التزوير عبر إستخدام الوسائل الإلكترونية

Forgery through the use of electronic means

م.م منى عصري حمد

Muna asree hamed

كلية أبن خلدون الجامعة

IBN KHALDUN PRIVATE UNIVERSITY COLLEGE

Munaasree2@gmail.com

الملخص

أن جريمة التزوير الإلكتروني شأنها شأن بقية الجرائم الإلكترونية حديثة النشأة، بحيث أن التشريع العراقي يتسم بعدم إحاطة الموضوع بكل جوانبه، فجريمة التزوير الإلكتروني تختلف عن جريمة التزوير التقليدي من حيث الوسيلة المستخدمة ومحل الجريمة، فيشترط لقيام جريمة التزوير الإلكتروني أن يستخدم الحاسب الآلي، وتكون مخرجات هذا الأخير هي محل الجريمة، وبالتالي فإن النصوص المجرمة لتزوير المحررات أي التزوير التقليدي، لا تكفي لمكافحة التزوير الإلكتروني.

وتُعد جريمة التزوير الإلكتروني من الجرائم الحديثة التي تستلزم دراسات مستقبلية لوضع المبادئ العامة لهذه الجريمة، خصوصاً وأنها ترتبط مع التطور الإلكتروني ووسائل الإتصال الحديثة، وهذا ما يتطلب تدخلاً تشريعياً من أجل وضع حماية قانونية متكاملة وسد الثغرات التي تعتري قانون العقوبات وقانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي الجديد.

الكلمات المفتاحية: الجريمة، التزوير، الالكتروني، التشريع العراقي، التزوير التقليدي، الحاسب الالي، المحررات، الجرائم الحديثة، قانون العقوبات، قانون المعاملات الالكترونية.

Abstract

The crime of electronic forgery is like the rest of the newly emerging electronic crimes، so that the Iraqi legislation is characterized by not covering the issue in all its aspects. The latter is the subject of crime، and therefore the texts criminalizing forgery of documents، that is، traditional forgery، are not sufficient to combat electronic forgery.

The crime of electronic forgery is one of the modern crimes that require future studies to establish the general principles of this crime، especially as it is linked with electronic development and modern means of communication، and this requires legislative intervention in order to establish integrated legal protection and fill the gaps in the Penal Code and the Law of Electronic Transactions and Data of Nature The new profile.

keywords: Crime، forgery، electronic، Iraqi legislation، traditional forgery، computer، papers، modern crimes، penal code، electronic transactions law.

المقدمة

يحيط بكل ظاهرة الكثير من الاسئلة التي تتعلق في طبيعتها ،بعد أن تصبح واقعا في حياتنا ومن هنا تأتي أهمية البحث عن التطور التكنلوجي في مجال الاتصال الآلكتروني ،الذي غزا جميع ميادين الحياة بشكل لا يقتصر على النطاق المحلي أو الآقليمي فقط، بل يمتد الى العالم ككل ،حتى أصبح يشكل قلقا لجميع المهتمين بهذا المجال ،في محاولة لتقليل مستوى الآنشطة الأجرامية في المجتمع بعدما أظهرت الاحصائيات أن الجرائم الآلكترونية أصبحت ظاهرة نامية .

وما لاشك فيه أن الجرائم الآلكترونية تمثل ظاهرة اجرامية ذات طبيعة خاصة بها، لآنها ترتكب ضمن نطاق المعالجة الألكترونية للبيانات، سواء أكان في تجميعها أو تجهيزها أو في أدخالها الى الحاسوب من جهة أولى ،أو من خلال توفير إمكانية التحرير والتصحيح والتعديل والمسح والتخزين والاسترجاع والطباعة من جهة أخرى [1].

وتجدر الأشارة هنا الى أن جريمة تزوير البيانات هي من الجرائم الأكثر إنتشارا، فلا تكاد تخلو جريمة من جرائم نظم المعلومات من شكل من أشكال تزوير أو تقليد أو إصطناع توقيع أو كتابة إلكترونية أو ذكية أو أية وسيلة أخرى، أو أستعمال البطاقة الألكترونية المقلدة المزورة مع علمه بذلك، أو أصطناع وثائق أو سجلات أو قيود ألكترونية عمدا أو إحداث تغير أو تلاعب في سند وإستخدامه للمصلحة الشخصية[2].

كما أن أنعكاس الثورة الرقمية التي فجرتها تكنلوجيا الاتصالات غيرت من المفهوم

---

(١) هدى فتوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، مصر، ١٩٩٢، ص ١٨

(٢) كاظم الزيدي ،مكافحة الجرائم المعلوماتية في التشريع العراقي، بحث منشور على موقع www.iraqiga.iq

التقليدي لجريمة التزوير ،وذلك بعد إستخدام ماسحات الليزر الرقمية الملونة وغير الملونة، ودخول الحاسبات الآلية ،ومايرتبط بها من ماسحات وطابعات في ارتكاب التزوير في لمستندات والوثائق[1].

وفي ضوء ذلك يمكننا الجزم بأن الجرائم الالكترونية عامة، وجريمة التزوير الالكتروني حاصة ،تتمتع بطبيعة قانونية خاصة، كما أن الواقع الذي يطرح نفسه حول أرتكاب جريمة التزوير عبر أستخدام الوسائل الالكترونية ،يكمن في أن هذه الجريمة تعتبر من الجرائم المستحدثة التي لم تنل حظها من الدراسة والبحث اللازمين، وعلينا تسليط الضوء عليها لفهمها فهما علميا شاملا ومتكاملا على اعتبار أن ذلك الفهم هو المدخل الطبيعي للتوصل الى مواجهة هذه الجرائم والتصدي لها بالفاعلية المطلوبة ووضعها تحت السيطرة.

المبحث الاول: مفهوم التزوير عبر استخدام الوسائل الالكترونية

الجرائم التي ترتكب بواسطة استخدام شبكة الانترنت كثيرة ومتنوعة ومنها الواقعة على الأموال ومنها الواقعة على الأشخاص بل كذلك الجرائم الواقعة على الملكيات ومنها حقوق المؤلفات والمخترعات . والى أكثر من ذلك أصبحت الجرائم المستخدمة عن طريق الانترنت أكثر خطورة بدخول الجرائم الماسة بأمن الدولة الداخلي وكذلك الجرائم الماسة بأمن الدولة الخارجي وكذلك الجرائم التي تمس بالمعاهدات أو الجرائم ذات الطبيعة الدولية كالجرائم الإرهابية.

(١) فخري عثمان ،جرائم بطاقة الأئتمان ،الطبعة الاولى، دار الشروق، القاهرة،مصر،١٩٩٥،ص٦

المطلب الاول :- خصائص جريمة التزوير الالكتروني

حدد الفقه الجزائي خصائص منفردة لجريمة التزوير الالكتروني لاتتوفر في أي من افعال التزوير التقليدي بحسب أسلوبها وطريقة أرتكابها وهي :

الفرع الاول : - الحاسب الألي هو أداة أرتكاب جريمة التزوير الالكتروني

فحوى هذه الخاصية انه الجريمة دائما ما يكون الحاسب الألي هو الأداة لآرتكابها ،فلا يمكن يمكن تسمية هذه الجريمة أو وصفها بجريمة ألكترونية دون أستخدام الحاسب الألي، لأنه هو وسيلة النفاذ إلى شبكة الإنترنت، ومن ثم لا يمكن تصور ارتكاب جريمة التزوير الإلكتروني من دونه . ولا عبرة هنا لشكل الحاسوب الذي قد يتخذ شكله التقليدي ،أو شكل الحاسوب النقال، أو قد يكون ضمن الهاتف النقال، أو حتى ضمن ساعة اليد، وبالتالي تنفيذ الجريمة أي كان نوعها [1] .

الفرع الثاني : - جرائم عابرة للدول .

يطلق تعبير جرائم عابرة للدول على تلك الجرائم التي تقع بين أكثر من دولة، بمعنى أنها لا تعترف بالحدود الجغرافية للدول، كجرائم تبيض الاموال والمخدرات وغيرها، أما في عصر الحاسب الآلي ومع أنتشار شبكة الأتصالات العالمية (الأنترنت)،وبعد ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم في هذه الشبكة ،أصبح التنقل والأتصال فيما بينها أمرا سهلا ،ففي هذه البيئة يمكن أن توصف جرائم الحاسب الآلي بأنها جرائم عابرة للدول، إذ غالبا ما يكون الجاني في بلد والمجني عليه في بلد أخر، كما قد يكون الضرر في بلد ثالث في الوقت نفسه، وعليه تعتبر جرائم الحاسب الآلي شكلا

(١) حسين الغافري، جرائم بين الشريعة الإسلامية والقانون ،دار النهضة العربية ،القاهرة، مصر ،٢٠٠٨، ص ٤٢ .

جديدا من الجرائم العابرة للحدود الوطنية والأقليمية والقارية .

وأعتبار جرائم الحاسب الآلي جرائم عابرة للدول، يظهر الحاجه الماسة إلى التعاون في مجال مكافحة هذه الجرائم وضبط فاعليها، وتجدر الإشارة هنا إلى جهود الإنتربول في هذا المجال من خلال ضباط الارتباط المنتشرين في كافة الدول عبر العالم، والمكلفين بتوفير قاعدة بيانات ضخمة يمكن أن تشكل نقطة إنطلاق للتصدي ومكافحة هذه الجرائم[1].

الفرع الثالث : - إمكانات الحاسب الآلي في أرتكاب هذه الجريمة.

يستخدم مرتكب جريمة التزوير الإلكتروني طريقة أوتوماتيكية تمكنه من كتابة الوثائق المطلوبة أو تغير محتواها بدقه متناهية.

