعة والدقة وسهولة تبادل المعلومات، إلا أنها أفرزت في المقابل أنماطاً جديدة من الجرائم التي تستهدف البيئة الرقمية ومكوناتها المختلفة.

ومن بين هذه الجرائم المستحدثة تبرز جريمة التزوير المعلوماتي باعتبارها من أخطر الجرائم التي تهدد الثقة في المعاملات الإلكترونية وتمس أمن المعلومات وسلامة البيانات الرقمية، إذ لم يعد التزوير يقتصر على المحررات الورقية التقليدية، وإنما امتد ليشمل المحررات الإلكترونية والبيانات المخزنة داخل الأنظمة المعلوماتية وقواعد البيانات والتوقيعات الإلكترونية. وقد ساعدت الخصائص التقنية للبيئة الرقمية، كسهولة نسخ البيانات وتعديلها وإخفاء آثار الجريمة، على انتشار هذا النوع من الإجرام بصورة متزايدة، مما جعل التشريعات الجنائية أمام تحديات جديدة تستوجب تطوير وسائل الحماية القانونية لمواجهة هذه الأفعال الإجرامية.

كما أثار التزوير المعلوماتي العديد من الإشكالات القانونية والفقهية، لاسيما فيما يتعلق بتحديد مفهومه وأركانه ومدى إمكانية إخضاعه للقواعد التقليدية المنظمة لجريمة التزوير، أو ضرورة إفراز نصوص قانونية خاصة تتلاءم مع طبيعته التقنية المستحدثة. وقد اختلفت مواقف التشريعات المقارنة في معالجة هذه الجريمة، فبينما اتجهت بعض الدول إلى وضع نصوص خاصة لمكافحتها، فضلت دول أخرى الاعتماد على القواعد العامة للتزوير مع توسيع نطاق تطبيقها ليشمل المحررات الإلكترونية.

وفي هذا السياق، سعى كل من المشرع الجزائري والمشرع المصري إلى مواكبة التطورات التكنولوجية المتسارعة من خلال إصدار نصوص قانونية تهدف إلى مكافحة الجرائم المعلوماتية وتوفير الحماية الجنائية للمعاملات الإلكترونية، غير أن معالجة جريمة التزوير المعلوماتي لا تزال تثير العديد من التساؤلات المتعلقة بمدى كفاية هذه النصوص وفعاليتها في مواجهة هذا النوع من الجرائم.

مقدمة.....

وانطلاقاً من ذلك، تتناول هذه الدراسة موضوع "التزوير المعلوماتي: دراسة تفصيلية تحليلية مقارنة بين التشريع الجزائري والمصري"، بهدف الوقوف على الإطار القانوني لهذه الجريمة وتحليل أركانها وأحكامها والعقوبات المقررة لها، مع إبراز أوجه التشابه والاختلاف بين التشريعين محل الدراسة، وصولاً إلى تقييم مدى نجاح السياسة الجنائية في كل منهما في توفير حماية فعالة للبيئة الرقمية ومواجهة أخطار التزوير المعلوماتي.

أهمية الدراسة

تكتسي هذه الدراسة أهمية علمية وعملية بالغة، فمن الناحية العلمية تسهم في إثراء المكتبة القانونية بدراسة متخصصة تتناول جريمة التزوير المعلوماتي باعتبارها من الجرائم المستحدثة التي ما زالت محل نقاش فقهي وتشريعي واسع. كما تساعد في توضيح المفاهيم القانونية المرتبطة بالتزوير المعلوماتي وبيان خصائصه وأركانه وتمييزه عن الجرائم المعلوماتية الأخرى.

أما من الناحية العملية، فتبرز أهمية الدراسة في ارتباطها المباشر بالواقع العملي الذي يشهد تزايداً مستمراً في استخدام الوسائل الإلكترونية في مختلف المعاملات، الأمر الذي يجعل من مكافحة التزوير المعلوماتي ضرورة ملحة لحماية الثقة في البيئة الرقمية. كما تسعى الدراسة إلى تقييم فعالية النصوص القانونية المعمول بها في الجزائر ومصر، والكشف عن أوجه النقص التشريعي إن وجدت، بما يسهم في تقديم رؤية قانونية يمكن الاستفادة منها في تطوير السياسة الجنائية المتعلقة بمكافحة التزوير المعلوماتي.

الدراسات السابقة

1- دراسة: "التزوير المعلوماتي في عصر الرقمنة: بين قابلية الخضوع للنصوص القديمة وضرورة تبني نصوص خاصة"

تناولت هذه الدراسة إشكالية خضوع التزوير المعلوماتي للقواعد التقليدية المنظمة لجريمة التزوير أو ضرورة استحداث نصوص قانونية خاصة به. وركزت على مفهوم التزوير المعلوماتي وخصائصه ومحل الجريمة وأركانها، كما ناقشت مواقف التشريعات المقارنة من هذه الجريمة، وانتهت إلى أن خصوصية البيئة الرقمية تفرض تدخلاً تشريعياً خاصاً لمواجهة هذا النوع من الجرائم.

مقدمة.....

2- دراسة: "جريمة التزوير المعلوماتي دراسة مقارنة في القانون الفرنسي والمصري والعراقي"

هدفت هذه الدراسة إلى تحليل السياسة التشريعية المتبعة في معالجة جريمة التزوير المعلوماتي في كل من فرنسا ومصر والعراق، مع بيان أوجه الاختلاف في تنظيم الجريمة وأركانها والعقوبات المقررة لها. وقد خلصت إلى وجود تفاوت تشريعي واضح بين هذه الأنظمة القانونية، وأوصت بضرورة تطوير النصوص الخاصة بالتزوير المعلوماتي في بعض التشريعات العربية.

3- دراسة: "الجريمة المعلوماتية في التشريع الجزائري"

ركزت هذه الدراسة على مفهوم الجريمة المعلوماتية وأهم صورها وخصائصها، كما تناولت الإطار التشريعي الذي اعتمده المشرع الجزائري لمكافحة الجرائم المعلوماتية. وتوصلت إلى أن الجهود التشريعية الجزائرية، رغم أهميتها، لا تزال بحاجة إلى مزيد من التطوير لمواكبة التطور السريع للإجرام المعلوماتي..

4- دراسة: "المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري في ضوء أحكام القانون رقم

175 لسنة 2018"

تناولت هذه الدراسة أحكام قانون مكافحة جرائم تقنية المعلومات المصري، وحللت مختلف التدابير الموضوعية والإجرائية التي جاء بها لمواجهة الجرائم المرتبطة بتكنولوجيا المعلومات. كما ركزت على مدى فعالية هذا القانون في حماية البيئة الرقمية ومكافحة الجرائم المستحدثة، وأكدت أهمية مواصلة تطوير المنظومة التشريعية لمواكبة التطور التكنولوجي المتسارع.

وتختلف دراستنا عن الدراسات السابقة في أنها تنصب بصورة مباشرة على جريمة التزوير المعلوماتي من خلال إجراء دراسة تفصيلية تحليلية مقارنة بين التشريع الجزائري والتشريع المصري، مع التركيز على التنظيم القانوني للجريمة وأركانها وأحكامها والعقوبات المقررة لها، وبيان مدى فعالية السياسة الجنائية في كلا التشريعين في مواجهة هذا النمط المستحدث من الجرائم.

أسباب اختيار الموضوع

يرجع اختيارنا لموضوع التزوير المعلوماتي: دراسة تفصيلية تحليلية مقارنة بين التشريع الجزائري والتشريع المصري إلى مجموعة من الأسباب الذاتية والموضوعية التي دفعتنا إلى البحث في هذا المجال القانوني الحديث، وذلك على النحو الآتي:

مقدمة.....

أولاً: الأسباب الذاتية

- رغبتنا الشخصية في دراسة جريمة التزوير المعلوماتي باعتبارها من الموضوعات القانونية المستحدثة التي فرضتها التطورات التكنولوجية المعاصرة، ومحاولة الإحاطة بمختلف جوانبها القانونية والعملية .
- اهتمامنا بالجرائم المعلوماتية وما تثيره من إشكالات قانونية وفقهية تتعلق بمدى كفاية النصوص التقليدية في مواجهتها، الأمر الذي دفعنا إلى التعمق في دراسة هذا الموضوع وتحليل أحكامه .
- ميلنا إلى الدراسات المقارنة التي تسمح بالوقوف على مختلف التوجهات التشريعية والاستفادة من التجارب القانونية المقارنة في معالجة الظواهر الإجرامية المستحدثة .
- الرغبة في إثراء معارفنا القانونية في مجال القانون الجنائي المعلوماتي الذي أصبح من أهم فروع القانون الجنائي المعاصر .

ثانياً: الأسباب الموضوعية

- التوسع الكبير في استخدام وسائل التكنولوجيا الحديثة والأنظمة المعلوماتية في مختلف المجالات وما نتج عنه من تزايد الجرائم المرتبطة بالبيئة الرقمية .
- الخطورة المتنامية لجريمة التزوير المعلوماتي وما يترتب عليها من أضرار تمس الثقة العامة وأمن المعاملات الإلكترونية والمصالح المالية والإدارية للأفراد والمؤسسات .
- الحاجة إلى دراسة مدى فعالية النصوص القانونية التي اعتمدها كل من المشرع الجزائري والمشرع المصري في مواجهة هذه الجريمة ومكافحتها .
- قلة الدراسات القانونية المتخصصة التي تتناول التزوير المعلوماتي من منظور مقارن بين التشريع الجزائري والتشريع المصري .
- أهمية إبراز أوجه التشابه والاختلاف بين النظامين القانونيين والوقوف على مدى نجاح كل منهما في توفير الحماية الجنائية للبيانات والمحركات الإلكترونية .

أهداف الدراسة

مقدمة.....

تهدف هذه الدراسة إلى تحقيق جملة من الأهداف العلمية والقانونية، من أهمها:

- تسليط الضوء على جريمة التزوير المعلوماتي باعتبارها من الجرائم المستحدثة التي أفرزها التطور التكنولوجي والثورة الرقمية .
- بيان مفهوم التزوير المعلوماتي وخصائصه وأركانه القانونية وتمييزه عن الجرائم المعلوماتية المشابهة له .
- دراسة التنظيم القانوني لجريمة التزوير المعلوماتي في كل من التشريع الجزائري والتشريع المصري وتحليل النصوص القانونية المنظمة لها .
- إبراز أوجه التشابه والاختلاف بين التشريعين الجزائري والمصري في مجال مكافحة التزوير المعلوماتي .
- تقييم مدى فعالية السياسة الجنائية المعتمدة في كلا التشريعين في مواجهة هذا النوع من الجرائم واقتراح الحلول المناسبة لتطوير الحماية القانونية للبيئة الرقمية .

صعوبات الدراسة

واجهتنا أثناء إعداد هذه الدراسة مجموعة من الصعوبات، من أبرزها:

- صعوبة الإحاطة بمختلف الجوانب التقنية المرتبطة بجريمة التزوير المعلوماتي نظرا لطبيعتها المتشعبة وارتباطها بالتطور التكنولوجي المستمر .
- تشتت النصوص القانونية المنظمة للموضوع، خاصة في التشريع الجزائري، بين عدة قوانين ونصوص تشريعية مختلفة .
- قلة الاجتهادات القضائية المنشورة المتعلقة بجريمة التزوير المعلوماتي مقارنة بالجرائم التقليدية .
- صعوبة الحصول على بعض المراجع والدراسات المتخصصة التي تعالج التزوير المعلوماتي بصورة مباشرة ومفصلة .
- التغير المستمر في أساليب ارتكاب الجرائم المعلوماتية مما يجعل بعض الدراسات السابقة غير كافية للإحاطة بكافة صور الجريمة الحديثة .

المنهج المتبع في البحث

مقدمة.....

نظرا لطبيعة موضوع التزوير المعلوماتي وتشعب جوانبه القانونية والتقنية، فقد اقتضت دراسته الاعتماد على أكثر من منهج علمي.

فقد اعتمدنا المنهج الوصفي من أجل عرض المفاهيم الأساسية المتعلقة بالتزوير المعلوماتي وبيان خصائصه وأشكاله المختلفة، بما يساعد على فهم الإطار العام للموضوع وتحديد معالمه.

كما اعتمدنا المنهج التحليلي لتحليل النصوص القانونية المنظمة لجريمة التزوير المعلوماتي في كل من التشريع الجزائري والتشريع المصري، والوقوف على مدى فعالية الأحكام القانونية المقررة لمكافحتها.

واعتمدنا كذلك المنهج المقارن باعتباره المنهج الأكثر ملاءمة لموضوع الدراسة، حيث تم من خلاله إجراء مقارنة بين التشريع الجزائري والتشريع المصري للكشف عن أوجه الاتفاق والاختلاف بينهما، وتقييم مدى نجاح كل منهما في توفير الحماية الجنائية اللازمة للبيئة الرقمية.

الإشكالية

أصبح التزوير المعلوماتي من أخطر الجرائم التي تهدد أمن المعلومات والثقة في المعاملات الإلكترونية، خاصة مع التطور المتسارع للتكنولوجيا واعتماد مختلف القطاعات على النظم المعلوماتية في حفظ البيانات وتبادلها. وقد فرضت هذه الجريمة تحديات قانونية جديدة أمام التشريعات الجنائية التقليدية، الأمر الذي استوجب تدخل المشرعين لوضع قواعد قانونية تتلاءم مع طبيعتها الخاصة وتكفل حماية فعالة للمحركات والبيانات الإلكترونية.

وفي هذا الإطار تثار الإشكالية الرئيسية الآتية:

إلى أي مدى وفق المشرع الجزائري والمشرع المصري في إرساء حماية جنائية فعالة

لمواجهة جريمة التزوير المعلوماتي ومواكبة التطورات التقنية المرتبطة بها؟

ويتفرع عن هذه الإشكالية عدد من التساؤلات الفرعية:

- ما المقصود بالتزوير المعلوماتي وما هي أركانه القانونية؟
- ما هو التنظيم القانوني الذي اعتمده كل من المشرع الجزائري والمشرع المصري لمكافحة هذه الجريمة؟
- ما أوجه التشابه والاختلاف بين التشريعين في مجال مكافحة التزوير المعلوماتي؟

- ما مدى فعالية الأحكام الموضوعية والإجرائية المقررة لمواجهة هذه الجريمة؟

تقسيم الدراسة

للإجابة عن الإشكالية المطروحة والإحاطة بمختلف الجوانب القانونية المرتبطة بجريمة التزوير المعلوماتي، ارتأينا تقسيم هذه الدراسة إلى فصلين رئيسيين متكاملين.

خصصنا الفصل الأول لدراسة الإطار المفاهيمي لجريمة التزوير المعلوماتي، باعتباره الأساس النظري الذي تقوم عليه الدراسة، حيث تناولنا في المبحث الأول ماهية جريمة التزوير المعلوماتي من خلال تعريفها وبيان خصائصها وتمييزها عن الجرائم المشابهة لها. أما المبحث الثاني فقد خصصناه لدراسة الأساس القانوني للجريمة، من خلال بيان أركانها القانونية ومحل الجريمة والقواعد الإجرائية المتعلقة بمكافحة التزوير المعلوماتي.

أما الفصل الثاني فقد خصصناه لدراسة جريمة التزوير المعلوماتي في كل من التشريع الجزائري والتشريع المصري من خلال منظور مقارن، حيث تناولنا في المبحث الأول التنظيم القانوني للجريمة في التشريع المصري ببيان أساسها التشريعي وأحكامها الموضوعية والإجرائية. ثم خصصنا المبحث الثاني لدراسة أوجه المقارنة بين التشريعين الجزائري والمصري من خلال إبراز أوجه التشابه وأوجه الاختلاف بينهما، وصولاً إلى تقييم السياسة التشريعية المعتمدة في كلا النظامين القانونيين واقتراح بعض السبل الكفيلة بتطوير الحماية الجنائية المقررة لمواجهة جريمة التزوير المعلوماتي ومواكبة التطورات التقنية الحديثة.

الفصل الأول: الإطار المفاهيمي لجريمة التزوير

المعلوماتي

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

أدى التطور المتسارع في تكنولوجيا المعلومات والاتصال إلى ظهور أنماط جديدة من الجرائم التي تستهدف الأنظمة المعلوماتية والبيانات الإلكترونية، ومن أبرزها جريمة التزوير المعلوماتي التي أصبحت تشكل تهديدًا حقيقيًا للثقة والأمان في المعاملات الإلكترونية. فقد ساهم الاعتماد المتزايد على الوسائط الرقمية في حفظ وتبادل المعلومات في توفير بيئة جديدة لارتكاب أفعال التزوير بوسائل تقنية متطورة تختلف عن الوسائل التقليدية المعروفة.

ونظرًا لما تتميز به هذه الجريمة من خصوصية تتعلق بطبيعة محلها ووسائل ارتكابها، فقد أصبح من الضروري الوقوف على مفهومها وخصائصها وأساسها القانوني، من أجل الإحاطة بمختلف الجوانب المرتبطة بها وفهم الأحكام القانونية المنظمة لها وعليه، قسمنا هذا الفصل إلى مبحثين؛

المبحث الأول: ماهية جريمة التزوير المعلوماتي،

المبحث الثاني: الأساس القانوني لجريمة التزوير المعلوماتي عند المشرع الجزائري

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

المبحث الأول: ماهية جريمة التزوير المعلوماتي

تعد جريمة التزوير المعلوماتي من الجرائم المستحدثة التي فرضها التطور التكنولوجي والتحول نحو الرقمنة في مختلف المجالات، الأمر الذي أدى إلى انتقال العديد من صور التزوير من المحررات التقليدية إلى المحررات والبيانات الإلكترونية. ولتحديد المقصود بهذه الجريمة بصورة دقيقة، يتعين التعرف على مفهومها في الفقه والقانون، وبيان أوجه الاختلاف بينها وبين الجرائم المشابهة لها، فضلاً عن إبراز أهم الخصائص التي تميزها عن غيرها من الجرائم الإلكترونية¹.

المطلب الأول: تعريف التزوير المعلوماتي في الفقه والقانون

يعد تحديد مفهوم التزوير المعلوماتي خطوة أساسية لفهم طبيعة هذه الجريمة والتمييز بينها وبين غيرها من الجرائم المرتبطة بالتقنيات الحديثة. ولتحقيق ذلك، ينبغي الوقوف على مختلف التعريفات الفقهية والقانونية التي تناولت هذا المفهوم، لما لها من دور في توضيح عناصره وإبراز خصائصه الأساسية.

الفرع الأول: تعريف جريمة التزوير

تعد جريمة التزوير المعلوماتي من الجرائم الإلكترونية الحديثة التي ارتبط ظهورها بالتطور التكنولوجي وانتشار استخدام الحواسيب والأنظمة المعلوماتية في مختلف المعاملات الإدارية والمالية والتجارية. ونظراً لخطورة هذه الجريمة وما تمثله من اعتداء على الثقة العامة والمراكز القانونية للأفراد والمؤسسات، فإن تحديد مفهومها يقتضي التطرق إلى مفهوم التزوير لغة و فقها و قانوناً، ثم بيان المقصود بالتزوير الإلكتروني أو المعلوماتي².

أولاً: التزوير لغة

التزوير في اللغة مشتق من الزور، ويقصد به الكذب والباطل وتحريف الحقيقة عن وجهها الصحيح، كما يدل على التمويه والتلفيق وإدخال الباطل في صورة الحق. ويُعد مفهومًا واسعاً يشمل مختلف صور الغش والخداع والتدليس التي يقصد منها إظهار الأمر على غير حقيقته³.

¹ أحمد أبو الروس، جرائم التزييف والتزوير والرشوة والاختلاس، المال العام، الكتاب الخامس، المكتب الجامعي، الحديث الاسكندرية. د.س.ص. 25

² بوصقيعة، أحسن. التحقيق القضائي. ط 6. الجزائر: دار هومة للطباعة والنشر، 2006، ص 48

³ المرجع نفسه ص 50

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

ثانيا: التزوير فقهاً

تعددت التعريفات الفقهية للتزوير، إلا أنها تتفق جميعاً على أن جوهر التزوير يتمثل في تغيير الحقيقة بقصد الغش والإضرار بالغير. فقد عرف بأنه تغيير الحقيقة في محرر بإحدى الطرق التي حددها القانون تغييراً من شأنه أن يسبب ضرراً، كما عرف بأنه تغيير الحقيقة بقصد الغش في محرر أعد لإثبات واقعة معينة بما يؤدي إلى الإضرار بحقوق الغير أو مصالحهم⁴.

وعرف الفقيه جارسون التزوير بأنه تغيير الحقيقة بسوء نية في محرر بإحدى الوسائل التي يقرها القانون على نحو من شأنه إحداث ضرر، كما عرفه الفقه المصري بأنه تغيير الحقيقة بقصد الغش في محرر يحمي القانون ويتمتع بقيمة إثباتية متى ترتب على هذا التغيير ضرر أو احتمال وقوعه⁵.

وفي ظل التطور التكنولوجي واتساع نطاق التعامل بالوثائق الإلكترونية، امتد مفهوم التزوير ليشمل المستندات الرقمية ووسائل الدفع الإلكترونية الحديثة، كالشيكات الإلكترونية والبطاقات المصرفية وأنظمة تحويل الأموال والعملة الرقمية. ويتم ذلك من خلال إدخال بيانات غير صحيحة أو تعديل بيانات صحيحة أو حذفها أو إضافة بيانات جديدة بقصد تحقيق منفعة غير مشروعة للجاني أو للغير⁶. كما يمكن أن يقع التزوير الإلكتروني على مختلف المستندات الإلكترونية المحفوظة داخل الأنظمة المعلوماتية، وذلك من خلال إضافة بيانات غير حقيقية أو تعديل توقيع إلكتروني أو تغيير محتوى مستند إلكتروني بحذف أو شطب شرط جوهري أو إخفاء معلومات أساسية، بما يؤدي إلى تغيير الحقيقة والإضرار بالغير.

ثالثاً: التزوير قانوناً

لم تضع معظم التشريعات الجنائية تعريفاً جامعاً مانعاً للتزوير، وإنما اكتفت ببيان صوره وطرق ارتكابه والعقوبات المقررة له، تاركة مهمة تحديد مفهومه للفقه والقضاء. ويقصد بالتزوير قانوناً تغيير الحقيقة في محرر أو سند بإحدى الطرق التي يحددها القانون تغييراً من شأنه إحداث ضرر أو احتمال وقوعه.

⁴ أحمد أبو الروس، المرجع السابق ذكره ص 27

⁵ عبد الله بلقاسم، "الطبيعة الخاصة لجريمة التزوير في المحررات الإلكترونية"، مجلة الدراسات القانونية المقارنة، المجلد

06، العدد 02، جامعة التكوين المتواصل، تيزي وزو، 2020، ص 879.

⁶ المرجع نفسه ص 880

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

وقد عرفه العربي بلحاج بأنه تغيير الحقيقة مع العلم بمخالفتها للواقع باستعمال وسائل الغش والخداع التي يجرمها القانون الجنائي، بينما يرى الفقه الجنائي أن التزوير يتمثل في تغيير الحقيقة بقصد الغش في سند أو وثيقة أو أي محرر آخر بإحدى الطرق المادية أو المعنوية التي يحددها القانون، بما يؤدي إلى الإضرار بالمصلحة العامة أو الخاصة⁷.

الفرع الثاني : جريمة التزوير المعلوماتي

يقصد بالتزوير الإلكتروني أو المعلوماتي تغيير الحقيقة في البيانات أو المعلومات أو المستندات الإلكترونية المخزنة أو المعالجة أو المتداولة بواسطة الأنظمة المعلوماتية، وذلك باستعمال وسائل تقنية أو برامج حاسوبية بقصد الغش أو تحقيق منفعة غير مشروعة أو الإضرار بالغير.

أولاً: التعريف اللغوي

يتكون مصطلح الجريمة الإلكترونية من كلمتين:

1- الجريمة:

تعود كلمة الجريمة إلى الفعل "جرم"، الذي يدل على الكسب والافتراء، ويُقصد بها ارتكاب الذنب أو الجناية. كما تستعمل للدلالة على التعدي على حقوق الغير أو مخالفة القواعد القانونية والأخلاقية، ومن ثم فإن الجريمة تعني الفعل غير المشروع الذي يترتب عليه ضرر ويستوجب العقاب⁸.

2- الإلكترونية:

هي صفة مشتقة من الإلكترونيات، وتطلق على كل ما يتعلق بالأجهزة والأنظمة الإلكترونية، وخاصة الحاسوب وشبكات الاتصال الحديثة وتقنيات معالجة المعلومات ونقلها⁹.

ثانياً: التعريف الاصطلاحي

تعددت التعريفات الفقهية للجريمة الإلكترونية، إلا أنها تتفق جميعها على ارتباط هذا النوع من الجرائم باستخدام الوسائل التقنية الحديثة. فقد عرفت بأنها كل جريمة ترتكب باستعمال وسيلة إلكترونية،

⁷ عبد الله بلقاسم، المرجع السابق ذكره ص، ص 880-881

⁸ المرجع نفسه ص882

⁹ عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دارالفكر الجامعي، مصر،

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

كالحاسوب أو شبكة الإنترنت، من خلال اختراق الأنظمة المعلوماتية أو البريد الإلكتروني أو مختلف وسائل التواصل الاجتماعي، بقصد الإضرار بالأفراد أو المؤسسات أو الدول، أو الحصول على منافع غير مشروعة، أو نشر معلومات وبيانات بصورة غير قانونية¹⁰.

كما اعتبر المجلس الأوروبي، في تقريره المتعلق بجرائم الحاسوب، أن الجريمة الإلكترونية تتحقق في كل حالة يتم فيها تغيير البيانات أو البرامج أو محوها أو إدخالها أو التلاعب بها بأي صورة كانت داخل أنظمة المعالجة الآلية للبيانات، متى ترتب عن ذلك ضرر اقتصادي أو اعتداء على حقوق الملكية أو تحقيق منفعة غير مشروعة للجاني أو لغيره¹¹.

ويرى جانب من الفقه أن الجريمة الإلكترونية هي كل فعل غير مشروع يستخدم فيه الجاني نظامًا معلوماتيًا أو شبكة حاسوبية للوصول إلى البيانات والبرامج بقصد نسخها أو تعديلها أو حذفها أو تزويرها أو تخريبها أو الاستيلاء عليها أو توزيعها بطرق غير مشروعة¹².

كما عرفها بعض الفقهاء بأنها كل نشاط إجرامي تستعمل فيه التقنيات الإلكترونية والحاسوب وشبكات الإنترنت بصورة مباشرة أو غير مباشرة كوسيلة لتنفيذ السلوك الإجرامي وتحقيق أهدافه.

وقد عرف المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات المنعقد بالبرازيل سنة 1994 التزوير الإلكتروني بأنه كل تلاعب ببيانات المعالجة الآلية يتم باستخدام الحاسوب ويُعد من قبيل أفعال التزوير المعاقب عليها لو ارتُكب بالوسائل التقليدية¹³.

ومن خلال هذه التعريفات يتضح أن مجرد استخدام الحاسوب أو كونه محلاً للجريمة لا يكفي لاعتبارها جريمة إلكترونية؛ إذ قد يكون الحاسوب مجرد محل تقليدي للجريمة، كما في حالة سرقة أو سرقة ملحقاته. كذلك قد يُستخدم الحاسوب كوسيلة اتصال بين الجناة دون أن يضفي ذلك على الجريمة وصف الجريمة الإلكترونية.

¹⁰ عادل محمد الشرجي، عبد السلام محمد المايل، علي قابوسة، "الجريمة الإلكترونية في الفضاء الإلكتروني: المفهوم، الأسباب، سبل المكافحة مع التعرض لحالة ليبيا"، مجلة الجريمة الإلكترونية في الفضاء الإلكتروني، العدد 04، ص 242.

¹¹ طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، السنة الجامعية 2011-2012، ص 25

¹² عادل محمد الشرجي، عبد السلام محمد المايل، علي قابوسة، المرجع السابق ذكره ص ص 244-245

¹³ طرشي نورة، المرجع السابق ذكره، ص 27

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

ثالثا: التعريف القانوني للجريمة الإلكترونية في التشريع الجزائري

اصطلح المشرع الجزائري على تسمية الجريمة الإلكترونية بـ الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حيث نصت المادة الثانية من القانون رقم 04-09 المؤرخ في 05 أوت 2009¹⁴ والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على أنها: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.¹⁵

ومن خلال هذا التعريف يتبين أن المشرع الجزائري اعتمد معيار الدور الذي تؤديه المنظومة المعلوماتية في ارتكاب الجريمة، فشمّل الجرائم الموجهة مباشرة ضد أنظمة المعالجة الآلية للمعطيات، والمنصوص عليها في قانون العقوبات من المادة 394 مكرر إلى المادة 394 مكرر 7، كما وسع نطاق التجريم ليشمل كل جريمة ترتكب أو يُسهّل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية¹⁶. ويؤخذ على هذا التعريف اتساعه الشديد، إذ يشمل عدداً كبيراً من الجرائم التي قد تُرتكب باستعمال الوسائل المعلوماتية دون أن تكون في أصلها جرائم معلوماتية بالمعنى الضيق. ومع ذلك، فإنه يعكس توجه المشرع نحو توفير حماية قانونية شاملة للفضاء الرقمي.

