وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة عبد الحميد بن باديس مستغانم
كلية الحقوق و العلوم السياسية
قسم: القانون الخاص

المرجع:.....

مذكرة نهاية الدراسة لنيل شهادة الماستر

المسئولية المدنية في المجال الرياضي

إجراءات البحث والتحري في الجريمة الإلكترونية

ميدان الحقوق و العلوم السياسية
الشعبة:حقوق.
التخصص: قانون قضائي
من إعداد الطالب(ة):
فداق محمد
تحت إشراف الأستاذ(ة):
لعيمش غزالة

أعضاء لجنة المناقشة

الأستاذ(ة).....بن عوايل علي.....رئيسا

الأستاذ(ة)..... لعيمش غزالة.....مشرفا مقررا

الأستاذ(ة).....بوسحبة الجيلالي.....مناقشا

السنة الجامعية: 2022/2021

نوقشت يوم:2022/07/03

شكر وتقدير

الحمد لله الذي علم بالقلم، علم الإنسان ما لم يعلم، الصلاة والسلام على سيدنا محمد وعلى أله وصحبه أجمعين.

يسعدني أن أتقدم بالشكر و وافر التقدير وعظيم الامتنان إلى الأستاذة المشرفة على بحثي لعيمش غزالة التي كانت خير معين وخير مرشد، فجزاها الله كل خير، ومتعها بالصحة والعافية.

والشكر موصول لكلية الحقوق والعلوم السياسية " جامعة عبد الحميد بن باديس من أستاذة وإداريين.

محمد

الإهداء

أهدي هذا العمل إلى :

نبع الحب والحنان – الغالية أمي مدها الله بطول العمر والصحة

أغلى وأعز إنسان على قلبي "أبي" أدامه الله نعمة لا تزول

إلى الإخوة والأخوات والأصدقاء

محمد

مقدمة

تمخض عن الفكر الإنساني في العقدين الرابع والخامس من القرن الماضي عن ابتكار أعظم ما قدمته الحضارة الإنسانية إلا وهو الحاسوب، مما أهل لحقبة جديدة بالغة الأهمية أحدثت تأثيرا في بنية المجتمع، حيث تطورت وذلك نتيجة لاكتساح جميع النواحي التي تتطلبها الحياة البشرية، مما جعل منها مصدرا أساسيا للأشخاص، وكذا المؤسسات للاعتماد عليه في كافة شئونهم نظرا للسرعة والدقة في تخزين المعلومات ومعالجتها في وقت قصير.

حيث عرفت هذه الفترة المعلوماتية تطورا مذهلان كما ساعد اقترانها بالتكنولوجيات أخرى على تعميم استعمالها وتعدد وظائفها، فالحديث اليوم لم يعد عن الحاسوب وقدراته في اختزال الوقت وتخزين المعلومات أو إنجاز العمليات المعقدة، وا ٍنما عن تكنولوجيا الإعلام والاتصال، والفضاء الافتراضي الذي نشأ نتيجة ارتباط المعلومات بمختلف المواصلات السلكية واللاسلكية.

حيث أصبحت هذه الوسيلة ليست حكرا فقط على الدول المتقدمة، وا ٍنما تعدت إلى غير ذلك (الدول النامية)، مما زاد من أهمية هذه التكنولوجيات، حيث عرفت بما يسمى بعصر المعلومات، ففي محاضرة ألقاها "كيراك أرثر" مدير إدارة السلامة العامة والعدل التابعة لشركة ميكروسوفت، خلال مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية بالدوحة خلال شهر أفريل 2005، أكد أن حجم البيانات الرقمية المتنامي سيبلغ بحلول عام 2020 أربعين عام زيتابايت، عد ما بلغ 1.8 زيتابيات عام 2012، إضافة إلى تأكيد أن 1.7 مليار شخص يستخدمون رسائل التواصل الاجتماعي وأن أكثر من 6.8 مليار شخص يستخدمون الهاتف النقال.

ومع التغلغل المتزايد للمعلومات وتكنولوجيا الاتصال في مختلف النشاطات البشرية، إذ اعتبرت فضاءا مفتوحا لا حدود له مقارنة بالحدود الإقليمية للدول، وذلك

لكون جميع الدول والمنظمات والمؤسسات خاصة المالية المرتبطة ارتباط وثيق بها من أجل ممارسة أعمالهم ونشاطاتهم، وتقديم مختلف الخدمات لزبائنهم.

الأمر الذي أدى بأصحاب النوايا الإجرامية إلى الاتجاه إلى الاستعمال غير الشرعي لهذه المنظمات المعلوماتية، من أجل ارتكاب أعمالهم الإجرامية المختلفة، من جهة الانتفاع بها، ومن جهة أخرى التملص من لمسئولية الجزائية، وأمام هذا الزحف المتزايد للأنظمة المعلومات ظهر شكل جديد من الإجرام وهو ما يعرف بالإجرام أو الجرائم المعلوماتية.