وذلك بفضل إمكانات الحاسب الآلي التي تتيح التعديل والتصحيح والمحو والتخزين والآسترجاع والطباعة، وجميع الأفعال المادية التي لها علاقة وثيقه بأرتكاب جريمة التزوير الإلكتروني [2].

وتمتاز جرائم الحاسب الآلي بالتباعد الجغرافي بين الجاني والمجني عليه، نضيف على ذلك أن الجاني يستخدم لإرتكاب جريمة التزوير الإلكتروني وسائل فنية تقنية معقدة في الكثير من الاحيان ،كما يتمثل الركن المادي فيها بعمل سريع قد لا يستغرق أكثر من بضع ثوان بالأضافة إلى سهولة محو الدليل والتلاعب فيه وسهولة الدخول إليه ،وأمام هذا كله تبرز صعوبة الإثبات في جريمة التزوير الالكتروني، خصوصا مع الأفتقار إلى

---

(١) حسناء حسن، جريمة التزوير المعلوماتي، كلية القانون والعلوم السياسية، جامعة ديالى، ديلى، العراق، ٢٠١٧، ص١٥.

(٢) عبدالله، السراني، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، ط ١،جامعة نايف ،الرياض،السعودية،٢٠١١،ص ٦٧،٦٦.

وجود دليل مادي تقليدي (دم، شعر، بصمة،.....) .

الفرع الرابع :- مرتكب التزوير الآلكتروني ذو معرفة تقنية فائقة في مجال الحاسب الآلي.

تعتبر جريمة التزوير الآلكتروني جريمة غير تقليدية فهي لاترتكب بطريقه عشوائية أو غير مدروسة ،بل يحتاج إرتكابها إلى درجة عالية من التخصص والكفاءة في أستخدام الحاسب الآلي والأنترنت ،فضلا عن تمتع مرتكبها بسعة الأفق والحيلة ،فهم أفراد ذوو مكانة في المجتمع ويتمتعون بقدر كاف من العلم والألمام بمعارف ومهارات فنية متقدمة في مجال الحاسب الآلي والأنترنت ،كما تعد المهارة التقنية المطلوبة لتنفيذ جرائم الإنترنت من أبرز خصائص مجرمي الأنترنت ، والتي تم أكتسابها عن طريق الدراسة المتخصصة أو عن طريق الخبرة المكتسبة في مجال تكنلوجيا المعلومات ،إلا أن ذلك لا يعني ضرورة أن يكون المجرم على قدر كبير من العلم في هذا المجال، فالواقع العملي أثبت أن أشهر مجرمي الأنترنت لم يحصلوا على مهاراتهم التقنية عن طريق التعليم ،بل عن طريق الخبرة المكتسبة من العمل في هذا المضمون[1].

الفرع الخامس: صعوبة أكتشاف جريمة التزوير الإلكتروني

تظل الجريمة الألكترونية مستترة ما لم يتم الإبلاغ عنها ،والصعوبة التي تواجه أجهزة الأمن والمحققين هي أن هذه الجرائم لاتصل إلى علم السلطات المعنية ،وذلك لصعوبة إكتشافها من قبل الأشخاص العاديين ،أو حتى الشركات والمؤسسات التي وقعت مجنيا عليها،أو لأن هذه الجهات تحاول درء الأثر السلبي للأبلاغ عما وقع ،وذلك حرصا على ثقة العملاء أمامها،فلا تبلغ عن تلك الجرائم التي أرتكبت ضدها .

(١) شمسان الخليلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الأنترنت ،دار النهضة العربية ،بيروت،لبنان،٢٠٠٩،ص ٣٨.

ومن الصعوبات التي تواجه عملية أستخلاص الدليل في الجريمة الألكترونية ،نقص الخبرة لدى رجال الضابطية العدلية وجهات التحري والتحقيق ،وكذلك لدى العدالة الجزائية المتمثلة في سلطات الإتهام والحكم ،بخاصة فيما يتعلق بثقافة الحاسب الآلي والألمام بعناصر الجرائم المعلوماتية وكيفية التعامل معها،وهو أمر يستغرق وقتا أبطا من وقت أنتشار الجريمه ،لأن الجريمة الإلكترونية تتقدم بسرعة هائلة،وهذا الفارق في التقدم ينعكس سلبا على فنية إجراء الاستدلالات والتحقيقات ،ومن هنا تأتي الدعوة إلى وجوب تأهيل سلطات االأمن وجهات التحقيق والتحري والحكم في شأن هذه الجرائم .[1]

كما أن غياب الدليل المرئي في الجرائم الالكترونية المختلفة ،كالتي تقع على عمليات الإلكترونية ،أو على العمليات الألكترونية للاعمال المصرفية ،أو على أعمال الحكومة الإلكترونية يؤدي إلى صعوبة إقامة الدليل على هذه الجرائم بسبب طبيعة المحل الذي وقعت فيه الجريمة وبسبب أن مرتكب الجريمة لايترك وراءه أي أثار قد تدل عليه أو تكشف عنه ،وذلك بعد حسبان أن أغلب المعلومات والبيانات التي تتداول عبر الحاسبات الآلية ،والتي من خلالها تتم الجريمة الآلكترونية ،تكون في هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للانسان قرائتها أو إدراكها ألا من خلال هذه الحاسبات الآلية ،فالجرائم التي ترتكب على العمليات الإلكترونية التي تعتمد في موضوعها على التشفير والأكواد السرية ،والنبضات والأرقام والتخزين الألكتروني ،يصعب أن تخلف وراءها أثار مرئية قد تكشف عنها، أو يستدل من خلالها على الجناة.

(١) عبد الفتاح حجازي، الأثبات الجنائي في جرائم الكومبيوتر والأنترنت، دار الكتب القانونية، القاهرة، مصر، ٢٠٠٧، ص ٩٧.

وكمثال لذلك نجد أن التجسس المعلوماتي بنسخ الملفات وسرقتها أو تزويرها،يصعب على الشركات التي تكون الضحية لمثل هذه الافعال من أكتشاف أمرها وملاحقة الجناة . كما أنه من المعلوم أن جهات التحري والتحقيق أعتادت على الأعتماد في جمع الدليل على الوسائل التقليدية للاثبات الجنائي ،والتي تعتمد على الإثبات المادي للجريمة فقط .

ونجد أيضا سهولة في إخفاء الدليل في الجرائم الإلكترونية ،بحيث أن الجناة الذين يستخدمون الوسائل الإلكترونية في أرتكاب جرائمهم ،يتميزون بالذكاء والإتقان الفني للعمل الذي يقومون به والذي يتميز بالطبيعية الفنية ،ولذلك فأنهم يتمكنون من إخفاء الأفعال غير المشروعة التي يقومون بها أثناء تشغيلهم لهذه الوسائل الالكترونية ،ويستخدمون في ذلك التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي يتم تسجيل البيانات عن طريقها، كما أنّهم قد ينسخون هذه الملفات ويتحصلون على نسخ منها بقصد استعمالها تحقيقاً لمصالحهم الخاصة، وقد يخربون الأنظمة تخريباً منطقياً، بحيث يمكن تمويهه كما لو كان مصدره خطأ تقنياً[1]. وما يزيد من خطورة إمكانية وسهولة إخفاء الأدلة المتحصلة من الوسائل الإلكترونية أنه يمكن محو الدليل في زمن قصير، فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو يدمرها في زمن قصير جداً، بحيث لا تتمكن السلطات من كشف جرائمه في الحالة التي قد تعلم بها، ويلاحظ أن المجني عليهم كالبنوك والمؤسسات الادخارية وشركات الإقراض والسمسرة، قد يساهمون بدورهم في عدم إماطة اللثام عن هذه الجرائم من خلال إحجامهم عن تقديم الدليل الذي قد يكون بحوزتهم عن هذه الجرائم، وقد يكون مقصدهم من ذلك

(١) يراجع مظاهر صعوبة اثبات الجريمة الالكترونية، صحيفة المصريون، رئيس مجلس ادارتها جمال سلطان، ١٧/ ٩/ ٢٠١٨، منشور على الموقع التالي: www.almesryoon.com تاريخ الزيارة ١١/ ٤/ ٢٠٢٢.

استقرار حركة التعامل الاقتصادي بالنسبة لهم، بحيث يخشى القائمون على إدارتها من شيوع أمر الجرائم التي تقع داخلها، والتي قد تؤثر سلباً على الثقة فيها من العملاء المتعاملين معها، ما قد يؤدي إلى انصرافهم عنها، وهو ما قد يصيبهم بأضرار قد تزيد عن كشف ستر هذه الجرائم وتقديم مرتكبيها إلى العدالة.

لذلك اقترح البعض، بخاصة في الولايات المتحدة الأمريكية، أن تفرض النصوص المتعلقة بجرائم الحاسبات التزاماً على عاتق موظفي الجهة المجني عليها بالإبلاغ عن الجرائم التي تحدث داخلها ويتحقق علمهم بها.

بالإضافة إلى ما تقدم من صعوبات في كشف جريمة التزوير عبر استخدام الوسائل الإلكترونية أصبح من المسلم به أن المجرم الإلكتروني يستخدم إسماً مستعاراً، ولا يدخل إلى الشبكة عن طريق حسابه الآلي، وإنما عن طريق مقاهي الإنترنت، كما يلاحظ أن أكثرية هذه الجرائم تتعلق ببيانات مخزنة داخل دولة أجنبية بواسطة شبكة الاتصال عن بعد، ولذلك فإنه قد يصعب ضبط مثل هذه الأدلة لأن هذا الإجراء يتعارض مع مبدأ السيادة الذي تحرص عليه كل دولة، ولعل هذا الأمر يكشف لنا عن أهمية التعاون القضائي الدولي في مجال الإنابة القضائية، بخاصة في مجال الجرائم العابرة للقارات، ومنها الجرائم التي تقع بسبب ثورة الإتصالات عن بعد[1].