وبناءً على مختلف التعريفات السابقة، يمكن تعريف الجريمة الإلكترونية بأنها: كل سلوك مجرم قانوناً يكون الحاسوب أو شبكة الإنترنت أو أي وسيلة إلكترونية أخرى أداة لارتكابه أو محلاً لوقوعه، ويستهدف البيانات أو الأنظمة المعلوماتية أو المصالح المرتبطة بها داخل البيئة الرقمي

المطلب الثاني: تمييز التزوير المعلوماتي عن الجرائم المشابهة

مع التطور الكبير الذي شهدته تكنولوجيا المعلومات وانتشار استخدام الوسائل الإلكترونية في مختلف مجالات الحياة، ظهرت جريمة التزوير المعلوماتي كإحدى الجرائم المستحدثة التي أشارت العديد من

¹⁴ القانون رقم 04-09 المؤرخ في 14 شعبان عام 1430 الموافق لـ 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، الصادر بتاريخ 16 أوت 2009.

¹⁵ طرشي نورة، المرجع السابق ذكره، ص 29

¹⁶ المرجع نفسه ص 30

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

الإشكالات القانونية. ونظرا لتشابهها مع بعض الجرائم الأخرى، خاصة التزوير التقليدي وبعض الجرائم الإلكترونية، أصبح من الضروري توضيح أوجه الاختلاف بينها وبين هذه الجرائم. ويساعد هذا التمييز على فهم الطبيعة القانونية للتزوير المعلوماتي وتحديد خصائصه وأركانه بشكل أدق، مما يساهم في تكييفه القانوني الصحيح وتحديد الأحكام المطبقة عليه¹⁷.

الفرع الأول: التمييز بين التزوير المعلوماتي والتزوير التقليدي

على الرغم من أن التزوير المعلوماتي يعد امتدادا حديثا لجريمة التزوير المعروفة في القوانين الجنائية، إلا أن التطور التكنولوجي الذي شهده العالم أدى إلى ظهور اختلافات جوهرية بينه وبين التزوير التقليدي. فالجريمة في صورتها التقليدية ارتبطت بالمحررات الورقية والوثائق المادية، بينما ارتبط التزوير المعلوماتي بالمحررات الإلكترونية والبيانات الرقمية التي أصبحت تشكل أساسا للمعاملات الحديثة. ولهذا أصبح من الضروري التمييز بين النوعين من خلال مجموعة من العناصر الأساسية¹⁸.

أولاً: من حيث محل الجريمة

يتمثل محل الجريمة في التزوير التقليدي في المحررات الورقية الرسمية أو العرفية التي تتضمن بيانات أو معلومات معدة للإثبات، مثل العقود والشهادات والسجلات والأوامر الإدارية وغيرها من الوثائق المكتوبة. وقد استقرت التشريعات الجنائية لفترة طويلة على اعتبار هذه المحررات الركيزة الأساسية التي تقوم عليها جريمة التزوير.

أما في التزوير المعلوماتي فإن محل الجريمة لم يعد محررا ورقيا، بل أصبح يتمثل في البيانات والمعلومات الإلكترونية المخزنة أو المعالجة بواسطة الحاسوب، وكذلك المحررات الإلكترونية وقواعد البيانات والبرامج والوثائق الرقمية. وقد فرض هذا التحول نفسه نتيجة الانتقال التدريجي من الإدارة الورقية

¹⁷براهيمي يوسف. "جريمة التزوير في المحررات الرسمية وفق القانون الجزائري." رسالة ماجستير، جامعة الجزائر 1،

2019، ص27

¹⁸بلقاسم محجوب، التزوير الإلكتروني، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق، جامعة محمد خيضر بسكرة،

2016/2017، ص26

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

إلى الإدارة الإلكترونية ومن المعاملات التقليدية إلى المعاملات الرقمية، الأمر الذي جعل البيانات الإلكترونية تتمتع بقيمة قانونية وإثباتية لا تقل أهمية عن المحررات الورقية¹⁹.

ثانيا: من حيث وسيلة ارتكاب الجريمة

يختلف أسلوب تنفيذ الجريمة في كل من التزوير التقليدي والتزوير المعلوماتي اختلافاً واضحاً. ففي التزوير التقليدي يعتمد الجاني على وسائل مادية ملموسة كإضافة عبارات إلى المحرر أو حذف بعضها أو تقليد التوقيعات أو اصطناع الأختام أو تغيير التواريخ والبيانات الواردة فيه. ولذلك فإن عملية التزوير تتم بصورة مباشرة على المحرر نفسه.

أما في التزوير المعلوماتي فإن الجاني يستخدم وسائل تقنية متطورة تعتمد على نظم المعلومات والحاسوب والبرمجيات المختلفة. فقد يقوم بتعديل البيانات المخزنة داخل قاعدة البيانات أو إدخال معلومات غير صحيحة أو حذف معلومات صحيحة أو استبدالها بأخرى مزورة، كما قد يعتمد إلى تغيير محتوى المستندات الإلكترونية أو التلاعب بالتوقيعات الإلكترونية أو ببرامج المعالجة الآلية للبيانات. ومن ثم فإن الوسيلة المستخدمة في هذا النوع من الجرائم تختلف جذرياً عن الوسائل التقليدية المعروفة²⁰.

ثالثا: من حيث طبيعة الأثر الناتج عن الجريمة

يتميز التزوير التقليدي عادة بترك آثار مادية يمكن ملاحظتها أو اكتشافها من خلال الفحص الفني للمحرر. فقد تظهر آثار الكشط أو المحو أو اختلاف الحبر أو عدم تطابق التوقيع أو الختم مع الأصل، وهي أمور تساعد جهات التحقيق والخبراء على كشف التزوير وإثباته.

أما التزوير المعلوماتي فإنه غالباً لا يترك أثراً مادياً ظاهراً، لأن التغيير يتم داخل البيئة الرقمية. فالبيانات قد تبدو صحيحة وسليمة ظاهرياً رغم تعرضها للتعديل أو التحريف، الأمر الذي يجعل اكتشاف الجريمة أكثر تعقيداً ويستلزم الاستعانة بخبراء الأدلة الرقمية وتقنيات الفحص الإلكتروني المتخصصة للكشف عن آثار التعديل أو التلاعب الذي تعرضت له البيانات²¹.

رابعا: من حيث سهولة ارتكاب الجريمة واكتشافها

¹⁹المرجع نفسه ص ص28-29

²⁰بلفاسم محجوب، المرجع السابق ذكره صص28-29

²¹المرجع نفسه ص 30

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

يعد التزوير التقليدي أكثر ارتباطاً بالوجود المادي للمحرر، وهو ما يفرض على الجاني التعامل المباشر معه، الأمر الذي قد يزيد من احتمال اكتشافه أو ضبطه أثناء تنفيذ الجريمة أو بعدها. كما أن محدودية عدد النسخ الورقية للمحرر تساعد في أحيان كثيرة على اكتشاف التغيير الذي طرأ عليه.

أما التزوير المعلوماتي فيتسم بقدر كبير من السرعة والخفاء، حيث يستطيع الجاني تنفيذ الجريمة خلال فترة زمنية قصيرة ومن أي مكان في العالم متى تمكن من الوصول إلى النظام المعلوماتي المستهدف. كما أن إمكانية حذف الآثار الرقمية أو إخفائها تجعل عملية الكشف عن الجريمة أكثر صعوبة مقارنة بالتزوير التقليدي. ولهذا السبب يعد التزوير المعلوماتي من الجرائم التي تتطلب وسائل تحقيق متطورة وخبرات تقنية عالية²².

خامساً: من حيث النطاق المكاني للجريمة

في الغالب ترتكب جرائم التزوير التقليدي داخل نطاق جغرافي محدد، حيث يكون المحرر موجوداً في مكان معين ويتم التعامل معه داخل إقليم دولة معينة، وهو ما يسهل تحديد الاختصاص القضائي والقانون الواجب التطبيق أما التزوير المعلوماتي فقد تجاوز الحدود الجغرافية التقليدية، إذ يمكن أن يكون الجاني في دولة، والنظام المعلوماتي المستهدف في دولة ثانية، والضرر الناتج عن الجريمة واقعاً في دولة ثالثة. ولذلك اكتسب هذا النوع من الجرائم طابعاً دولياً وعابراً للحدود، مما يفرض تعاوناً دولياً وتشريعياً بين الدول لمكافحته وملاحقة مرتكبيه²³.

الفرع الثاني: التمييز بين التزوير المعلوماتي والجرائم الإلكترونية الأخرى

لا يقتصر التمييز على المقارنة بين التزوير المعلوماتي والتزوير التقليدي فحسب، وإنما يمتد كذلك إلى الجرائم الإلكترونية الأخرى التي قد تتشابه معه من حيث استخدام الوسائل التقنية، لكنها تختلف عنه من حيث الهدف أو السلوك الإجرامي أو النتيجة التي يسعى الجاني إلى تحقيقها²⁴.

أولاً: التمييز بين التزوير المعلوماتي وجريمة الدخول غير المشروع إلى الأنظمة المعلوماتية

²² بلقاسم محجوب، المرجع السابق ذكره ص30

²³ براهيم يوسف. المرجع السابق ذكره، ص29

²⁴ المرجع نفسه ص 31

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

يقصد بالدخول غير المشروع ولوج شخص إلى نظام معلوماتي أو شبكة معلوماتية دون الحصول على إذن أو ترخيص قانوني. وتتحقق هذه الجريمة بمجرد حصول الدخول غير المصرح به، حتى ولو لم يقم الجاني بأي تعديل أو حذف أو تغيير للبيانات الموجودة داخل النظام.

أما التزوير المعلوماتي فلا يكفي فيه مجرد الدخول إلى النظام، بل يتطلب سلوكا إضافيا يتمثل في تغيير الحقيقة من خلال التلاعب بالبيانات أو تعديلها أو حذفها أو استحداث بيانات جديدة مخالفة للواقع. ولذلك فإن الدخول غير المشروع قد يكون مرحلة تمهيدية أو وسيلة لارتكاب التزوير المعلوماتي، لكنه لا يشكل بذاته جريمة تزوير ما لم يقترن بفعل التغيير أو التحريف²⁵.

ثانيا: التمييز بين التزوير المعلوماتي والاحتيال الإلكتروني

يقوم الاحتيال الإلكتروني على استخدام وسائل الخداع والتضليل للحصول على مال أو منفعة غير مشروعة من المجني عليه. فالهدف الأساسي للجاني في هذه الجريمة هو تحقيق مكسب مادي أو مالي عن طريق إيهام الضحية بوقائع غير صحيحة أو استغلال ثقته.

أما التزوير المعلوماتي فإن جوهره يتمثل في المساس بالحقيقة ذاتها من خلال تغيير البيانات أو المحررات الإلكترونية وإظهارها بمظهر صحيح مخالف للواقع. وقد يستخدم التزوير المعلوماتي كوسيلة لتنفيذ الاحتيال الإلكتروني، إلا أن الجريمتين تظان مستقلتين من الناحية القانونية، لأن لكل منهما أركانا وأهدافا خاصة بها²⁶.

ثالثا: التمييز بين التزوير المعلوماتي وجريمة الإلتاف المعلوماتي

تهدف جريمة الإلتاف المعلوماتي إلى القضاء على البيانات أو تعطيلها أو إفسادها أو جعلها غير قابلة للاستعمال، بحيث يفقد النظام المعلوماتي وظيفته أو تتعطل المعلومات الموجودة فيه. أما التزوير المعلوماتي فلا يستهدف إزالة البيانات أو إعدامها، وإنما يهدف إلى الإبقاء عليها مع تغيير مضمونها أو محتواها بحيث تعكس واقعا غير صحيح. ومن ثم فإن الاعتداء في جريمة الإلتاف يقع على

²⁵براهيمي يوسف. المرجع السابق ذكره، ص33

²⁶بلقاسم محجوب، التزوير الإلكتروني، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق، جامعة محمد خيضر بسكرة،

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

وجود البيانات وسلامتها التقنية، بينما يقع الاعتداء في التزوير المعلوماتي على صحة البيانات ومصادقيتها وقيمتها القانونية²⁷.

رابعا: التمييز بين التزوير المعلوماتي وسرقة البيانات الإلكترونية

يقصد بسرقة البيانات الحصول على المعلومات أو نسخها أو نقلها دون موافقة صاحبها أو دون سند قانوني يبرر ذلك. ويكون الهدف عادة الاستفادة من تلك المعلومات أو إفشاؤها أو بيعها أو استغلالها بطرق غير مشروعة.

أما التزوير المعلوماتي فلا يقتصر على الوصول إلى البيانات أو الحصول عليها، بل يتطلب التدخل فيها وتغيير مضمونها أو اصطناع بيانات جديدة غير مطابقة للحقيقة. وبالتالي فإن السرقة تمس حق الحياة أو السرية، بينما يمس التزوير الثقة والمصادقية التي تتمتع بها البيانات الإلكترونية²⁸.

خامسا: التمييز بين التزوير المعلوماتي واستعمال المحرر الإلكتروني المزور

يتحقق التزوير المعلوماتي بمجرد تغيير الحقيقة في المحرر الإلكتروني أو البيانات الرقمية، سواء باستحداث محرر مزور أو بتعديل محرر قائم. أما استعمال المحرر الإلكتروني المزور فيقوم عندما يلجأ شخص إلى تقديم ذلك المحرر أو الاحتجاج به أو الاستفادة منه مع علمه بأنه مزور.

وعليه فإن التزوير يختلف عن الاستعمال من حيث السلوك الإجرامي، فقد يكون مرتكب التزوير هو نفسه من يستعمل المحرر المزور، وقد يكون شخصا آخر لم يشارك في عملية التزوير لكنه استخدم المحرر مع علمه بعدم صحته. ولذلك تعامل التشريعات الجنائية مع الجريمتين باعتبارهما جريمتين مستقلتين رغم الارتباط الوثيق بينهما²⁹.

ومن خلال ما سبق يتبين أن التزوير المعلوماتي يتمتع بخصوصية تميزه عن التزوير التقليدي وعن مختلف الجرائم الإلكترونية الأخرى، وذلك بسبب طبيعة محل الجريمة ووسائل ارتكابها وآثارها القانونية

²⁷المرجع نفسه ص ص 20-21

²⁸أجعود، سعاد. "السياسة الجنائية للمشرع الجزائري في مواجهة جرائم التزوير للحصول على الإعانات والمساعدات العمومية والإعفاءات الاجتماعية في ظل جائحة كوفيد 19: دراسة تحليلية في ضوء الأمر 20-06 المعدل والمتمم لقانون العقوبات الجزائري". مجلة الحقوق والعلوم السياسية، المجلد 9، العدد 2، 11 أكتوبر 2022، ص 587

²⁹بلقاسم محجوب، التزوير الإلكتروني، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق، جامعة محمد خيضر بسكرة،

19/2016-2017 ص 19

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

والتقنية، الأمر الذي يبرر الاتجاه المتزايد نحو وضع قواعد قانونية خاصة تكفل حماية المحررات والبيانات الإلكترونية من مختلف صور التلاعب والتحريف.

المطلب الثالث: خصائص جريمة التزوير المعلوماتية

تُعد جريمة التزوير المعلوماتية من أخطر الجرائم الإلكترونية لما تمثله من اعتداء على الثقة العامة، ولما قد تسببه من أضرار تمس الحقوق والمراكز القانونية للأفراد والمؤسسات، خاصة إذا تعلقت بوثائق رسمية أو محررات إدارية. وتتميز هذه الجريمة بعدة خصائص، من أهمها³⁰:

1- الطابع العابر للحدود: تتجاوز جريمة التزوير المعلوماتية الحدود الجغرافية للدول، إذ يمكن للجاني أن يوجد

في دولة معينة بينما تقع آثار الجريمة في دولة أخرى، وذلك بسبب الطبيعة العالمية لشبكات الاتصال والإنترنت التي لا تعترف بالحدود الإقليمية التقليدية.

2- إمكانية ارتكابها في مختلف مراحل تشغيل النظام المعلوماتي: يمكن ارتكاب جريمة التزوير المعلوماتي في

أي مرحلة من مراحل المعالجة الآلية للبيانات، سواء في مرحلة الإدخال أو المعالجة أو الإخراج.

مرحلة الإدخال: يمكن إدراج بيانات غير صحيحة أو إغفال إدخال بيانات أساسية بقصد تغيير الحقيقة، كإضافة أسماء أشخاص غير موجودين فعلياً إلى قاعدة البيانات.

مرحلة المعالجة : فيمكن التلاعب بالبرامج أو تعديلها لتحقيق أهداف إجرامية معينة من خلال التأثير في طريقة معالجة البيانات.

مرحلة الإخراج: يمكن تغيير النتائج النهائية بعد معالجتها بصورة صحيحة، وذلك عبر الدخول إلى النظام المعلوماتي والتلاعب بالمرجات، كقيام أحد الطلبة باختراق نظام الجامعة وتعديل علاماته الدراسية³¹.

3- عدم ترك آثار مادية ظاهرة

يتميز التزوير المعلوماتي بعدم ترك آثار مادية واضحة على المحرر الإلكتروني، بخلاف التزوير التقليدي في المحررات الورقية الذي قد تظهر فيه آثار الحذف أو الإضافة أو الكشط أو استعمال المواد الكيميائية. لذلك يُعد التزوير المعلوماتي جريمة فنية غير ملموسة يصعب اكتشافها بالوسائل التقليدية³².

³⁰ براهيم يوسف. المرجع السابق ذكره، ص35

³¹ أجعود سعاد. المرجع السابق ذكره صص 589-590

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

4- خصوصية شخصية الجاني ودوافعه

غالبا ما يتطلب ارتكاب جريمة التزوير المعلوماتي قدرًا من الخبرة والمعرفة التقنية في مجال الحاسوب ونظم المعلومات، لذلك يكون مرتكبوها في كثير من الأحيان من المتخصصين في المجال المعلوماتي أو من القراصنة ومخترقي الأنظمة وينقسم هؤلاء عادة إلى فئتين رئيسيتين³³:

- **الهاكرز (Hackers)** وهم القراصنة الهواة الذين يسعون غالبا إلى اختبار قدراتهم التقنية أو اكتشاف الثغرات .
- **الكرakers (Crackers)** وهم القراصنة المحترفون الذين يستغلون مهاراتهم التقنية لتحقيق أهداف غير مشروعة .

وقد تكون دوافع الجاني مادية، كالحصول على مكاسب مالية غير مشروعة، أو معنوية تتمثل في إثبات القدرات التقنية والتفاخر بالمهارات المعلوماتية. وتُعد هذه الجريمة من الجرائم العمدية التي تتطلب توافر القصد الجنائي، إذ لا يُتصور قيامها نتيجة الخطأ أو الإهمال غير المقصود، ما لم ينص القانون على خلاف ذلك.³⁴

المبحث الثاني: أركان جريمة التزوير المعلوماتي

تقوم جريمة التزوير المعلوماتي على مجموعة من الأركان القانونية التي لا يمكن تصور قيامها إلا بتوافرها مجتمعة، إذ تمثل الأساس الذي تستند إليه المسؤولية الجزائية لمرتكب هذا النوع من الجرائم. ونظرا لخصوصية البيئة الرقمية التي تقع فيها الجريمة، فقد اكتسبت هذه الأركان طابعاً مميزاً يختلف في

³² بلقاسم محجوب، المرجع السابق ذكره ص.22-23

³³ بلقاسم محجوب، المرجع السابق ذكره ص.23

³⁴ أجعود سعاد. المرجع السابق ذكره ص.591

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

بعض جوانبه عن جرائم التزوير التقليدية، خاصة فيما يتعلق بطبيعة السلوك الإجرامي ومحل الجريمة. وعليه، سيتم التطرق في هذا المبحث إلى الركن المعنوي والركن المادي، ثم بيان محل الجريمة باعتباره أحد العناصر الجوهرية لقيام التزوير المعلوماتي³⁵.

المطلب الأول: الركن المادي والركن المعنوي لجريمة التزوير المعلوماتي

تقوم جريمة التزوير المعلوماتي، شأنها شأن سائر الجرائم، على ركنين أساسيين يتمثلان في الركن المادي والركن المعنوي، إذ لا يكفي مجرد المساس بالبيانات أو المعطيات الإلكترونية لقيام الجريمة، وإنما يشترط أن يصدر هذا السلوك عن إرادة إجرامية تتجه إلى تغيير الحقيقة في البيئة الرقمية. وتزداد أهمية دراسة هذين الركنين بالنظر إلى الطبيعة الخاصة للتزوير المعلوماتي، الذي لا يقع على محررات ورقية تقليدية وإنما على بيانات ومعلومات إلكترونية مخزنة أو متداولة عبر الأنظمة المعلوماتية، الأمر الذي أكسب هذه الجريمة خصوصية قانونية وتقنية تميزها عن جرائم التزوير التقليدية. وقد سعى المشرع الجزائري إلى توفير الحماية الجزائية لهذه المعطيات من خلال الأحكام الواردة في قانون العقوبات، ولا سيما المواد المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات³⁶.

الفرع الأول: الركن المادي لجريمة التزوير المعلوماتي في التشريع الجزائري

يقصد بالركن المادي لجريمة التزوير المعلوماتي ذلك النشاط الإجرامي الملموس الذي يؤدي إلى تغيير الحقيقة في البيانات أو المعطيات الإلكترونية المخزنة أو المعالجة داخل الأنظمة المعلوماتية. ويعد هذا الركن الأساس الذي تقوم عليه الجريمة، إذ لا يمكن تصور وجود تزوير معلوماتي دون تدخل مادي يؤدي إلى إدخال بيانات غير صحيحة أو تعديلها أو حذفها أو استبدالها بما يغير من مضمونها الحقيقي. وقد حرص المشرع الجزائري على توفير حماية جزائية لهذه الأفعال من خلال مجموعة من النصوص القانونية الواردة أساساً في القسم السابع مكرر من قانون العقوبات تحت عنوان «المساس بأنظمة المعالجة الآلية للمعطيات»، بالإضافة إلى الأحكام المستحدثة الواردة في القانون رقم 24-02 المتعلق بمكافحة التزوير

³⁵مراد عبد الجابر الرجحي، جريمة التزوير الإلكتروني كجريمة مستحدثة في التشريع الجزائري، كلية الحقوق، جامعة القاهرة، العدد 20، سنة 2020. صص 58-59

³⁶صدراتي، وفاء. آليات مكافحة جريمة التزوير الإلكتروني. أطروحة لنيل شهادة دكتوراه العلوم في القانون الجنائي، جامعة العربي التبسي، تبسة، 2014-2015، ص 27

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

واستعمال المزور³⁷، والقانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.³⁸

ويتجسد الركن المادي لجريمة التزوير المعلوماتي من خلال ثلاثة عناصر أساسية تتمثل في السلوك الإجرامي، ومحل الجريمة، والنتيجة الإجرامية وعلاقة السببية.

أولاً: السلوك الإجرامي

يقوم السلوك الإجرامي في جريمة التزوير المعلوماتي على كل فعل يؤدي إلى تغيير الحقيقة الرقمية داخل النظام المعلوماتي بطريقة غير مشروعة. وقد حدد المشرع الجزائري صور هذا السلوك بموجب المادة 394 مكرر 1 من قانون العقوبات التي تنص على معاقبة كل من «أدخل بطريق الغش معطيات في نظام للمعالجة الآلية للمعطيات أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها ومن خلال هذا النص تتضح صور السلوك الإجرامي في ثلاث حالات رئيسية³⁹:

- إدخال معطيات كاذبة أو وهمية داخل النظام المعلوماتي بقصد إظهارها على أنها صحيحة، كإدراج بيانات مالية أو إدارية غير مطابقة للحقيقة .
- تعديل المعطيات الإلكترونية الموجودة مسبقاً داخل النظام، سواء بالإضافة أو التغيير أو الاستبدال، بما يؤدي إلى تغيير مضمونها الحقيقي .
- إزالة أو حذف المعطيات الإلكترونية كلياً أو جزئياً بهدف طمس الحقيقة أو إخفاء معلومات معينة أو استبدالها بأخرى مزورة .

³⁷ القانون رقم 02-24 المؤرخ في 16 شعبان عام 1445 الموافق 26 فبراير سنة 2024، والمتعلق بمكافحة التزوير واستعمال المزور، الصادر في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 15 بتاريخ 29 فبراير 2024

³⁸ صدراتي وفاء . المرجع السابق ذكره ص ص 31-32

³⁹ المرجع نفسه ص 32

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

ولا يقتصر التجريم على الأفعال التي تمثل التزوير ذاته، بل يمتد إلى الأعمال التحضيرية التي تسهل ارتكابه. فقد نصت المادة 394 مكرر⁴⁰ من قانون العقوبات على معاقبة كل من يقوم عمداً بتصميم أو إنتاج أو توفير أو نشر برامج أو أدوات معلوماتية تستعمل في ارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات أو تسهل تنفيذها. وتكمن أهمية هذا النص في تجريم الوسائل التقنية التي يعتمد عليها مرتكبو جرائم التزوير المعلوماتي للوصول إلى البيانات والتلاعب بها.

كما تجرم المادة 394 مكرر الدخول أو البقاء عن طريق الغش داخل منظومة المعالجة الآلية للمعطيات، إذ يعد الاختراق غير المشروع في كثير من الأحيان المرحلة الأولى التي تسبق عملية تزوير البيانات أو تعديلها. وقد شدد المشرع العقوبة إذا ترتب عن هذا الدخول حذف أو تغيير للمعطيات الموجودة داخل النظام⁴¹.

وتزداد خطورة السلوك الإجرامي عندما يستهدف الأنظمة المعلوماتية التابعة للدولة أو المؤسسات العمومية أو الهيئات ذات الطابع السيادي، وهو ما دفع المشرع إلى تشديد العقوبات بموجب المادة 394 مكرر 3 من قانون العقوبات حماية للمصلحة العامة والأمن المعلوماتي الوطني.

ثانياً: محل الجريمة

يقصد بمحل الجريمة العنصر الذي ينصب عليه السلوك الإجرامي مباشرة. ويتمثل محل التزوير المعلوماتي في البيانات والمعطيات الإلكترونية المخزنة أو المعالجة أو المتداولة داخل الأنظمة المعلوماتية.

⁴⁰ المادة 394 مكرر 2 من القانون رقم 04-15 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات الجزائري تنص على : "يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 100.000 دج إلى 500.000 دج، كل من يقوم عمداً وعن طريق الغش بتصميم أو تجميع أو توفير أو نشر أو الاتجار في معطيات أو برامج أو أي وسيلة أخرى مصممة أو مهيأة خصيصاً لارتكاب الجرائم المنصوص عليها في هذا القسم. ويعاقب بنفس العقوبة كل من حاز أو أفشى أو نشر أو استعمل معطيات متحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

⁴¹ بلقاسم محجوب، المرجع السابق ذكره ص38

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

ويشمل ذلك مختلف أشكال البيانات الرقمية، مثل الملفات الإلكترونية، وقواعد البيانات، والسجلات الإدارية، والعقود الإلكترونية، والمحركات الرقمية، والتوقيعات الإلكترونية، والوثائق البيومترية، وجميع المعلومات التي تكتسب قيمة قانونية أو مالية أو إدارية⁴².

وقد عزز القانون رقم 02-24 هذه الحماية من خلال توسيع نطاق التجريم ليشمل المحررات الإلكترونية والوثائق الرقمية الرسمية. ويتضح ذلك من المادة 31⁴³ التي تعاقب على تزوير المحررات العمومية والرسمية، سواء تم ذلك عن طريق تقليد أو تزيف الكتابة أو التوقيع التقليدي أو الإلكتروني، وهو ما يوفر حماية قانونية مباشرة للوثائق الرقمية التي تصدرها الإدارات والمؤسسات العمومية.

كما يمتد نطاق الحماية إلى كل من يستعمل الوثائق أو البيانات الرقمية المزورة مع علمه بتزويرها، إذ يعد استعمال المحرر الإلكتروني المزور صورة مستقلة من صور الاعتداء على الثقة العامة، ويعاقب مرتكبه بالعقوبات ذاتها المقررة لمرتكب التزوير الأصلي وفقاً لأحكام القانون رقم 02-24.

ثالثاً: النتيجة الإجرامية وعلاقة السببية

تتمثل النتيجة الإجرامية في جريمة التزوير المعلوماتي في تغيير الحقيقة الرقمية وتشويه المضمون الأصلي للبيانات أو المعطيات الإلكترونية بما يجعلها غير معبرة عن الواقع الذي أنشئت لإثباته. ويتحقق ذلك بمجرد المساس بسلامة البيانات أو مصداقيتها أو قيمتها القانونية.

وقد تأخذ هذه النتيجة صوراً متعددة، فقد تتمثل في إحداث ضرر مادي من خلال الاستيلاء على أموال الغير أو الحصول على مزايا غير مشروعة، كما قد تتمثل في الإضرار بالمؤسسات أو الإدارات العمومية عبر تغيير البيانات الرسمية أو العبث بالسجلات الإلكترونية أو تعطيل الخدمات الرقمية⁴⁴.