إذ أنه وبظهور هذا النوع من الإجرام جعل من المجتمع الدولي التدخل من أجل وضع حد لانتشاره، فكان لا بد من وضع أطر قانونية ملائمة جديدة أو إدخال تعديلات على قوانين سارية المفعول بما يتلاءم والوضع الجديد، لتحديد شروط استعمال هذه الوسائل في مختلف المعاملات، من خلال نصوص جزائية لحماية الأنظمة المعلوماتية، وردع إساءة استعمالها سواء محليا أو دوليا في إطار الاتفاقيات الدولية.

فالتقدم العلمي التكنولوجي لا يمكن أن يسير أو يعمل وحده بمعزل عن أي تقدم قانوني يواكبه ويحافظ عليه، ويكفل حمايته ويضع الحلول لما قد يطرأ من مشكلات بسبب استعماله، ففي هذه الحالة يمكن للتقدم التكنولوجي أن يصبح أدناه للبناء وأساس لكل تطور، ويمكن أن يكون أداة لارتكاب الجريمة إذا أسيء استخدامه.

وهو ما يوجب على القانون أن يمتد نصوصه إلى هذه الأنشطة الجديدة التي تفرزها التكنولوجيا حتى تتخذ الجريمة في نصوص منضبطة واحدة، إذ أصبحت النصوص التقليدية لا يمكن أن تسري أو تطبق على هذا النوع من الجرائم، مما أدى إلى ظهور مشكلات إجرامية في هذا المجال.

والجزائر باعتبارها واحدة من الدول التي مسها أو تعرضت لمثل هذا النوع من التطور التكنولوجي سواء كان إيجابيا أو سلبيا، فهي أيضا معينة بالمكافحة فكان لا بد من إيجاد إطار قانوني مناسبا لسد الفراغ الإجرائي، لذلك وضعت مجموعة من الإجراءات

منها ما يعتبر قاسما مشتركا بين الجرائم التقليدية والجرائم المعلوماتية عن طريق تعديل قانون الإجراءات الجزائية بتقنين وسائل وإجراءات خاصة تتماشى وطبيعة الجرائم المستحدثة ومنها الجريمة المعلوماتية، ومنها إجراءات تطبق فقط على الجريمة المعلوماتية فقط، والتي تم النص عليها في قانون جديد يتعلق بالوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحته في القانون رقم 04/09 المؤرخ في أوت 2009.

أهمية البحث:

تكمن أهمية البحث أساسا في كون الجرائم المعلوماتية جريمة جديدة، بالتالي لا يمكن تطبيق الإجراءات التي تطبق على الجرائم التقليدية لأنها من الموضوعات لتي لم تنل حقها من البحث والتحقيق والمحاكمة، على المستوى الجزائي، حيث نجد القواعد الإجرائية التقليدية لا يمكن أن تطبق عليها لاسيما أن هذا لموضوع يتسم بالحداثة وقلة المراجع التي يمكن الاعتماد عليها.

بالإضافة إلى كون الجرائم المعلوماتية حديثة النشأة، ويمتد تأثيرها إلى جميع الأصعدة لارتباطها بتطور تكنولوجيا الإعلام والاتصال، والتي تستخدم في جميع المجالات الحياة سواء من طرف الأفراد أو المؤسسات، إذ تجعل التعاملات معها صعبا ومعقدا، مما يحتم إيجاد طرق جديدة وتابعة لمكافحتها، ومما سبق نطرح الإشكالية التالية:

ما مدى فعالية القوانين الجزائرية للتصدي للجريمة الإلكترونية؟

أسباب اختيار الموضوع:

1. الأسباب الذاتية:

- رغبة وميول شخصي لدراسة جريمة من الجرائم المستحدثة
- أنه موضوع يستحق البحث ويثير الفضول.

2. الأسباب الموضوعية:

التعمق في تفاصيل الجرائم لمعلوماتية وما يحيط بها من اعتداء على نظم المعلوماتية ومعالجة الأنظمة الآلية وغيرها

- التعرف على القواعد الإجرائية والجزاءات التأديبية المترتبة عن ارتكاب الجريمة المعلوماتية .
- إثراء المكتبة القانونية الجزائرية بمراجع في الموضوع.

ولقد اعتمدنا في دراستنا هذه على المنهج التحليلي والمنهج الوصفي لأنهما يعتبران الأنسب لمثل هذه الدراسات.

كما ارتأينا تقسيم البحث وفق الخطة الثنائية إلى:

الفصل الأول: الإطار العام للجريمة الإلكترونية

الفصل الثاني: آليات حماية الجريمة الإلكترونية في التشريع الجزائري

الفصل الأول

الإطار العام للجريمة الإلكترونية

تمهيد:

عرفت البشرية في نهاية القرن الماضي اتساعات وتزايدا مطردا لنطاق استخدام تقنية المعلوماتية في المجتمع، ونظرا للتطور السريع لهذه التقنية، فقد مكنت من استعمالات متعددة وفي جميع المجالات، مما أدى إلى ظهور نوع جديد من الجرائم أطلق عليها تسمية الجرائم الإلكترونية.