وأخيراً رغم مناداة بلدان العالم بضرورة التعاون الدولي في مكافحة الجريمة الإلكترونية، الا أنّ هناك عوائق تحول دون ذلك وهي عدم وجود نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي لهذه الجريمة، إذ أن الأنظمة القانونية في بلدان العالم قاطبة لم تتفق على صورة محددة يندرج في إطارها ما يسمى « إساءة استخدام نظم

(١) علي قهوجي، الحماية الجنائية للبيانات المعالجة الكترونياً، مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، كلية الشريعة والقانون، الإمارات، ٢٠٠٠، صفحة ٣.

المعلومات الواجب اتباعها»، كذلك ليس هناك تعريف محدد لهذا النشاط الإجرامي، بسبب قصور التشريع وعدم وجود تنسيق ومعاهدات ثنائية أو جماعية بين الدول على نحو يسمح بالتعاون المثمر في شأن مكافحة الجريمة الإلكترونية، بخاصة في ما يتعلق بأعمال الاستدلال والتحقيق(١).

المطلب الثاني: صور التزوير الالكتروني

إن التزوير الإلكتروني يتخذ أشكالاً عديدة، فقد يقع على محرر أو على عقداً، أو وثيقة هوية أو جواز سفر، أو شهادة ميلاد أو وفاة أو بريد، كما قد يأخذ شكل بطاقة إلكترونية مثل بطاقات التأمين الصحي، أو بطاقات التعريف، أو البطاقات الإئتمانية وغيرها. وهذه الوثائق تقترن بتوقيع إلكتروني يثبت صحتها، ونسبتها إلى صاحبها، ولذلك فإنّ هذا التوقيع على قدر من الأهمية، ويقتضي حمايته جزائياً من الاعتداءات التي قد تقع عليه، ومن أخطر هذه الاعتداءات تزوير هذا التوقيع(٢).

ولذلك سوف نتطرق إلى أهم صور التزوير الإلكتروني.

الفرع الأول: تزوير التوقيع الإلكتروني

إن انتشار الحاسب الآلي والاعتماد عليه في كافة مناحي الحياة بصورة شبه كلية، أفرز طرقاً ووسائل حديثة في التعامل لا تتفق مع فكرة التوقيع بمفهومها التقليدي، بخاصة بعد انتشار نظم المعالجة الإلكترونية للمعلومات في الشركات والإدارات والبنوك، واعتمادها المباشر على هذه النظم بحيث أنه لا مجال للإجراءات اليدوية في ظلها، فقد أصبح التوقيع اليدوي عقبة من المستحيل تكيفها مع النظم الحديثة للإدارة، ولهذا تم

(١) علي قهوجي، المرجع نفسه، ص٤.

(٢) عبد الفتاح حجازي، النظام القانوني للتوقيع الإلكتروني، الطبعة الأولى، دار الكتب القانونية، القاهرة، مصر، ٢٠٠٧، صفحة ٧.

الإتجاه نحو بديل لذلك التوقيع اليدوي، وهو التوقيع الالكتروني[1].

ومن هذا المنطلق جرمت بعض التشريعات فعل تزوير التوقيع الإلكتروني في نصوص خاصة، وذلك بعد أن أصبح له نفس القيمة القانونية التي يتمتع بها التوقيع العادي، لذلك وضعت الحماية اللازمة لتجنب مثل تلك الجرائم. نذكر من تلك التشريعات[2]:

-القانون النموذجي حول التجارة الإلكترونية الصادر عن لجنة القانون التجاري الدولي لدى الأمم المتحدة بموجب القرار رقم ١٦٢/ ٥١ تاريخ ١٩٩٦/ ١/ ١٦، الذي أقر بالقوة الثبوتية للسند والتوقيع الإلكترونيين.

-التوجيه الصادر عن البرلمان الأوروبي بتاريخ ١٩٩٩/ ١٢/ ١٣ حول التوقيع الإلكتروني وتسهيل استعماله من أجل حسن سير العمل في السوق الداخلي الأوروبي. كما أقرّ البرلمان الأوروبي توجيهاً آخر بتاريخ ٢٠٠٠/ ٦/ ٨ حول التجارة الإلكترونية والتأكيد على الإهتمام بتوقيع العقود بالطرق الإلكترونية.

-قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، الذي اعتمدته لجنة القانون التجاري الدولي لدى الأمم المتحدة في دورتها الرابعة والثلاثين بتاريخ ٢٠٠١/ ٧/ ٥، لتنظيم التوقيع الإلكتروني في سياق العلاقات ذات الطابع التجاري. ويعتبر هذا القانون قانوناً استرشادياً في مجاله، لكنه لا يتضمن كل التفاصيل المتعلقة بالتوقيع الإلكتروني، بل يفسح المجال لإصدار قوانين خاصة به.

-إقرار عدة دول قوانين خاصة بتنظيم التجارة الإلكترونية والسندات والتواقيع

---

(١) عبد الفتاح حجازي، النظام القانوني للتوقيع الإلكتروني، مرجع سابق، صفحة ١٠.

(٢) يراجع أمجد الجهني، جرائم بطاقة الدفع الإلكتروني عبر شبكة الإنترنت منشور على موقع: http://www.cojss.com تاريخ الزيارة ١١/ ٠٤/ ٢٠٢٢.

الإلكترونية، أهمها بريطانيا عام ١٩٩٥، وألمانيا وإيطاليا عام ١٩٩٧، والولايات المتحدة الأمريكية وفرنسا وتونس عام ٢٠٠٠، ومصر عام ٢٠٠٤، وغيرها الكثير.

الفرع الثاني: تزوير البطاقة المصرفية

يقصد بالبطاقة المصرفية ذلك النوع المحدد من البطاقات البلاستيكية التي تعطي الحق لصاحبها بإجراء عمليات الشراء والسحب والإئتمان، وبهذا الوصف تتميز هذه البطاقات بعدة خصائص خاصة، ما يستلزم بطبيعة الحال وجود نظام محكم كفيل بحمايتها.

لذلك وجب علينا أن نبين هذا الموضوع من خلال تعريف البطاقة المصرفية وتحديد أنواعها .

أولاً: تعريف البطاقة المصرفية:

إن التعريف القانوني للبطاقة المصرفية هو عقد بمقتضاه يقوم مصدر البطاقة بفتح حساب بمبلغ معين لمصلحة حامل البطاقة الذي يستطيع بواسطتها الوفاء بمشترياته لدى المحال التجارية، وهذه الأخيرة ترتبط مع مصدر البطاقة بعقد يتعهد بموجبه بقبول الوفاء بمتطلبات حاملي البطاقة الصادرة من الطرف الأول، على أن تتم التسوية النهائية بعد كل دورة محددة[١].

أما على مستوى فقهاء القانون، فهناك من عرفها على أنها بطاقة مصنوعة من مادة بلاستيكية تحتوي على شريط ممغنط يتضمن بيانات عن حساب العميل لدى المصرف، كما يتضمن شريطاً لاصقاً مدوناً عليه توقيع صاحب الحساب بالإضافة إلى صورة شخصية للعميل، وتستخدم هذه البطاقة في سحب المبالغ النقدية وفي دفع ثمن المشتريات.

(١) رياض بصلة، جرائم بطاقات الائتمان، الطبعة الأولى، دار الشروق، القاهرة، مصر، ١٩٩٥، صفحة ٨.

وهناك من عرفها على أنها عبارة عن مستند يعطيه مصدره لشخص طبيعي أو اعتباري بناءً على عقد بينهما يمكنه من شراء السلع والخدمات دون دفع الثمن حالاً لإلتزام المصدر بالدفع، كما يمكنه أيضاً سحب النقود من البنوك.

ومع اندفاع العالم بقوة نحو المعلوماتية والبرمجيات الحديثة والتطور الإلكتروني، أصبحت بطاقات الإئتمان هي وسيلة الدفع الأكثر استخداماً وانتشاراً وقبولاً في العالم، وذلك بعد أن نمت هذه البطاقات وتطورت تطوراً كبيراً حتى وصلت إلى ما هي عليه الآن.

وهكذا بدأت بطاقات الدفع الإلكتروني تحل محل النقود والشيكات، وتستخدم على نطاق واسع، نظراً لما تتمتع به من سهولة في الدفع، وإمكانية التعامل بها محلياً وعالمياً، فضلاً عن كونها ذات مسؤولية قانونية في حال تعرضت للتزوير أو الفقد أو السرقة، الأمر الذي دعا البعض إلى اعتبارها جزءاً لا يتجزأ من ثقافة النظام الاقتصادي العالمي المعاصر. وقد صاحب انتشار بطاقة

الائتمان وتزايد حجم التعامل بهما نمو مطرد في الجرائم المصاحبة لاستخدامها، كتزوير هذه البطاقات أو سرقتها لاستخدامها بالتحايل والاستيلاء على مال الغير، ومما يزيد من خطورة الأمر هو سهولة تزوير بطاقات الائتمان من ناحية، وعدم وجود آلية عالمية لإحكام السيرة على ضمان سرية بيانات هذه البطاقة من ناحية ثانية، وصعوبة إثبات تزوير البطاقة والتلاعب فيها من ناحية ثالثة.

أما بالنسبة للعناصر الأساسية الواجب توافرها في البطاقة الإئتمانية، تتمثل في أطرافها الثلاثة التالية[1]:

(١) رياض بصلة، المرجع نفسه، ص٣١.