⁴² عبد الله بن جلوي عبد الله الأبرقي، الضرر في جريمة تزوير المحررات، رسالة ماجستير، كلية الدراسات العليا، قسم العدالة الجنائية، 2007-2008، ص31

⁴³ المادة 31 من القانون رقم 02-24 المؤرخ في 16 شعبان عام 1445 الموافق 26 فبراير سنة 2024، المتعلق بمكافحة التزوير واستعمال المزور و تنص على : يعاقب بالحبس من 10 سنوات إلى 20 سنة كل من يرتكب جنائية تزوير في المحررات الرسمية أو العمومية. وقد وسّع المشرع الجزائري نطاق هذه الحماية القانونية بشكل جذري عبر هذا القانون بمساواة المحررات والوثائق الإلكترونية والرقمية بالوثائق الورقية التقليدية من حيث العقاب الجنائي وخطورة الفعل

⁴⁴ عبد الله بن جلوي عبد الله الأبرقي المرجع السابق ذكره ص36

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

كما يشترط وجود علاقة سببية بين السلوك الإجرامي والنتيجة المترتبة عنه، أي أن يكون التغيير الذي أصاب البيانات أو المعطيات نتيجة مباشرة للفعل الذي قام به الجاني. فإذا ثبت أن النتيجة تعود إلى سبب أجنبي أو خطأ تقني مستقل عن فعل الجاني انتفت علاقة السببية وبالتالي تنتفي المسؤولية الجزائية عن جريمة التزوير المعلوماتي.⁴⁵

ولتعزيز فعالية المتابعة الجزائية لهذه الجرائم، منح القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصالومكافحتها سلطات خاصة للضبطية القضائية والجهات المختصة، من بينها تفتيش الأنظمة المعلوماتية وحجز الأدلة الرقمية وتتبع حركة المعطيات الإلكترونية وإلزام مقدمي خدمات الإنترنت بالاحتفاظ بالبيانات التقنية اللازمة للكشف عن عمليات التعديل أو الحذف أو الإدخال غير المشروع للمعطيات. وتساهم هذه الإجراءات في إثبات عناصر الركن المادي وتحديد المسؤولية الجزائية لمرتكبي جرائم التزوير المعلوماتي.⁴⁶

وعليه، يتضح أن المشرع الجزائري أحاط الركن المادي لجريمة التزوير المعلوماتي بمنظومة قانونية متكاملة، تجمع بين التجريم الموضوعي للأفعال الماسة بالبيانات الإلكترونية والعقوبات المقررة لها، وبين الآليات الإجرائية الكفيلة بالكشف عنها وإثباتها، بما يضمن حماية الثقة والأمن القانوني في البيئة الرقمية.

الفرع الثاني: الركن المعنوي لجريمة التزوير المعلوماتي

يقصد بالركن المعنوي الحالة النفسية التي يكون عليها الجاني وقت ارتكاب الجريمة، والمتمثلة في اتجاه إرادته إلى ارتكاب الفعل المجرم مع علمه بطبيعته وعدم مشروعيته. ولا يكفي لقيام جريمة التزوير المعلوماتي تحقق الركن المادي المتمثل في تغيير الحقيقة داخل الأنظمة المعلوماتية أو المساس بالبيانات الإلكترونية، بل يجب أن يكون هذا السلوك صادراً عن إرادة واعية ومتجهة نحو تحقيق نتيجة غير مشروعة. وتعد جريمة التزوير المعلوماتي من الجرائم العمدية التي تتطلب توافر القصد الجنائي، وهو ما يستفاد من مختلف النصوص القانونية المنظمة لهذه الجريمة في التشريع الجزائري.⁴⁷

⁴⁵ صدراتي وفاء. المرجع السابق ذكره ص 35

⁴⁶ مراد عبد الجابر الرجحي، المرجع السابق ذكره ص 62

⁴⁷ المرجع نفسه ص 63

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

ويتكون الركن المعنوي لجريمة التزوير المعلوماتي من عنصرين أساسيين هما :القصد الجنائي العام والقصد الجنائي الخاص.

أولاً: القصد الجنائي العام

يقصد بالقصد الجنائي العام علم الجاني بجميع العناصر المكونة للجريمة، وإرادته الحرة في ارتكاب الفعل المجرم. ويتحقق هذا القصد عندما يعلم الفاعل أن البيانات أو المحررات الإلكترونية التي يتعامل معها تتمتع بالحماية القانونية، وأن فعله المتمثل في إدخال أو تعديل أو حذف أو محو البيانات يؤدي إلى تغيير الحقيقة وإظهارها على غير صورتها الأصلية، ثم تتجه إرادته إلى تنفيذ هذا الفعل رغم علمه بعدم مشروعيته⁴⁸.

ويجد هذا العنصر أساسه القانوني في المادة 394 مكرر 1 من قانون العقوبات الجزائري المعدلة بموجب الأمر رقم 06-24،⁴⁹ والتي تجرم إدخال المعطيات أو تعديلها أو حذفها داخل نظام المعالجة الآلية للمعطيات "عمداً وعن طريق الغش". ومن ثم فإن المشرع اشترط صراحة توافر العلم والإرادة والغش لقيام الجريمة، وهو ما يستبعد حالات الخطأ غير العمدية أو الأعطال التقنية أو الأخطاء الناتجة عن الجهل أو الإهمال.

كما يستفاد هذا الشرط من المادة 3 من القانون رقم 02-24 المتعلق بمكافحة التزوير واستعمال المزور⁵⁰، التي عرفت التزوير بأنه كل تغيير للحقيقة أو للمصادقية في محررات أو بيانات بأي وسيلة

⁴⁸ عبد الله بن جلوي عبد الله الأبرقي المرجع السابق ذكره ص39

⁴⁹ المادة 394 مكرر 1 من القانون رقم 06-24 المؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2024، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات الجزائري، وتنص على : "يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام للمعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها."

⁵⁰ المادة 3 من القانون رقم 02-24 المؤرخ في 16 شعبان عام 1445 الموافق 26 فبراير سنة 2024، المتعلق بمكافحة التزوير واستعمال المزور وتنص على : "يقصد بالتزوير، في مفهوم هذا القانون، كل تغيير للحقيقة، عن طريق الغش، في إحدى المحررات أو الوثائق أو الدعائم المنصوص عليها في هذا القانون، بأي وسيلة كانت، من شأنه إحداث ضرر والذي يهدف أو من شأنه أن يترتب عليه إقرار حق أو صفة أو واقعة ترتب آثاراً قانونية. ويشمل التزوير، التقليد والتزييف المنصوص عليهما في هذا القانون."

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

كانت، متى كان من شأنه إحداث ضرر مادي أو معنوي بالمصلحة العامة أو بالغير، وهو تعريف يفترض توافر إرادة متعمدة لتغيير الحقيقة.

ثانياً: القصد الجنائي الخاص

إلى جانب القصد الجنائي العام، يشترط المشرع توافر قصد جنائي خاص يتمثل في الغاية أو الهدف الذي يسعى الجاني إلى تحقيقه من وراء فعل التزوير. ويتمثل هذا القصد في نية استعمال البيانات أو المحررات المزورة للحصول على منفعة غير مشروعة أو الإضرار بالغير أو التأثير في مركز قانوني أو مالي أو إداري معين ويظهر هذا القصد من خلال الأهداف التي تدفع الجاني إلى ارتكاب فعل التزوير، ومن أهمها⁵¹:

- الحصول على منفعة مالية أو مادية غير مشروعة .
- الاستيلاء على أموال الغير أو تحويلها إلكترونياً .
- تزوير وثائق أو بيانات رقمية بقصد استعمالها كوسيلة إثبات أمام الجهات الإدارية أو القضائية .
- الإضرار بمصالح الأفراد أو المؤسسات أو الهيئات العمومية .
- إخفاء جريمة سابقة أو تسهيل ارتكاب جريمة أخرى .
- المساس بمصادقية الأنظمة المعلوماتية أو عرقلة عملها.

ويظهر القصد الجنائي الخاص في العديد من صور التزوير المعلوماتي، كقيام الجاني بتعديل بيانات مالية إلكترونية للاستيلاء على أموال الغير، أو تزوير سجلات إدارية أو جامعية للحصول على مزايا أو امتيازات غير مستحقة، أو اصطناع وثائق إلكترونية مزورة بغرض استعمالها أمام الجهات الإدارية أو القضائية.

⁵¹المستاري، نور الهدى. التزوير واستعمال المزور في الصفقات العمومية. مذكرة لنيل شهادة الماجستير، في إطار مدرسة الدكتوراه في القانون، جامعة الجيلالي الياصب، سيدي بلعباس، 2012-2013.ص26

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

ويتجلى هذا العنصر بوضوح في المادة 42⁵² من القانون رقم 02-24 التي تعاقب كل من يتحصل على وثيقة صحيحة بناءً على تصريحات كاذبة أو وثائق مزورة، حيث تتجه إرادة الفاعل إلى الحصول على حق أو امتياز لا يستحقه باستعمال وسائل الغش والتدليس. كما يظهر القصد الخاص في الجرائم المنصوص عليها في المادة 31⁵³ المتعلقة بتزوير المحررات الرسمية والعمومية، وفي المادة 35 الخاصة بتزوير⁵⁴ المحررات التجارية والمصرفية والعرفية، إذ يفترض ارتكاب هذه الجرائم نية استعمال المحرر المزور وتحقيق مصلحة غير مشروعة من ورائه⁵⁵.

ثالثاً: العلم بالتزوير واستعمال المحرر المزور

من الصور الخاصة للركن المعنوي في جرائم التزوير المعلوماتي علم الجاني بحقيقة التزوير عند استعمال المحرر أو البيانات المزورة. وقد كرس المشرع هذا المبدأ في المادة 71⁵⁶ من القانون رقم 02-24، التي ساوت بين مرتكب التزوير ومستعمل المحرر المزور متى ثبت علم هذا الأخير بحقيقة التزوير. ويعد عنصر العلم هنا شرطاً أساسياً لقيام المسؤولية الجزائية، فلا يكفي مجرد استعمال المحرر المزور، بل يجب أن يكون المستعمل على دراية مسبقة بواقعة التزوير وأن تتجه إرادته إلى الاستفادة من الآثار

⁵² المادة 42 من القانون رقم 02-24 المؤرخ في 16 شعبان عام 1445 الموافق 26 فبراير سنة 2024، المتعلق بمكافحة التزوير واستعمال المزور تنص على: يجب على الجهة القضائية المنظورة أمامها الدعوى، في حالة الإدانة بإحدى الجرائم المنصوص عليها في هذا القانون، أن تحكم على المحكوم عليه برد الإعانات والمزايا أو دفع قيمتها، وذلك دون الإخلال بالتعويضات المدنية المقررة

⁵³ المادة 31: "يعاقب بالسجن المؤقت من عشر (10) سنوات إلى عشرين (20) سنة، وبغرامة من 1.000.000 دج إلى 2.000.000 دج، كل شخص، ما عدا الأشخاص المذكورين في المادة 32 من هذا القانون، ارتكب تزويراً في محررات رسمية أو عمومية: إما بتقليد أو تزيف الكتابة أو التوقيع. إما باصطناع اتفاقات أو نصوص أو التزامات أو مخالصات، أو بإدراجها في هذه المحررات لاحقاً. إما بالإضافة أو الإسقاط أو التغيير في الشروط أو الوقائع أو الصفات التي أعدت هذه المحررات لإثباتها أو تقريرها."

⁵⁴ المادة 35: "يعاقب بالحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج، كل من ارتكب تزويراً في محررات تجارية أو مصرفية أو مالية، بإحدى الطرق المنصوص عليها في المادة 31 من هذا القانون. وتطبق نفس العقوبات على كل من أصدر فاتورة تثبت وقائع غير صحيحة مادياً."

⁵⁵ عبد الله بن جلوي عبد الله الأبرقي المرجع السابق ذكره ص42

⁵⁶ المادة 71 من القانون رقم 02-24 المتعلق بمكافحة التزوير واستعمال المزور وتنص على ما يلي: يعاقب على استعمال المزور بنفس العقوبات المقررة للتزوير المنصوص عليها في هذا القانون، مع مراعاة الاستثناءات الواردة فيه."

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

القانونية المترتبة عليه. ولذلك تنتفي المسؤولية الجزائية إذا أثبت الشخص حسن نيته وجهله بكون المحرر أو البيانات محل الاستعمال مزورة⁵⁷.

رابعا: أثر الصفة والغرض الإجرامي في تشديد المسؤولية

أولى المشرع الجزائري أهمية خاصة للغرض الإجرامي ولصفة الجاني في جرائم التزوير، حيث شدد العقوبات متى اقترن التزوير بأهداف خطيرة أو صدر عن أشخاص يتمتعون بصفة وظيفية خاصة. فقد نصت المادة 32⁵⁸ من القانون رقم 02-24 على تشديد العقوبة إذا ارتكب التزوير قاضٍ أو موظف عمومي أو ضابط عمومي أثناء تأدية مهامه، وهو ما يعكس خطورة استغلال الثقة العامة لتحقيق أغراض غير مشروعة.

كما شددت المادة 394 مكرر⁵⁹ من قانون العقوبات العقوبة إذا استهدف التزوير المعلوماتي معطيات أو أنظمة ذات طابع سيادي تخص الدولة، لما يشكله ذلك من مساس بأمن الدولة ومصالحها الأساسية.

وعليه، فإن الركن المعنوي لجريمة التزوير المعلوماتي يقوم على أربعة عناصر مترابطة هي: العلم بالفعل المجرم، والإرادة الحرة في ارتكابه، والغاية غير المشروعة من التزوير، والعلم بحقيقة التزوير عند استعمال المحرر أو البيانات المزورة. ومضى اجتمعت هذه العناصر إلى جانب الركن المادي، قامت جريمة التزوير المعلوماتي وترتبت المسؤولية الجزائية في حق مرتكبها وفقاً لأحكام التشريع الجزائري⁶⁰

⁵⁷ مراد عبد الجابر الرجحي، جريمة التزوير الإلكتروني كجريمة مستحدثة في التشريع الجزائري، كلية الحقوق، جامعة القاهرة، العدد 20، سنة 2020، ص 21

⁵⁸ المادة 32 : "يعاقب بالسجن المؤقت من عشرين (20) سنة إلى ثلاثين (30) سنة، كل قاض أو موظف عمومي أو ضابط عمومي ارتكب، عمدا وعن طريق الغش، أثناء تأدية وظائفه، تزويرا في محررات رسمية أو عمومية، سواء كان ذلك بتقريره وقائع يعلم أنها كاذبة في صورة وقائع صحيحة أو الشهادة كذبا بأن وقائع قد اعترف بها أو وقعت في حضوره، أو بأي طريقة من الطرق المنصوص عليها في المادة 31 من هذا القانون."

⁵⁹ "المادة 394 مكرر 3 من القانون رقم 06-24 المعدل والمتمم لقانون العقوبات، المتعلق بقانون العقوبات، المؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2024، وتنص على: "تضاعف العقوبات المقررة في المواد 394 مكرر و394 مكرر 1 و394 مكرر 2، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون إخلال بتطبيق عقوبات أشد."

⁶⁰ شرقي الأخضر، "الأساليب الخاصة للبحث والتحري عن الجرائم المستحدثة في التشريع الجزائري"، مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد 10، العدد 2، 5 جوان 2025، ص 178

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

المطلب الثاني: محل جريمة التزوير المعلوماتي

يقصد بمحل جريمة التزوير المعلوماتي الوعاء أو الدعامة التي يقع عليها فعل التزوير وتكون محلا لتغيير الحقيقة بوسائل تقنية ومعلوماتية. وإذا كان محل التزوير في الجرائم التقليدية يتمثل في المحررات الورقية وما تتضمنه من بيانات وكتابات، فإن التطور التكنولوجي الذي عرفته المعاملات الحديثة أدى إلى ظهور أوعية جديدة للمعلومات تمثلت في البيانات الرقمية والمحررات الإلكترونية، والتي أصبحت تؤدي الوظائف ذاتها التي تؤديها المحررات التقليدية في إثبات الحقوق والالتزامات وتوثيق التصرفات القانونية. وقد أدرك المشرع الجزائري هذه التحولات، فمد الحماية القانونية إلى البيانات والمحررات الإلكترونية من خلال مجموعة من النصوص الواردة في قانون العقوبات والقانون المدني والقانون رقم 15-04⁶¹ المتعلق بالتوقيع والتصديق الإلكترونيين والقانون رقم 18-07⁶² المتعلق بحماية المعطيات ذات الطابع الشخصي، إضافة إلى القانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور⁶³.

أولاً: المعطيات والبيانات المعلوماتية

تمثل المعطيات والبيانات المعلوماتية الركيزة الأساسية التي تقوم عليها جريمة التزوير المعلوماتي، إذ تعد المادة الأولية التي تعالجها الأنظمة المعلوماتية وتخزنها وتسترجعها وتبادلها إلكترونياً. ويقصد بها جميع المعلومات أو الرموز أو الأرقام أو الإشارات أو الصور أو الأصوات أو البرامج التي يتم إدخالها أو حفظها أو معالجتها بواسطة نظام للمعالجة الآلية للمعطيات.

وقد أولى المشرع الجزائري أهمية خاصة لهذه البيانات بالنظر إلى دورها الحيوي في مختلف المجالات الاقتصادية والإدارية والقضائية والمالية، حيث أصبحت المؤسسات العمومية والخاصة تعتمد عليها في إدارة نشاطاتها وحفظ سجلاتها وتوثيق معاملاتها. ومن ثم فإن أي مساس بها من خلال التعديل أو

⁶¹ القانون رقم 15-04 المؤرخ في 11 ربيع الثاني 1436 الموافق لـ 01 فبراير 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 06، الصادرة بتاريخ 10 فبراير 2015.

⁶² القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 34، الصادرة بتاريخ 2 شعبان عام 1439 هـ الموافق 17 يونيو سنة 2018 م

⁶³ شرقي الأخضر، "المرجع السابق ذكره"، ص 180

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

الإضافة أو الحذف أو التحريف يؤدي إلى المساس بمصادقية المعلومات وبالتالي المفترضة في الأنظمة المعلوماتية⁶⁴.

وتتجسد الحماية القانونية لهذه المعطيات في المادة 394 مكرر 1 من قانون العقوبات التي تنص على معاقبة كل من «أدخل بطريق الغش معطيات في نظام للمعالجة الآلية للمعطيات أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها». ويتضح من هذا النص أن المشرع اعتبر المعطيات الرقمية ذاتها محلاً للجريمة، إذ إن الاعتداء لا يقع على الجهاز أو الوسيط الإلكتروني في حد ذاته، وإنما على المعلومات التي يحتويها⁶⁵.

كما عزز المشرع هذه الحماية بموجب المادة 394 مكرر 3 من قانون العقوبات التي شددت العقوبات إذا تعلقت الجريمة بمعطيات تخص الدولة أو الجماعات المحلية أو المؤسسات والهيئات الخاضعة للقانون العام، لما تمثله هذه البيانات من أهمية استراتيجية وأمنية وتشمل المعطيات التي يمكن أن تكون محلاً للتزوير المعلوماتي⁶⁶:

- 1- البيانات البنكية والمالية المتعلقة بالحسابات والتحويلات والأرصدة الإلكترونية.
- 2- قواعد البيانات الإدارية الخاصة بالحالة المدنية والضرائب والجمارك والسجل التجاري.
- 3- الملفات الطبية والإلكترونية الخاصة بالمؤسسات الصحية.
- 4- البيانات المخزنة في المؤسسات الاقتصادية والتجارية.
- 5- البيانات المرتبطة بالوثائق البيومترية وجوازات السفر وبطاقات التعريف الوطنية.
- 6- المعطيات الشخصية المتعلقة بالأفراد.

وفي هذا الإطار، أقر القانون رقم 18-07 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حماية قانونية للبيانات الشخصية، ومنع أي تعديل أو معالجة أو استغلال غير مشروع لها. وعليه، فإن أي تغيير للحقيقة الواردة في هذه البيانات أو

⁶⁴المرجع نفسه ص181

⁶⁵المرجع نفسه ص ص181-182

⁶⁶شعباني، نوال. "مظاهر تفعيل قواعد مكافحة جرائم التزوير المقررة بموجب القانون رقم 24-02 المتعلق بمكافحة

التزوير واستعمال المزور". *Revue critique de droit et sciences politiques*، المجلد 20، العدد 1،

2025. ص466

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

تحريف لمحتواها يمكن أن يشكل صورة من صور التزوير المعلوماتي متى ترتب عنه المساس بالحقوق أو المصالح التي يحميها القانون⁶⁷.

ثانيا: المحررات الإلكترونية

إلى جانب البيانات الرقمية، تشكل المحررات الإلكترونية محلاً أساسياً لجريمة التزوير المعلوماتي، خاصة مع اتساع نطاق التعامل الإلكتروني واعتماد الإدارات والمؤسسات والأفراد على الوثائق الرقمية في إبرام التصرفات القانونية وإثباتها.

ويقصد بالمحرر الإلكتروني كل وثيقة أو رسالة أو سجل أو دعامة إلكترونية تتضمن بيانات أو معلومات منشأة أو مخزنة أو مرسلة أو مستقبلة بوسائل إلكترونية، وتكون قابلة للحفظ والاسترجاع والاستعمال في إثبات حق أو التزام أو واقعة قانونية.

وقد اعترف المشرع الجزائري بالحجية القانونية للمحرر الإلكتروني بموجب المادة 323 مكرر 1 من القانون المدني التي نصت على أن «الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها»⁶⁸.

ويترتب على هذا الاعتراف القانوني أن المحرر الإلكتروني أصبح يتمتع بالقيمة القانونية نفسها التي يتمتع بها المحرر الورقي، وبالتالي فإن أي تغيير للحقيقة الواردة فيه عن طريق الإضافة أو الحذف أو التعديل أو الاصطناع يعد تزويراً متى توافرت باقي الشروط القانونية اللازمة ومن أهم صور المحررات الإلكترونية التي يمكن أن تكون محلاً للتزوير المعلوماتي⁶⁹:

1- العقود الإلكترونية المبرمة عبر الوسائط الرقمية.

2- الفواتير الإلكترونية والمستندات المحاسبية الرقمية.

3- المراسلات الإلكترونية الرسمية والإدارية

⁶⁷ شرقي الأخضر، "المرجع السابق ذكره"، ص 185

⁶⁸ عبد الله بن جلوي عبد الله الأبرقي، الضرر في جريمة تزوير المحررات، رسالة ماجستير، كلية الدراسات العليا، قسم

العدالة الجنائية، 2007-2008 ص 30

⁶⁹ المرجع نفسه ص 31-32

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

4- الشهادات والوثائق الإدارية المستخرجة إلكترونياً.

5- السجلات التجارية الإلكترونية.

6- الأوامر البنكية الإلكترونية.

7- الأحكام والسجلات القضائية الإلكترونية.

8- الوثائق البيومترية الرقمية.

كما تمت الحماية القانونية إلى التوقيع الإلكتروني الذي يعد جزءاً لا يتجزأ من المحرر الإلكتروني. فقد نصت المادة 5 من القانون رقم 04-15 المؤرخ في 01 فبراير 2015⁷⁰ المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين على أن التوقيع الإلكتروني الموصوف يتمتع بالحجية القانونية ذاتها المقررة للتوقيع الخطي التقليدي. وبناءً عليه، فإن تقليد التوقيع الإلكتروني أو انتحال هوية صاحبه أو تزوير شهادة التصديق الإلكتروني أو التلاعب بمفاتيح التشفير الخاصة به يعد صورة من صور التزوير المعلوماتي لأنه يؤدي إلى نسبة المحرر إلى شخص لم يصدر عنه في الواقع⁷¹.

كما عزز القانون رقم 02-24 المتعلق بمكافحة التزوير واستعمال المزور الحماية الجنائية للمحررات الإلكترونية، خاصة المحررات الرسمية والعمومية. فقد نصت المادة 31 منه على معاقبة كل من يرتكب تزويراً في محرر رسمي أو عمومي، وتمتد هذه الحماية إلى المحررات الإلكترونية الرسمية متى كانت معدة لإثبات حق أو واقعة أو مركز قانوني معين، مثل العقود التوثيقية الإلكترونية والوثائق البيومترية والسجلات الإدارية والقضائية الرقمية.⁷²

وبذلك يتضح أن محل جريمة التزوير المعلوماتي في التشريع الجزائري لا يقتصر على البيانات الرقمية المجردة، وإنما يشمل أيضاً مختلف المحررات الإلكترونية والتوقيعات الرقمية والوثائق الرسمية الإلكترونية،

⁷⁰ وهاب سعيدة، آليات مكافحة جريمة التزوير الإلكتروني، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، جامعة العربي بن مهيدي، سنة 2020-2021، صص 26-27

⁷¹ وهاب سعيدة، آليات مكافحة جريمة التزوير الإلكتروني، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، جامعة العربي بن مهيدي، سنة 2020-2021، صص 42-43

⁷² المرجع نفسه ص 44

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

وهو ما يعكس إرادة المشرع في توفير حماية قانونية شاملة لمختلف عناصر البيئة الرقمية وضمان الثقة في المعاملات الإلكترونية الحديثة⁷³.

المطلب الثالث: القواعد الإجرائية لمكافحة جريمة التزوير المعلوماتي

تستوجب مكافحة جريمة التزوير المعلوماتي اعتماد مجموعة من القواعد والإجراءات القانونية التي تهدف إلى الوقاية منها والكشف عن مرتكبيها ومتابعتهم قضائيا. ونظرا للطبيعة التقنية لهذه الجريمة وما تنشيره من صعوبات في الإثبات، فقد أقر المشرع الجزائري تدابير وقائية وإجراءات جزائية خاصة لضمان حماية البيانات والمحركات الإلكترونية وتعزيز فعالية مكافحتها.

الفرع الأول: الإجراءات الوقائية لمكافحة جريمة التزوير المعلوماتي

أصبحت الوقاية من جريمة التزوير المعلوماتي من المسائل التي تحظى باهتمام متزايد في التشريعات الحديثة، وذلك نتيجة الانتشار الواسع لتكنولوجيا المعلومات والاتصال واعتماد الأفراد والمؤسسات والإدارات العمومية على الأنظمة الإلكترونية في مختلف المعاملات اليومية. فقد أدى هذا التحول الرقمي إلى ظهور مخاطر جديدة تمس سلامة البيانات والمحركات الإلكترونية، وأصبح التلاعب بالمعلومات أو تغييرها أو اصطناعها يتم بوسائل تقنية متطورة يصعب اكتشافها بالوسائل التقليدية.⁷⁴

أولاً: الحماية التشريعية والتنظيمية للبيانات والمحركات الإلكترونية

تعد الحماية التشريعية والتنظيمية من أهم التدابير الوقائية لمكافحة جريمة التزوير المعلوماتي، إذ تهدف إلى توفير إطار قانوني يضمن سلامة البيانات والمحركات الإلكترونية ويحميها من التلاعب أو التغيير غير المشروع. ومع تزايد الاعتماد على الوسائل الرقمية في مختلف المعاملات، أصبح من الضروري إخضاع هذه المحركات لحماية قانونية تكفل الحفاظ على مصداقيتها وقيمتها القانونية.

وقد عمل المشرع الجزائري على مواكبة هذا التطور من خلال سنّ مجموعة من النصوص القانونية التي تنظم المعاملات الإلكترونية وتجرم الأفعال الماسة بالبيانات الرقمية. وفي هذا السياق، جاء القانون رقم

⁷³ براهمي، يوسف. "جريمة التزوير في المحركات الرسمية وفق القانون الجزائري". رسالة ماجستير، جامعة الجزائر 1،

2019. ص22

⁷⁴ محمد الطاهر رجال، "مراجعة التحقيق القضائي في التشريع الجزائري"، مجلة طبنة للدراسات العلمية الأكاديمية، المجلد 5،

العدد 5، 2020. ص224

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

24-02 المتعلق بمكافحة التزوير واستعمال المزور لتعزيز الحماية الجنائية للمحررات الإلكترونية، كما أقر القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين الحجة القانونية للتوقيع الإلكتروني، بينما وضع القانون رقم 09-04 آليات خاصة للوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها وتتجلى هذه الحماية في عدة مظاهر أهمها⁷⁵:

- 1- تجريم التزوير الواقع على البيانات والمحررات الإلكترونية: من خلال معاقبة كل صور تغيير الحقيقة أو التلاعب بالمعلومات الرقمية.
- 2- الاعتراف بالحجة القانونية للمحررات الإلكترونية: بما يضمن الثقة في المعاملات المنجزة عبر الوسائط الرقمية.
- 3- تنظيم التوقيع والتصديق الإلكترونيين: لحماية هوية المتعاملين وضمان صحة المحررات الإلكترونية.
- 4- حماية الأنظمة المعلوماتية وقواعد البيانات: عبر وضع قواعد قانونية تمنع الولوج غير المشروع والتعدي على المعلومات⁷⁶.

ومن ثم، تشكل الحماية التشريعية والتنظيمية الأساس القانوني الذي تقوم عليه الوقاية من جريمة التزوير المعلوماتي، من خلال توفير بيئة رقمية آمنة وتعزيز الثقة في المعاملات الإلكترونية.