ولقد أثارت هذه الجرائم تساؤلات كثيرة باعتبارها ظاهرة جديدة ونظرا لجسامة أخطارها وفداحة خسائرها وسرعة انتشارها، أصبح التعامل مع صور هذه الجرائم موضع اهتمام بالغ من الفئتين والمهتمين بأمن الصرح الإلكتروني، لتحديد مفهومها وخصائصها، والتمييز بينها وبين ما يقترب منها من ظواهر، ومعرفة العوامل المختلفة التي تتدخل في هذا التحديد.

المبحث الأول: ماهية الجريمة الإلكترونية

يوصف العصر الحالي بأنه العصر الرقمي أو ما يسمى بالعصر الإلكتروني الرقمي، فهو يتضمن تطورات تكنولوجيا هائلة وكبيرة ومعقدة تخدم جميع المجالات العامة والخاصة داخل الإطار الضيق للدول، مما يؤدي إلى خدمة المجتمع الدولي بأكمله فهذه التكنولوجيا تخدم جميع مجالات الحياة.

المطلب الأول: مفهوم الجريمة الإلكترونية

لا يوجد إجماع على تعريف الجريمة الإلكترونية من حيث كيف تُعرف أو ما هي الجرائم التي تتضمنها الجريمة الإلكترونية.

وكما يقول فان دير هلست و ونيف "هناك غياب لتعريف عام وا ٍطار نظري متسق في هذا الحقل من الجريمة وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية والرقمية.

الفرع الأول: التعريف الجريمة الإلكترونية

على الرغم من تنامي جهود التصدي لظاهرة الإجرام الإلكتروني إلا أنه لا يوجد تعريف محدد ومتفق عليه بين الفقهاء حول مفهوم الجريمة الإلكترونية، فقد ذهب جانب من الفقه إلى تناولها بالتعريف على نحو ضيق وجانب أخر عرفها على نحو موسع.

أولا:التعريف الضيق للجريمة الإلكترونية

تعرف الجريمة لإلكترونية على أنها: "الجريمة التي يتم ارتكابها إذا قام شخص ما بطريقة مباشرة أو غير مباشرة في استغلال الحاسوب أو تطبيقاته بعمل غير مشروع وضار للمصلحة العامة، ومصلحة الأفراد الخاصة.

ويعرفها الفقيهان الفرنسيان " Le Stantو Vivant " بأنها" :مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب" [1]..

[1]: Vivant et autres: Informatique et droit pénal. Les biens informatiques objets de fraude. Lamy informatique.1991.n°3445.p1511.

ويدخل في نطاق تعريفات مفهوم الجريمة المعلوماتية الضيقة، تعريف مكتب تقييم التقنية بالولايات المتحدة الأمريكية، حيث يعرف الجريمة المعلوماتية من خلال تحديد مفهوم جريمة الحاسب بأنها: "الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا"[1].

ذهب الفقيهان (Credo)و(Michel) إلى أن جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء على بطاقات الائتمان، وانتهاك ماكينات الحساب الآلي بما تتضمنه من شيكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة الحاسب في حد ذاته وأي من مكوناته [2].

هذا الاتجاه الموسع بأنها":كل سلوك اجرامى يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر".

ويعرفها Tièdement بأنها:" كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب"

من خلال هذه التعريفات يتبين لنا أن هذا الاتجاه يوسع من مفهوم الجريمة المعلوماتية، حيث أن مجرد مشاركة الحاسب الآلي في السلوك الإجرامي يضفي عليه وصف الجريمة الإلكترونية".[3]

---

[1]: عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت،الطبعة الأولى، دار الفكر الجامعي، مصر ،2006، ص98.

[2]: طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير، في القانون الجنائي، جامعة الجزائر1 ، كلية الحقوق،2012-2001، ص16.

[3] : عرب يونس، جرائم الكمبيوتر والانترنت،ورقة عمل مقدمة إلى مؤتمر الأمن العربي،2002، ص4.

ثانيا: التعريف الواسع

على عكس الاتجاه السابق، يرى فريق آخر من الفقهاء ضرورة التوسيع من مفهوم هذه الجريمة وتختلف مواقفهم حسب نظر هم إلى الدرجة التي يمكن أن تمتد إليها الجريمة المعلوماتي .

وذهب رأى أخر من الفقه إلى تعريف الجريمة المعلوماتية بأنها: عمل أو امتناع يأتيه الإنسان، إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقاب".

ويرى جانب من الفقه من أنصار هذا الاتجاه الموسع بأنها: كل سلوك اجرامى يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر".

من خلال هذه التعريفات يتبين لنا أن هذا الاتجاه يوسع من مفهوم الجريمة الإلكترونية حيث أن مجرد مشاركة الحاسب الآلي في السلوك لإجرامي يضفي عليه وصف الجريمة الإلكترونية، ومن تم يتضح لنا صعوبة قبول هذا التوجه، فجهاز الحاسب الآلي قد لا يعدو أن يكون محلا تقليديا في بعض الجرائم كسرقة الحاسب ذاته أو الأقراص أو الأسطوانات الممغنطة أو اللواحق على سبيل المثال، ومن ثم لا يمكن إعطاء وصف الجريمة المعلوماتية على سلوك الفاعل كرد أن الحاسب الآلي أو أي من مكوناته كانوا محلا للجريمة.