– الطرف الأول: الجهة التي لها حق إصدار البطاقة، وقد تكون مؤسسة أو شركة أو بنكاً. – الطرف الثاني: «حامل البطاقة»، وهو الشخص الذي يحصل على بطاقة الدفع الإلكتروني من الجهة المصدرة، بغرض استخدامه الشخصي لها باعتبارها وسيلة دفع لدى التجار للحصول على السلع والخدمات، أو استخدامها في الحصول على احتياجاته النقدية من خلال أجهزة الصرف الأوتوماتيكي في أنحاء العالم كافة. الطرف الثالث: «القابل» ويسمى في العرف المصرفي والتجاري بالتاجر، وهو الجهة التي تقبل الوفاء بواسطة بطاقات الدفع الإلكتروني نظير ما يقدمه لحامليها الشرعيين من سلع أو خدمات، وذلك في مقابل توقيعهم له على إشعارات البيع.

من خلال ما تقدم، تبين معنا أن البطاقة الإئتمانية هي عقد بين مصدر البطاقة الذي عمل على فتح اعتماد بمبلغ معين لمصلحة الطرف الآخر، وهو صاحب أو حامل البطاقة الذي يستطيع بواسطتها الدفع أو الوفاء بمشترياته لدى المحلات التجارية التي ترتبط مع مصدر البطاقة، بعقد يتضمن قبول الوفاء من صاحب أو حامل البطاقة الإئتمانية.

الفرع الثالث: تقليد الشيك الالكتروني او الرقمي

تكمن علة العقاب في هذه الجريمة على تقدير المشرع الإلكتروني أهمية الشيك الإلكتروني والرقمي في الحياة التجارية الإلكترونية المحلية والدولية في عالم تقنية المعاملات، إذ لا يتاح لهذا الشيك دوره التجاري والإقتصادي ما لم تكفل له هذه الثقة في أوسع نطاق، ما يقتضي وضع نص تجريمي يقتصر دوره على كفالة هذه الحماية من التقليد، بحيث أن الشيك يعتبر أداة وفاء، ويقوم في الحياة التجارية بدور النقود، فكما يفي المدين بدينه عن طريق تسليم دائنه شيكاً ورقياً بالمبلغ المدين به، فهو يفي بهذا الدين

عن طريق سحب شيك إلكتروني لمصلحته بهذا المبلغ[1].

وقيام الشيك الإلكتروني بهذه الوظيفة يحقق مصلحة اجتماعية مهمة، إذ يقلل من مخاطر تزويره أو سرقته، ويساهم في تخفيف عبء حمل دفتر للشيكات، ويسرع في عمليات تحويل النقود في المصارف داخلياً ودولياً.

وغني عن البيان أنه لا يتاح للشيك الإلكتروني أو الرقمي أداء هذه الوظيفة إلا إذا كان محل ثقة واطمئنان كاملين من المتعاملين، فكانت نظرة المستفيد من الشيك الإلكتروني هي ذات نظرته إلى الشيك الورقي[2].

وقد أدى ظهور تقنية المعلومات الحديثة إلى بروز أنواع من البرمجة تشكل تعدياً على البرامج المعالجة آلياً في الشبكة المعلوماتية كتقليد الشيكات الإلكترونية والرقمية، وهي تُمثل ظاهرة إجرامية جديدة تطال الكيان المعلوماتي للشيك لم تكن معروفة من قبل، ولا شك أنها تهدد على نحو مؤكد الثقة بالشيكات الإلكترونية المتداولة.

الفرع الرابع: استعمال الشيك الالكتروني او الرقمي المقلد

لقد فصل المشرع بين جريمة تقليد الشيك وجريمة استعماله، فأهم النتائج التي تترتب على هذه التفرقة هي أن من قلد شيكا يستحق عقوبة الجريمة التامة، ولو استحال عليه بعد ذلك استعماله أو تظهيره، كما لو ضبط عقب التقليد أو ضبط الشيك المقاد، كذلك الحال لو تم سرقة البيانات لاحقاً أو محاها شخص، أو عدل اختياراً عن

(١) عبرت محكمة التمييز الجزائية اللبنانية عن هذا المعنى في قولها: «من المقرر أن الشيك هو وسيلة دفع آنية لأموال نقدية تتسم بتخلي الساحب للمسحوب له عن تنظيم الشيك عن مؤونة واعتبارها ملكاً له، وقابلة للتظهير لأمر الغير، ولا يمكن أن تتضمن هذه المعاملة أي شرط (قرار الغرفة ٦، رقم ١٢٨، تاريخ ١٩٧٣/ ٦/ ١١، موسوعة عالية الحديثة، المجلد ٢، ص٢٠١٣).

(٢) محمود حسني، جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، دار الطبعة اللبنانية، بيروت، لبنان، ١٩٧٥، ص٣٣٩.

التعامل بالشيك المقلد، فذلك العدول جاء متأخرا، إذ جاء بعد أن اكتملت عناصر الركن المادي، وتأتي علة الحكم هنا كون العدول عن الجريمة نتج عن تقدير الجاني أن الشيك المقلد أو المنسوخ غير صالح لخداع الجمهور المتعامل آليا، في حين أنه صالح لذلك.

ومن نتائج هذه التفرقة أنه إذا أعقب الجاني فعل التقليد بأن قام بتظهير الشيك الذي قلده، فهو يرتكب جريمتين.

واذا كانت القاعدة أن مجرد إعداد آلات التقليد وأدواته، أو بحجة أقوى مجرد حيازتها، يعتبر عملاً تحضيرياً، وذلك بالنظر إلى خطورته. فقد عاقب المشرع الإلكتروني على استيراد أو إنتاج أو حيازة أو تقديم أو نشر دون سبب مشروع، جهازا أو برنامجاً إلكترونياً أو أي بيانات معدة أو مكيفة بهدف اقتراف جريمة التزوير الإلكتروني أو سائر الجرائم الإلكترونية[1].

أولا: السلوك الجرمي لاستعمال الشيك الالكتروني

يعتبر الاستعمال فعل إيجابي ويعني إدخال الشيك في الحيازة ابتداء، وقوامه عنصران، الأول هو إرادة تلقي حيازة الشيك المقلد وممارسة السلطات التي تنطوي عليها هذه الحيازة.

أما الثاني فهو إدخال الشيك في نطاق السيطرة الفعلية مباشرة، ثم استعماله بقبض القيمة أو تظهيرها للغير.

كما تعتبر هذه الجريمة قصدية، ويتخذ ركنها المعنوي صورتي القصد العام والقصد الخاص أي أن يعلم الجاني بالمحل الذي انصب عليه فعله وماهيته، فيعلم أنه حاز شيكاً

(١) المادة ١١٤ من قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي.

مقلّداً، وأن إرادته إتجهت إلى هذا الفعل. فمن وجد في حاسوبه شيكاً مقلداً دسه له شخص بغير علمه وإرادته، فإنّ القصد ينتفي لديه، ويتوجب أن يتوافر لدى المتلقي للشيك المقلد قصد خاص وهو نية التداول بالشك الإلكتروني المقلَّد[1].

المبحث الثاني

أركان جريمة التزوير عبر استخدام الوسائل الالكترونية

لابد من التطرق الى بيان أركان جريمة التزوير الالكتروني:

اولاً : الركن المادي

يتضح أن الركن المادي في الجريمة محل البحث يتكون من ثلاثة عناصر.

١- تحريف متعمد للحقيقة.

٢- وقوع التحريف على دعامة إلكترونية أو سند أو وثيقة أو أية دعامة أخرى تشكل مستنداً إلكترونياً.

٣- استخدام جهاز إلكتروني (الحاسب الآلي)

فتغيير الحقيقة هو إبدالها بغيرها، وتغيير الحقيقة في التزوير الإلكتروني يتم بأية طريقة يقرها القانون، كإدخال بعض البيانات أو المعلومات إلى برنامج من خلال إستغلال الأخطاء والعيوب التي يحويها هذا البرنامج، أو بمحو بعض أو كل البيانات الوارد ذكرها في البرنامج من خلال الحذف أو الشطب، كما هو الحال بالنسبة للشخص الذي دخل إلى برنامج سجلات الشرطة في مصر، وقام بحذف بعض أسماء المجرمين

(١) سمير عالية، الجرائم الإلكترونية في القانون الجديد رقم ٨١ ٢٠١٨ والمقارن (حرية التواصل الإلكتروني والقواعد العقابية الإجرائية)، مرجع سابق، صفحة ٢٠٣.

المطلوبين للعدالة وذلك عام ١٩٧٩[١]، كما يتحقق تغيير الحقيقة أيضاً بإتلاف كل أو بعض البيانات، لكن لا يعد تزويراً إذا وقع الإتلاف على البرنامج الذي تحويه تلك البيانات أو المعلومات، لأننا هنا لا نكون بصدد جريمة التزوير الإلكتروني وإنما نكون أمام جريمة أخرى وهي (جريمة إتلاف المعلومات)[٢].

وتجدر الإشارة الى أن التزوير الإلكتروني لا يتم من قبل خبير في مجال الحاسب الآلي فحسب وإنما يمكن أن يقع من شخص عادي ليس له أي دراية بتشغيل الكمبيوتر، ولا يتمتع بأي قدر من الكفاءات والمهارات الفنية أو العلمية لتشغيل هذا الجهاز الإلكتروني، ومع ذلك يرتكب التزوير الإلكتروني كما هو الحال بالنسبة للشخص الذي يقوم بالإدلاء بمعلومات أو بيانات غير صحيحة إلى مبرمج الحاسب الآلي مع علمه بتزويرها، كما هو الحال بالنسبة للشخص الذي يعمد إلى فتح حساب جار فيقوم باستعمال إسم شخص آخر، أو الإتصاف بصفة ليست له، أو بتقرير وقائع كاذبة، أو بغير ذلك من الطرق لتدوين أو إثبات واقعة غير صحيحة بخصوص أمر من شأن المستند اثباته[٣].