ثانيا: تأمين الأنظمة المعلوماتية وقواعد البيانات الإلكترونية

يشكل تأمين الأنظمة المعلوماتية وقواعد البيانات الإلكترونية إحدى أهم الوسائل الوقائية للحد من جريمة التزوير المعلوماتي، باعتبار أن هذه الجريمة ترتبط في الغالب بالوصول غير المشروع إلى الأنظمة الإلكترونية والتلاعب بالمعلومات المخزنة داخلها. فكلما كانت الأنظمة المعلوماتية مؤمنة بصورة جيدة، تراجعت فرص اختراقها أو استغلالها في تغيير البيانات أو اصطناع محررات إلكترونية مزورة.

ولهذا تعمل المؤسسات والإدارات على اعتماد مجموعة من الوسائل التقنية التي تهدف إلى حماية المعلومات وضمان سلامتها من أي تعديل غير مشروع. وتشمل هذه الوسائل استخدام برامج الحماية من

⁷⁵ براهيمي يوسف. المرجع السابق ذكره. ص24

⁷⁶ براهيمي يوسف. المرجع السابق ذكره. ص24

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

الفيروسات والبرمجيات الخبيثة، وتفعيل جدران الحماية الإلكترونية، واعتماد أنظمة التشفير التي تمنع الوصول إلى البيانات أو الاطلاع عليها من قبل أشخاص غير مخولين⁷⁷.

كما تعتمد العديد من الهيئات على أنظمة مراقبة الشبكات وكشف محاولات الاختراق، إلى جانب وضع ضوابط دقيقة للتحكم في صلاحيات المستخدمين، بحيث يقتصر الوصول إلى المعلومات الحساسة على الأشخاص المخولين قانوناً ووظيفياً. ويساهم ذلك في الحد من مخاطر التلاعب بالبيانات أو تغيير محتواها دون ترخيص.

وتتجلى أهمية هذه التدابير فيما توفره من حماية لسلامة المعلومات ومصداقيتها، إذ تساعد على اكتشاف أي محاولة للاعتداء على الأنظمة المعلوماتية في مراحلها الأولى، كما تضمن تتبع العمليات المنجزة على البيانات ومعرفة الجهة التي قامت بها. ولهذا أصبح الأمن المعلوماتي اليوم ضرورة أساسية لحماية المعاملات الإلكترونية والوقاية من مختلف صور التزوير المعلوماتي. ويمكن إبراز أهم مظاهر تأمين الأنظمة المعلوماتية وقواعد البيانات الإلكترونية فيما يأتي⁷⁸:

- 1- استعمال برامج الحماية والتشفير الإلكتروني: لحماية البيانات من الاختراق أو التعديل غير المشروع، وضمان سريتها أثناء التخزين أو التداول عبر الشبكات.
- 2- مراقبة الشبكات وكشف محاولات الاختراق: من خلال أنظمة الرصد والمتابعة المستمرة للأنشطة المشبوهة والتنبيه إلى أي محاولة للوصول غير المشروع إلى المعلومات.
- 3- تنظيم صلاحيات الوصول إلى المعلومات: عبر تقييد الاطلاع على البيانات وتعديلها بالأشخاص المخولين فقط، وفقاً لطبيعة المهام الموكلة إليهم.
- 4- حماية قواعد البيانات والنسخ الاحتياطي للمعلومات: لضمان استمرارية البيانات والمحافظة عليها من الضياع أو الإتلاف أو التلاعب، وتمكين المؤسسات من استرجاعها عند الحاجة.

⁷⁷ محمد الطاهر رحال، المرجع السابق ذكره ص.ص 225-22

⁷⁸ محمد الطاهر رحال، "المرجع السابق ذكره ص ص 225-226

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

ومن ثم، يعد تأمين الأنظمة المعلوماتية وقواعد البيانات خط الدفاع الأول في مواجهة جريمة التزوير المعلوماتي، لما يوفره من حماية تقنية فعالة تحول دون الوصول غير المشروع إلى المعلومات أو تغييرها، وتساهم في تعزيز الثقة في البيئة الرقمية والمعاملات الإلكترونية⁷⁹.

ثالثا: اعتماد التوقيع الإلكتروني والرقمنة المؤمنة للمعاملات

يعد التوقيع الإلكتروني من أهم الوسائل الحديثة التي تساهم في الوقاية من جريمة التزوير المعلوماتي، لما يوفره من ضمانات تتعلق بالتحقق من هوية صاحب المحرر الإلكتروني والتأكد من سلامة محتواه. فبمجرد توقيع الوثيقة إلكترونيا يصبح من السهل اكتشاف أي تعديل أو تغيير يطرأ عليها، وهو ما يحد من إمكانيات التلاعب بالمحررات الإلكترونية أو اصطناعها بطرق غير مشروعة.

وقد نظم المشرع الجزائري هذه الآلية بموجب القانون رقم 15-04 المؤرخ في 01 فيفري 2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، حيث منح التوقيع الإلكتروني الحجية القانونية اللازمة وجعله وسيلة معترف بها في الإثبات، مما ساهم في تعزيز الثقة في المعاملات الإلكترونية وحماية أطرافها من مختلف صور التزوير⁸⁰.

ومن جهة أخرى، ساهمت الرقمنة في تعزيز الوقاية من التزوير المعلوماتي من خلال استبدال الوثائق الورقية التقليدية بالوثائق والبيانات الإلكترونية المحفوظة داخل أنظمة معلوماتية مؤمنة. وتسمح هذه الأنظمة بتسجيل مختلف العمليات التي تجرى على البيانات، مع تحديد تاريخ كل عملية وهوية الشخص الذي قام بها، الأمر الذي يسهل مراقبة المعاملات والكشف عن أي محاولة للتلاعب أو تغيير الحقيقة.

وتتجسد أهمية التوقيع الإلكتروني والرقمنة في الوقاية من التزوير المعلوماتي من خلال ما يأتي⁸¹:

- 1- **التحقق من هوية صاحب المحرر الإلكتروني:** بما يضمن نسبة الوثيقة إلى صاحبها الحقيقي ويحد من حالات انتحال الهوية.

⁷⁹براهيمي يوسف. المرجع السابق ذكره. ص26

⁸⁰براهيمي يوسف. المرجع السابق ذكره. ص28

⁸¹أمين، محمد صبحي. "الطبعة القانونية لجريمة التزوير في المحررات الرسمية." مجلة القانون العام الجزائري المقارن،

جامعة جيلالي اليابس، سيدي بلعباس، 2017. صص 201-203

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

2- ضمان سلامة المحررات الإلكترونية: من خلال كشف أي تعديل أو تغيير يطرأ على الوثيقة بعد توقيعها أو حفظها.

3- تعزيز حجية المعاملات الإلكترونية: عبر منحها قيمة قانونية في الإثبات مماثلة للمحررات التقليدية متى استوفت الشروط القانونية.

4- تتبع العمليات المنجزة على البيانات الإلكترونية: بفضل الأنظمة الرقمية التي تسمح بتسجيل مختلف التعديلات والعمليات المنفذة على المعلومات.

ومن ثم، يشكل التوقيع الإلكتروني والرقمنة ركيزتين أساسيتين في منظومة الوقاية من جريمة التزوير المعلوماتي، لما يوفرانه من حماية للبيانات والمحررات الإلكترونية ويسهمان في تعزيز الثقة والأمن داخل البيئة الرقمية⁸².

رابعاً: التكوين والتوعية وتعزيز دور الهيئات المختصة

لا تقتصر الوقاية من جريمة التزوير المعلوماتي على الجوانب القانونية والتقنية فقط، بل تتطلب أيضاً تأهيل العنصر البشري ورفع مستوى الوعي الأمني لدى المستخدمين والموظفين. فكثير من عمليات التزوير الإلكتروني تنجح نتيجة الإهمال أو الجهل بطرق الحماية وأساليب الاحتيال الإلكتروني، مما يجعل التوعية والتكوين من الوسائل الأساسية للوقاية من هذه الجريمة⁸³.

ولهذا تعمل الإدارات والمؤسسات على تنظيم دورات تدريبية وبرامج تكوينية متخصصة لفائدة الموظفين والأعوان المكلفين بمعالجة البيانات الإلكترونية، بهدف تعريفهم بأحدث أساليب التزوير المعلوماتي وطرق اكتشافها. كما تضطلع الهيئات الأمنية والمصالح المختصة بمكافحة الجرائم المعلوماتية بدور مهم في مراقبة الفضاء الرقمي والكشف المبكر عن الأنشطة المشبوهة، استناداً إلى الصلاحيات المخولة لها بموجب القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. وتساهم هذه الهيئات في تعزيز الأمن الرقمي من خلال الرصد والتحليل وتبادل المعلومات

⁸² بن نوارن عبد الرحمن، الإطار القانوني لممارسة الطعن ضد المحررات الرسمية أمام القضاء في التشريع الجزائري،

مجلة الحقوق والعلوم الإسلامية، جامعة الجلفة، الجزائر، العدد 14، أفريل 2021، ص 95

⁸³ براهيم يوسف. "المرجع السابق ذكره ص ص 22

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

والتنسيق مع مختلف الجهات المعنية، بما يحد من فرص وقوع جرائم التزوير المعلوماتي ويعزز حماية المعاملات الإلكترونية⁸⁴.

وعليه، يتضح أن الإجراءات الوقائية لمكافحة جريمة التزوير المعلوماتي تقوم على أربعة محاور رئيسية تتمثل في الحماية التشريعية والتنظيمية للبيانات الإلكترونية، وتأمين الأنظمة المعلوماتية وقواعد البيانات، واعتماد التوقيع الإلكتروني والرقمنة المؤمنة للمعاملات، إضافة إلى التكوين والتوعية وتعزيز دور الهيئات المختصة. وتمثل هذه التدابير منظومة متكاملة تهدف إلى حماية المحررات الإلكترونية وصيانة الثقة العامة في المعاملات الرقمية والحد من مخاطر التزوير قبل وقوعه.

الفرع الثاني: الإجراءات الجزائية لمكافحة التزوير المعلوماتي

إذا كانت الإجراءات الوقائية تهدف إلى الحد من وقوع جريمة التزوير المعلوماتي قبل ارتكابها، فإن الإجراءات الجزائية تتدخل بعد وقوع الجريمة للكشف عن مرتكبيها وجمع الأدلة المتعلقة بها وتقديم الجناة إلى العدالة. وتتميز جريمة التزوير المعلوماتي بخصوصية إجرائية ناتجة عن طبيعتها التقنية واعتمادها على الوسائط الإلكترونية، وهو ما يفرض على السلطات المختصة الاستعانة بوسائل قانونية وفنية حديثة تمكنها من تتبع الجريمة وإثباتها. وقد نظم المشرع الجزائري هذه الإجراءات من خلال قانون الإجراءات الجزائية، إضافة إلى القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والقانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور. وتتم هذه الإجراءات بعدة مراحل تبدأ بالبحث والتحري، ثم التحقيق القضائي، وصولاً إلى المحاكمة وتنفيذ العقوبة⁸⁵.

أولاً: إجراءات البحث والتحري والكشف عن الجريمة

تعد مرحلة البحث والتحري أولى المراحل الإجرائية التي تلي اكتشاف جريمة التزوير المعلوماتي، حيث يتولى ضباط الشرطة القضائية جمع الاستدلالات والبحث عن الأدلة التي تثبت وقوع الجريمة وتحدد هوية مرتكبيها. وتستمد الضبطية القضائية صلاحياتها من المواد 12 وما بعدها من قانون الإجراءات الجزائية،

⁸⁴ محمد الطاهر رحال، "المرجع السابق ذكره ص ص 227

⁸⁵ خليفي فتيحة، ومهداوي محمد صالح، "التزوير المعلوماتي في البيئة الرقمية"، مجلة الدراسات القانونية، المجلد 8، العدد 2، 2022، ص 255-256.

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

والتي تخول لها معاينة الجرائم وجمع الأدلة والبحث عن مرتكبيها وتشمل هذه المرحلة عدة إجراءات أهمها⁸⁶:

1- **معاينة المحررات والبيانات الإلكترونية محل التزوير** يقوم ضباط الشرطة القضائية بمعاينة الوثائق أو البيانات الإلكترونية المشكوك في صحتها، مع اتخاذ التدابير اللازمة للمحافظة عليها ومنع أي تعديل أو إتلاف قد يؤثر على قيمتها الإثباتية. وتعد هذه المعاينة من أهم الإجراءات الأولية لأنها تسمح بتحديد طبيعة التزوير ووسائله.

2- **سماع المشتبه فيهم والشهود** يسمح هذا الإجراء بجمع المعلومات المتعلقة بظروف ارتكاب الجريمة وتحديد الأشخاص المتورطين فيها. ويتم سماع الأشخاص المعنيين وفقا للضمانات القانونية المنصوص عليها في قانون الإجراءات الجزائية، مع احترام حقوق الدفاع وقرينة البراءة .

3- **التفتيش والحجز** خولت المواد 79 إلى 82 من قانون الإجراءات الجزائية لضباط الشرطة القضائية صلاحية القيام بالتفتيش والحجز وفق الشروط القانونية المقررة. وفي جرائم التزوير المعلوماتي قد يشمل التفتيش الحواسيب والهواتف الذكية والخوادم ووسائل التخزين الإلكترونية التي يحتمل احتواؤها على أدلة متعلقة بالجريمة .

4- **التوقيف للنظر** نظم المشرع هذا الإجراء بموجب المواد 51 مكرر وما يليها من قانون الإجراءات الجزائية، حيث يجوز وضع المشتبه فيه تحت تصرف الضبطية القضائية لمدة محددة قانونا لاستكمال التحريات وجمع الأدلة، مع ضرورة احترام جميع الضمانات القانونية المقررة له⁸⁷ .

ثانيا: الوسائل التقنية الحديثة في البحث والتحري

نظرا للطبيعة الإلكترونية لجريمة التزوير المعلوماتي، لم يعد الاعتماد على الوسائل التقليدية كافيا للكشف عنها، لذلك اعتمد المشرع الجزائري مجموعة من الآليات التقنية الحديثة التي تتلاءم مع هذا النوع من الجرائم. ومن أهم هذه الوسائل⁸⁸:

⁸⁶براهمي حنان، جريمة التزوير في الوثيقة الإدارية ذات الطبيعة المعلوماتية، أطروحة مقدمة لنيل شهادة الدكتوراه، إشراف

عمر فرحاتي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2015. ص34

⁸⁷براهمي حنان، المرجع السابق ذكره ص37

⁸⁸المرجع نفسه ص38

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

- 1- **التفتيش الإلكتروني** ويتمثل في فحص الأجهزة والأنظمة المعلوماتية والوسائط الرقمية بحثاً عن البرامج أو الملفات أو البيانات المستعملة في التزوير. ويعد هذا الإجراء امتداداً للتفتيش التقليدي مع مراعاة خصوصية البيئة الرقمية .
- 2- **المراقبة الإلكترونية** أجاز القانون رقم 04-09 اعتماد وسائل المراقبة التقنية وتتبع النشاطات المشبوهة عبر شبكات الاتصال الإلكترونية، وذلك تحت رقابة السلطة القضائية المختصة. وتساعد هذه الوسيلة في كشف الجرائم قبل اكتمالها أو تحديد مرتكبيها بعد وقوعها.
- 3- **الاعتماد على الأدلة الرقمية** تشمل الأدلة الرقمية الرسائل الإلكترونية، والملفات الرقمية، وسجلات الأنظمة وقواعد البيانات، وهي أدلة أصبحت تحظى بأهمية كبيرة في إثبات الجرائم المعلوماتية عموماً وجريمة التزوير المعلوماتي على وجه الخصوص
- 4- **الاستعانة بالخبرة الفنية** يعتبر اللجوء إلى الخبرة الفنية من أهم الوسائل الإجرائية في هذا المجال، حيث يستعين القاضي أو الضبطية القضائية بخبراء متخصصين في الإعلام الآلي وتحليل البيانات الإلكترونية لفحص الوثائق والملفات الرقمية والكشف عن مظاهر التزوير فيها⁸⁹.

ثالثاً: التحقيق القضائي في جرائم التزوير المعلوماتي

بعد انتهاء مرحلة التحريات، تنتقل القضية إلى مرحلة التحقيق القضائي التي يشرف عليها قاضي التحقيق وفقاً للمواد 66 وما يليها من قانون الإجراءات الجزائية. وتتمثل مهمة قاضي التحقيق في جمع الأدلة بصورة معمقة والتحقق من صحة الوقائع المنسوبة إلى المتهمين قبل إحالتهم على جهة الحكم وتتمثل أهم إجراءات التحقيق فيما يلي⁹⁰:

- 1- **استجواب المتهم** يقوم قاضي التحقيق بمواجهة المتهم بالأفعال المنسوبة إليه وتمكينه من تقديم دفاعه، مع احترام حقه في الاستعانة بمحام وفقاً للمواد 100⁹¹ و105⁹² من قانون الإجراءات الجزائية .

⁸⁹ خليفتي فتيحة، ومهداوي محمد صالح، المرجع السابق ذكره ص 259

⁹⁰ خليفتي فتيحة، ومهداوي محمد صالح، المرجع السابق ذكره ص 261

⁹¹ المادة 100، الأمر رقم 66-155، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم (بموجب القانون رقم 24-04 المؤرخ في 26 فبراير 2024) وتنص على : يتثبت قاضي التحقيق عند أول مثول للمتهم أمامه من هويته ويحيطه علماً

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

- 2- سماع الشهود والضحايا يستمع قاضي التحقيق إلى الشهود والمتضررين من الجريمة لتكوين تصور دقيق حول ظروف ارتكابها والنتائج المترتبة عنها .
- 3- إصدار أوامر التفتيش والحجز يجوز لقاضي التحقيق إصدار أوامر بتفتيش الأماكن أو الأنظمة المعلوماتية وحجز الأدوات والوسائط المستعملة في التزوير متى اقتضت ضرورة التحقيق ذلك .
- 4- إجراء الخبرة القضائية تكتسي الخبرة أهمية خاصة في جرائم التزوير المعلوماتي بسبب طبيعتها التقنية، حيث يتم تكليف خبراء مختصين بفحص الأدلة الرقمية والوثائق الإلكترونية وبيان مدى تعرضها للتعديل أو التزوير⁹³ .

رابعاً: المحاكمة وإصدار الأحكام

تمثل المحاكمة المرحلة النهائية للإجراءات الجزائية، حيث تعرض القضية أمام المحكمة المختصة للفصل في مدى ثبوت الجريمة ونسبتها إلى المتهم. وتتم المحاكمة وفقاً للمبادئ الأساسية المنصوص عليها في قانون الإجراءات الجزائية، وعلى رأسها مبدأ علنية الجلسات المنصوص عليه في المادة 285، وحق الدفاع، ومبدأ المواجهة بين الخصوم وخلال المحاكمة يتم⁹⁴:

1- عرض الأدلة ومناقشتها سواء تعلق الأمر بالمحركات الإلكترونية محل التزوير أو بالتقارير الفنية والأدلة الرقمية.

2- سماع الشهود والخبراء من أجل توضيح الجوانب التقنية والقانونية المرتبطة بالجريمة.

بالوقائع المنسوبة إليه وبمناصرتها القانونية، وينبذه بأنه حر في عدم الإدلاء بأي تصريح، وينوه عن هذا التنبيه في المحضر. وإذا أراد المتهم الإدلاء بتصريحات تلقاها قاضي التحقيق فوراً. ويتعين على قاضي التحقيق إخطار المتهم بحقه في اختيار محام عنه، فإن لم يختار محامياً عين له قاضي التحقيق محامياً من تلقاء نفسه بناءً على طلبه، وينوه عن ذلك في المحضر."

⁹² المادة : 105 لا يجوز استجواب المتهم ولا سماع الطرف المدني إلا بحضور محاميها أو بعد استدعاء هذا المحامي قانوناً، ما لم يتنازل المتهم أو الطرف المدني عن ذلك صراحة، وينوه عن هذا التنازل في المحضر. ويستدعى محامي المتهم والطرف المدني بكتاب موصى عليه أو بموجب إشعار يسلم له مقابل وصل، أو بأي وسيلة اتصال مكتوبة أخرى، وذلك قبل يومين (2) على الأقل من تاريخ الاستجواب أو سماع الأقوال. وتوضع ملفات الإجراءات تحت تصرف محامي المتهم قبل كل استجواب بـ أربع وعشرين (24) ساعة على الأقل، كما توضع تحت تصرف محامي الطرف المدني قبل كل سماع لأقواله بنفس الأجل

⁹³ خليفتي فتيحة، ومهداوي محمد صالح، المرجع السابق ذكره ص 264

⁹⁴ محمد الطاهر رحال، "المرجع السابق ذكره ص 259

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

- 3- تقديم مرافعات النيابة والدفاع حيث تعرض النيابة طلباتها بينما يقدم الدفاع دفعه وملاحظاته القانونية.
- 4- إصدار الحكم القضائي بعد المداولة، تصدر المحكمة حكمها إما بالإدانة أو البراءة وفقا لما استقر لديها من أدلة ووقائع .

ومن ثم، يتضح أن الإجراءات الجزائية لمكافحة التزوير المعلوماتي تقوم على منظومة متكاملة تبدأ بالبحث والتحري وجمع الأدلة، مروراً بالتحقيق القضائي المتخصص، وصولاً إلى المحاكمة وتوقيع العقوبات. وقد حرص المشرع الجزائري من خلال قانون الإجراءات الجزائية والقانون رقم 09-04 والقانون رقم 24-02 على تزويد السلطات المختصة بوسائل قانونية وتقنية فعالة تمكنها من مواجهة هذا النوع من الجرائم مع ضمان احترام الحقوق والحريات الأساسية للأفراد⁹⁵.

خلاصة الفصل :

من خلال هذا الفصل تم التطرق إلى جريمة التزوير المعلوماتي باعتبارها من الجرائم المستحدثة المرتبطة بالتطور التكنولوجي والتحول الرقمي. وقد تم توضيح مفهومها من خلال التعريفات الفقهية والقانونية، مع بيان أوجه الاختلاف بينها وبين التزوير التقليدي وبعض الجرائم الإلكترونية المشابهة، بالإضافة إلى إبراز أهم خصائصها التي تميزها عن غيرها من الجرائم.

كما تم تناول الأساس القانوني لهذه الجريمة من خلال دراسة أركانها المتمثلة في الركن المادي والركن المعنوي، مع بيان محل الجريمة الذي يتمثل في البيانات والمحركات الإلكترونية باعتبارها محلاً للحماية

⁹⁵ بن نوارن عبد الرحمن، المرجع السابق ذكره .ص100

الفصل الأول:..... الإطار المفاهيمي لجريمة التزوير المعلوماتي

القانونية. وتم كذلك استعراض القواعد الإجرائية الخاصة بمكافحتها، سواء من خلال التدابير الوقائية الرامية إلى حماية الأنظمة المعلوماتية والحد من فرص التزوير، أو من خلال الإجراءات الجزائية المتعلقة بالبحث والتحري والتحقيق والمحاكمة.

وعليه، يتبين أن المشرع الجزائري سعى إلى توفير إطار قانوني وإجرائي متكامل لمواجهة جريمة التزوير المعلوماتي، بما يضمن حماية الثقة في المعاملات الإلكترونية وصيانة أمن المعلومات، وهو ما يشكل أساسا للانتقال إلى دراسة الجوانب التطبيقية والأحكام القانونية المرتبطة بهذه الجريمة.

**الفصل الثاني: جريمة تزوير المعلومات بين التشريع
الجزائري والمصري**

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

بعد دراسة الإطار المفاهيمي لجريمة التزوير المعلوماتي وبيان طبيعتها القانونية وأركانها والقواعد الإجرائية المتعلقة بمكافحتها، تبرز أهمية الوقوف على موقف التشريعات المقارنة من هذه الجريمة، خاصة في ظل التطور المستمر لوسائل ارتكابها واتساع نطاق آثارها. ويعد كل من التشريع الجزائري والتشريع المصري من التشريعات العربية التي أولت اهتماما متزايدا لمواجهة الجرائم المعلوماتية من خلال سن نصوص قانونية تهدف إلى حماية نظم المعلومات والبيانات الإلكترونية من مختلف صور الاعتداء والتلاعب.

ورغم اتفاق التشريعين على ضرورة تجريم الأفعال التي تمس سلامة ومصداقية البيانات والمحركات الإلكترونية، إلا أن كل منهما اعتمد أسلوبا خاصا في تنظيم أحكام التزوير المعلوماتي وتحديد أركانه والعقوبات المقررة له، وهو ما يقتضي إجراء دراسة مقارنة للكشف عن أوجه الاتفاق والاختلاف بينهما وتقييم مدى فعالية الحماية القانونية التي يوفرها كل تشريع.

وعليه، سيتم في هذا الفصل دراسة التنظيم القانوني لجريمة التزوير المعلوماتي في كل من التشريع الجزائري والتشريع المصري، ثم إبراز أوجه التشابه والاختلاف بينهما، وصولا إلى تقييم الأحكام القانونية المعمول بها واقتراح بعض الحلول الكفيلة بتعزيز مكافحة هذه الجريمة ومواكبة التطورات التقنية الحديثة.

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

المبحث الأول: التنظيم القانوني لجريمة التزوير المعلوماتي في التشريع المصري

اهتم المشرع المصري بمواجهة الجرائم المرتبطة بالبيئة الرقمية من خلال وضع منظومة قانونية تتلاءم مع التطور التكنولوجي وما نتج عنه من صور مستحدثة للاعتداء على البيانات والمحركات الإلكترونية. وتجسد ذلك من خلال سن نصوص خاصة تجرم التزوير المعلوماتي وتحدد أركانه وعقوباته وإجراءات متابعته. وعليه يقتضي بيان التنظيم القانوني لهذه الجريمة الوقوف على الأساس التشريعي الذي يحكمها والأحكام الموضوعية والإجرائية المقررة لمكافحتها¹.

المطلب الأول: الأساس التشريعي لتجريم التزوير المعلوماتي في القانون المصري

شهدت مصر خلال العقود الأخيرة تطورا ملحوظا في مجال استخدام وسائل الاتصال والتقنيات الرقمية، وهو ما أدى إلى ظهور أنماط جديدة من الجرائم التي تستهدف البيانات والمحركات الإلكترونية. وقد فرض هذا الواقع على المشرع المصري ضرورة تحديث المنظومة القانونية بما يضمن توفير الحماية الجنائية للمعاملات الإلكترونية ومواجهة صور الاعتداء التي تتم عبر النظم المعلوماتية. وتجسد ذلك من خلال تبني سياسة تشريعية متدرجة بدأت بالاعتماد على النصوص التقليدية الواردة في قانون العقوبات، ثم انتقلت إلى إصدار تشريعات خاصة تتلاءم مع خصوصية البيئة الرقمية، وعلى رأسها قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018². وعليه يقتضي بيان الأساس التشريعي لتجريم التزوير المعلوماتي الوقوف على تطور السياسة الجنائية المصرية في هذا المجال، ثم استعراض الأحكام التي تضمنها قانون مكافحة جرائم تقنية المعلومات، وأخيرا بيان العلاقة بينه وبين أحكام قانون العقوبات³.

الفرع الأول : تطور السياسة الجنائية المصرية في مواجهة الجرائم المعلوماتية

شهدت السياسة الجنائية المصرية تطورا ملحوظا في مجال مكافحة الجرائم المعلوماتية نتيجة التقدم التكنولوجي المتسارع واتساع نطاق استخدام الحاسوب وشبكات الإنترنت في مختلف مجالات الحياة. وقد فرض هذا التطور تحديات جديدة أمام المنظومة القانونية التقليدية التي لم تكن مهيأة لمواجهة الأفعال

¹ إبراهيم الديب حسانين زايد، "جريمة التزوير المعلوماتية: دراسة مقارنة في القانون الفرنسي والمصري والعراقي"، مجلة جامعة البيان للدراسات والبحوث القانونية، المجلد 4، العدد 1، جامعة البيان، العراق، ص. 555

² قانون رقم 175 لسنة 2018 الصادر في 14 أغسطس 2018 والمتعلق بمكافحة جرائم تقنية المعلومات، نُشر في الجريدة الرسمية لجمهورية مصر العربية بالعدد 32 مكرر (أ) الصادر بتاريخ 14 أغسطس 2018.

³ إبراهيم الديب حسانين زايد، "المرجع السابق ذكره"، ص. 556

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

الإجرامية المرتكبة في البيئة الرقمية، الأمر الذي دفع المشرع المصري إلى تبني سياسة تشريعية متدرجة انتقلت من الاعتماد على القواعد العامة إلى إقرار تنظيم قانوني متخصص لمكافحة الجرائم المعلوماتية¹.

1- مرحلة الاعتماد على القواعد العامة في قانون العقوبات

في المرحلة الأولى، لم يكن التشريع المصري يتضمن نصوصاً خاصة بالجرائم المعلوماتية، ولذلك كانت جهات القضاء تلجأ إلى تطبيق الأحكام العامة الواردة في قانون العقوبات رقم 58 لسنة 1937² لمحاولة مواجهة الأفعال المرتكبة باستخدام الوسائط الإلكترونية. غير أن هذا الاتجاه واجه عدة صعوبات عملية وقانونية بسبب اختلاف طبيعة الجرائم المعلوماتية عن الجرائم التقليدية.

ففي جريمة السرقة، يشترط القانون أن يكون محل الجريمة مالا منقولاً مملوكاً للغير، بينما تتمثل البيانات والمعلومات الإلكترونية في عناصر غير مادية يمكن نسخها أو نقلها دون فقدان صاحبها الأصلي لحيازتها، وهو ما أثار إشكالات بشأن إمكانية اعتبارها محلاً للسرقة بالمعنى التقليدي.