ثالثا: تعريف الاتفاقيات الدولية

عرف خبراء منظمة التعاون الاقتصادي والتنمية جريمة الكمبيوتر بأنها[1]: كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و / أو نقلها"، ويتبنى هذا التعريف الفقه الألماني لذي يعتمد هذا التعريف بناء على معيارين هما: وصف السلوك واتصال السلوك بالمعالجة الآلية للبيانات أو نقلها.

[1]: موقع منظمة التعاون الاقتصادي والتنمية، WWW.Oecd.Org ، تم زيارة الموقع بتاريخ 2022/04/20 على الساعة 21:45.

قدمت المادة الأولى من الاتفاقية الدولية للإجرام المعلوماتي تعريف للنظام المعلوماتي على النحو التالي:"يقصد بمنظومة الكمبيوتر أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو ذات صلة بذلك ويقوم إحداهما أو أكثر من واحد منها تبعا للبرنامج بعمل معالجة آلية للبيانات ويقصد ببيانات الكمبيوتر أية عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل مناسب لعملية المعالجة داخل منظومة الكمبيوتر بما في ذلك البرنامج المناسب لجعل منظومة الكمبيوتر تؤدي وظائفها" [1].

عرف المؤتمر العاشر للأمم المتحدة لمنع الجريمة ومعاقبة المجرمين الجريمة الإلكترونية بأنها":أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية" [2].

عرفت اتفاقية بودابست في المادة الأولى منها بعنوان تعريف خاص بأغراض هذه الاتفاقية منظومة معلوماتية ومعطيات معلوماتية: أ/منظومة معلوماتية" :أي جهاز أو مجموعة من الأجهزة المتصلة يبعضها أو ذات صلة بذلك ويقوم أحدها أو أكثر من واحد منها تتبعا للبرنامج بعمل معالج آلية للمعطيات".

عرف المؤتمر العاشر للأمم المتحدة لمنع الجريمة ومعاقبة المجرمين الجريمة المعلوماتية بأنها: أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية.

[1] : موقع منظمة التعاون الاقتصادي والتنمية WWW.Oecd.Org . ، نفس تاريخ الزيارة السابق الإشارة إليه.

[2]: عقد هذا المؤتمر في فيينا في الفترة ما بين (10-17) أفريل2000.

رابعا: تعريف القانون الجزائري

اصطلح المشرع الجزائري على تسمية الجرائم المعلوماتية بمصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وقد أضاف مصطلح الجرائم الأكثر تعقيدا أي نوع أخر لها ضمن أخر تعديل لقانون الإجراءات الجزائية بالأمر رقم 11/21 المؤرخ في 25 أوت 2021.[1]

تدارك المشرع الجزائري مؤخرا ولو نسبيا الفراغ القانوني في مجال الجرائم المعلوماتية وذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون 15/04 المؤرخ في2004.11.10 المتضمن تعديل قانون العقوبات[2]، ولكن المشرع تناول في النصوص المستحدثة الاعتداءات الماسة بالأنظمة المعلوماتية وأغفل الاعتداءات الماسة بمنتجات الإعلام الآلي.

فقد أورد المشرع ظرفي تشديد لعقوبة الدخول غير المشروع وهما :في حالة ما إذا ترتب عن الدخول غير المشروع حذف أو تغيير المعطيات، أو تخريب نظام اشتغال المنظومة .وقد نص المشرع في المادة المذكورة على تجريم فعل الشروع في جريمة الدخول غير المصرح به وذلك بقوله "أو يحاول ذلك[3].

الفرع الثاني: صور الجريمة المعلوماتية

إذا كانت الجرائم المعلوماتية لها صور متعددة بتعدد دور التقنية المعلوماتية من جهة وتعدد صور الجرائم التقليدية ممنجهة أخرى، فإن ذلك لا يعني تناول هذا الموضوع بالطريقة المدرسية التقليدية التي تتمثل في سرد كل الجرائم التي يتناولها قانون العقوبات، بل يجب التعرض للحالات التي تثير مشكلة في تطبيق النصوص القانونية إما لتعذر المطابقة بينها و بين النصوص التقليدية أو بسبب الفراغ التشريعي لمواجهة هذه الجرائم

[1] : الأمر رقم 11/21 المؤرخ في 25 أوت 2011المتضمن تعديل قانون الإجراءات الجزائية الجزائري.

[2]: القانون15/04 المؤرخ في 10 نوفمبر2004 المعدل و المتمم للأمر 156/66المؤرخ في 8 جوان1966 المتضمن قانون العقوبات (ج ر 71 بتاريخ10 /2004/11.)

[3]: أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري،الطبعة الأولى، دار هومة،2012، ص99 .