في واقعة ذات علاقة، قام موظف في أحد البنوك الأمريكية بتشغيل الحاسب الآلي وتزوير حسابات أصدقائه في البنك بحيث تزيد أرصدتهم عن الرصيد الحقيقي ويقومون بدورهم بسحب هذه المبالغ التي نالوها بدون وجه حق[٤].

---

(١) حفصي عباس، جرائم التزوير الإلكترونية، أطروحة مقدمة لنيل شهادة دكتوراه في العلوم الإسلامية، جامعة وهران، الجزائر ،٢٠١٤، ص٥٩.

(٢) عبد الفتاح حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، مصر ٢٠٠٢، صفحة ٢٩٦.

(٣) المادة ٢٩٠ من قانون العقوبات العراقي.

(٤) أيمن فكري، جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة، الاسكندرية، مصر،

وعليه فإن تغيير الحقيقة كعنصر من عناصر الركن المادي لجريمة التزوير الإلكتروني والتي تقع على البيانات والمعلومات بأي لغة كانت، وبأي طريقة وجدت سواء كانت صوراً أو رموزاً أو علامات يشترط أن تتم باستخدام الحاسب الألي لغرض تمييزها عن جريمة التزوير التقليدية.

ثانياً: الموضوع الجرمي

يتبين بأن هناك نوعان من المحررات، محررات عادية (ورقية) متعارف عليها عند الجمهور، ومحررات ظهرت بظهور ثورة تكنولوجيا الحاسبات، وهي ما يطلق عليها المحررات الإلكترونية، فالأول هو كل سند أو وثيقة أو محرر يحتوي على علامات أو كلمات ينتقل بها المعنى من شخص الى أخر بمجرد النظر اليه، ويتسم بعدة سمات، وهي أن يكون متخذاً شكلاً كتابياً وبأي لغة كانت محلية أو أجنبية ولا عبرة بالمادة التي سطرت عليها الكتابة، فقد تكون ورقة أو خشباً أو جلداً، أو تكون بخط اليد أو بالآلة الكاتبة أو الطابعة، كما يشترط بأن تكون الكتابة منسوبة لشخص معين معروف أو يمكن معرفته[1].

أما المحررات الإلكترونية فقد عرفها قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية عام ١٩٩٦ من خلال تعريفه لرسالة البيانات، فنصت المادة الثانية من هذا القانون على أن المحررات الإلكترونية هي المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكترونية أو البريد الإلكتروني أو البرق أو

٢٠٠٧، صفحة ٣٨٢.

(١) فتوح الشاذلي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠٠٣، صفحة ٢٣٣.

التلكس أو النسخ البرقي[1].

كما أن قانون التوقيع الإلكتروني المصري عرف المحرر الإلكتروني بأنه « رسالة البيانات التي تتضمن معلومات تنشأ كلياً أو جزئياً بوسيلة إلكترونية أو رقمية أو ضوئية، أو آية وسيلة أخرى متشابهة[2].

وقد ذهب البعض إلى عقد مقارنة بين المستند الإلكتروني والمستند العادي (الورقي)، فيرى أن بينهما أوجه شبه تتمثل في أن كل منهما يحوى مجموعة من الرموز التي تعبر عن مجموعة من الأفكار والمعاني وأن كل منهما ينطوي على فكرة الضرر التي هي علة التجريم، كما أن المستند الإلكتروني قد يكون رسمياً أو عادياً مثله تماماً مثل المحرر الورقي. أما أوجه الاختلاف بينهما تتمثل في أن المحرر الورقي يتم تسطير محتواه بوسيلة الكتابة العادية ويمكن معرفة محتواه بمجرد النظر اليه، أما المستند الإلكتروني يتضمن كتابة إلكترونية لا يمكن الوقوف على محتواها الا من خلال الحاسب الآلي أو نظام تشغيل إلكتروني. واذا كان المحرر الورقي يمكن تحديد هوية محرّره، فإن بعض المستندات الإلكترونية تتم بوسائل لا يمكن من خلالها تحديد شخص محررها أو صفته[3].

وفي ضوء الاعتبارات السابقة نرى أن نستعمل تعبير المحرر الإلكتروني في دراستنا، لأن تعبير المحرر لا يشمل المحرر الورقي والمحرر الإلكتروني معاً، خاصة أن المحرّر

(١) الفقرة أ من المادة ٢، من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية.

(٢) الفقرة ب من المادة ١، من قانون التوقيع الإلكتروني المصري.

(٣) أشرف شمس الدين، الحماية الجنائية للمستند الإلكتروني، دراسة مقارنة، بحث منشور في أعمال المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، الامارات العربية المتحدة، ٢٠٠٨، صفحة ٣٥٨.

الإلكتروني يتمتع بأهمية خاصة، تتمثل في أن بعض التشريعات تمنحه قوة قانونية تماثل المحرر الورقي، وقد تفوقه قي بعض الحالات. غير أن المحرر الإلكتروني قد يكون أكثر انتشاراً من المحرر الورقي، وذلك لإتصاله بطائفة مهمة من النظم الإدارية والتجارية والمالية، وبصفة خاصة في الهيئات والمنشآت التي تعمل في مجال البنوك والتأمين والخدمات الطبية وغيرها. كما يذهب الرأي الغالب في الفقه إلى أن النصوص القائمة في قانون العقوبات، وضعت لتنظيم الأمور المتعلقة بالمحرر الورقي، ولا يمكن أن تسري على المحرر الإلكتروني، وأنّ الأمر يتطلب صدور تنظيم تشريعي خاص بالمحررات الإلكترونية[1].

ثالثاً: الركن المعنوي

الركن المعنوي في جريمة تزوير المستندات المعالجة آلياً له ذات المدلول في جريمة تزوير المحررات، ويتخذ صورة القصد الجرمي العام بعنصريه « العلم والارادة « إلى جانب القصد الخاص[2].

فالقصد الجرمي العام هو كما وصفه نموذجاً في القانون هو « انصراف الإرادة الى السلوك المكون للجريمة، مع الوعي بالملابسات التي يتطلب هذا النموذج احاطتها بالسلوك المكون للجريمة، وعليه يجب أن يكون الشخص عالماً بأنه يغير الحقيقة في المحرر الإلكتروني عن طريق الحاسوب، وأن هذا التغيير من شأنه إحداث الضرر أو

(١) عمر الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دراسة تحليلية نقدية لنصوص التشريع المصري مقارناً بالتشريع الفرنسي، الطبعة الثانية، دون دار نشر، القاهرة، مصر، ١٩٩٥، صفحة ٧٩.

(٢) علي القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، الإسكندرية، مصر، ١٩٩٩، صفحة ١٥٢.

من المحتمل حدوث الضرر.

والقصد الجرمي الخاص هو الهدف الذي يعمل الجاني على تحقيقه من جراء جريمته، ولا يكون بشكل منفرد انما يكون مقترناً بالقصد العام، فإن الركن المعنوي لجريمة التزوير الإلكتروني يتطلب أن يتوافر لدى الجاني القصد الخاص والمتمثل في تزييف جوهر المحررات أو ظروفها بطريقة الغش، أي ضرورة اقتران العلم بنية الغش والمتمثلة في نية استعمال المحرر المزور فيما زور من أجله[1].

ومما تجدر الإشارة إليه أن التزوير الإلكتروني هو من الجرائم القصدية التي يشترط لقيامها توفر القصد الجرمي وهو توجيه الفاعل إرادته إلى ارتكاب الفعل المكون للجريمة، هادفاً لتحقيق نتيجة الجريمة التي وقعت أو أية نتيجة أخرى»[2].

ويتضح من النص المتقدم بأن القصد الجرمي يستلزم لتحققه توفر عنصران هما العلم والإرادة، وبعبارة أخرى هي أن يكون الجاني عالماً بأنه يرتكب جرماً أو سلوكاً غير مشروع معاقب عليه في التشريعات العقابية، ومع ذلك أقدم على ارتكابه، بمعنى أنه يجب أن يكون عالماً بأن إدخال المعلومات والبيانات الى مضمون المحرّرات، أو محو تلك المعلومات أو تحويرها أو إتلافها، أو القيام بأية افعال أخرى من شانها ان تؤدي إلى التأثير على المجرى الطبيعي لمعالجة البيانات، ولا يكفي هذا بل لابد من أن تكون إرادته متوجهة الى إحداث النتيجة الجرمية من جراء سلوكه غير المشروع، وهي الإضرار بالغير سواء كان ضرراً معنوياً أو مادياً أو اجتماعياً.

---

(١) بلحاج العربي، أبحاث ومذكرات في القانون والفقه الإسلامي، ديوان المطبوعات الجامعية، بن عكنون، الجزائر، ١٩٩٦، صفحة ٥٢٥.

(٢) فخري الحديثي، شرح قانون العقوبات (القسم العام) الطبعة الثانية، المكتبة القانونية، بغداد، العراق ،٢٠٠٧، صفحة ١١٢.