كما واجه تطبيق أحكام التزوير صعوبات مماثلة، إذ ارتبط مفهوم المحرر في التشريع التقليدي بالدعامة الورقية وما تتضمنه من كتابة وتوقيع ظاهر، في حين أن المحررات الإلكترونية تتخذ شكلاً رقمياً غير قابل للإدراك المباشر دون الاستعانة بوسائل تقنية، الأمر الذي أثار جدلاً حول مدى خضوعها للحماية الجنائية المقررة للمحررات التقليدية.

أما بالنسبة لجريمة النصب، فقد استندت أحكامها إلى فكرة استعمال وسائل احتيالية للتأثير في إرادة المجني عليه والاستيلاء على ماله، بينما قد يقع الخداع في الجرائم المعلوماتية على نظام معلوماتي أو برنامج إلكتروني دون تدخل مباشر لشخص طبيعي، مما جعل النصوص التقليدية عاجزة عن استيعاب بعض صور الإجرام المستحدثة³.

2- مرحلة الاعتراف القانوني بالمحررات الإلكترونية

¹ إبراهيم الديب حسانين زايد، "المرجع السابق ذكره"، ص. 557

² قانون العقوبات رقم 58 لسنة 1937، الصادر بتاريخ 31 يوليو 1937، والمنشور في الوقائع المصرية بالعدد رقم (71) بتاريخ 5 أغسطس 1937، والمعمول به اعتباراً من 15 أكتوبر 1937.

³ أحمد أمين، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، دون تاريخ نشر. ص. 68

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

أمام تزايد الاعتماد على المعاملات الإلكترونية والتوسع في استخدام وسائل الاتصال الحديثة، اتجه المشرع المصري إلى إرساء أساس قانوني للمحررات والتوقيعات الإلكترونية من خلال إصدار قانون التوقيع الإلكتروني رقم 15 لسنة 2004¹.

وقد شكل هذا القانون خطوة مهمة في تطور السياسة الجنائية المصرية، إذ اعترف بالحجية القانونية للمحررات الإلكترونية والتوقيعات الرقمية متى استوفت الشروط الفنية والقانونية المقررة. كما ساهم في تجاوز النظرة التقليدية للمحرر، فلم يعد مرتبطاً حصراً بالدعامة الورقية، بل أصبح يشمل المحررات المنشأة أو المخزنة أو المتداولة إلكترونياً.

وأدى هذا الاعتراف التشريعي إلى توفير أساس قانوني لحماية المحررات الإلكترونية من مختلف صور الاعتداء، بما فيها أفعال التزوير والتلاعب بالبيانات، ومهد الطريق أمام تطوير منظومة قانونية أكثر تخصصاً لمواجهة الجرائم المعلوماتية².

3- مرحلة التشريع المتخصص لمكافحة الجرائم المعلوماتية

مع تزايد المخاطر الناجمة عن الجرائم الإلكترونية واتساع آثارها الاقتصادية والأمنية والاجتماعية، تبنى المشرع المصري سياسة جنائية أكثر تخصصاً بإصدار قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، الذي يعد الإطار التشريعي الرئيسي لمواجهة الجرائم المرتكبة عبر الوسائط الرقمية.

وقد تميز هذا القانون بتوسيع نطاق الحماية الجنائية ليشمل الأنظمة المعلوماتية وقواعد البيانات والمواقع الإلكترونية والحسابات الرقمية، كما جرم العديد من الأفعال المستحدثة مثل الدخول غير المشروع إلى الأنظمة المعلوماتية، والاعتداء على سلامة البيانات الإلكترونية، وإتلاف أو تعديل أو محو المعلومات المخزنة، فضلاً عن الجرائم الماسة بالحياة الخاصة عبر شبكة الإنترنت.

ولم يقتصر دور القانون على الجانب الموضوعي، بل تضمن أيضاً قواعد إجرائية خاصة تتلاءم مع طبيعة الدليل الرقمي، حيث أقر حجية الأدلة المستخرجة من النظم والأجهزة المعلوماتية متى تم جمعها وفقاً للضوابط القانونية والفنية المقررة. كما ألزم مقدمي خدمات الاتصالات بحفظ بعض البيانات التقنية

¹ قانون تنظيم التوقيع الإلكتروني رقم 15 لسنة 2004، الصادر عن رئيس الجمهورية بتاريخ 21 أبريل 2004، والمنشور في الجريدة الرسمية بجمهورية مصر العربية في العدد رقم 17 تابع (د) بتاريخ 22 أبريل 2004، والمعمول به اعتباراً من 23 أبريل 2004 (اليوم التالي لتاريخ نشره).

² إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، الدار الجامعية الجديدة، الإسكندرية، 2008، ص 44

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

لفترات محددة لتسهيل أعمال البحث والتحري والكشف عن مرتكبي الجرائم المعلوماتية، ومنح السلطات المختصة صلاحيات اتخاذ التدابير اللازمة لمواجهة المواقع والأنشطة الإلكترونية غير المشروعة¹.

ومن خلال هذا التطور التشريعي يتضح أن السياسة الجنائية المصرية انتقلت من مرحلة الاعتماد على النصوص التقليدية غير الكافية لمواجهة الجرائم المعلوماتية إلى مرحلة التشريع المتخصص الذي يواكب التحولات الرقمية ويوفر حماية جنائية أكثر فعالية للبيئة الإلكترونية، بما ينسجم مع متطلبات الأمن المعلوماتي والتطور التكنولوجي المعاصر.

الفرع الثالث: الأحكام الواردة في قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018

يعد قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 الإطار التشريعي الأساسي الذي اعتمده المشرع المصري لمواجهة الجرائم المعلوماتية، حيث جاء استجابة للتطور المتسارع في مجال تكنولوجيا المعلومات والاتصالات وما نتج عنه من ظهور أنماط جديدة من السلوك الإجرامي تستهدف البيانات والأنظمة المعلوماتية والمحركات الإلكترونية. وقد هدف القانون إلى توفير حماية جنائية شاملة للفضاء الرقمي من خلال وضع قواعد موضوعية وإجرائية تتلاءم مع طبيعة الجرائم الإلكترونية².

أ- التعريفات القانونية وتحديد نطاق الحماية الجنائية

استهل المشرع المصري القانون بمجموعة من التعريفات الواردة في المادة الأولى، وذلك بغرض ضبط المفاهيم التقنية التي يقوم عليها التنظيم القانوني للجرائم المعلوماتية. فقد عرف البيانات والمعلومات الإلكترونية بأنها كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو نقله أو مشاركته باستخدام وسائل تقنية المعلومات، كما عرف النظام المعلوماتي والموقع الإلكتروني والحساب الخاص³.

وتكتسي هذه التعريفات أهمية بالغة لأنها تحدد محل الحماية الجنائية وتزيل اللبس الذي قد يثور بشأن نطاق تطبيق القانون، كما تساهم في توحيد التفسير القضائي للنصوص القانونية المتعلقة بالجرائم الإلكترونية. وبذلك أصبحت البيانات والمعلومات الإلكترونية تتمتع بحماية قانونية مستقلة باعتبارها محلا للاعتداء الجنائي شأنها شأن الأموال والمحركات التقليدية⁴.

¹ أحمد أمين، المرجع السابق ذكره ص.ص 70-71

² المرجع نفسه ص 72

³ إيهاب فوزي السقا، المرجع السابق ذكره ص.ص 48-49

⁴ إيهاب فوزي السقا، المرجع السابق ذكره ص. 51

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

ب- تجريم الاعتداء على الأنظمة المعلوماتية والبيانات الإلكترونية

حرص المشرع على حماية الأنظمة المعلوماتية من مختلف صور الاعتداء التي قد تهدد أمنها أو تعرقل أداء وظائفها. ولذلك جرم الدخول غير المشروع إلى المواقع والحسابات والأنظمة المعلوماتية وفقاً للمادة 14 من القانون¹، سواء كان هذا الدخول بغرض الاطلاع على البيانات أو الحصول عليها أو تعديلها أو إتلافها.

كما نصت المادة 17² على تجريم كل فعل يؤدي إلى إتلاف البيانات أو المعلومات الإلكترونية أو محوها أو تعديلها أو نسخها أو إعادة نشرها دون وجه حق. ويهدف هذا التجريم إلى المحافظة على سلامة البيانات الإلكترونية وضمان استقرار المعاملات التي تعتمد عليها، خاصة في ظل تزايد الاعتماد على الوسائل الرقمية في مختلف الأنشطة الاقتصادية والإدارية³.

ويعكس هذا الاتجاه إدراك المشرع لأهمية البيانات الإلكترونية باعتبارها أحد أهم عناصر الثروة المعلوماتية التي تستوجب الحماية الجنائية من أي اعتداء غير مشروع.

ت- حماية المحررات الإلكترونية من التزوير والانتحال

يعد هذا الجانب من أكثر الأحكام ارتباطاً بجريمة التزوير المعلوماتي، إذ سعى المشرع إلى توفير حماية جنائية للمحررات الإلكترونية التي أصبحت تؤدي الدور ذاته الذي تؤديه المحررات التقليدية في إثبات الحقوق والالتزامات.

وفي هذا الإطار جرم القانون اصطناع المواقع الإلكترونية أو الحسابات الخاصة أو البريد الإلكتروني ونسبتها كذبا إلى شخص طبيعي أو معنوي، وهو ما نصت عليه المادة 24 من القانون. كما شدد العقوبة

¹ المادة 14 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 تنص على الآتي: "يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمداً، أو دخل بخطأ غير عمدي واستمر متواجداً، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول، في موقع أو حساب خاص أو نظام معلوماتي تدار بمعرفة جهة ما."

² المادة 17 تنص على الآتي: "يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو أبطأ أو شوّه أو مَحَطَّ أو غيّر تصميم موقع أو حساب خاص أو نظام معلوماتي أو بريد إلكتروني مُدار بمعرفة جهة ما."

³ إيهاب فوزي السقا، المرجع السابق ذكره ص. 53.

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

إذا استعمل الحساب أو الموقع المزور في الإساءة إلى صاحبه أو المساس بشرفه أو اعتباره أو الإضرار بمصالحه¹.

وتشمل الحماية القانونية كذلك مختلف صور التلاعب بالبيانات الإلكترونية التي تؤدي إلى تغيير الحقيقة في محرر إلكتروني أو مستند رقمي، سواء تم ذلك بإدخال بيانات غير صحيحة أو حذف بيانات صحيحة أو تعديلها بصورة تؤثر في مضمون المحرر وآثاره القانونية. ومن ثم يشكل هذا القانون أحد أهم الأسس التشريعية التي يستند إليها تجريم التزوير المعلوماتي في مصر.

ث - حماية الحياة الخاصة والبيانات الشخصية

لم تقتصر الحماية التي أقرها القانون على الأنظمة والبيانات الإلكترونية فحسب، بل امتدت أيضا إلى حماية خصوصية الأفراد داخل البيئة الرقمية. فقد نصت المادة 25 على تجريم الاعتداء على حرمة الحياة الخاصة باستخدام وسائل تقنية المعلومات، بما في ذلك نشر أو تداول الصور أو البيانات أو المعلومات الشخصية دون موافقة أصحابها.

كما جرم المشرع إرسال الرسائل الإلكترونية بكثافة دون موافقة المتلقي، ونشر المحتويات التي تنتهك الخصوصية أو تمس الحياة الخاصة للأفراد. ويهدف ذلك إلى حماية الحقوق الشخصية للمستخدمين وضمان عدم استغلال الوسائل التقنية في الإضرار بسمعته أو المساس بحرياتهم الفردية².

ج - تشديد العقوبات في الجرائم الماسة بالأمن القومي

انتهج المشرع المصري سياسة جنائية صارمة في مواجهة الجرائم المعلوماتية التي تمس المصالح الحيوية للدولة، فنص في المادة 34³ على تشديد العقوبات إذا ارتكبت الجرائم ضد المواقع أو الأنظمة المعلوماتية التابعة للجهات الحكومية أو الهيئات العامة أو المؤسسات ذات الأهمية الاستراتيجية.

¹ د. طه عثمان المغربي، "تزوير المحررات الإلكترونية"، مجلة البحوث القانونية والاقتصادية، العدد 72، سنة 2020، ص 158.

² إيهاب فوزي السقا، المرجع السابق ذكره ص 56.

³ المادة 34 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 (والمدرجة تحت الفصل السادس الخاص بـ الظروف المشددة في الجريمة) تنص على الآتي: "إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر، أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعي تكون العقوبة السجن المشدد".

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

كما تتشدد العقوبة إذا ترتب على الجريمة الإضرار بالأمن القومي أو بالمصالح الاقتصادية أو بالمرافق الحيوية للدولة. وقد تصل العقوبات في هذه الحالات إلى السجن المشدد والغرامات المالية المرتفعة، وهو ما يعكس خطورة الاعتداء على البنية التحتية الرقمية للدولة¹.

ح- المسؤولية الجنائية للشخص الاعتباري

من أبرز المستجدات التي جاء بها القانون إقراره للمسؤولية الجنائية للشخص الاعتباري، وذلك لمواجهة الجرائم المعلوماتية التي قد ترتكب في إطار نشاط الشركات والمؤسسات.

فقد نصت المادة 36² على معاقبة المسؤول عن الإدارة الفعلية للشخص الاعتباري إذا ثبت علمه بوقوع الجريمة أو إذا كان ارتكابها نتيجة إخلاله الجسيم بواجبات الإشراف والرقابة. كما أجاز القانون توقيع جزاءات على الشخص الاعتباري ذاته، من بينها الغرامة والمصادرة ووقف النشاط أو إلغاء الترخيص أو الحل في بعض الحالات.

ويهدف هذا التنظيم إلى منع استغلال الشخصية المعنوية كوسيلة للإفلات من المسؤولية الجنائية وضمان التزام المؤسسات بالقواعد القانونية المتعلقة بأمن المعلومات³.

خ- الأحكام الإجرائية الخاصة بالتحقيق والإثبات

إدراكا من المشرع لخصوصية الجرائم المعلوماتية وطبيعة الأدلة الرقمية، فقد تضمن القانون مجموعة من الأحكام الإجرائية الخاصة التي تسهل اكتشاف هذه الجرائم وإثباتها.

فقد نصت المادة 11⁴ على منح الأدلة الرقمية المستمدة من الأجهزة والأنظمة والشبكات المعلوماتية الحجية القانونية المقررة للأدلة الجنائية متى تم الحصول عليها وفقا للضوابط الفنية والقانونية المحددة.

¹ د. طه عثمان المغربي المرجع السابق ذكره ص ص 160-161

² المادة 36 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 (والمدرجة تحت الباب الخامس الخاص بـ المسؤولية الجنائية للأشخاص الاعتبارية) تنص على الآتي: معاقبة المسؤول عن الإدارة الفعلية للشخص الاعتباري بذات عقوبة الفاعل الأصلي إذا ارتكبت جريمة تقنية باسمه ولحسابه، مع علمه بها أو تسهيله لها.

³ إيهاب فوزي السقا، المرجع السابق ذكره ص 62

⁴ المادة 11 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 (والمدرجة تحت الباب الرابع الخاص بـ الأحكام الإجرائية وحجية الدليل الرقمي) تنص على الآتي: "يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

كما ألزمت المادة الثانية مقدمي خدمات الاتصالات والإنترنت بحفظ بيانات الاستخدام لمدة مائة وثمانين يوما وتقديمها للسلطات المختصة عند الطلب.

ومن جهة أخرى، منحت المادة السابعة جهات التحقيق سلطة طلب حجب المواقع الإلكترونية التي تستخدم في ارتكاب الجرائم المعلوماتية أو التي تشكل تهديدا للأمن القومي، بما يوفر وسيلة فعالة لمواجهة المخاطر الناجمة عن إساءة استخدام الفضاء الإلكتروني¹.

وعليه، يتضح أن قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 قد أرسى منظومة قانونية متكاملة لمكافحة الجرائم المعلوماتية، من خلال الجمع بين الأحكام الموضوعية التي تجرم مختلف صور الاعتداء على البيئة الرقمية، والأحكام الإجرائية التي تضمن فعالية البحث والتحقيق والإثبات، وهو ما جعله الركيزة الأساسية لحماية البيانات والمحركات الإلكترونية ومواجهة جرائم التزوير المعلوماتي في التشريع المصري².

الفرع الثالث: العلاقة بين قانون العقوبات وقانون مكافحة جرائم تقنية المعلومات

تقوم العلاقة بين قانون العقوبات المصري وقانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 على أساس التكامل التشريعي، حيث لا يعد أي منهما بديلا عن الآخر، وإنما يشكلان معا منظومة قانونية متكاملة تهدف إلى توفير الحماية الجنائية للحقوق والمصالح التي قد تتعرض للاعتداء في البيئة الرقمية. وقد فرضت الطبيعة الخاصة للجرائم المعلوماتية على المشرع المصري استحداث نصوص خاصة تتلاءم مع خصائصها التقنية، مع الإبقاء على دور القواعد العامة الواردة في قانون العقوبات باعتبارها الإطار المرجعي للمسؤولية الجنائية³.

أ- تطبيق مبدأ تكامل النصوص العامة والخاصة

الوسائط الإلكترونية، أو النظام المعلوماتي أو برامج الحاسب، أو من أي وسيلة لتقنية المعلومات ذات الحجية القانونية للأدلة الجنائية المادية في الإثبات الجنائي متى استوفت الشروط والمعايير الفنية الواردة باللائحة التنفيذية لهذا القانون.¹ بن لعربي أسماء، والفحمة مديحة، "التزوير المعلوماتي في عصر الرقمنة: بين قابلية الخضوع للقواعد العامة وضرورة تبني نصوص خاصة"، مجلة الفكر القانوني والسياسي، المجلد الثامن، العدد الثاني، 2024، ص ص 449-450

² عواد، حامد هادي عواد، صور وأنماط الجرائم المستحدثة في القانون الجنائي، أطروحة دكتوراه في الحقوق، قسم القانون الجنائي، كلية الحقوق، جامعة المنصورة، 2026، ص 58

³ عواد، حامد هادي عواد، المرجع السابق ذكره ص 62

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

يخضع تنظيم الجرائم المعلوماتية في مصر للقاعدة القانونية التي تقضي بأن الخاص يقيد العام، وهو ما يعني أولوية تطبيق أحكام قانون مكافحة جرائم تقنية المعلومات كلما وجد نص خاص يعالج الفعل الإجرامي المرتكب ويحدد العقوبة المقررة له. أما في الحالات التي لا يتضمن فيها القانون الخاص حكما صريحا، فيرجع إلى الأحكام العامة الواردة في قانون العقوبات رقم 58 لسنة 1937¹.

ويترتب على ذلك استمرار سريان القواعد العامة المتعلقة بالشروع والمساهمة الجنائية والاشتراك والعود والظروف المشددة والأعذار القانونية وأسباب الإباحة وموانع المسؤولية الجنائية، ما لم يرد نص خاص يخالفها. وبذلك يشكل قانون العقوبات الأساس العام الذي تستند إليه السياسة الجنائية المصرية، في حين يمثل قانون مكافحة جرائم تقنية المعلومات تشريعا خاصا يهدف إلى مواجهة صور الإجرام المستحدثة في البيئة الرقمية².

ب- التكامل التشريعي في جريمة التزوير المعلوماتي

تظهر العلاقة التكاملية بين القانونين بصورة واضحة في جريمة التزوير المعلوماتي، إذ إن أحكام التزوير الواردة في المواد من 211 إلى 215 من قانون العقوبات وضعت أساسا لحماية المحررات الرسمية والعرفية التقليدية. غير أن التطور التكنولوجي أدى إلى ظهور المحررات الإلكترونية التي تؤدي الوظائف ذاتها التي تؤديها المحررات الورقية.

ولمواجهة هذا التطور، اعترف المشرع المصري بالمحررات الإلكترونية والتوقيعات الرقمية بموجب قانون التوقيع الإلكتروني رقم 15 لسنة 2004، ثم وفر لها حماية جنائية إضافية من خلال قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 الذي جرم الدخول غير المشروع إلى الأنظمة المعلوماتية والاعتداء على البيانات الإلكترونية وتعديلها أو إتلافها³.

وبناء على ذلك، إذا قام شخص باختراق قاعدة بيانات جهة حكومية وتعديل بيانات رسمية مخزنة إلكترونيا، فإن فعله قد يشكل جريمة دخول غير مشروع وفقا للمادة 14 من قانون مكافحة جرائم تقنية المعلومات، كما قد يشكل اعتداء على سلامة البيانات الإلكترونية وفقا للمادة 17 من القانون نفسه، وفي

¹ المرجع نفسه ص 62-63

² المرجع نفسه ص 64

³ مجيد سحر فؤاد، الجرائم المستحدثة: دراسة معمقة ومقارنة في عدة جرائم، الطبعة الأولى، المركز العربي للنشر والتوزيع، جمهورية مصر العربية، 2019، ص 37

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

الوقت ذاته يمكن أن تقوم جريمة التزوير متى ترتب على هذا التعديل تغيير الحقيقة في محرر إلكتروني له حجية قانونية. ومن ثم تتحقق الحماية الجنائية من خلال تضافر أحكام قانون العقوبات وقانون مكافحة جرائم تقنية المعلومات وقانون التوقيع الإلكتروني¹.

ت - التكامل الإجرائي في مجال الإثبات والتحقيق

لا يقتصر التكامل بين القانونين على الجانب الموضوعي، وإنما يمتد كذلك إلى الجانب الإجرائي. فقد استحدث قانون مكافحة جرائم تقنية المعلومات قواعد خاصة تتعلق بجمع الأدلة الرقمية وحفظها وإضفاء الحجية القانونية عليها، حيث نصت المادة 11 على الاعتراف بالأدلة المستمدة من الأجهزة والنظم والشبكات المعلوماتية متى تم الحصول عليها وفقا للضوابط الفنية والقانونية المقررة².

ومع ذلك، فإن هذه الأحكام لا تلغي وسائل الإثبات التقليدية المنصوص عليها في قانون الإجراءات الجنائية، بل تكملها. فإلى جانب الدليل الرقمي يمكن الاستناد إلى الاعتراف وشهادة الشهود والمعاينة والخبرة الفنية وغيرها من وسائل الإثبات المشروعة. ويؤدي اجتماع هذه الأدلة إلى تكوين اقتناع القاضي الجنائي وتمكينه من الوصول إلى الحقيقة القضائية بشأن الواقعة الإجرامية.

ومن ثم فإن مكافحة التزوير المعلوماتي في التشريع المصري تقوم على تكامل موضوعي وإجرائي بين أحكام قانون العقوبات وقانون مكافحة جرائم تقنية المعلومات، بما يضمن توفير حماية قانونية فعالة للمحررات والبيانات الإلكترونية ومواكبة التطورات المتسارعة في مجال تكنولوجيا المعلومات³.

المطلب الثاني: الأحكام الموضوعية لجريمة التزوير المعلوماتي في القانون المصري

بعد أن بينا الأساس التشريعي الذي اعتمده المشرع المصري لمواجهة الجرائم المعلوماتية بصفة عامة، تبرز أهمية دراسة الأحكام الموضوعية المنظمة لجريمة التزوير المعلوماتي بصفة خاصة. ويقتضي ذلك الوقوف على مختلف الصور التي يمكن أن تتخذها هذه الجريمة في البيئة الرقمية، وبيان الأشخاص الذين يمكن أن تنعقد في حقهم المسؤولية الجنائية، فضلا عن تحديد العقوبات المقررة لمكافحتها. وعليه

¹ عواد، حامد هادي عواد، المرجع السابق ذكره ص66

² مجيد سحر فؤاد، المرجع السابق ذكره ص.ص 38-39

³ المرجع نفسه ص40

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

سيتم تناول صور التزوير المعلوماتي وأحكام المسؤولية الجنائية والعقوبات المقررة لها في التشريع المصري¹.

الفرع الأول: صور وأفعال التزوير المعلوماتي المعاقب عليها عند المشرع المصري

يعد التزوير المعلوماتي من أخطر صور الإجرام المستحدث التي أفرزها التطور التكنولوجي والاعتماد المتزايد على الوسائل الإلكترونية في مختلف المعاملات الإدارية والمالية والتجارية. وتكمن خطورة هذه الجريمة في كونها تستهدف الثقة المفترضة في البيانات والمحركات الإلكترونية التي أصبحت تؤدي دورا محوريا في إثبات الحقوق والالتزامات. ولأجل مواجهة هذه الأفعال، اعتمد المشرع المصري منظومة تشريعية متكاملة تجمع بين أحكام قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 وقانون التوقيع الإلكتروني رقم 15 لسنة 2004، فضلا عن بعض الأحكام العامة الواردة في قانون العقوبات، وذلك بهدف توفير حماية جنائية شاملة للمحركات والبيانات الإلكترونية من مختلف صور التلاعب والتزوير².

وتتجسد أهم صور وأفعال التزوير المعلوماتي المعاقب عليها في التشريع المصري فيما يأتي³:

أ- اصطناع الهويات الرقمية والحسابات الإلكترونية المزورة

تعد هذه الصورة من أكثر صور التزوير المعلوماتي انتشارا في البيئة الرقمية، وتتحقق عندما يقوم الجاني بإنشاء كيان إلكتروني غير حقيقي ونسبته إلى شخص طبيعي أو معنوي بقصد إيهام الغير بوجود علاقة بين هذا الكيان وصاحبه الحقيقي. ويشمل ذلك اصطناع أو تقليد البريد الإلكتروني أو الحسابات الخاصة أو الصفحات الإلكترونية أو المواقع الرقمية أو غيرها من الوسائط المستخدمة في التواصل وتبادل المعلومات.

وقد تصدى المشرع المصري لهذه الأفعال من خلال المادة 24 من قانون مكافحة جرائم تقنية المعلومات¹ رقم 175 لسنة 2018، التي جرمت اصطناع بريد إلكتروني أو موقع أو حساب خاص ونسبته زورا إلى

¹ مجيد سحر فؤاد، المرجع السابق ذكره ص41

² جارش عادل، الإرهاب الجديد: دراسة في المفهوم والطبيعة والأنواع وإجراءات المواجهة، مجلة العلوم القانونية والسياسية، المجلد 9، العدد 3، 2018، ص159

³ المرجع نفسه ص160

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

شخص طبيعي أو اعتباري. كما شدد العقوبة إذا استعمل الحساب أو الموقع المزور في الإساءة إلى المجني عليه أو الإضرار بسمعته أو الاعتداء على حقوقه ومصالحه المشروعة.

وتزداد خطورة هذه الصورة عندما يتعلق الأمر بانتحال هوية جهة حكومية أو مؤسسة عامة، لما قد يترتب على ذلك من المساس بالثقة العامة وتعريض الأفراد والمؤسسات لخطر التضليل والاحتيال. ولهذا قرر المشرع عقوبات أشد إذا كان الحساب أو الموقع أو البريد الإلكتروني المزور منسوباً إلى أحد الأشخاص الاعتبارية العامة أو الجهات التابعة للدولة².

وتكمن أهمية هذه الحماية في أن الحسابات والمواقع الإلكترونية أصبحت تمثل وسيلة رئيسية لإبرام المعاملات وتبادل المعلومات، الأمر الذي يجعل المساس بها صورة من صور التزوير التي لا تقل خطورة عن تزوير المحررات التقليدية.

ب- التلاعب بالبيانات والمحررات الإلكترونية وتغيير الحقيقة فيها

تتمثل هذه الصورة في الاعتداء المباشر على البيانات أو المعلومات أو المحررات الإلكترونية من خلال إدخال بيانات غير صحيحة أو حذف بيانات صحيحة أو تعديلها أو محوها أو استبدالها ببيانات أخرى تؤدي إلى تغيير الحقيقة داخل النظام المعلوماتي ويعد هذا النوع من التزوير الأقرب إلى المفهوم التقليدي للتزوير المعروف في قانون العقوبات، لأن جوهره يقوم على تغيير الحقيقة في محرر أو سجل إلكتروني بقصد استعماله فيما أعد له وترتيب آثار قانونية أو مالية أو إدارية غير مشروعة³.

وقد جرم المشرع المصري هذه الأفعال بموجب المادة 17 من قانون مكافحة جرائم تقنية المعلومات، التي عاقبت كل من أتلف أو محا أو عدل أو غير أو أعاد نشر البيانات أو المعلومات أو البرامج المخزنة

¹ المادة 24 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 (والمدرجة تحت الفصل الثاني الخاص بـ الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني، والمعروفة بـ "عقوبة الحسابات الوهمية") تنص على الآتي : عقوبات جنائية تبدأ بالحبس وغرامة (من 10 إلى 30 ألف جنيه) لكل من أنشأ حساباً أو بريداً إلكترونياً أو موقعاً زائفاً ونسبه لشخص طبيعي أو اعتباري. وتُشدد العقوبة لتصل إلى الحبس مدة لا تقل عن سنة وغرامة (من 50 إلى 200 ألف جنيه) إذا تم استخدام هذا الحساب في الإساءة. كما تصل العقوبة إلى السجن وغرامة (من 100 إلى 300 ألف جنيه) في حال كان الحساب المزور يخص شخصية اعتبارية عامة

² جارح عادل، المرجع السابق ذكره ص.ص 162-163

³ جارح عادل، المرجع السابق ذكره ص.ص 166

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

على نظام معلوماتي دون وجه حق. كما تمتد الحماية إلى قواعد البيانات والسجلات الإلكترونية التي تعتمد عليها الجهات العامة والخاصة في إدارة شؤونها¹.