ولما كان المجال لا يتسع للحديث عن كل أنواع الجريمة المعلوماتية فقد تخيرنا أكثرها إثارة للمشكلات القانونية وهي جرائم الاعتداء على الحياة الخاصة و جرائم الأموال وجريمة التزوير.

أولاً : جرائم الاعتداء على الحياة الخاصة للأفراد

المقصود من التطرق لموضوع جرائم الاعتداء على الحياة الخاصة للأشخاص التعرض لتلك الجرائم التي يتعذر علينا مواجهتها بالنصوص التقلدية، فالاعتداء عليها يتم بواسطة هذه التقنية التي أدت إلى سلب مادية السلوك ومناقشة الحالات التي تثير مشكلة في تطبيق النصوص التقليدية وتكشف مدى الحاجة إلى التصدي التشريعي لهذا النوع من الجرائم وهي جرائم الاعتداء على الحياة الخاصة.

ثانيا: جرائم الاعتداء على الأموال

جرم الاعتداء على الأموال في صوره التقليدية كالسرقة والنصب وخيانة الأمانة واختلاس الأموال العامة ، فقد كان ذلك في ظل عصر لا يعرف سوى النقود الورقية أو المعدنية وما يحل محلها من صكوك أو أوراق مالية كالكمبيالات والسند الأدنى في عصر المصارف التقليدية ذات المقر المحدد مكانيا وقد كان أقصى ما وصلت اليه من تقدم متمثلا في إجراء التحويلات المصرفية بإجراءات ورقية معقدة و مقابل رسوم مالية معينة. فإذا كان الركن المادي للسرقة المتمثل في الاختلاس يمكن ان يطبق على التحويلات المالية غير المشروعة التي تتم عبر المصارف التقليدية فذلك لأن جريمة السرقة من الجرائم ذات القالب الحر لم يحدد المشرع شكل السلوك الإجرامي لها ، يمكن أن يتم بأي فعل يؤدي الى حرمان المجني عليه من المال المنقول وا ٍدخاله في حيازة الجاني ، كذلك الحال بالنسب لجريمة النصب حيث يتحقق السلوك الإجرامي لها بالاستيلاء على أموال الآخر بالطرق الاحتيالية.[1]

[1] : محمد سامي الشوا – ثورة المعلومات وانعكاساتها على قانون العقوبات – دار النهضة العربية – القاهرة 1994 ص 155.

ثالثاً : جريمة التزوير

الوثيقة هي مجموعة من المعاملات والرموز التي تعبر تعبيرا اصطلاحيا عن مجموعة مترابطة من الافكار والمعاني الصادرة عن شخص او اشخاص معينين ، وتكمن القيمة الحقيقية لها ليس في مادتها او ما تحتويه بل تكمن فيما لهذا التعبير من دلالة اجتماعية [1].

فجوهر جريمة التزوير هو الاخلال بالثقة العامة التي اراد المشرع حمايتها في هذه الوثيقة لما لها من اثار قانونية باعتبارها وسيلة للإثبات[2].

ولما كان ذلك ، فإن قوة الوثيقة في الاثبات هى جوهر الحماية الجنائية لها ومن هنا ذهبت بعض الآراء الفقهية الى أن كل مادة تصلح للاثبات يجوز أن تكون محلا للتزوير مهما كان شكلها او مساحتها ولا اهمية للمادة المستعملة في الكتابة يستوى ان تكون مصنوعة من خشب او جلد[3] فاذا كانت فكرة التوسع في مفهم الوثيقة مطروحة في الفقة الجنائي قبل ظهور جرائم المعلوماتية فإن هذا التوسع يبدو أكثر الحاحا في ظل الفراغ التشريعي لمواجهة جرائم التزوير المرتكبة بواسطة الحاسب الالي.

المطلب الثاني: البنيان القانوني للجريمة الإلكترونية ومميزاتها

تعد الجرائم الإلكترونية من الجرائم المستحدثة التي بدأت في الانتشار بشكل واسع في الآونة الأخيرة، وذلك بسبب الاستعمال السيئ للثورة التكنولوجية، مما دفع الكثير من الحكومات إلى إظهار اهتمام متزايد لمكافحة الجرم الإلكتروني وسد ثغرات الأنظمة المعلوماتية، والجريمة الإلكترونية كغيرها من الجرائم التقليدية تقوم على أركان وأساس قانوني

[1]: محمود نجيب حسني – شرح قانون العقوبات – القسم الخاص – الجرائم المضرة بالمصلحة العامة – دار النهضة العربية - القاهرة 1972 ص 322.

[2]: المرجع نفسه، نفس الصفحة.

[3] :حسن صادق المرصفاوي – قانون العقوبات الخاص – منشأة المعارف – الإسكندرية مصر 1991، ص 116.

للجريمة الإلكترونية مجموعة من الخصائص التي تنفرد بها عن الجرائم التقليدية، ومن أهم هذه الخصائص أن الجرائم الالكترونية تتطلب وجود جهاز إلكتروني ومعرفة كيفية استخدامه وا ٍن الهدف من هذه الجرائم الكيانات المعنوية لهذا الجهاز، كما أن الجريمة الإلكترونية لا حدود لها، وهذه الجرائم صعبة الإثبات والاكتشاف.