وعليه إذا كان جاهلاً بأن الفعل الذي يرتكبه غير مشروع فلا يتحقق لديه القصد الجرمي، وكذلك الحال إذا انتفى علم الجاني بأي ركن من أركان الجريمة، فلا يترتب عليه توافر القصد الجرمي لأنه يفترض أن يكون الفاعل عالماً بكافة أركان جريمته، ومن ناحية أخرى، يستوجب قيام القصد الجرمي في التزوير الإلكتروني أن تكون إرادة الجاني متجهة الى إحداث النتيجة الجرمية التي وقعت أو أية نتيجة جرمية أخرى، وهي الاضرار بالآخرين حتى وإن كان هذا الإضرار محتمل الوقوع، وعليه فإن الركن المعنوي يتحقق في جريمة التزوير المعلوماتي بعلم القائم بفعل التزوير بأن الإدخال أو الإتلاف أو المحو أو التحوير للبيانات والبرامج المعالجة آلياً يؤدي إلى التأثير على المجرى الطبيعي لتلك البيانات أو المعلومات[1].

رابعاً: الضرر في التزوير الإلكتروني

الضرر هو عنصر جوهري في جريمة التزوير، إذ لا يمكن قيام هذه الجريمة، دون أن يكون من شأنه أن يسبب ضرراً، فحيث ينعدم الضرر لا تقوم جريمة التزوير، ولذلك فإن المحكمة ملزمة بأن تظهر في حكمها توافر عنصر الضرر، وإلا يكون حكمها معيباً[2].

فلا يعاقب على التزوير إلا اذا رتب ضرراً، أو كان من شأنه إحداث ضرر، والجريمة تكون كاملة متى توفرت عناصرها، وأن حق الدولة في العقاب وإتخاذ الإجراءات القانونية يثبت بمجرد حدوث الجريمة واكتمال عناصرها[3].

---

(١) فخري الحديثي، شرح قانون العقوبات (القسم العام)، مرجع سابق، صفحة ١٢٣.

(٢) عبد الفتاح حجازي، مكافحة جرائم الكومبيوتر والإنترنت، الطبعة الأولى، دار النهضة العربية، القاهره، مصر، ٢٠٠٩، صفحة ٢٩٦.

(٣) عادل عازر، النظرية العامة في ظروف الجريمة، المطبعة العالمية، القاهرة، مصر، ١٩٦٧، صفحة ٨٩.

وبالنسبة لجريمة التزوير الإلكتروني، يشكل الضرر عنصراً مهما وضرورياً، وبالتالي لا بد من الوقوف عنده، إذ لا يكفي لقيام جريمة التزوير الإلكتروني تغيير الحقيقة في محرر أو سند أو وثيقة بإحدى الطرق التي يقرها القانون فقط، دون أن ينتج عن ذلك التغيير ضرراً، سواء كان هذا الضرر مادياً أم أدبياً ام إجتماعياً، سواء كان ينصب على المصلحة العامة أو على مصلحة شخص من الأشخاص، وسواء كان ضرراً واقعاً في الحال أو محتمل الوقوع، كما لا يشترط في هذا الضرر أن يمس شخص معين بالذات، بل يعتبر متحققاً متى ما مس أي فرد من أفراد المجتمع غير معين بالذات، لأن من شأن كل ذلك أن يسبب الأضرار بحقوق الغير أياً كانت صفة ذلك الغير اعتبارية أو طبيعية، شخص معنوي أو شخص طبيعي، ولقد إتفق غالبية الفقهاء على أن الضرر الذي يكفي لفرض العقاب في جريمة التزوير، سواء كانت تقليدية أو إلكترونية الضرر المادي، فهو يمثل الأذى الذي يصيب الغير من جراء المساس بمحتوياته أو بمصلحة هو مشروعة تؤدي إلى جعل حال ذلك الغير أسوأ مما كانت عليه قبل وقوع الاعتداء[1].

كما يتضح من استطلاع آراء الفقهاء، أنه لا قيام لجريمة التزوير عبر استخدام الوسائل الإلكترونية دون أن يكون للمحرر الإلكتروني قيمة في الاثبات، وبالتالي لا يمكن العقاب على تغيير الحقيقة في الوثيقة المعالجة آليا (المحرر الإلكتروني) ما لم تكن لهذا المحرر قيمة في الإثبات[2].

---

(١) يراجع منتدى الدكتورة شيماء عطاالله، استاذ القانون الجنائي المساعد في كلية الحقوق، جامعة الزقازيق، أنظر في الموقع:
http://www.shaimaaatalla.com\vb\showthread.phd?t=٣٩٤٠ تاريخ الزيارة ١٢/ ٤/ ٢٠٢٢.

(٢) أحمد تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، دار النهضة العربية، بيروت، لبنان، ٢٠٠٠، صفحة ٤٠٨.

وبخصوص هذا الشأن يذهب جانب من الفقهاء إلى أنه كي يكون للمحرر الإلكتروني قيمة في الإثبات، فإنه يجب أن يكون هناك صلة أو رابطة بينه وبين قانون الاثبات المرتبط بتزوير المستند، فإذا لم يكن المحرر الإلكتروني يثبت حقاً معيناً لأحد الأشخاص، فإنه لا يمكن العقاب على تغيير الحقيقة الذي يقع فيه[1].

المطلب الاول: الاختصاص القضائي في الجرائم الالكترونية

ان القضاء المختص بنظر الأفعال الجرمية للموقع الإلكتروني لا يحظى دائما بالوضوح أو القبول أمام حقيقة أن اغلب هذه الأفعال الجرمية يتم ارتكابها من أفراد من خارج الحدود، أو أنها تمر عبر شبكات وأنظمة معلومات خارج الحدود، حتى عندما يرتكبها شخص من داخل الدولة على نظام في الدولة نفسها، وهي أحدى ثغرات التشريع، ومن هنا تظهر أهمية اختبار مدى ملائمة قواعد الاختصاص والقانون الواجب التطبيق، وما إذا كانت النظريات والقواعد القائمة في هذا المجال تطال هذه الأفعال الجرمية، أم يتعين النص على قواعد خاصة بها لخصوصيتها ولما تثيره من مشكلات في حقل الاختصاص القضائي ويرتبط بمشكلة الاختصاص وتطبيق القانون مشكلات امتداد أنشطة الملاحقة القانونية والتحري والضبط والتفتيش خارج الحدود وما يحتاجه ذلك إلى تعاون شامل للموازنة بين موجبات المكافحة ووجوب حماية السيادة الوطنية[2].

فطبيعتها ليس لها مكان ثابت أو بلد معين، وليس لها هيئة أو جهة تشرف عليها أو مسؤولة عنها، ما يترتب وجود تشريع جنائي محدد، يحكم الأفعال الجرمية المعلوماتية، ويرجع تعدد القوانين والأنظمة لارتباط القانون الجنائي بالسيادة الوطنية، وتكمن

(١) أحمد تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، المرجع نفسه، صفحة ٤٢٣.
(٢) محمد امين الشوابكة، جرائم الحاسوب والإنترنت، ط١، دار الثقافة، عمان، ٢٠٠٤. ص ١٣.

الإشكالية أن بعض الأفعال والسلوكيات تكون مجرمة في بعض الدول ومباحة بأخرى، كما لا توجد نصوص بأغلب الدول تنظم مثل هذه السلوكيات.

ومبدأ الإقليمية يعني أن القانون الجنائي يتم تطبيقه على كافة الأفعال الجرمية التي تقع في رقعة الدولة(٢)[١].بغض النظر عن جنسية مرتكبها، ومع هذا فإن تطور الأفعال الجرمية وتوسعه إلى دول العالم يتطلب وجود اتفاقيات دولية لتسليم الجناة، لكن أغلب الدول لاتقوم بتسلم رعاياها وفقا لمبدأ سيادة الدولة من ناحية، ومن ناحية أخرى عدم جواز محاكمة شخص عن فعل واحد لأكثر من مرة، وهو ما يتعارض مع المبدأ أساسي في القانون الجنائي[٢].

وقد حدد المشرع العراقي جهة الاختصاص القضائية المختصة بمثل تلك الأفعال الجرمية الإلكترونية على أنها جرائم عالمية وليست دولية، على وفق مبدأ الاختصاص الشامل، إذ يتم تطبيق القانون الجنائي للدولة على كل جريمة يقبض على مرتكبيها بإقليم الدولة أيا كان الإقليم الذي ارتكب فيه وأيا كانت جنسية مرتكبها[٣]، شريطة أن تكون الجريمة ذات صفة عالمية، وهو ما ينطبق على الأفعال الجرمية الإلكترونية، وتسري أحكام هذا القانون بموجب نص المادة (١٣)[٤] من قانون العقوبات العراقي،

---

(١) ينظر المادة(٦) من قانون العقوبات العراقي رقم (١١١) ١٩٦٩ والتي تنص على انه:(تسري احكام هذا القانون على جميع الجرائم التي ترتكب في العراق وتعتبر الجريمة مرتكبة في العراق اذا وقع فيه فعل من الافعال المكونة لها او اذا تحققت فيه نتيجتان او كان يراد ان تتحقق فيه....).

(٢) لموسخ محمد، تنازع الاختصاص في الجرائم الإلكترونية، جامعة قاصدي مرباح، مجلة دفاتر السياسة والقانون، ع ٢، ٢٠٠٩، ص ١٤٣-١٥٧.

(٣) فخري عبد الرزاق الحديثي، شرح قانون العقوبات: القسم العام، بغداد ،١٩٩٢، ص ٩٦.

(٤) ينظر: المادة (١٣) من قانون العقوبات العراقي (تسري أحكام هذا القانون على كل من وجد في العراق بعد أن ارتكب في الخارج بوصفه فاعلا أو شريكا في جريمة من الجرائم التالية:

ومن الشروط الواردة فيها:

- أن تقع خارج العراق جريمة نصت عليها المادة (١٣) ولا عبرة بصفة الجاني من حيث كونه فاعل أصليا أو شريكا.
- أن يكون الجاني موجوداً في العراق بعد ارتكاب الفعل الجرمي.
- أن يكون الجاني أجنبياً.
- أن يكون الفعل المعاقب عليه بمقتضى القانون العراقي وقوانين الدول الأخرى(١)[1].