وتظهر هذه الصورة بوضوح في حالات تعديل البيانات الواردة في السجلات الإدارية أو المالية أو المصرفية، كإدخال بيانات غير صحيحة في قاعدة بيانات العملاء أو تغيير الأرصدة البنكية أو تعديل المعلومات الشخصية للمواطنين المخزنة في الأنظمة الحكومية. ومتى أدى هذا التغيير إلى خلق مركز قانوني غير حقيقي أو ترتيب آثار قانونية مخالفة للحقيقة، فإن الفعل يكتسب وصف التزوير المعلوماتي.

كما تتدرج ضمن هذه الصورة الأفعال المرتبطة بوسائل الدفع الإلكتروني والبطاقات البنكية، حيث جرم المشرع اصطناع أو تقليد أو تزوير بطاقات الدفع الإلكتروني أو استخدامها مع العلم بتزويرها، لما يترتب على ذلك من مساس بالثقة والأمان في المعاملات المالية الإلكترونية².

ت- تزوير التوقيع الإلكتروني وشهادات التصديق الرقمي

أدى التوسع في استخدام وسائل التوثيق الإلكتروني إلى منح التوقيع الإلكتروني حجية قانونية مماثلة للحجية المقررة للتوقيع التقليدي، وهو ما كرسه المشرع المصري من خلال قانون التوقيع الإلكتروني رقم 15 لسنة 2004. وبناء على ذلك أصبح الاعتداء على التوقيع الإلكتروني أو تزويره يشكل صورة مستقلة من صور التزوير المعلوماتي تستوجب الحماية الجنائية.

وتتحقق هذه الصورة عندما يقوم الجاني بتقليد أو اصطناع توقيع إلكتروني يخص شخصا آخر، أو باستخدام منظومة إنشاء التوقيع الإلكتروني الخاصة بالغير دون إذن منه، أو باستعمال توقيع إلكتروني مزور مع العلم بحقيقة تزويره. كما تشمل تقديم بيانات أو مستندات غير صحيحة للحصول على شهادات التصديق الإلكتروني أو استغلالها بصورة غير مشروعة³.

¹ المرجع نفسه ص 167

² عبد العزيز محمد الصغير، الضمانات الدستورية للمواطنين بين الشريعة والقانون، الطبعة الأولى، المركز القومي

للإصدارات القانونية، القاهرة، 2011، ص 74.

³ الفوزان، محمد بن براك، المفاهيم والأبعاد في الاستراتيجية الوطنية لحماية النزاهة ومكافحة الفساد الصادرة بقرار مجلس الوزراء رقم 43، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، 1433هـ/2012م. ص 23

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

وقد نصت المادة 23 من قانون التوقيع الإلكتروني على معاقبة هذه الأفعال، نظرا لما تمثله من تهديد مباشر لمصادقية المحررات الإلكترونية وللثقة الواجب توافرها في المعاملات الرقمية. فالتوقيع الإلكتروني يعد الأداة الأساسية لإثبات هوية صاحب المحرر والتأكد من سلامة محتواه وعدم تعرضه للتعديل أو التغيير.

وتزداد خطورة هذا النوع من التزوير إذا تعلق بمحررات إلكترونية رسمية أو بمعاملات مالية وتجارية ذات قيمة كبيرة، إذ قد يؤدي إلى إحداث أضرار جسيمة بالأفراد والمؤسسات وبالاقتصاد الرقمي بصفة عامة¹.

الفرع الثاني: المسؤولية الجنائية عن جريمة التزوير المعلوماتي

تقوم المسؤولية الجنائية عن جريمة التزوير المعلوماتي في التشريع المصري على مجموعة من القواعد القانونية المستمدة أساسا من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، وقانون التوقيع الإلكتروني رقم 15 لسنة 2004، إلى جانب الأحكام العامة الواردة في قانون العقوبات رقم 58 لسنة 1937. وقد اتجه المشرع المصري إلى توسيع نطاق المسؤولية الجنائية بما يضمن مواجهة مختلف صور التزوير التي تقع على البيانات والمحررات الإلكترونية، فلم تقتصر المسؤولية على الشخص الطبيعي مرتكب الجريمة، بل امتدت في بعض الحالات إلى الشخص الاعتباري، مع إقرار حالات للإعفاء أو التخفيف من العقوبة وفق ضوابط قانونية محددة².

أ- المسؤولية الجنائية للشخص الطبيعي

تعد المسؤولية الجنائية للشخص الطبيعي الأصل في النظام الجنائي المصري، إذ يسأل كل شخص يرتكب فعلا مجرما بنص القانون متى توافرت أركان الجريمة وشروط إسنادها إليه. وفي مجال التزوير المعلوماتي تقوم هذه المسؤولية عند ارتكاب أحد الأفعال المجرمة بموجب قانون مكافحة جرائم تقنية المعلومات أو قانون التوقيع الإلكتروني.

ويستفاد من نصوص المواد 14 و17 و23 و24 من القانون رقم 175 لسنة 2018 أن المشرع جرم مجموعة من الأفعال التي تشكل صورا للتزوير المعلوماتي، من بينها الدخول غير المشروع إلى الأنظمة

¹ جارح عادل، المرجع السابق ذكره ص.169

² محمود، مجدي سلامة، الجرائم الإلكترونية في القانون المصري، دار النهضة العربية، القاهرة، 2020. ص43

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

المعلوماتية، وتعديل البيانات أو محوها أو إتلافها، واصطناع الحسابات والمواقع الإلكترونية ونسبتها زورا إلى الغير، فضلا عن الاعتداء على وسائل الدفع الإلكتروني والبيانات المرتبطة بها¹.

كما نصت المادة 23 من قانون التوقيع الإلكتروني رقم 15 لسنة 2004 على تجريم تزوير التوقيع الإلكتروني أو استعماله مع العلم بتزويره، وكذلك الحصول على شهادات التصديق الإلكتروني بناء على بيانات غير صحيحة أو استعمالها بصورة غير مشروعة.

ولقيام المسؤولية الجنائية يشترط أن يصدر عن الجاني سلوك إيجابي يؤدي إلى تغيير الحقيقة في البيانات أو المحررات الإلكترونية أو إنشاء مظهر كاذب من شأنه تضليل الغير أو ترتيب آثار قانونية غير مشروعة. كما يجب أن يتوافر القصد الجنائي باعتبار أن جرائم التزوير المعلوماتي من الجرائم العمدية التي تتطلب علم الجاني بعدم مشروعية فعله واتجاه إرادته إلى تحقيق النتيجة الإجرامية.

وتخضع مساءلة الجاني كذلك للأحكام العامة الواردة في قانون العقوبات، خاصة ما يتعلق بالمساهمة الجنائية والاشتراك في الجريمة والشروع فيها والظروف المشددة أو المخففة للعقوبة².

ب - المسؤولية الجنائية للشخص الاعتباري

استحدث المشرع المصري نظاما خاصا لمسؤولية الشخص الاعتباري عن الجرائم المعلوماتية بموجب المادة 36 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، وذلك لمواجهة الجرائم التي ترتكب في إطار نشاط الشركات والمؤسسات أو لمصلحتها.

وتقوم هذه المسؤولية إذا ارتكبت جريمة التزوير المعلوماتي باسم الشخص الاعتباري أو لحسابه أو لفائدته، وكان المسؤول عن الإدارة الفعلية للشخص الاعتباري على علم بالجريمة أو ثبت أن وقوعها كان نتيجة إخلاله الجسيم بواجبات الإشراف والرقابة.

ويترتب على ذلك معاقبة المسؤول عن الإدارة الفعلية بالعقوبات المقررة للجريمة ذاتها متى ثبت توافر شروط مسؤوليته، كما يجوز للمحكمة توقيع عقوبات وتدابير على الشخص الاعتباري نفسه. ومن بين هذه

¹ محمود، مجدي سلامة، المرجع السابق ذكره ص.ص 46-47

² المرجع نفسه ص 48

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

الجزاءات الغرامة والمصادرة، فضلا عن إمكانية وقف الترخيص أو إلغائه أو غلق المنشأة أو حل الشخص الاعتباري في الحالات التي يجيزها القانون¹.

ويعكس هذا الاتجاه رغبة المشرع في منع استغلال الشركات والمؤسسات كوسيلة لارتكاب الجرائم المعلوماتية أو التستر عليها، خاصة في ظل ما تملكه هذه الجهات من إمكانيات تقنية تمكنها من الوصول إلى البيانات والأنظمة الإلكترونية واستعمالها بصورة غير مشروعة.

ت - الإعفاء من العقوبة والتخفيف منها

إلى جانب تقرير المسؤولية الجنائية، نص المشرع المصري على بعض الحالات التي يترتب عليها الإعفاء من العقوبة أو التخفيف منها، وذلك بموجب المادة 39 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 فقد قرر المشرع إعفاء الجاني من العقوبة إذا بادر بإبلاغ السلطات القضائية أو الإدارية المختصة بالجريمة قبل البدء في تنفيذها وقبل اكتشافها من قبل السلطات، وكان من شأن هذا الإبلاغ منع وقوع الجريمة أو المساعدة في ضبط مرتكبيها أو كشف وسائل ارتكابها.

كما منح المحكمة سلطة تقديرية في الإعفاء من العقوبة أو تخفيفها إذا تم الإبلاغ بعد علم السلطات بالجريمة، متى أدى هذا الإبلاغ إلى الكشف عن باقي الجناة أو ضبط الأدوات المستخدمة أو استرداد الأموال أو البيانات أو المحررات الإلكترونية محل الجريمة ويهدف هذا النظام إلى تشجيع التعاون مع السلطات المختصة وتعزيز فعالية السياسة الجنائية في مواجهة الجرائم المعلوماتية، بالنظر إلى ما تتميز به من تعقيد تقني وصعوبة في الكشف عن مرتكبيها بالوسائل التقليدية².

وعليه، يتضح أن المسؤولية الجنائية عن جريمة التزوير المعلوماتي في التشريع المصري تقوم على ثلاثة أسس رئيسية تتمثل في مساءلة الشخص الطبيعي مرتكب الجريمة وفقا لأحكام قانون مكافحة جرائم تقنية المعلومات وقانون التوقيع الإلكتروني وقانون العقوبات، ومساءلة الشخص الاعتباري متى ارتكبت الجريمة باسمه أو لحسابه وفقا للمادة 36 من القانون رقم 175 لسنة 2018، ثم إقرار حالات خاصة للإعفاء أو

¹ مجيد سحر فؤاد، المرجع السابق ذكره ص44

² محمود، مجدي سلامة، المرجع السابق ذكره ص.49

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

التخفيف من العقوبة بموجب المادة 39¹ من القانون ذاته دعما لجهود مكافحة الجرائم المعلوماتية والكشف عن مرتكبيها².

الفرع الثالث: العقوبات المقررة لجريمة التزوير المعلوماتي

حرص المشرع المصري على إقرار نظام عقابي متكامل لمواجهة جريمة التزوير المعلوماتي، بالنظر إلى ما تنطوي عليه من مساس بالثقة العامة وبسلامة المعاملات الإلكترونية والمحركات الرقمية. وقد توزعت الأحكام العقابية المنظمة لهذه الجريمة بين قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 وقانون التوقيع الإلكتروني رقم 15 لسنة 2004، مع إمكانية تطبيق أحكام قانون العقوبات متى شكل الفعل جريمة تزوير بالمعنى التقليدي. ويتميز النظام العقابي المصري بالتدرج في العقوبة بحسب جسامة الفعل وطبيعة المصلحة المعتدى عليها، فضلا عن تقرير ظروف مشددة وعقوبات تكميلية وتدابير احترازية تهدف إلى تحقيق الردع وحماية الأمن المعلوماتي³.

أ- العقوبات المقررة لاصطناع الحسابات والمواقع الإلكترونية المزورة

أولى المشرع المصري عناية خاصة لجرائم اصطناع الحسابات والمواقع والبريد الإلكتروني، باعتبارها من أكثر صور التزوير المعلوماتي انتشارا في البيئة الرقمية. وقد نظم هذه الجريمة في المادة 24 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018.

فإذا اقتصر الفعل على مجرد إنشاء حساب أو بريد إلكتروني أو موقع إلكتروني ونسبته زورا إلى شخص طبيعي أو معنوي دون استعماله في الإضرار بالغير، عوقب الجاني بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز ثلاثين ألف جنيه أو بإحدى هاتين العقوبتين.

¹ المادة 39 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 (والمدرجة تحت الفصل السابع الخاص بـ الإغفاء من العقوبة) تنص على الآتي: "يُعفى من العقوبات المقررة للجرائم المنصوص عليها في هذا القانون، كل من بادر من الجناة بإبلاغ السلطات القضائية أو جهات الضبط القضائي بالجريمة قبل البدء في تنفيذها وقبل كشفها، فإذا كشف عنها بعد كشف الجريمة جاز للمحكمة إعفاؤه من العقوبة أو التخفيف منها، إذا أدى البلاغ إلى ضبط باقي الجناة أو الأدلة أو النظم أو الوسائل المستعملة في الجريمة

² أحمد عبد الله، الجرائم البيئية في مصر، دار الفكر العربي، القاهرة، 2021، ص 50

³ المرجع نفسه ص 51

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

أما إذا استعمل الجاني الحساب أو الموقع أو البريد الإلكتروني المزور في الإساءة إلى المجني عليه أو المساس باعتباره أو حقوقه أو مصالحه المشروعة، فإن العقوبة تتشدد لتصبح الحبس مدة لا تقل عن سنة وغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه أو بإحدى هاتين العقوبتين¹. وتبلغ العقوبة أقصى درجاتها إذا تعلق التزوير بحساب أو موقع أو بريد إلكتروني منسوب إلى جهة حكومية أو شخص اعتباري عام، حيث نصت المادة ذاتها على عقوبة الحبس مدة لا تقل عن ثلاث سنوات وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه أو بإحدى هاتين العقوبتين. ويعكس هذا التشديد حرص المشرع على حماية الثقة العامة ومنع انتحال صفة الجهات الرسمية واستغلالها في التضليل أو الاحتيال².

ب- العقوبات المقررة للاعتداء على البيانات والمحركات الإلكترونية

تمثل البيانات والمحركات الإلكترونية جوهر البيئة الرقمية الحديثة، ولذلك أفرد لها المشرع المصري حماية جنائية خاصة من خلال المادة 17 من قانون مكافحة جرائم تقنية المعلومات.

وتطبق هذه المادة على كل شخص يقوم دون وجه حق بمحو البيانات أو المعلومات أو البرامج الإلكترونية أو تعديلها أو إلغائها أو إتلافها أو تشويهها أو إعادة نشرها بما يؤدي إلى تغيير الحقيقة داخل النظام المعلوماتي. وتتمثل العقوبة في الحبس مدة لا تقل عن سنتين وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه أو بإحدى هاتين العقوبتين.

وتكتسب هذه الجريمة أهمية خاصة في مجال التزوير المعلوماتي لأن جوهر التزوير يتمثل في تغيير الحقيقة داخل المحرر أو السجل الإلكتروني. ومن ثم فإن أي تلاعب بقاعدة بيانات حكومية أو مصرفية أو تجارية يفضي إلى تعديل محتوى المحركات الإلكترونية أو إظهار بيانات غير صحيحة يمكن أن يندرج ضمن هذه الجريمة³.

¹ أحمد عبد الله، المرجع السابق ذكره ، ص 53

² إسماعيل، محمد صادق، الجريمة الإلكترونية في مصر وأساليب مكافحتها، ضمن كتاب: الجرائم الإلكترونية، ص 109-123، منشور بموقع المرجع الإلكتروني، 1 يوليو 2022. الاطلاع بتاريخ 15 جوان 2026 :

<https://manshurat.org/node/14677>

³ أحمد عبد الله، المرجع السابق ذكره ، ص 59

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

كما تشمل الحماية السجلات الإلكترونية وقواعد البيانات التي تعتمد عليها المؤسسات العامة والخاصة في إثبات الحقوق والالتزامات، مما يجعل العقوبة وسيلة لحماية الثقة في المعاملات الإلكترونية واستقرارها.

ت - العقوبات المقررة لتزوير وسائل الدفع الإلكتروني والبطاقات البنكية

نظرا للتوسع الكبير في استخدام وسائل الدفع الإلكتروني، خص المشرع المصري هذه الوسائل بحماية جنائية خاصة من خلال المادة 23 من قانون مكافحة جرائم تقنية المعلومات.

فقد جرم اصطناع أو تقليد أو تزوير بطاقات الدفع الإلكتروني أو بطاقات الائتمان أو بياناتها أو استعمالها مع العلم بتزويرها. ويعاقب مرتكب هذه الأفعال بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين¹.

أما إذا استخدمت البطاقة المزورة أو البيانات المستولى عليها فعلا في الاستيلاء على أموال الغير أو الحصول على خدمات أو مزايا مالية بصورة غير مشروعة، فإن العقوبة تتشدد لتصل إلى الحبس مدة لا تقل عن سنة وغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين. ويعكس هذا الاتجاه خطورة الاعتداء على وسائل الدفع الإلكتروني باعتبارها أحد أهم مكونات الاقتصاد الرقمي المعاصر.

ث - العقوبات المقررة لتزوير التوقيع الإلكتروني وشهادات التصديق الرقمي

لم يكتف المشرع بحماية البيانات والمحركات الإلكترونية، بل امتدت الحماية إلى التوقيع الإلكتروني الذي أصبح يتمتع بالحجية القانونية ذاتها المقررة للتوقيع التقليدي بموجب قانون التوقيع الإلكتروني رقم 15 لسنة 2004 ولهذا نصت المادة 23 من القانون المذكور على معاقبة كل من زور توقيعاً إلكترونياً أو استعمل توقيعاً إلكترونياً مزوراً مع علمه بذلك، كما عاقبت كل من قدم بيانات غير صحيحة للحصول على شهادة تصديق إلكتروني أو استعمل هذه الشهادة بصورة غير مشروعة.

وتتمثل العقوبة في الحبس أو الغرامة التي تتراوح بين عشرة آلاف جنيه ومائة ألف جنيه أو بإحدى هاتين العقوبتين، وذلك مع عدم الإخلال بأي عقوبة أشد مقررة في قانون العقوبات أو أي قانون آخر.

وتظهر أهمية هذه العقوبات في أنها تستهدف حماية الثقة القانونية في المعاملات الإلكترونية التي تعتمد على التوقيع الإلكتروني كوسيلة لإثبات الهوية وإضفاء الحجية على المحركات الرقمية².

¹ محمود، مجدي سلامة، المرجع السابق ذكره صص 62-63

² صالح قنان، الجرائم المستحدثة في التشريع المصري والليبي، جامعة القاهرة، 2019، ص ص 28-29

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

ج- الظروف المشددة للعقوبة

لم يساو المشرع بين جميع صور التزوير المعلوماتي، بل ميز بين الجرائم العادية والجرائم التي تمس المصالح الحيوية للدولة أو الأمن القومي.

وفي هذا الإطار نصت المادة 34 من قانون مكافحة جرائم تقنية المعلومات على تشديد العقوبات إذا ارتكبت الجريمة ضد موقع أو حساب أو نظام معلوماتي يدار بمعرفة الدولة أو أحد الأشخاص الاعتبارية العامة، أو إذا ارتكبت بقصد الإضرار بالأمن القومي أو بالاقتصاد الوطني أو بالمرافق الحيوية للدولة. وفي هذه الحالات ترتفع العقوبة إلى السجن المشدد، فضلا عن الغرامات المالية الكبيرة التي قد تصل إلى مليون جنيه. ويهدف هذا التشديد إلى توفير حماية خاصة للبنية التحتية الرقمية للدولة باعتبارها جزءا من منظومة الأمن القومي¹.

ح- العقوبات التبعية والتدابير الاحترازية

إلى جانب العقوبات الأصلية، أجاز المشرع المصري للمحكمة توقيع مجموعة من العقوبات التبعية والتدابير الاحترازية التي تهدف إلى منع تكرار الجريمة والقضاء على الوسائل المستخدمة في ارتكابها.

فقد نصت المادة 37² من قانون مكافحة جرائم تقنية المعلومات على إمكانية الحكم بحرمان المحكوم عليه من استخدام بعض وسائل تقنية المعلومات أو مزاوله نشاط معين يتعلق باستخدام الشبكات والأنظمة المعلوماتية لمدة لا تتجاوز ثلاث سنوات.

كما نصت المادة 38¹ على المصادرة الوجوبية للأجهزة والمعدات والبرامج والوسائط الإلكترونية المستخدمة في ارتكاب الجريمة أو المتحصلة منها، وذلك لمنع إعادة استخدامها في نشاط إجرامي مستقبلي.

¹ صالح قنان، المرجع السابق ذكره ص31

² المادة 37 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 (والمدرجة تحت الباب الخامس الخاص بالأحكام القضائية والإجراءات) تنص على الآتي: "مع عدم الإخلال بحقوق الغير حسن النية، تقضى المحكمة في حالة الإدانة بأى جريمة من الجرائم المنصوص عليها في هذا القانون، بمصادرة الأجهزة أو المعدات أو الوسائط الإلكترونية، أو البرامج أو المنظومات المعلوماتية، أو خطوط الاتصالات، أو غيرها من الوسائل مما يكون قد استخدم في ارتكاب الجريمة، أو سُهلت له، أو كانت متحصلة منها، كما تقضى بمحو المحتوى المقيد أو بغلاق الموقع أو الحساب الخاص بحسب الأحوال".

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

وأجازت المادة نفسها الحكم بغلق الموقع الإلكتروني أو المحل أو المنشأة التي ارتكبت الجريمة من خلالها، سواء بصورة مؤقتة أو نهائية بحسب جسامة الفعل والظروف المحيطة به. وتعد هذه التدابير من أهم وسائل مكافحة الحديثة لأنها تستهدف البيئة التقنية التي ارتكبت فيها الجريمة وليس الجاني فقط².

خ- تطبيق قاعدة العقوبة الأشد

قد تتداخل جريمة التزوير المعلوماتي مع جرائم التزوير التقليدية المنصوص عليها في قانون العقوبات المصري، خاصة عندما يتعلق الأمر بالمحررات الرسمية أو العرفية التي اتخذت شكلا إلكترونيا.

فإذا أدى التزوير المعلوماتي إلى إنشاء محرر رسمي مزور أو استعماله، كما لو قام الجاني بتزوير شهادة جامعية إلكترونية أو محرر إداري رسمي واستخدمه للحصول على حق أو ميزة غير مستحقة، فإن الفعل قد يشكل جريمة معلوماتية وجريمة تزوير في محرر رسمي في آن واحد.

وفي هذه الحالة تطبق أحكام المادة 32 من قانون العقوبات المتعلقة بتعدد الأوصاف الجنائية، حيث تقضي المحكمة بالعقوبة المقررة للجريمة الأشد. وبذلك يمكن أن تطبق العقوبات المقررة لجنايات التزوير في المحررات الرسمية إذا كانت أشد من العقوبات الواردة في قانون مكافحة جرائم تقنية المعلومات³.

وعليه، يتبين أن المشرع المصري اعتمد سياسة عقابية متدرجة ومتكاملة لمواجهة جريمة التزوير المعلوماتي، تقوم على تنوع العقوبات بحسب خطورة الفعل المرتكب، مع تشديدها عند المساس بالمصالح الحيوية للدولة، وإقرار تدابير احترازية وعقوبات تكميلية تستهدف الوسائل التقنية المستخدمة في الجريمة،

¹ المادة 38 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 (والمدرجة تحت الفصل الثامن الخاص بـ العقوبات التبعية) تنص على الآتي : وفقاً لـ منصة مسار الرقمية: "مع عدم الإخلال بحقوق الغير حسن النية، على المحكمة في حالة الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها في هذا القانون، أن تقضى بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانوناً، أو غيرها مما يكون قد استخدم في ارتكاب الجريمة، أو سهل أو ساهم في ارتكابها."

² محمود، مجدي سلامة، المرجع السابق ذكره صص 62-63

³رامي متولي القاضي، "المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري في ضوء أحكام القانون رقم (175) لسنة 2018م مقارناً بالمواثيق الدولية والتشريعات المقارنة"، مجلة كلية الشرطة، العدد 75، مارس 2021، ص

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

فضلا عن إمكانية تطبيق العقوبات الأشد المنصوص عليها في قانون العقوبات ضمانا لتحقيق الردع وحماية الثقة في البيئة الرقمية¹.

المطلب الثالث: الأحكام الإجرائية الخاصة بمكافحة التزوير المعلوماتي

تثير جريمة التزوير المعلوماتي صعوبات إجرائية تفوق تلك التي تثيرها جرائم التزوير التقليدية، ويرجع ذلك إلى طبيعة البيئة الرقمية التي ترتكب فيها هذه الجريمة، حيث تعتمد على البيانات الإلكترونية والأنظمة المعلوماتية والشبكات الرقمية التي يمكن التلاعب بها أو إخفاؤها أو محوها في وقت وجيز. كما أن مرتكبي هذه الجرائم غالبا ما يستفيدون من الوسائل التقنية الحديثة لإخفاء هوياتهم أو محو آثار أفعالهم، الأمر الذي يجعل اكتشاف الجريمة وإثباتها أكثر تعقيدا مقارنة بالجرائم التقليدية.

ولمواجهة هذه التحديات، استحدث المشرع المصري بموجب قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 مجموعة من الأحكام الإجرائية الخاصة التي تراعي خصوصية الجريمة المعلوماتية وتوفر للسلطات المختصة الوسائل القانونية والفنية اللازمة للكشف عنها وضبط مرتكبيها.²

أ- حجية الدليل الرقمي وضوابط إثبات جريمة التزوير المعلوماتي

يعد الدليل الرقمي من أهم وسائل الإثبات في جرائم التزوير المعلوماتي، لأن هذه الجرائم ترتكب في محيط إلكتروني يعتمد على البيانات والبرامج والسجلات الرقمية بدلا من المحررات الورقية التقليدية. ولهذا السبب أولى المشرع المصري أهمية خاصة للدليل الرقمي، حيث نصت المادة 11 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 على أن تكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو النظام المعلوماتي أو البرامج المعلوماتية أو أي وسيلة من وسائل تقنية المعلومات الحجية المقررة للأدلة الجنائية المادية متى استوفت الشروط الفنية والقانونية المقررة.³

ويستفاد من هذا النص أن المشرع المصري وضع الدليل الرقمي في مرتبة مساوية للأدلة الجنائية التقليدية، كالمحررات الرسمية أو البصمات أو التقارير الفنية، وهو ما يمثل تطورا مهما في مجال الإثبات

¹المرجع نفسه ص73

²رامي متولي القاضي، المرجع السابق ذكره ص 72

³علي، محمود عبد العزيز، جرائم الإنترنت ووسائل مكافحتها في التشريع المصري، دار الفكر والقانون، المنصورة،

2019..ص78

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

الجنائي. غير أن الاعتداد بالدليل الرقمي يقتضي توافر مجموعة من الضوابط الفنية التي حددتها اللائحة التنفيذية للقانون الصادرة بموجب قرار رئيس مجلس الوزراء رقم 1699 لسنة 2020.

ومن أهم هذه الضوابط المحافظة على سلامة الدليل الرقمي منذ لحظة ضبطه وحتى تقديمه أمام القضاء، والتأكد من عدم تعرضه لأي تعديل أو حذف أو تشويه. كما يجب توثيق جميع الإجراءات المتخذة أثناء جمع البيانات الرقمية وفحصها وتحليلها، مع بيان الأجهزة والبرامج المستخدمة في عملية الفحص. ويشترط كذلك أن تكون البيانات قابلة للقراءة والاستخراج والتحليل بواسطة الجهات الفنية المختصة، حتى يتسنى للمحكمة التحقق من صحتها وسلامتها¹.

وتتعدد صور الأدلة الرقمية في جرائم التزوير المعلوماتي، فقد تتمثل في سجلات الدخول إلى الأنظمة المعلوماتية، أو ملفات الحاسب الآلي، أو قواعد البيانات، أو الرسائل الإلكترونية، أو سجلات الخوادم الإلكترونية، أو بيانات التوقيع الإلكتروني، أو نتائج الفحص الفني للأجهزة المضبوطة. وتكتسب هذه الأدلة أهمية بالغة لأنها غالباً ما تشكل الوسيلة الأساسية لإثبات تغيير الحقيقة داخل النظام المعلوماتي وتحديد الشخص المسؤول عن ذلك.

ب- التزامات مقدمي خدمات الاتصالات والإنترنت في كشف جرائم التزوير المعلوماتي

أدرك المشرع المصري أن مكافحة الجرائم المعلوماتية لا يمكن أن تتحقق بفعالية دون تعاون الجهات التي تدير البنية التحتية الرقمية، ولذلك فرض على مقدمي خدمات الاتصالات والإنترنت مجموعة من الالتزامات القانونية التي تساعد السلطات المختصة على كشف الجرائم المعلوماتية وتتبع مرتكبيها.