الفرع الأول: أركان الجريمة الإلكترونية

أولا: الركن الشرعي

يقصد بالركن الشرعي للجريمة وجود نص يجرم الفعل ويوضع العقاب المترتب عليه وقت وقوع هذا الفعل، يبنى على ذلك عدم جواز ملاحظة الشخص عن فعل ارتكبه قبل صدور نص التجريم، وعن فعل ارتكبه بعد إلغاء نص التجريم، كما لا يجوز قياس أفعال لم ينص المشرع على تجريمها وأفعال أخرى ورد نص التجريم عليها مهما يكن بينها من تشابه من حيث الدوافع أو الفاعلية أو النتائج أو العناصر، ذلك أنه لا يجوز أيضا التوسع في تفسير النصوص الجزائية، وعلى القضاة التقيد بمدلول النص والالتزام بمضامينه.[1]

يترتب على إ عمال قاعدة شرعية الجرائم والعقوبة نتيجة مهمة، تتمثل في عدم رجعية القاعدة الجنائية، أي بمفهوم المخالفة تنطبق القواعد الجنائية بأثر فوري وال مجال لإعمالها بأثر رجعي، إلا إذا نص القانون على ذلك صراحة في النص القانوني أو إذا ما أعملت قاعدة تطبيق القانون الأصلح للمتهم.[2]

إن الركن الشرعي للجريمة الذي هو الصفة غير المشروعة للفعل الذي يقوم به الجاني له ركنين أساسين:

- مطابقة الفعل لنص التجريم.

[1] : أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، مرجع سبق ذكره، ص100.

[2] : قربوز حليمة، الجريمة المعلوماتية في التشريع الجزائري والقانون المقارن، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2009_2006، ص41.

- أن لا يخضع الفعل المرتكب لسبب من أسباب الإباحة.

يقصد بمطابقة الفعل لنص التجريم هو تطابق الأفعال التي يجر مها القانون مع النصوص التشريعية الموجودة، أما بالنسبة لخضوع الفعل لسبب من أسباب الإباحة فقد ذهب اجتهاد المحكمة العليا إلى أنه لتطبيق نظرية العقوبة المبررة أن يكون النص الواجب التطبيق

يقرر نفس العقوبة. [1]

ثانيا: الركن المعنوي

إن الر كن المعنوي في الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات تتّخذ صورة القصد الجنائي.

1. الركن المعنوي بالنسبة للدخول والبقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات:

إن الر كن المعنوي لجريمة الدخول والبقاء غير المشروعين، يتّخذ صورة القصد الجنائي من علم و إرادة باعتبارها من الجرائم العمدية، وقد عبر نص المادة 394 مكرر عن القصد الجنائي العام بتطلّبه أن يكون الدخول أو البقاء عن طريق الغش فاستخدام هذه العبارة يعني أن الفاعل على علم بأن دخوله أو بقاءه في نظام المعالجة الآلية للمعطيات غير مشروع. [2]

يتطلّب القصد العام أن يحيط علم الجاني بكل واقعة ذات أهمية قانونية في تكوين الجريمة، وبناء أركانها، واستكمال عناصرها، وخاصة الركن المادي منها، وأول هذه العناصر هو موضوع الحق المعتدى عليه، فيتعين توافر علم الجاني بأن فعله ينصب على نظام المعالجة الآلية للمعطيات بما يتضمنه من معلومات وبرامج، باعتباره محل

[1] : قربوز حليمة، الجريمة المعلوماتية في التشريع الجزائري والقانون المقارن، المرجع السابق، ص42.

[2] : حاجب هيام، الجريمة المعلوماتية، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء،2005-2006،ص91.

الحق الذي يحميه المشرع فإذا اعتقد الفاعل بناء على أسباب معقولة بأنّه يقوم على سبيل المثال بإجراء بعض العمليات الحسابية عن طريق الحاسب الآلي، دون أن يتّجه علمه إلى أنه يقوم بالدخول أو البقاء في نظام المعالجة الآلية للمعطيات، فإن قصد الدخول أو البقاء لا يتوافر فيها.[1]

وهناك وقائع يسأل فيها الجاني عن الجريمة دون أن يتطلّب القانون علمه بها، فحين يقرر القانون لبعض الجرائم عقاباً معيناً إذا أحدث الفعل نتيجة ذات جسامة معنية، وإذا ازدادت جسامة هذه النّتيجة فأفضت إلى نتيجة أشد جسامة، شدد القانون العقاب، ويتطلّب المشرع انصراف القصد الجنائي إلى النّتيجة الأقل جسامة،ولكنّه لا يتطلّب انصرافه إلى النّتيجة الأشد جسامة، بحيث يسأل الجاني عنها بالرغم من عدم توقعها لها.