كما أورد في الفصل الثالث من مسودة قانون مكافحة الجرائم الإلكترونية العراقي في المادة (٩) أن لمجلس القضاء صلاحيات تأسيس محاكم تختص بالنظر بالدعاوى الجزائية المختصة بهذا النوع من الأفعال الجرمية الإلكترونية.

تنازع الاختصاص في جرائم الاعتداء على الموقع

تثير جرائم الموقع الالكتروني العديد من المشاكل ومنها تحديد السلطة المختصة في التحقيق بها، والاختصاص عموما هو السلطة التي يقرها القانون للقضاء في ان ينظر دعاوى من نوع معين وتتجه اغلب الدول الى تطوير انظمتها القانونية لمواجهة هذه الجرائم وتحرص على اعطاء محاكمها وقوانينها الاختصاص بالنظر في الجرائم الالكترونية ومنها التي تمس الموقع الالكتروني[2].

تخريب أو تعطيل وسائل المخابرات والمواصلات الدولية والتجاربالنساء أو بالصغار أو بالرقيق أو بالمخدرات).

(١) عباس الحسني، شرح قانون العقوبات العراقي الجديد، القسم العام، ط٢، مج الأول، مطبعة الإرشاد، بغداد، ١٩٧٢، ص٤٢.

(٢) ناير نبيل عمر، الحماية الجنائية للمحل الالكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، الاسكندرية، ٢٠١٢، ص ١٨٢.

وبالنظر لطبيعة وخصائص هذه الجرائم في كونها بدأت بالأنتشار في اغلب دول العالم وليست لها اية جهة تشرف عليها او مسؤولة عنها مما يثير لدينا مشكلة تحديد الاختصاص فيها من حيث القانون الواجب التطبيق والمحكمة المختصة، ولاسيما ان الدول تعتمد على السيادة الوطنية وتضمن ذلك في قوانينها الجنائية سواء كانت في الجانب الموضوعي(التجريم والعقاب) ام في الجانب الشكلي (الاجراءات الجنائية) والقاعدة العامة هناء لحل هذه المشكلة المتبعة في اغلب الدول هي تطبيق مبدأ اقليمية القانون الجنائي، اي تختص قوانين الدولة بتجريم الافعال داخل اراضيها وتحدد اجراءات محاكمة مرتكبيها، بمعنى ان محاكمها هي المختصة في ذلك[1].

اما في بعض الحالات فان جرائم الاعتداء على المواقع الالكترونية قد ترتكب من خارج اقليم الدولة، او تكون هذه الجرائم ماسة باكثر من دولة لاسيما وانها جرائم ذات طابع عالمي لذا لابد ان يحدد اي قضاء مختص للنظر فيها ومحاسبة مرتكبيها على وفق اي قانون تجرم وهذا ما يؤدي الى تنازع في الاختصاص، ولا سبيل في حل ذلك الى بالرجوع الى مبدأ عينية القانون الجنائي وهذا ما تاخذ به اغلب التشريعات الجنائية، اذ تستثني بعض الجرائم من قاعدة اقليمية القانون، بوجب ذلك ان جرائم الماسة بالموقع الالكتروني يمكن ان تدخل ضمن الاختصاص العيني على اعتبار انها جرائم عابرة للحدود وتستثنى من قاعدة الاختصاص الاقليمي[2].

وقد حددت التشريعات الخاصة بالجرائم الالكترونية عموما، ومنها الجرائم التي تطال امن وسلامة الموقع الالكتروني، الاختصاص القانون والمحكمة المختصة، ومنها

---

(١) للمزيد ينظرد. محمود نجيب حسني، شرح قانون العقوبات القسم العام، ط٦، دارالنهضة العربية، القاهرة، ١٩٨٩، ص ١٢١.

(٢) مأمون سلامة، قانون العقوبات القسم العام، مطبعة جامعة القاهرة، القاهرة، ١٩٩١، ص٧٥.

ماجاء في قانون مكافحة تقنية المعلومات الاماراتي في المادة (٤٧) منه بان تسري احكامه على كل من ارتكب احد الجرائم الواردة فيه سواء كانت داخل الدولة او خارجها، بمعنى ان المشرع الاماراتي قد حدد المحكمة المختصة والقانون الواجب التطبيق لهذه الجرائم، وايضا نجد أن المشرع العراقي في مسودة قانون مكافحة الجرائم الالكترونية قد حسم مسالة تنازع الاختصاص في المادة (٣) منه على ان تسري احكامه على الجرائم المنصوصة فيه سواء ارتكبت في العراق او خارجه.

المطلب الثاني: الطعن في الأحكام وحالات الاعفاء من الجزاء

استكمالا لبحث قواعد الاجراءات الجنائية في هذه الجرائم لابد ان نتطرق لمسألة قواعد الطعن بالاحكام الجزائية الصادره فيها، وكذلك تحديد حالات الاعفاء من العقاب وقواعده، وهذا ما نبحثه في الفرعين الاتيين:

الفرع الاول: الطعن في الاحكام الجزائية

ان طرق الطعن في الأحكام هي الوسائل التي حددها القانون على سبيل الحصر، والتي بمقتضاها يتمكن الخصوم من التظلم من الأحكام الصادرة عليه بقصد إعادة النظر فيما قضت به، إذ هي الوسائل التي تمكن الشخص الذي يرى أن الحكم الصادر قد اضر بمركزه من الطعن به والاعتراض عليه لدى محكمة أعلى من تلك التي أصدرته[1].

وقد تناول المشرع العراقي طرق الطعن ونظمه بموجب احكامه، وان رجعنا لها نجدها عدة طرق وحالات يستطيع من خلالها المحكوم علية من ان يطعن بالحكم الصادر بحقه، وطرق الطعن تشمل، الاعتراض على الحكم الغيابي والتمييز وتصحيح

(١) أحمد أبو الوفا، أصول المحاكمات المدنية، الدار الجامعية، بيروت، ١٩٨٣، ص ٦٧٥

القرار التمييزي واعادة المحاكمة، وسيتم شرحها تباعا في الفقرات الاتية:

اولا الاعتراض على الحكم الغيابي: يمكن للمحكوم عليه الهارب رغم صدور حكم غيابي بادانته ان يعترض على هذا الحكم بالرغم من انه صدر بغيابه، اذ اعطاه المشرع الحق في ذلك بموجب احكام المواد(٢٤٣ الى ٢٤٨) حيث يحق له ان يقدم الاعتراض بعد ان يبلغ بالحكم الغيابي بموجب عريضة يقدمها الى المحكمة نفسها او بموجب محضر ينظم في المحكمة او بمركز الشرطة بعد القاء القبض عليه[١] يمكن للمتهم المحكوم عليه غيابياً بجريمة من جرائم الموقع الالكتروني الحق بالطعن بالحكم الصادر بحقه.

ثانيا التمييز: يعد التمييزمن اهم طرق الطعن بالاحكام، اذ يمكن لعدة جهات ان تطعن بقرار الادانة بموجب احكام المادة(٢٤٩) من قانون اصول المحاكمات الجزائية، وهي كل من الادعاء العام والمتهم والمشتكي، والمدعي المدني والمسؤول مدنيا، اذ لهم ان يطعنوا بالحكم الصادر بالادانة، ولابد ان يكون الطعن بالتمييز مستندا الى اسباب معقوله وحصرا في القرارات الفاصلة في الدعوى وقد حدد القانون اسباب الطعن بالتمييز وهي مخالفة القانون او الخطأ في تطبيقه، او الخطأ في الاجراءات او في تقدير الادلة، وكذلك الخطأ في تقدير العقوبة[٢]. ومما تقدم يستطيع المحكوم عليه ان يطعن بقرار الحكم الصادر بحقه في جريمة الكترونية، اذا توافر لديه سبب من اسباب الطعن تمييزا.

ثالثا: تصحيح القرار التمييزي: ان هذا الطريق من طرق الطعن انفرد به المشرع العراقي دون غيره، والغاية منه هو استدراك اخطاء محكمة التمييز الاتحادية عند نظرها

(١) ينظرالمادة(٢٤٣/ ب) من قانون اصول المحاكمات الجزائية.

(٢) ينظر المادة(٢٤٩/ أ) من قانون اصول المحاكمات الجزائية.

في الطعن تمييزا[1]. اما عن الجهة صاحبة الحق في طلب تصحيح القرار التمييزي، فقد اعطى المشرع الحق للمحكوم عليه او الادعاء العام او المشتكي[2]، ويجب ان ينصب طلب التصحيح على خطأ في تطبيق القانون اي القوانين العقابية، وقوانين الاجراءات الجنائية[3]. ويتضح من ذلك ان للمتهم الحق في تصحيح القرار التمييزي، الذي سبق وان طعن فيه تمييزاً، في اي جريمة من الجرائم التي تطال امن وسلامة الموقع الالكتروني، اذا شاب الحكم خطا ما في تطبيق القانون.

رابعا اعادة المحاكمة: يعد هذا الطريق من طرق الطعن غير العادية كون المشرع قد ذكر الحالات التي تجيز اعادة المحاكمة على سبيل الحصر، ومن ضمن الحالات التي من الممكن اعادة المحاكمة فيها بالجرائم الماسة الموقع الألكتروني اذا ثبت ان الجريمة قد ارتكبها شخص اخر غير المحكوم عليه، او اذا حكم على المتهم بموجب رأي خبير تبين انه غير مختص في هذا المجال ولم يقدم تقريرا يفيد بالادانة وثبت فيما بعد انه محرف للحقيقة، او وجود شهادة شاهد زور او بناء على مستند ثبت انه مزور، وكذلك اذا ظهرت حالات اخرى تثبت براءة المتهم المحكوم عليه[4].