وقد نصت المادة الثانية من قانون مكافحة جرائم تقنية المعلومات على إلزام مقدمي الخدمة بحفظ وتخزين بيانات منظومة الاتصالات لمدة مائة وثمانين يوماً متصلة. وتشمل هذه البيانات المعلومات الكفيلة بتحديد هوية المستخدم، وبيانات حركة الاتصال، ووقت الاتصال ومدته، وعناوين بروتوكول الإنترنت، والبيانات المتعلقة بالأجهزة المستخدمة في الدخول إلى الشبكة².

وتكمن أهمية هذه البيانات في أنها تمكن جهات التحقيق من إعادة تتبع النشاط الإلكتروني المرتبط بالجريمة، وتحديد الأجهزة أو الحسابات التي استخدمت في ارتكاب فعل التزوير المعلوماتي. فعلى سبيل المثال، إذا تم تعديل بيانات إلكترونية داخل قاعدة بيانات حكومية أو مصرفية، فإن الرجوع إلى بيانات

¹ حسين، محمد حسن، المسؤولية الجنائية عن الجرائم الإلكترونية في القانون المصري، دار الكتب القانونية، 2018، ص78

² علي، محمود عبد العزيز، المرجع السابق ذكره ص78

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

الاتصال المحفوظة لدى مزود الخدمة قد يساعد في تحديد مصدر الاتصال الذي تمت من خلاله عملية التعديل غير المشروع¹.

كما ألزم المشرع مقدمي الخدمة بالحفاظ على سرية البيانات المخزنة وعدم الكشف عنها إلا بناء على أمر صادر من جهة التحقيق المختصة أو تنفيذاً لحكم قضائي. ويهدف هذا الالتزام إلى تحقيق التوازن بين متطلبات مكافحة الجريمة من جهة، وحماية الحياة الخاصة والبيانات الشخصية للمستخدمين من جهة أخرى.

ت - سلطات التحري والتحقيق في جرائم التزوير المعلوماتي

نظراً للطبيعة الخاصة للجرائم المعلوماتية وسهولة إخفاء أدلتها، منح المشرع المصري جهات التحري والتحقيق سلطات استثنائية تتلاءم مع خطورة هذه الجرائم وطبيعة الوسائل المستخدمة في ارتكابها.

ومن أهم هذه السلطات سلطة حجب المواقع الإلكترونية المنصوص عليها في المادة 7 من قانون مكافحة جرائم تقنية المعلومات. فتمتد قامت أدلة على أن موقعاً إلكترونياً أو حساباً أو صفحة رقمية يستخدم في ارتكاب جرائم معلوماتية أو يشكل تهديداً للأمن القومي أو للمصالح الحيوية للدولة، يجوز لجهة التحقيق المختصة أن تأمر بحجبه لمنع استمرار النشاط الإجرامي وتقليل الأضرار الناجمة عنه.

كما خولت المادة 9² للنائب العام أو من يفوضه سلطة إصدار أوامر مبررة بمنع المتهم من السفر أو إدراجه على قوائم ترقب الوصول إذا اقتضت مصلحة التحقيق ذلك، وخاصة في الجرائم الخطيرة التي يحتمل فيها فرار المتهم أو صعوبة ملاحقته لاحقاً³.

وإلى جانب هذه السلطات الخاصة، تتمتع جهات التحقيق بكافة الصلاحيات المقررة في قانون الإجراءات الجنائية، ومن ذلك إصدار أوامر التفتيش والضبط، وضبط الأجهزة الإلكترونية والهواتف الذكية والحواسيب والخوادم الرقمية، والاستعانة بالخبراء والفنيين لفحصها واستخراج البيانات منها.

¹ المرجع نفسه ص 79

² المادة 9 من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 والمعنونة بـ (المنع من السفر) تنص على ما يلي: تمنح هذه المادة النائب العام أو من ينوب عنه الحق في إصدار أمر مسبب بمنع المتهم من السفر أو إدراجه في قوائم ترقب الوصول عند وجود أدلة جديّة في جرائم تقنية المعلومات. يحق للمتهم التظلم من هذا القرار أمام محكمة الجنايات المختصة خلال 15 يوماً من علمه به، مع إمكانية تجديد التظلم كل 3 أشهر في حال رفض

³ يوسف خالد محمد، التزوير الإلكتروني وإشكالات الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، 2021، ص 39

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

كما يمكن للسلطات المختصة الاستعانة بالإدارة العامة لتكنولوجيا المعلومات أو الجهات الفنية المختصة التابعة لوزارة الداخلية أو الجهات القضائية لإجراء الفحص الفني وتحليل الأدلة الرقمية وإعداد التقارير اللازمة التي تستند إليها المحكمة في تكوين قناعتها¹.

ومن الناحية العملية يمر إثبات جريمة التزوير المعلوماتي بعدة مراحل تبدأ برصد النشاط الإلكتروني المشبوه، ثم تحديد مصدره من خلال البيانات المحفوظة لدى مقدمي الخدمة، ثم ضبط الأجهزة والوسائط الإلكترونية المستخدمة، وبعد ذلك إجراء الفحص الفني للأدلة الرقمية واستخراج البيانات ذات الصلة بالجريمة، وأخيرا إعداد تقرير فني يبين كيفية وقوع الجريمة ونسبتها إلى المتهم².

ث - الاختصاص القضائي في جرائم التزوير المعلوماتي

نظرا لما تتسم به الجرائم المعلوماتية من تعقيد تقني وتشابك قانوني، اتجه المشرع المصري إلى إسناد الاختصاص بنظر هذه الجرائم إلى جهات قضائية متخصصة تمتلك الخبرة الكافية للتعامل مع المسائل الفنية المرتبطة بها.

وفي هذا السياق تختص النيابة الاقتصادية بالتحقيق في الجرائم المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات، بينما تختص المحاكم الاقتصادية المنشأة بموجب القانون رقم 120 لسنة 2008 بالفصل في الدعاوى المتعلقة بهذه الجرائم³.

وتتظر دوائر الجناح الاقتصادية أو الجنايات الاقتصادية القضايا بحسب الوصف القانوني للجريمة والعقوبة المقررة لها. ويهدف هذا التنظيم إلى تحقيق سرعة الفصل في القضايا المعلوماتية وتوفير قضاة وأعضاء نيابة يتمتعون بخبرة أكبر في مجال الأدلة الرقمية والتقارير الفنية المعقدة.

كما يسهم الاختصاص القضائي المتخصص في توحيد التفسير القضائي للنصوص المتعلقة بالجرائم المعلوماتية وضمان التطبيق السليم للأحكام القانونية والفنية ذات الصلة، وهو ما ينعكس إيجابا على فعالية مكافحة جرائم التزوير المعلوماتي وتحقيق الأمن القانوني في البيئة الرقمية⁴.

¹ المرجع نفسه ص ص 40-41

² يوسف خالد محمد، المرجع السابق ذكره ص ص 42-43

³ المرجع نفسه ص 44

⁴ إبراهيم، محمد السيد، السياسة الجنائية لمواجهة الجرائم السيبرانية في مصر، المركز القومي للإصدارات القانونية، القاهرة،

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

وعليه، يتضح أن المشرع المصري قد وضع منظومة إجرائية متكاملة لمواجهة جريمة التزوير المعلوماتي، تقوم على الاعتراف بالحجية القانونية للدليل الرقمي، وإلزام مقدمي خدمات الاتصالات بحفظ البيانات اللازمة للكشف عن الجرائم، ومنح جهات التحري والتحقيق سلطات خاصة تتناسب مع طبيعة البيئة الرقمية، فضلا عن إسناد الاختصاص إلى جهات قضائية متخصصة، بما يضمن تحقيق حماية جنائية فعالة للبيانات والمحركات الإلكترونية وملاحقة مرتكبي جرائم التزوير المعلوماتي بكفاءة وفعالية.

المبحث الثاني: أوجه المقارنة بين التشريعين المصري والجزائري في مجال التزوير المعلوماتي

أفرز التطور التكنولوجي تحديات قانونية متشابهة دفعت كلا من المشرع المصري والمشرع الجزائري إلى التدخل لتنظيم جريمة التزوير المعلوماتي ومواجهتها بنصوص خاصة تتلاءم مع طبيعة البيئة الرقمية. ورغم اتفاق التشريعين في الهدف المتمثل في حماية البيانات والمحركات الإلكترونية وضمان الثقة في المعاملات الرقمية، إلا أنهما يختلفان في بعض الجوانب المتعلقة بالتجريم والعقاب والإجراءات المتبعة. ومن ثم تكتسي المقارنة بينهما أهمية بالغة للكشف عن نقاط القوة والقصور في كل نظام قانوني، وتقييم مدى فعاليته في مواجهة هذا النوع من الجرائم المستحدثة. وعليه سيتم تناول أوجه التشابه وأوجه الاختلاف بين التشريعين، ثم الوقوف على أهم المقترحات الكفيلة بتطوير الحماية القانونية للتزوير المعلوماتي¹.

المطلب الأول: أوجه التشابه بين التشريعين المصري والجزائري

على الرغم من اختلاف البيئة التشريعية لكل من مصر والجزائر، فإن كلا المشرعين اتجها إلى تبني سياسة جنائية حديثة لمواجهة جرائم تقنية المعلومات بصفة عامة وجريمة التزوير المعلوماتي بصفة خاصة. ويظهر التقارب بين التشريعين في العديد من الجوانب الموضوعية والإجرائية، سواء من حيث الاعتراف بالمحركات الإلكترونية، أو تجريم الأفعال الماسة بالبيانات الرقمية، أو إقرار وسائل خاصة للإثبات والتحقيق في الجرائم المعلوماتية. ويمكن إبراز أهم أوجه التشابه فيما يأتي²:

أ- الاعتراف القانوني بالمحركات الإلكترونية والتوقيع الإلكتروني

¹ عيمور راضية، "الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري"، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 6، العدد 1، جامعة عمار ثلجي بالأغواط، الجزائر، 31 مارس 2022، ص ص 87-88

² زنتوت عبد الكريم، "الجريمة الإلكترونية وسبل مواجهتها في الجزائر"، مجلة الحقوق والحريات، المجلد 13، العدد 01، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، 01 أبريل 2025، ص ص 315-316

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

يتفق التشريعان المصري والجزائري على منح المحررات الإلكترونية والتوقيعات الإلكترونية الحجية القانونية اللازمة في الإثبات، وعدم قصر الحماية القانونية على المحررات الورقية التقليدية فقط.

ففي مصر، اعترف المشرع بالمحررات والتوقيعات الإلكترونية بموجب قانون التوقيع الإلكتروني رقم 15 لسنة 2004، ومنحها الحجية القانونية متى استوفت الشروط المقررة قانوناً. كما اعتبرها محلاً للحماية الجنائية شأنها شأن المحررات التقليدية¹.

أما في الجزائر، فقد كرس المشرع المبدأ ذاته من خلال المادة 323 مكرر 1 من القانون المدني، والقانون رقم 04-15 المتعلق بالتوقيع والتصديق الإلكترونيين، حيث ساوى بين الكتابة الإلكترونية والكتابة الورقية في مجال الإثبات متى توافرت شروط السلامة وإمكانية التحقق من هوية مصدرها.

ويكشف ذلك عن اتجاه مشترك لدى المشرعين نحو حماية الثقة في المعاملات الإلكترونية وإضفاء القيمة القانونية على المحررات الرقمية².

ب- تجريم الأفعال الماسة بالبيانات والأنظمة المعلوماتية

يتشابه التشريعان في تجريم مختلف صور الاعتداء على البيانات والأنظمة المعلوماتية التي قد تؤدي إلى تغيير الحقيقة داخل البيئة الرقمية.

فالمشرع المصري جرم الدخول غير المشروع إلى الأنظمة المعلوماتية، والاعتداء على سلامة البيانات، وتعديلها أو إتلافها أو حذفها دون وجه حق بموجب قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018.

وبالمقابل، جرم المشرع الجزائري الأفعال ذاتها من خلال المواد 394 مكرر وما يليها من قانون العقوبات، والتي تعاقب على الدخول غير المشروع إلى أنظمة المعالجة الآلية للمعطيات، وإدخال أو تعديل أو حذف البيانات بطريق الغش.

ويلاحظ أن كلا التشريعين يعتبر التلاعب بالبيانات الإلكترونية صورة من صور الاعتداء على الثقة العامة والأمن المعلوماتي، الأمر الذي يبرر التدخل الجنائي لحمايتها³.

ت- حماية المحررات والبيانات الإلكترونية من التزوير

¹المرجع نفسه ص318

²زنتوت عبد الكريم، "المرجع السابق ذكره ص 320

³المرجع نفسه ص321

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

يتفق التشريعان كذلك في اعتبار البيانات والمحركات الإلكترونية محلاً لجريمة التزوير متى أدى السلوك الإجرامي إلى تغيير الحقيقة فيها بصورة من شأنها إحداث ضرر.

ففي مصر، تتكامل أحكام قانون مكافحة جرائم تقنية المعلومات مع قانون التوقيع الإلكتروني وقواعد التزوير الواردة في قانون العقوبات لحماية المحركات الإلكترونية من مختلف صور الاصطناع أو التعديل أو التحريف.

أما في الجزائر، فقد عزز القانون رقم 02-24 المتعلق بمكافحة التزوير واستعمال المزور الحماية الجنائية للمحركات الإلكترونية والتوقيعات الرقمية والوثائق الرسمية الإلكترونية، وأخضعها للأحكام المقررة للتزوير متى توافرت أركان الجريمة¹.

ومن ثم فإن كلا المشرعين تجاوز المفهوم التقليدي للمحرر، ووسع نطاق الحماية الجنائية ليشمل الوثائق الرقمية الحديثة.

ث - اعتماد الدليل الرقمي كوسيلة للإثبات الجنائي

يعد الاعتراف بالدليل الرقمي من أبرز نقاط التشابه بين التشريعين، إذ أدرك كل منهما أن مكافحة الجرائم المعلوماتية لا يمكن أن تتحقق بالاعتماد على وسائل الإثبات التقليدية وحدها.

فقد نصت المادة 11 من قانون مكافحة جرائم تقنية المعلومات المصري على منح الأدلة الرقمية الحجية القانونية المقررة للأدلة الجنائية المادية متى استوفت الشروط الفنية اللازمة.

كما اعتمد المشرع الجزائري الأدلة الرقمية في إطار مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وأجاز الاستعانة بالخبرة الفنية وتحليل البيانات الإلكترونية لإثبات الجرائم المعلوماتية، بما فيها جرائم التزوير المعلوماتي².

ويعكس ذلك إدراك المشرعين للطبيعة الخاصة للأدلة الرقمية وضرورة الاعتراف بقيمتها الإثباتية أمام القضاء.

¹ - سالم، محمد علي، وهجيج، حسون عبيد، "الجريمة المعلوماتية"، مجلة جامعة بابل للعلوم الإنسانية، جامعة بابل، العراق،

المجلد 14، العدد 2، 2007، ص ص 85-86

² زنتوت عبد الكريم، "المرجع السابق ذكره ص 323

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

ج- منح سلطات خاصة لأجهزة التحري والتحقيق

يتشابه التشريعان في منح السلطات المختصة صلاحيات استثنائية تتلاءم مع خصوصية الجرائم المعلوماتية وصعوبة اكتشافها.

ففي مصر، منح قانون مكافحة جرائم تقنية المعلومات جهات التحقيق صلاحيات تتعلق بحجب المواقع الإلكترونية، وتتبع البيانات الرقمية، والاستعانة بمقدمي الخدمة للحصول على المعلومات اللازمة للتحقيق. وفي الجزائر، منح القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها سلطات خاصة للضبطية القضائية، من بينها تفتيش الأنظمة المعلوماتية، وحجز الأدلة الرقمية، وتتبع حركة المعطيات الإلكترونية، والاستعانة بالوسائل التقنية الحديثة للكشف عن الجرائم¹.

ويبرز من ذلك وجود توجه تشريعي مشترك نحو تطوير آليات البحث والتحري بما يتلاءم مع البيئة الرقمية.

ح- تشديد العقوبات عند المساس بالمصالح العامة والجهات الحكومية

يتفق المشرعان المصري والجزائري على تشديد العقوبات عندما تستهدف الجريمة الأنظمة أو البيانات التابعة للدولة أو المؤسسات العامة.

ففي مصر، نصت المادة 34 من قانون مكافحة جرائم تقنية المعلومات على تشديد العقوبة إذا ارتكبت الجريمة ضد موقع أو نظام معلوماتي تابع للدولة أو إذا مست الأمن القومي أو المصالح الاقتصادية الحيوية.

وفي الجزائر، شدد المشرع العقوبات في المادة 394 مكرر 3 من قانون العقوبات إذا تعلق الاعتداء بمعطيات أو أنظمة معلوماتية تابعة للدولة أو الهيئات العمومية².

ويعكس هذا التشابه حرص التشريعين على توفير حماية جنائية مشددة للبنية المعلوماتية الوطنية وللمصالح الاستراتيجية للدولة.

¹ - سالم، محمد علي، وهجيج، حسون عبيد، "المرجع السابق ذكره ص 88

² المرجع نفسه ص 89

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

خ- الجمع بين الحماية الموضوعية والحماية الإجرائية

لا يقتصر التشابه بين التشريعين على الجانب الموضوعي المتعلق بالتجريم والعقاب، وإنما يمتد إلى الجانب الإجرائي أيضا، حيث اعتمد كل منهما منظومة متكاملة تجمع بين النصوص العقابية والآليات الإجرائية اللازمة للكشف عن الجرائم وإثباتها.

فكلا التشريعين نظم صور التجريم والعقوبات المقررة للتزوير المعلوماتي، وفي الوقت نفسه وضع قواعد خاصة تتعلق بالتحري والتحقيق وجمع الأدلة الرقمية والاستعانة بالخبرة الفنية، بما يضمن فعالية المواجهة الجنائية لهذا النوع من الجرائم.

وعليه، يتضح أن التشريعين المصري والجزائري يلتقيان في العديد من الأسس الجوهرية المتعلقة بمكافحة التزوير المعلوماتي، سواء من حيث الاعتراف بالمحركات الإلكترونية، أو تجريم الاعتداء على البيانات الرقمية، أو اعتماد الدليل الإلكتروني، أو تطوير آليات التحري والتحقيق، وهو ما يعكس تأثرهما بالاتجاهات التشريعية الحديثة الرامية إلى توفير حماية جنائية فعالة للبيئة الرقمية¹.

المطلب الثاني: أوجه الاختلاف بين التشريعين المصري والجزائري

على الرغم من وجود العديد من نقاط التشابه بين التشريعين المصري والجزائري في مجال مكافحة التزوير المعلوماتي، إلا أن كل منهما تبني مقاربة تشريعية خاصة تعكس خصوصية النظام القانوني الذي ينتمي إليه. وتظهر أوجه الاختلاف بصفة أساسية في أسلوب التجريم، ونطاق الحماية القانونية، والتنظيم الإجرائي، وطبيعة العقوبات المقررة، فضلا عن مدى استقلال جريمة التزوير المعلوماتي داخل المنظومة التشريعية لكل دولة. ويمكن بيان أهم هذه الاختلافات فيما يأتي²:

أ- الاختلاف في الأساس التشريعي لجريمة التزوير المعلوماتي

يتميز التشريع المصري بوجود تنظيم تشريعي أكثر تخصصا في مجال الجرائم المعلوماتية، حيث اعتمد المشرع على قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 باعتباره الإطار القانوني

¹ سالم، محمد علي، وهجيج، حسون عبيد، "المرجع السابق ذكره ص 90

² شريهان، ممدوح حسن، "الجريمة الإلكترونية وسبل مواجهتها على المستويين الوطني والدولي"، المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية، عمان، العدد 21، 2020. ص 368

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

الأساسي الذي ينظم الجرائم المرتكبة في البيئة الرقمية، إلى جانب قانون التوقيع الإلكتروني رقم 15 لسنة 2004 وقانون العقوبات.

أما المشرع الجزائري فقد اعتمد على مجموعة من النصوص القانونية المتفرقة، تشمل قانون العقوبات، والقانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والقانون رقم 04-15 المتعلق بالتوقيع والتصديق الإلكترونيين، ثم القانون رقم 02-24 المتعلق بمكافحة التزوير واستعمال المزور.

وعليه، يتجه التنظيم المصري نحو التخصص التشريعي بصورة أوضح، بينما يقوم التنظيم الجزائري على توزيع الأحكام بين عدة نصوص قانونية متكاملة¹.

ب - الاختلاف في تنظيم جريمة التزوير المعلوماتي

لم ينص المشرع المصري على جريمة مستقلة تحمل تسمية «التزوير المعلوماتي»، وإنما عالج صورها من خلال تجريم اصطناع الحسابات والمواقع الإلكترونية، والاعتداء على البيانات والبرامج، وتزوير وسائل الدفع الإلكتروني، مع إمكانية تطبيق أحكام التزوير التقليدي متى تعلق الأمر بمحررات إلكترونية تتمتع بالحجية القانونية.

أما المشرع الجزائري فقد خطا خطوة أبعد من ذلك، خاصة بعد صدور القانون رقم 02-24 المتعلق بمكافحة التزوير واستعمال المزور، حيث وسع نطاق الحماية الجنائية ليشمل المحررات الإلكترونية والتوقيعات الرقمية والوثائق البيومترية، وربطها مباشرة بأحكام التزوير واستعمال المزور². ومن ثم يظهر أن المشرع الجزائري اتجه إلى إدماج المحررات الإلكترونية ضمن منظومة التزوير بصورة أكثر صراحة مقارنة بالمشرع المصري.

ت - الاختلاف في نطاق الحماية الجنائية

يمتد نطاق الحماية في التشريع المصري إلى الحسابات الإلكترونية والمواقع والبريد الإلكتروني والأنظمة المعلوماتية وقواعد البيانات، حيث ركز قانون مكافحة جرائم تقنية المعلومات على حماية الفضاء الإلكتروني بمختلف مكوناته التقنية.

¹ المرجع نفسه ص 369

² شريهان، ممدوح حسن، "المرجع السابق ذكره ص 370

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

أما التشريع الجزائري فقد ركز بصورة أكبر على حماية المعطيات الإلكترونية والمحركات الرقمية والوثائق الرسمية والبيومترية، مع ربط الحماية بفكرة الثقة العامة التي تمثل الأساس التقليدي لجرائم التزوير. وبذلك يظهر أن الحماية المصرية تتجه نحو حماية البيئة الرقمية بمفهومها الواسع، في حين أن الحماية الجزائرية تركز بصورة أكبر على حماية البيانات والمحركات الإلكترونية باعتبارها وسيلة للإثبات والتوثيق¹.

ث- الاختلاف في التنظيم الإجرائي

أفرد المشرع المصري ضمن قانون مكافحة جرائم تقنية المعلومات أحكاما إجرائية مفصلة تتعلق بحجية الدليل الرقمي، وحجب المواقع الإلكترونية، ومنع السفر، وإلزام مقدمي الخدمة بحفظ بيانات المستخدمين لمدة مائة وثمانين يوما، فضلا عن تحديد اختصاص المحاكم الاقتصادية بنظر هذه الجرائم.

أما المشرع الجزائري فقد نظم الجوانب الإجرائية من خلال قانون الإجراءات الجزائية والقانون رقم 09-04، حيث منح الضبطية القضائية سلطات خاصة في مجال التفتيش الإلكتروني وتتبع البيانات وحجز الأدلة الرقمية، دون أن يجمع جميع هذه الأحكام داخل قانون موحد خاص بالجرائم المعلوماتية².

وعليه، يبدو التنظيم الإجرائي المصري أكثر تفصيلا وتخصصا، بينما يعتمد التنظيم الجزائري على التكامل بين عدة نصوص قانونية وإجرائية.

ج- الاختلاف في المسؤولية الجنائية للشخص الاعتباري

أقر المشرع المصري بصورة صريحة المسؤولية الجنائية للشخص الاعتباري في المادة 36 من قانون مكافحة جرائم تقنية المعلومات، حيث يمكن مساءلة الشركة أو المؤسسة إذا ارتكبت الجريمة باسمها أو لحسابها، مع معاقبة المسؤول عن الإدارة الفعلية متى ثبت علمه بالجريمة أو تقصيره في الرقابة.

أما المشرع الجزائري فيبقى الأساس العام للمسؤولية الجنائية قائما على الشخص الطبيعي، مع إمكانية مساءلة الشخص المعنوي وفقا للقواعد العامة الواردة في قانون العقوبات، دون وجود تنظيم خاص ومفصل

¹المرجع نفسه ص371

²شريهان، ممدوح حسن، "المرجع السابق ذكره ص.372

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

للمسؤولية الجنائية للشخص الاعتباري في جرائم التزوير المعلوماتي يماثل ما هو موجود في التشريع المصري¹.

ح- الاختلاف في العقوبات المقررة

يتجه المشرع المصري إلى فرض عقوبات مالية مرتفعة نسبيا في جرائم تقنية المعلومات، حيث تصل الغرامات في بعض الحالات إلى مليون جنيه مصري، بالإضافة إلى عقوبات الحبس والسجن المشدد عند المساس بالأمن القومي أو الأنظمة الحكومية.

أما المشرع الجزائري فيعتمد بصورة أكبر على العقوبات السالبة للحرية المقررة في قانون العقوبات والقانون رقم 02-24، مع غرامات مالية متفاوتة بحسب طبيعة الجريمة والجهة المستهدفة².

ويلاحظ أن التشريع المصري يركز على الردع المالي إلى جانب العقوبات السالبة للحرية، في حين يميل التشريع الجزائري إلى التشديد الجنائي التقليدي المرتبط بعقوبات الحبس والسجن.

خ- الاختلاف في الجهة القضائية المختصة

أسند المشرع المصري الاختصاص بنظر جرائم تقنية المعلومات إلى المحاكم الاقتصادية والنيابات الاقتصادية المتخصصة، وذلك بهدف توفير قضاة وأعضاء نيابة ذوي خبرة في الجرائم التقنية والأدلة الرقمية.

أما في الجزائر، فتخضع جرائم التزوير المعلوماتي للاختصاص العادي لجهات القضاء الجزائي، مع إمكانية الاستعانة بالخبرة الفنية والمصالح المختصة في مجال الجرائم الإلكترونية، دون وجود محاكم متخصصة حصرا في الجرائم المعلوماتية³.

د- الاختلاف في السياسة التشريعية المعتمدة

يقوم التشريع المصري على سياسة تشريعية استباقية تعتمد على إصدار قانون خاص وشامل لمكافحة جرائم تقنية المعلومات يتضمن أحكاما موضوعية وإجرائية متكاملة.

¹المرجع نفسه ص373

²المرجع نفسه ص374

³سالم محمد علي، وهجيج، حسون عبيد، "المرجع السابق ذكره" ص 95

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

في المقابل، تعتمد السياسة التشريعية الجزائرية على مبدأ التدرج التشريعي، حيث تم تطوير المنظومة القانونية عبر مراحل متعاقبة من خلال تعديل قانون العقوبات، ثم إصدار قوانين متخصصة في التوقيع الإلكتروني والجرائم المعلوماتية والتزوير واستعمال المزور.

وعليه، يمكن القول إن المشرع المصري اتجه إلى توحيد الأحكام المتعلقة بالجرائم المعلوماتية داخل إطار تشريعي متخصص، بينما فضل المشرع الجزائري توزيع المعالجة القانونية بين عدة نصوص متكاملة، وهو ما يمثل أبرز نقطة اختلاف بين النظامين القانونيين في مجال مكافحة التزوير المعلوماتي¹.

المطلب الثالث: التقييم القانوني للتشريعين المصري والجزائري في مجال التزوير المعلوماتي

أدى التطور المتسارع لتكنولوجيا المعلومات والاتصالات إلى فرض تحديات جديدة أمام التشريعات الجنائية التقليدية، خاصة في مجال التزوير المعلوماتي الذي أصبح يشكل تهديدا حقيقيا لأمن المعاملات الإلكترونية والثقة في المحررات الرقمية. وقد سعى كل من المشرع المصري والمشرع الجزائري إلى مواكبة هذه التحولات من خلال استحداث نصوص قانونية خاصة تهدف إلى تجريم الأفعال الماسة بالبيانات والأنظمة المعلوماتية وتوفير الحماية اللازمة للمحررات الإلكترونية. غير أن تقييم فعالية هذه النصوص يقتضي الوقوف على مدى نجاحها في تحقيق الحماية الجنائية المطلوبة ومدى قدرتها على الاستجابة للتحديات العملية التي تثيرها الجرائم المعلوماتية².

أ- تقييم السياسة التشريعية المعتمدة في مكافحة التزوير المعلوماتي

يتبين من خلال دراسة التشريعين أن كلا المشرعين تبني سياسة جنائية تقوم على توسيع نطاق الحماية القانونية لتشمل البيانات والمحررات الإلكترونية إلى جانب المحررات التقليدية. فقد اتجه المشرع المصري إلى سن قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 باعتباره إطارا تشريعا متكاملا يتضمن أحكاما موضوعية وإجرائية خاصة بالجرائم المعلوماتية، كما عزز هذه الحماية من خلال قانون التوقيع الإلكتروني رقم 15 لسنة 2004.