أما بالنِّسبة لإرادة الجاني فيجب أن تتّجه إلى الدخول أو البقاء غير المشروعين داخل النّظام، أي أن تتّجه إرادته لتحقيق هذه النّتيجة ، ولا عبرة بعد ذلك للباعث أو الغاية من وراء هذا الدخول أو البقاء سواء كان هذا الباعث هو الفضول، أو إثبات القدرة على المهارة والانتصار على النِّظام، حتى وإن كانت الغاية نبيلة كمن يدخل إلى النِّظام غير المصرح له بالدخول رغبةً في الكشف عن أوجه القصور التي تعتري النِّظام الذي تمكن من الدخول إليه، وذلك لتجنب هذا القصور مستقبلا.[2]

2. الركن المعنوي للاعتداءات على سير نظام المعالجة الآلية للمعطيات والاعتداءات على المعطيات خارج وداخل النظام:

إن الاعتداءات على سير نظام المعالجة الآلية للمعطيات بصورتيها التّعطيل أو العرقلة وإفساد النّظام، لا تكون إلاّ عمدية هذا ما يميزها عن الاعتداء غير العمدي لسير النِّظام الذي يشكّل ظرفاً مشدداً لجريمة الدخول والبقاء غير المشروعين داخل النِّظام.

[1] : حاجب هيام، الجريمة المعلوماتية، المرجع السابق، ص92.

[2] : المرجع نفسه، ص93.

وهذه الاعتداءات تتطلّب القصد الجنائي العام من علم وإرادة، شأنها شأن الاعتداءات العمدية على المعطيات، فيجب أن يعلم الفاعل بأنّه يقوم بإحدى هذه الأعمال التي أوردها النّص القانوني، والتي من شأنها إتلاف المعلومات، فيعلم بأنه يقوم بفعل الإدخال أو المحو أو التّعديل، ويعلم خطورة النّشاط الإجرامي الذي يقوم به وما يترتّب عنه من عقاب.[1]

ثالثا: الركن المادي

البد من فعل أو امتناع يمكن إثباته إذ لا عبرة بما في خلد الإنسان من أفكار لأنها لا تدخل دائرة التجريم، والركن المادي هنا يختلف من حال الأخر حسب التصنيف الذي يقع على الفعل وعليه لا يمكن حصر الجريمة المعلوماتية تحت تكييف واحد، فقد تشكل الواقعة المرتكبة والتي تحمل وصف الجريمة المعلوماتية واقعة قذف أو تهديد أو تحريض وبشكل مطابق تماما ملا يجري عليه قانون العقوبات من خلال بعض القواعد التي ينطبق حكمها حتى على الجرائم الواقعة عن طرق جهاز الكمبيوتر، وهذا لا يسبب إشكال، إذ يمكن تطبيق نصوص قانون العقوبات على هذه السلوكيات التقليدية، إلا أن هناك أنواعا من السلوك يتطلب التمييز بينها وبين سابقتها ، وهذا ما يدعو للتدخل التشريعي.[2]

يتكون الركن المادي للجريمة الإلكترونية من السلوك الإجرامي والنتيجة والعالقة السببية، علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقيق نتيجتها، مثال: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لا مناص من معاقبة الفاعل.

---

[1] : محمود عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتاب القانونية،
مصر، 2006، ص 22.

[2] : محمدالأمين البشري، التحقيق في الجرائم المستحدثة، الطبعة الأولى، دار الجامعة ، عمان، 2014، ص 332.

يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل إيجابي مرتكب مثال : جريمة الغش المعلوماتي: الركن المادي فيها هو تغيير الحقيقة في التسجيلات الإلكترونية أو المحررات الإلكترونية[1].

الفرع الثاني: خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية عن غيرها من الجرائم التقليدية ببعض السمات والخصائص والتي نوجزها فيما يلي:[2]

أ/ خصوصية الجريمة الإلكترونية:

تتسم الجريمة المعلوماتية بصعوبةاكتشافها وا ٍثباتها، ويرجع ذلك إلى عدة أسباب من بينها وسيلة تنفيذها التي تتميز في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد، بالإضافة إلى الإحجام عن الإبلاغ عنها في حالة اكتشافها لخشية المجني عليهم من فقد ثقة عملائهم، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة.

فعلى سبيل المثال أحصت وزارة الداخلية في فرنسا عام 1986 حوالي 1200جريمة معلوماتية في حين كان هناك حوالي 53600 جريمة ضد الأشخاص و 18900 جريمة تندرج تحت وصف جرائم الآداب و 3 مليون جريمة ضد الأموال، وفي أحدث تقارير مركز شكاوى احتيال الانترنت الأمريكي أظهر التحليل الشامل للشكاوى التي قدمت للمركز خلال سنة 2004 قد بلغت 6348 شكوى من ضمنها 5273 حالة تتعلق باختراق الكمبيوتر عبر الانترنت و 814 تتعلق بوسائل الدخول والاقتحام الأخرى كالدخول عبر الهاتف أو الدخول المباشر إلى النظام بشكل مادي مع الإشارة إلى أن هذه

[1] : محمدالأمين البشري، التحقيق في الجرائم المستحدثة، المرجع السابق، ص333.