يتبين مما سبق ان طرق الطعن هذه قد نظمها قانون اصول المحاكمات الجزائية بوصفه القانون العام في الاجراءات الجنائية، والتي من خلاله تحدد احكام الحماية الاجرائية للمواقع الالكترونية على اعتبار ان طرق الطعن احدى اهم مفاصل تلك الحماية.

---

(١) براء منذر كمال، شرح قانون اصول المحاكمات الجزائية، طه، مطبعة يادكار، السليمانية، ٢٠١٦، ص٣٥٢ .

(٢) ينظر المادة(٢٦٦/ أ) من قانون اصول المحاكمات الجزائية.

(٣) براء منذر كمال، مصدر سابق، ص٣٥٣.

(٤) ينظر نص المادة (٢٧٠) من قانون أصول المحاكمات الجزائية.

ونخلص مما تقدم أن طرق الطعن هذه هي أحكام عامة في القرارات الفاصلة بالدعاوى الجنائية، وبما أن جرائم الاعتداء على سلامة المواقع الالكترونية لا تختلف عن غيرها من الجرائم الأخرى من حيث المبدأ الذي يقضي بإتاحة الفرصة أمام المتقاضين بإعادة النظر بالقرارات الجنائية الصادرة بفصل الخصومة بينهم، الأ أنها قد تحتاج الى بعض الخصوصية التي تتناسب مع طبيعة تلك الجرائم الالكترونية المرتكبة في المواقع الافتراضية، من حيث طبيعة تلك الطرق التي لا بد من أن تتلاءم مع طبيعة تلك الجرائم ومحل الاعتداء فيها، وفي ظل عدم وجود نصوص خاصة لطرق الطعن والإجراءات الجنائية عموماً في تلك الجرائم لا سبيل إلا بالرجوع الى الأحكام العامة في طرق الطعن التي بيناها بشكل عام والتي نظمها قانون أصول المحاكمات العراقي رقم (٢٣) لسنة ١٩٧١ المعدل، فيما يخص إجراءات المحاكمة وطرق الطعن بالأحكام.

الفرع الثاني: الاعفاء من الجزاء في جرائم الاعتداء على الموقع الالكتروني

ان حالات الاعفاء من العقاب أو ماتسمى بالاعذار المعفية من العقاب والبعض يسميها كذلك(موانع العقاب) لأنها تحول دون العقوبة، رغم ثبوت الجريمة بكل اركانها، وبذلك تختلف عن موانع المسؤولية التي تتعلق بالركن المعنوي وتتحقق بانتفاء عنصر الاهلية الجنائية، ومن جهة اخرى تختلف عن اسباب الاباحة بكونها لا ترفع صفة التجريم عن الفعل، ولذلك لا يستفيد منها الا من تتوافر لديه دون غيره من المساهمين في الجريمة أي تمتاز بطابعها الشخصي، اما اسباب الاباحة فأنها ذات طبيعة مادية تتعلق بالتكييف القانوني برفع الصفة المجرمة عن الفعل فيصبح مباحاً ويستفيد منه الجميع الفاعل والمساهمون في الجريمة على حد سواء[1].

(١) للمزيد من التفصيل ينظر: د. اكرم نشأة ابراهيم، القواعد العامة في قانون العقوبات، ط١، مطبعة الفتيان، بغداد، ١٩٩٨ ص٣٤٦؛ د. احمد فتحي سرور، الوسيط في قانون العقوبات القسم

وقد تناولت التشريعات الجنائية محل الدراسة تنظيم مسألة الاعفاء في نصوصها، العقابية الخاصة المعنية بجرائم الموقع الالكتروني الى مسألة الاعفاء من العقاب، ونظمت حالاتها واحكامها، واول تلك التشريعات ما نص عليه قانون مكافحة جرائم تقنية المعلومات الاماراتي، في المادة (٤٥) والتي تضمنت احكام الاعفاء بأنه يمكن للمحكمة ان تقضي بتخفيف العقاب او الاعفاء منه نهائياً بحق المدان بناء على طلب من الادعاء العام، اذا تعاون مع السلطات التحقيقية بتقديم معلومات تسهل لها الوصول الى باقي الجناة وكشف ملابسات الجريمة.

وفي السياق نفسه تطرق نظام مكافحة الجرائم المعلوماتية السعودي الى تنظيم الاعفاء من العقاب وذلك بنص المادة (١١) اذ اعطى بموجبها للمحكمة ان تعفي من العقاب لاي من الجناة ممن يتعاون مع السلطات التحقيقية ويقدم ابلاغاً عن الجريمة قبل ان تكتشفها وتشرع في التحقيق فيها ويساعدها في كشف ملابسات تلك الجريمة ويدلي بمعلومات عمن اشتركو فيها وذلك لتسهيل كشف هوياتهم والوصول اليهم للاقتصاص منهم. اما بالنسبة للمشرع الاردني فانه لم يتطرق الى مسألة الاعفاء، من العقاب في قانون الجرائم الالكترونية، في حين نص المشرع المصري في المادة ٤١ من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ على أن: «يعفى من العقوبات، المقررة للجرائم المنصوص عليها في هذا القانون كل من بادر من الجناة أو الشركاء إلى إبلاغ السلطات القضائية أو السلطات العامة بما يعلمه عنها قبل البدء في تنفيذ الجريمة وقبل كشفها».

اما في التشريع العراقي نجد ان مشروع قانون مكافحة الجرائم الالكترونية، قد تناول

العام، ج١، دار النهظة العربية، القاهرة،١٩٨١، ص٧٧٥؛ نقلا عن محمد ذياب سطام، مصدر سابق،ص١٤٨.

مسألة الاعفاء من العقاب بموجب احكام المادة (٢٠) اذ نصت على انه» يعفى من العقوبة المقررة بموجب احكام هذا القانون كل من بادر من المتهمين سواء كان فاعلا اصليا او مشتركا الى ابلاغ السلطات المختصة بالمعلومات عن جريمة وقعت لمخالفة احكام هذا القانون قلا الكشف عنها، فاذا تم الابلاغ بتلك المعلومات بعد الكشف عنها يجوز للمحكمة المختصة اعفائه من العقاب شريطة ان يترتب على ذلك الادلاء ضبط باقي المتهمين» يفهم من خلال النص انف الذكر انه يعفى من العقاب المقرر للجرائم المنصوص عليها في هذا القانون ومنها الجرائم الماسة بالموقع الالكتروني، كل من يبادر بإخبار السلطات التحقيقية عن وقوع جريمة من هذه الجرائم، شريطة ان يكون هذا الابلاغ او الاخبار منتجا من حيث تسهيل الكشف عن المساهمين بهذه الجرائم ان كانت مرتكبة من قبل اكثر من شخص، ويساعدهم في اثبات ملابساتها، وان النص على الاعفاء يعد عاملا ايجابيا من اجل تشجيع الجاني وحثه على ابلاغ السلطات، عن باقي المساهمين في الجريمة، ومنع وقوعها خاصة اذا كان ذلك قبل البدء بتنفيذ الجريمة.

الخاتمة

يعتبر التزوير الالكتروني من أعقد الجرائم التي تنخر جسد العالم الالكتروني، ان الولوج إلى عالم الجريمة المتطورة ألا وهي جرائم التزوير الالكتروني والتي تتطور يوما بعد يوم مع تطور التكنولوجيا ووجود طبعا الوسيلة النافذة ألا وهو الحاسب الآلي وزيادة على الأدوات المستخدمة في الجريمة لابد من وجود شخص خلف الجهاز متمرس في السيرة والتحكم في الجهاز وأدواته. ألا وهو مستخدم الحاسب الآلي الذي يستطيع بما أوتي من مهارات تزوير البيانات في محررات رسمية أو قاعدة بيانات وذلك عن طريق البريد الالكتروني وهذا ما يؤدي إلى حدوث إضرار بالغير وهذا الغير قد

يكو ن شخصا معنويا أو اعتباريا وبالتالي حدوث الجريمة فكان من اللازم من البحث والوقوف عند هذا النوع من الجرائم وكشف اللثام.

ان جريمة التزوير الالكتروني تقوم على ركنان مادي ومعنـوي ،المادي ويتكون من المحرر المعلوماتي وتغيير الحقيقة والاستخدام الحاسوب في الجريمة ،كما يعتبر الضرر من مكونات الركن المادي، ويقوم الركن المعنوي على القصد العام والخاص. ولا تختلف طرق التزوير التقليدية بشقيها المادي و المعنوي عن جريمة التزوير الالكتروني. وبذلك فأن جريمة التزوير الالكتروني تختلف عن التزوير التقليدي من حيث الوسيلة المستخدمة في ارتكابها يشترط في قيام الأولى أن يستخدم الحاسب الآلي في حين ان الثانية ترتكب بأية وسيلة لتغيير الحقيقة فلا يشترط وسيلة معنية. وللتزوير الالكتروني عدة صور منها تزوير التوقيع الالكتروني وتزوير البطاقة المصرفية وتقليد الشيك الالكتروني ان الرقمي. فهناك دائماً ضحايا في الجريمة الالكترونية سواء كانو اشخاص طبيعين او معنويين. بالتالي ان جريمة التزوير الالكتروني شأنها شأن بقية جرائم الانترنيت والحاسب الالي جريمة حديثة النشأة وان التشريعات العاقبية التي وضعت تتسم بالقلة وعدم إحاطة الموضوع بكل جوانبه مما سبب تشريعاً سهل لضعاف النفوس استغل قدر المستطاع.