أما المشرع الجزائري فقد اعتمد سياسة تشريعية تدرجية تمثلت في تعديل قانون العقوبات واستحداث نصوص خاصة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ثم إصدار القانون رقم 04-15

¹المرجع نفسه ص96

²سوير سفيان، جرائم المعلوماتية، مذكرة ماجستير في العلوم الجنائية والإجرام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، الجزائر، 2011، ص69

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

المتعلق بالتوقيع والتصديق الإلكترونيين، وأخيرا القانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور. وقد سمح هذا المسار التشريعي بتوسيع الحماية الجنائية لتشمل مختلف صور التزوير المرتبطة بالبيئة الرقمية.

ويكشف ذلك عن إدراك المشرعين للتحويلات التي فرضتها الثورة الرقمية وحرصهما على توفير إطار قانوني يضمن حماية الثقة العامة في المعاملات الإلكترونية¹.

ب- مدى فعالية الحماية الجنائية المقررة للبيانات والمحركات الإلكترونية

يلاحظ أن التشريعين نجحا إلى حد كبير في تجاوز المفهوم التقليدي للمحرر الذي كان يقتصر على الدعامة الورقية، وأقرا مبدأ المساواة بين المحركات التقليدية والمحركات الإلكترونية من حيث الحجية القانونية والحماية الجنائية. كما وسعا نطاق التجريم ليشمل مختلف صور الاعتداء على البيانات والأنظمة المعلوماتية والتوقيعات الإلكترونية.

وقد عزز المشرع المصري هذه الحماية من خلال النص على جرائم مستقلة تتعلق بالدخول غير المشروع إلى الأنظمة المعلوماتية والاعتداء على البيانات الإلكترونية واصطناع الحسابات والمواقع الإلكترونية. كما منح الأدلة الرقمية حجية قانونية خاصة وقرر آليات إجرائية متطورة للكشف عن الجرائم المعلوماتية. وبالمقابل، عمل المشرع الجزائري على تدعيم الحماية الجنائية للمعطيات الإلكترونية من خلال النصوص الواردة في قانون العقوبات والقوانين الخاصة، مع إقرار وسائل تقنية وقانونية لمكافحة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال².

ورغم أهمية هذه الأحكام، فإن فعالية الحماية القانونية تبقى مرتبطة بمدى قدرة الأجهزة المختصة على تطبيقها ومواكبة التطور التقني المستمر الذي يميز هذا النوع من الجرائم.

ت- التحديات القانونية والعملية التي تواجه تطبيق النصوص المنظمة للتزوير المعلوماتي

على الرغم من التطور الذي عرفته المنظومتان التشريعتان، فإن التطبيق العملي يكشف عن وجود جملة من التحديات التي تؤثر في فعالية مكافحة التزوير المعلوماتي.

¹ المرجع نفسه ص ص 71-0

² سوير سفيان، المرجع السابق ذكره ص ص 39-40

الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

ويأتي في مقدمة هذه التحديات الطابع التقني المعقد للجريمة، إذ تتطلب عملية الكشف عنها وإثباتها خبرة فنية متخصصة في مجال الأنظمة المعلوماتية والأدلة الرقمية. كما أن سهولة محو البيانات أو تعديلها أو إخفائها تجعل عملية الإثبات أكثر تعقيدا مقارنة بالجرائم التقليدية¹.

ويضاف إلى ذلك الطابع العابر للحدود الذي يميز الجرائم المعلوماتية، حيث قد يرتكب الجاني فعله من دولة ويظهر أثره في دولة أخرى، مما يثير إشكالات تتعلق بالاختصاص القضائي والتعاون الدولي وتنفيذ إجراءات الملاحقة الجنائية.

كما أن التطور المستمر للوسائل التقنية المستعملة في التزوير الرقمي يفرض على المشرعين والأجهزة المكلفة بإنفاذ القانون مواكبة دائمة لهذه المستجدات حتى لا تصبح النصوص القانونية أقل قدرة على مواجهة الأشكال الحديثة للإجرام المعلوماتي.

ومن خلال ذلك يتضح أن التشريعين المصري والجزائري قد وفرا أساسا قانونيا مهما لمكافحة التزوير المعلوماتي، غير أن فعالية هذه الحماية تبقى رهينة بقدرة المنظومة القانونية والمؤسسية على التكيف المستمر مع التطورات التقنية التي تشهدها البيئة الرقمية².

خلاصة الفصل :

أبرزت هذه الدراسة أن جريمة التزوير المعلوماتي تعد من أخطر الجرائم المستحدثة التي أفرزها التطور التكنولوجي والاعتماد المتزايد على الوسائل الرقمية في مختلف المعاملات. وقد أدى انتقال المعاملات من البيئة التقليدية إلى البيئة الإلكترونية إلى ظهور صور جديدة للتزوير تستهدف البيانات والمحركات الإلكترونية والأنظمة المعلوماتية. وللتصدي لهذه المخاطر، تدخل كل من المشرع الجزائري والمشرع المصري بوضع قواعد قانونية خاصة تهدف إلى حماية الثقة في المعاملات الإلكترونية وضمان سلامة البيانات الرقمية. كما تبين أن التشريعين اتفقا في تجريم الأفعال الماسة بالمحركات الإلكترونية والاعتراف بحجية الدليل الرقمي واعتماد آليات خاصة للتحري والتحقيق. وفي المقابل، ظهرت بعض الاختلافات المتعلقة بالسياسة التشريعية المعتمدة ونطاق الحماية القانونية والتنظيم الإجرائي والعقوبات المقررة. وقد كشفت الدراسة كذلك أن فعالية مكافحة التزوير المعلوماتي لا تتوقف على النصوص القانونية فحسب، بل

¹ سالم، محمد علي، وهجيج، حسون عبيد، "المرجع السابق ذكره ص 99

² سوير سفيان، المرجع السابق ذكره ص.48

الفصل الثاني:.....جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري

تتطلب أيضا تطوير الوسائل التقنية وتعزيز الخبرة الفنية لدى الجهات المختصة. وعليه، يشكل التزوير المعلوماتي تحديا متجددا يفرض على التشريعات الجنائية مواصلة التكيف مع التطورات الرقمية بما يضمن حماية فعالة للمعاملات الإلكترونية وتحقيق الأمن القانوني والمعلوماتي.

الخاتمة

الخاتمة.....

أدى التطور الهائل الذي شهدته تكنولوجيا المعلومات والاتصالات خلال العقود الأخيرة إلى إحداث تحولات عميقة في مختلف مجالات الحياة، حيث أصبحت المعاملات الإدارية والمالية والتجارية تعتمد بشكل متزايد على الوسائط الرقمية والأنظمة المعلوماتية. وقد ساهم هذا التحول في تحقيق العديد من المزايا المتعلقة بسرعة إنجاز المعاملات وتبادل المعلومات وتخزينها، غير أنه أفرز في المقابل أنماطا جديدة من السلوك الإجرامي لم تكن معروفة في البيئة التقليدية، ومن أبرزها جريمة التزوير المعلوماتي التي أصبحت تشكل تهديدا حقيقيا للثقة العامة ولأمن المعاملات الإلكترونية.

وتكتسب هذه الجريمة خطورتها من كونها تستهدف البيانات والمحركات الإلكترونية التي أصبحت تؤدي وظائف جوهرية في إثبات الحقوق والالتزامات، كما أن ارتكابها يتم باستخدام وسائل تقنية متطورة تتيح للجاني إمكانية تغيير الحقيقة أو اصطناعها أو إخفاء آثار فعله في وقت وجيز، وهو ما يجعل اكتشافها وإثباتها أكثر تعقيدا مقارنة بجرائم التزوير التقليدية. كما أن الطبيعة العابرة للحدود التي تتميز بها الجرائم المعلوماتية تزيد من صعوبة ملاحقة مرتكبيها وتفرض ضرورة تطوير آليات التعاون الدولي في هذا المجال.

وقد هدفت هذه الدراسة إلى بيان الإطار القانوني لجريمة التزوير المعلوماتي وتحليل مختلف الجوانب المرتبطة بها، من خلال التطرق إلى مفهومها وخصائصها وأركانها القانونية، ثم دراسة التنظيم التشريعي الذي اعتمده كل من المشرع الجزائري والمشرع المصري لمواجهتها، مع إجراء مقارنة بين النظامين القانونيين للكشف عن أوجه التشابه والاختلاف بينهما وتقييم مدى فعالية الحماية الجنائية التي يوفرها كل منهما.

ومن خلال تحليل النصوص القانونية محل الدراسة، تبين أن كلا المشرعين قد أدركا خطورة التزوير المعلوماتي وآثاره السلبية على الأفراد والمؤسسات والدولة، الأمر الذي دفعهما إلى توسيع نطاق الحماية الجنائية ليشمل المحركات الإلكترونية والبيانات الرقمية والتوقيعات الإلكترونية. كما حرصا على تطوير قواعد الإثبات الجنائي بما يسمح بالاعتراف بالدليل الرقمي ومنحه قيمة قانونية تمكن الجهات القضائية من الاستناد إليه في إثبات الجرائم المعلوماتية.

كما أظهرت الدراسة أن التشريع المصري اتجه نحو اعتماد تنظيم قانوني متخصص من خلال قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، الذي جمع بين الأحكام الموضوعية

الخاتمة.....

والإجرائية المتعلقة بالجرائم المعلوماتية داخل إطار قانوني موحد، في حين اعتمد التشريع الجزائري على سياسة تشريعية تدرجية تقوم على توزيع الأحكام القانونية بين قانون العقوبات والقوانين الخاصة المتعلقة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتوقيع الإلكتروني ومكافحة التزوير واستعمال المزور.

ورغم الجهود التشريعية المبذولة في كلا البلدين، فإن الواقع العملي يبين أن مكافحة التزوير المعلوماتي ما تزال تواجه العديد من التحديات المرتبطة بالتطور التقني المتسارع وظهور وسائل جديدة لارتكاب الجريمة، فضلا عن الصعوبات المتعلقة بالكشف عن الجناة وجمع الأدلة الرقمية وإثباتها أمام القضاء. وهو ما يفرض مواصلة تحديث التشريعات وتعزيز الإمكانيات التقنية والبشرية للجهات المختصة، بما يضمن تحقيق حماية جنائية فعالة تتناسب مع طبيعة البيئة الرقمية ومتطلباتها.

النتائج

وعلى إثر ما سبق، يمكن استخلاص النتائج الآتية:

- 1- أظهر البحث أن التزوير المعلوماتي يمثل امتدادا حديثا لجريمة التزوير التقليدية، غير أنه يتميز بخصوصية محل الجريمة المتمثل في البيانات والمحركات الإلكترونية والأنظمة المعلوماتية.
- 2- تبين أن المشرعين المصري والجزائري قد اعترفا بالحاجة القانونية للمحركات الإلكترونية والتوقيعات الرقمية، وأخضعوها للحماية الجنائية المقررة للمحركات التقليدية متى توافرت الشروط القانونية اللازمة.
- 3- كشفت الدراسة عن وجود تقارب كبير بين التشريعين في مجال تجريم الأفعال الماسة بالبيانات والأنظمة المعلوماتية والاعتراف بالدليل الرقمي وتطوير إجراءات البحث والتحقيق في الجرائم المعلوماتية.
- 4- أظهرت المقارنة أن التشريع المصري يتميز بوجود إطار قانوني أكثر تخصصا وشمولا في مجال مكافحة الجرائم المعلوماتية، بينما يعتمد التشريع الجزائري على تكامل مجموعة من النصوص القانونية لمعالجة مختلف جوانب الجريمة.
- 5- أكدت الدراسة أن فعالية مكافحة التزوير المعلوماتي لا ترتبط فقط بوجود نصوص قانونية تجرم هذه الأفعال، وإنما تتوقف كذلك على توفر الخبرة التقنية والوسائل الفنية الحديثة والتعاون الوطني والدولي في مجال مكافحة الجرائم المعلوماتية.

التوصيات

- 1- ضرورة الاستمرار في مراجعة وتحديث التشريعات المتعلقة بالجرائم المعلوماتية بصورة دورية لضمان مواكبتها للتطورات التقنية المستمرة وظهور أساليب جديدة للتزوير الرقمي.
- 2- تعزيز التكوين والتدريب المتخصص للقضاة وأعضاء النيابة العامة وأعوان الضبطية القضائية في مجالات الأدلة الرقمية والتحقيقات المعلوماتية والأمن السيبراني.
- 3- دعم المخابر الجنائية الرقمية وتجهيزها بالتقنيات الحديثة والخبرات المتخصصة التي تمكنها من فحص الأدلة الإلكترونية وتحليلها بكفاءة عالية.
- 4- تكثيف التعاون القضائي والأمني الدولي وتبادل المعلومات والخبرات بين الدول لمواجهة الجرائم المعلوماتية ذات الطابع العابر للحدود وملاحقة مرتكبيها.
- 5- نشر الثقافة القانونية والوعي المعلوماتي لدى الأفراد والمؤسسات حول مخاطر التزوير المعلوماتي ووسائل الوقاية منه، مع تشجيع اعتماد أنظمة الحماية الإلكترونية والتوقيع الرقمي الموثوق.

آفاق الدراسة

تفتح هذه الدراسة آفاقا واسعة للبحث العلمي في مجال الجرائم المعلوماتية، خاصة في ظل التطورات المتسارعة التي يشهدها العالم الرقمي. ومن أبرز المواضيع التي تستحق الدراسة مستقبلا أثر تقنيات الذكاء الاصطناعي في ارتكاب جرائم التزوير المعلوماتي، ومدى كفاية التشريعات الحالية لمواجهة التزوير الناتج عن تقنيات التزييف العميق، ودور تقنية البلوك تشين في تعزيز حماية المحررات الإلكترونية والحد من مخاطر التزوير الرقمي. كما تبرز أهمية إجراء دراسات مقارنة أوسع تشمل التشريعات الدولية والاتفاقيات ذات الصلة بهدف الاستفادة من التجارب القانونية الرائدة في هذا المجال.

وفي الأخير، يمكن القول إن التزوير المعلوماتي أصبح من أبرز التحديات الجنائية التي فرضها العصر الرقمي، الأمر الذي يستوجب تضافر الجهود التشريعية والقضائية والتقنية من أجل توفير حماية قانونية فعالة للبيانات والمحررات الإلكترونية. كما أن تحقيق الأمن المعلوماتي وتعزيز الثقة في المعاملات الرقمية يظل رهينا بقدرة التشريعات الوطنية على مواكبة التطورات التكنولوجية المتلاحقة، وبمدى استعداد المؤسسات المختصة لتطوير وسائلها وآليات عملها بما يضمن مواجهة فعالة لهذا النوع من الجرائم المستحدثة وحماية المصالح الفردية والجماعية في البيئة الرقمية الحديثة.

قائمة المراجع

قائمة المراجع.....

المصادر:

أولاً: النصوص القانونية الجزائرية

- الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات الجزائري .
- القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، الصادر بتاريخ 16 أوت 2009 .
- القانون رقم 15-04 المؤرخ في 11 ربيع الثاني 1436 الموافق لـ 01 فبراير 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 06، الصادرة بتاريخ 10 فبراير 2015 .
- القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 34، الصادرة بتاريخ 17 يونيو سنة 2018 .
- القانون رقم 24-02 المؤرخ في 16 شعبان عام 1445 الموافق 26 فبراير سنة 2024، والمتعلق بمكافحة التزوير واستعمال المزور، الصادر في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 15 بتاريخ 29 فبراير 2024 .
- القانون رقم 24-04 المؤرخ في 26 فبراير 2024، المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية .
- الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، المعدل والمتمم .
- القانون رقم 24-06 المؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2024، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات الجزائري .

قائمة المراجع

ثانياً: النصوص القانونية المصرية

- قانون العقوبات رقم 58 لسنة 1937، الصادر بتاريخ 31 يوليو 1937، والمنشور في الوقائع المصرية بالعدد رقم (71) بتاريخ 5 أغسطس 1937، والمعمول به اعتباراً من 15 أكتوبر 1937 .
- قانون تنظيم التوقيع الإلكتروني رقم 15 لسنة 2004، الصادر عن رئيس الجمهورية بتاريخ 21 أبريل 2004، والمنشور في الجريدة الرسمية بجمهورية مصر العربية في العدد رقم 17 تابع (د) بتاريخ 22 أبريل 2004، والمعمول به اعتباراً من 23 أبريل 2004 .
- قانون رقم 175 لسنة 2018 الصادر في 14 أغسطس 2018 والمتعلق بمكافحة جرائم تقنية المعلومات، نُشر في الجريدة الرسمية لجمهورية مصر العربية بالعدد 32 مكرر (أ) الصادر بتاريخ 14 أغسطس 2018 .

المراجع :

الكتب :

1. أحمد أبو الروس، جرائم التزيف والتزوير والرشوة والاختلاس والمال العام، الكتاب الخامس، المكتب الجامعي الحديث، الإسكندرية، د.س .
2. أحمد أمين، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، دون تاريخ نشر .
3. أحمد عبد الله، الجرائم البيئية في مصر، دار الفكر العربي، القاهرة، 2021 .
4. إبراهيم، محمد السيد، السياسة الجنائية لمواجهة الجرائم السيبرانية في مصر، المركز القومي للإصدارات القانونية، القاهرة، 2022 .
5. بوصقعة، أحسن، التحقيق القضائي، ط6، دار هومة للطباعة والنشر، الجزائر، 2006 .
6. حسين، محمد حسن، المسؤولية الجنائية عن الجرائم الإلكترونية في القانون المصري، دار الكتب القانونية، 2018 .
7. عبد العزيز محمد الصغير، الضمانات الدستورية للمواطنين بين الشريعة والقانون، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2011 .

قائمة المراجع.....

8. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، مصر، 2019 .
9. علي، محمود عبد العزيز، جرائم الإنترنت ووسائل مكافحتها في التشريع المصري، دار الفكر والقانون، المنصورة، 2019 .
10. الفوزان، محمد بن براك، المفاهيم والأبعاد في الاستراتيجية الوطنية لحماية النزاهة ومكافحة الفساد الصادرة بقرار مجلس الوزراء رقم 43، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، 1433هـ/2012م .
11. إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، الدار الجامعية الجديدة، الإسكندرية، 2008 .
12. مجدي سلامة محمود، الجرائم الإلكترونية في القانون المصري، دار النهضة العربية، القاهرة، 2020 .
13. مجيد سحر فؤاد، الجرائم المستحدثة: دراسة معمقة ومقارنة في عدة جرائم، الطبعة الأولى، المركز العربي للنشر والتوزيع، جمهورية مصر العربية، 2019 .
14. يوسف خالد محمد، التزوير الإلكتروني وإشكالات الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، 2021 .

المقالات :

15. إبراهيم الديب حسانين زايد، "جريمة التزوير المعلوماتية: دراسة مقارنة في القانون الفرنسي والمصري والعراقي"، مجلة جامعة البيان للدراسات والبحوث القانونية، المجلد 4، العدد 1، جامعة البيان، العراق .
16. أجعود، سعاد، "السياسة الجنائية للمشروع الجزائري في مواجهة جرائم التزوير للحصول على الإعانات والمساعدات العمومية والإعفاءات الاجتماعية في ظل جائحة كوفيد 19: دراسة تحليلية في ضوء الأمر 20-06 المعدل والمتمم لقانون العقوبات الجزائري"، مجلة الحقوق والعلوم السياسية، المجلد 9، العدد 2، 2022 .

قائمة المراجع.....

17. أمين، محمد صبحي، "الطبيعة القانونية لجريمة التزوير في المحررات الرسمية"، مجلة القانون العام الجزائري المقارن، جامعة جيلالي اليابس، سيدي بلعباس، 2017 .
18. بن لعربي أسماء، والفحمة مديحة، "التزوير المعلوماتي في عصر الرقمنة: بين قابلية الخضوع للقواعد العامة وضرورة تبني نصوص خاصة"، مجلة الفكر القانوني والسياسي، المجلد 8، العدد 2، 2024 .
19. بن نوارن عبد الرحمن، "الإطار القانوني لممارسة الطعن ضد المحررات الرسمية أمام القضاء في التشريع الجزائري"، مجلة الحقوق والعلوم الإسلامية، جامعة الجلفة، العدد 14، أبريل 2021 .
20. شعباني، نوال، "مظاهر تفعيل قواعد مكافحة جرائم التزوير المقررة بموجب القانون رقم 02-24 المتعلق بمكافحة التزوير واستعمال المزور"، Revue critique de droit et sciences politiques، المجلد 20، العدد 1، 2025 .
21. شرقي الأخضر، "الأساليب الخاصة للبحث والتحري عن الجرائم المستحدثة في التشريع الجزائري"، مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد 10، العدد 2، 2025 .
22. شريهان، ممدوح حسن، "الجريمة الإلكترونية وسبل مواجهتها على المستويين الوطني والدولي"، المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية والتربوية، عمان، العدد 21، 2020 .
23. عادل محمد الشرجي، عبد السلام محمد المايل، علي قابوسة، "الجريمة الإلكترونية في الفضاء الإلكتروني: المفهوم، الأسباب، سبل المكافحة مع التعرض لحالة ليبيا"، مجلة الجريمة الإلكترونية في الفضاء الإلكتروني، العدد 04 .
24. عيمور راضية، "الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري"، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 6، العدد 1، جامعة عمار ثليجي بالأغواط، الجزائر، 2022 .
25. جارش عادل، "الإرهاب الجديد: دراسة في المفهوم والطبيعة والأنواع وإجراءات المواجهة"، مجلة العلوم القانونية والسياسية، المجلد 9، العدد 3، 2018 .
26. خليف فتحة، ومهداوي محمد صالح، "التزوير المعلوماتي في البيئة الرقمية"، مجلة الدراسات القانونية، المجلد 8، العدد 2، 2022 .
27. دمحم علي سالم، وحسون عبيد هجيج، "الجريمة المعلوماتية"، مجلة جامعة بابل للعلوم الإنسانية، جامعة بابل، العراق، المجلد 14، العدد 2، 2007 .
28. د. طه عثمان المغربي، "تزوير المحررات الإلكترونية"، مجلة البحوث القانونية والاقتصادية، العدد 72، 2020 .

قائمة المراجع.....

29. رامي متولي القاضي، "المواجهة الجنائية لجرائم تقنية المعلومات في التشريع المصري في ضوء أحكام القانون رقم (175) لسنة 2018م مقارنًا بالمواثيق الدولية والتشريعات المقارنة"، مجلة كلية الشرطة، العدد 75، مارس 2021 .
30. زنتوت عبد الكريم، "الجريمة الإلكترونية وسبل مواجهتها في الجزائر"، مجلة الحقوق والحريات، المجلد 13، العدد 01، جامعة محمد خيضر بسكرة، الجزائر، 2025 .
31. عبد الله بلقاسم، "الطبيعة الخاصة لجريمة التزوير في المحررات الإلكترونية"، مجلة الدراسات القانونية المقارنة، المجلد 06، العدد 02، جامعة التكوين المتواصل، تيزي وزو، 2020 .
32. محمد الطاهر رحال، "مراجعة التحقيق القضائي في التشريع الجزائري"، مجلة طبنة للدراسات العلمية الأكاديمية، المجلد 5، العدد 5، 2020 .
33. مراد عبد الجابر الرجحي، "جريمة التزوير الإلكتروني كجريمة مستحدثة في التشريع الجزائري"، كلية الحقوق، جامعة القاهرة، العدد 20، سنة 2020 .
34. إسماعيل محمد صادق، "الجريمة الإلكترونية في مصر وأساليب مكافحتها"، ضمن كتاب :الجرائم الإلكترونية، منشور إلكترونياً بتاريخ 01 يوليو 2022 .

المذكرات :

أولاً: أطروحات الدكتوراه

35. بلقاسم محبوب، *التزوير الإلكتروني*، أطروحة دكتوراه، كلية الحقوق، جامعة محمد خيضر بسكرة، 2016-2017 .
36. صدراتي وفاء، *آليات مكافحة جريمة التزوير الإلكتروني*، أطروحة لنيل شهادة دكتوراه العلوم في القانون الجنائي، جامعة العربي التبسي، تبسة، 2014-2015 .
37. وهاب سعيدة، *آليات مكافحة جريمة التزوير الإلكتروني*، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، جامعة العربي بن مهيدي، 2020-2021 .
38. براهيم حنان، *جريمة التزوير في الوثيقة الإدارية ذات الطبيعة المعلوماتية*، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2015 .

قائمة المراجع.....

39. عواد حامد هادي عواد، صور وأنماط الجرائم المستحدثة في القانون الجنائي، أطروحة دكتوراه في الحقوق، قسم القانون الجنائي، كلية الحقوق، جامعة المنصورة، 2026 .

ثانياً: مذكرات الماجستير

40. طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة ماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2011-2012 .

41. براهيم يوسف، جريمة التزوير في المحررات الرسمية وفق القانون الجزائري، رسالة ماجستير، جامعة الجزائر 1، 2019 .

42. عبد الله بن جلوي عبد الله الأبرقي، الضرر في جريمة تزوير المحررات، رسالة ماجستير، كلية الدراسات العليا، قسم العدالة الجنائية، 2007-2008 .

43. المستاري نور الهدى، التزوير واستعمال المزور في الصفقات العمومية، مذكرة ماجستير في إطار مدرسة الدكتوراه في القانون، جامعة الجيلالي الياصب، سيدي بلعباس، 2012-2013 .

44. سوير سفيان، جرائم المعلوماتية، مذكرة ماجستير في العلوم الجنائية والإجرام، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، الجزائر، 2011.

فهرس المحتويات

	شكر وعرفان
	الاهداء
أ	مقدمة
الفصل الأول: الإطار المفاهيمي لجريمة التزوير المعلوماتي	
10	المبحث الأول: ماهية جريمة التزوير المعلوماتي
10	المطلب الأول :تعريف التزوير المعلوماتي في الفقه والقانون
15	المطلب الثاني :تمييز التزوير المعلوماتي عن الجرائم المشابهة
18	المطلب الثالث :خصائص جريمة التزوير المعلوماتي
20	المبحث الثاني: الأساس القانوني لجريمة التزوير المعلوماتي
20	المطلب الأول :أركان الجريمة
30	المطلب الثاني :محل الجريمة
34	المطلب الثالث :القواعد الإجرائية لمكافحة جريمة التزوير
الفصل الثاني: جريمة التزوير المعلوماتي بين التشريع الجزائري والمصري	
48	المبحث الأول: التنظيم القانوني لجريمة التزوير المعلوماتي في التشريع المصري
48	المطلب الأول: الأساس التشريعي لتجريم التزوير المعلوماتي في القانون المصري .
58	المطلب الثاني: الأحكام الموضوعية لجريمة التزوير المعلوماتي
69	المطلب الثالث: الأحكام الإجرائية الخاصة بمكافحة التزوير المعلومات
73	المبحث الثاني: أوجه المقارنة بين التشريعين المصري و الجزائري
73	المطلب الأول :أوجه التشابه
77	المطلب الثاني :أوجه الاختلاف
80	المطلب الثالث :التقييم القانوني واقتراحات التطوير
86	الخاتمة
	قائمة المراجع
	ملخص

ملخص الدراسة:

تناولت هذه الدراسة جريمة التزوير المعلوماتي باعتبارها من أخطر الجرائم المستحدثة الناتجة عن التطور التكنولوجي والاعتماد المتزايد على الأنظمة المعلوماتية في مختلف المعاملات. هدفت الدراسة إلى بيان مفهوم التزوير المعلوماتي وخصائصه وأركانه القانونية، وتحليل الإطار التشريعي المنظم له في كل من الجزائر ومصر. كما سعت إلى إبراز أوجه التشابه والاختلاف بين التشريعين في مجال مكافحة هذه الجريمة، من خلال دراسة النصوص الموضوعية والإجرائية والعقوبات المقررة لها. واعتمدت الدراسة على المنهج الوصفي والتحليلي والمقارن لفهم مختلف الجوانب القانونية المرتبطة بالموضوع. وتوصلت إلى أن كلا التشريعين قد خطا خطوات مهمة في مواجهة التزوير المعلوماتي، غير أن التطور المتسارع للتقنيات الرقمية يفرض مواصلة تحديث المنظومة القانونية وتعزيز آليات الحماية الجنائية للبيئة الرقمية بما يضمن فعالية أكبر في مكافحة هذا النوع من الجرائم .

الكلمات المفتاحية: التزوير المعلوماتي، الجريمة الإلكترونية، المحررات الإلكترونية، البيانات الرقمية، التشريع الجزائري، التشريع المصري، الحماية الجنائية، الجرائم المعلوماتية.

Abstract

This study examines cyber forgery as one of the most serious crimes resulting from technological development and the widespread use of information systems in modern transactions. It aims to clarify the concept, characteristics, and legal elements of cyber forgery, while analyzing the legal framework governing this crime in both Algerian and Egyptian legislation. The study also highlights the similarities and differences between the two legal systems in combating cyber forgery through an examination of the relevant substantive and procedural rules and penalties. To achieve its objectives, the research adopts descriptive, analytical, and comparative approaches. The study concludes that both legislations have made significant efforts to address cyber forgery; however, the rapid evolution of digital technologies requires continuous legislative updates and stronger criminal protection mechanisms to ensure effective prevention and prosecution of such crimes.

Keywords:

Cyber Forgery, Cybercrime, Electronic Documents, Digital Data, Algerian Legislation, Egyptian Legislation, Criminal Protection, Information Technology Crimes.