[2] : محمود حماد مرهج الهيني، أصول البحث والتحقيق الجنائي، دار الكتاب القانونية، القاهرة، مصر، 2014، ص123.

الحالات هي فقط التي تم الإبلاغ عنها ولا تمثل الأرقام الحقيقية لعدد حالات الاحتيال الفعلي[1].

وفي مقابل انخفاض نسبة جرائم المعلوماتية في مواجهة الجرائم التقليدية، ترتفع الخسارة الناجمة عن الجرائم المعلوماتية بصورة كبيرة بالمقارنة بغيرها من الجرائم، فعلى سبيل المثال كانت الخسارة الناجمة عن 8000 حالة سرقة بالإكراه في فرنسا عام1986 حوالي 561 مليون فرنك الفرنسي، في حين يتضاعف هذا الرقم في حالة الجرائم المعلوماتية على الرغم من انخفاضها نسبة 8 مرات عن حالات السرقة بالإكراه.

وفي المقابل فانه، وعلى غرار الآراء التي تتجه إلى القول بأن الجريمة المعلوماتية لا يوجد شعور حقيقي بعدم الأمان في مواجهتها، أو أنه لا يوجد شعور عام بعدم أخلاقية هذه الأفعال، فإنه من الفقهاء من لا يتفقون مع هذه الآراء إذ أن الجريمة المعلوماتية لا تختلف عن غيرها من الجرائم من حيث اعتدائها على مصالح لها أهميتها لدى أفراد المجتمع، ومن ثم تستحق الحماية القانونية كون أن مساس هذه الأفعال بهذه المصالح هو الذي يبرر تجريمها.[2]

ب /دولية الجريمة الإلكترونية:

يمكن القول أن من أهم الخصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية، ومن اكتسابها طبيعة دولية، أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعدية الحدود، فبعد ظهور شبكات المعلومات لم تعد الحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال، قد أدت إلى نتيجة مؤداها أن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد.

---

[1]: نائلة عادل محمد فريد قورة-جرائم الحاسب الآلي الاقتصادية مرجع سبق ذكره، ص49.

[2] : المرجع نفسه، ص50.

كما أن السرعة الهائلة التي يتم من خلالها تنفيذ الجريمة المعلوماتية وحجم المعلومات والأموال المستهدفة والمسافة التي قد تفصل الجاني عن هذه المعلومات والأموال، قد ميزت الجريمة المعلوماتية عن الجريمة التقليدية بصورة كبيرة[1].

وقد أثارت الطبيعة الدولية للجرائم المعلوماتية تساؤلا مهما يتعلق بتحديد الدولة التي يختص قضاؤها بملاحقة الجريمة، فهل هي الدولة التي وقع بها النشاط الإجرامي، أم تلك التي توجد بها المعلومات محل الجريمة، أم تلك التي أضرت مصالحها نتيجة لهذا التلاعب، كما أثارت هذه الطبيعة أيضا الشكوك حول مدى فاعلية القوانين القائمة في التعامل مع الجريمة المعلوماتية وبصفة خاصة فيما يتعلق بجمع وقبول الأدلة[2].

لمواجهة جرائم المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم، فيجب أن يشمل هذا التعاون تبادل المعلومات، تسليم المجرمين، وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى، كما أن هذا التعاون يجب أن يمتد إلى مكافحة الجريمة المعلوماتية، وهو ما يقتضي أيضا تبادل المعلومات بين الدول المختلفة، وتعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو" إبرام الاتفاقيات الدولية."

تعد الاتفاقيات الخاصة بتسليم أو تبادل المجرمين من أهم الوسائل الكفيلة بضمان محاكمة مجرمي المعلوماتية، إلا أن الوصول إلى إبرام هذه الاتفاقيات يقتضي التنسيق بين قوانين الدول المختلفة لضمان تحقق" مبدأ ازدواجية التجريم "فيما يتعلق بجرائم المعلوماتية.

---

[1]: محمود حماد مرهج الهيني، أصول البحث والتحقيق الجنائي، مرجع سبق ذكره، ص125.

[2]: المرجع نفسه، ص126.

ونجد أن هذا المبدأ يقف عقبة رئيسية طالما أن كثيرا من القوانين لم يتم تعديلها بحيث تتلاءم مع هذه الجرائموا ن كان المشرع قد خطى خطوة إلى الأمام في هذا المجال بصدور القانون15/04 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات. [1]

والذي استحدث نصوصا خاصة بالجرائم الماسة بالأنظمة المعلوماتية في المواد من المادة مكرر إلى غاية المادة 394 مكرر 7[2] من القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات.

ونخلص مما سبق إلى أنه في سبيل مكافحة الجريمة المعلوماتية يجب أن تتحرك الدول المختلفة في محورين:

الأول : داخلي بحيث تتلاءم تشريعاتها الداخلية مع هذا النمط الجديد من الجرائم.

الثاني : دولي عن طريق عقد الاتفاقيات الدولية، حيث لا يستفيد مجرموا المعلوماتية عن عجز التشريعات الداخلية من ناحية، وغياب الاتفاقيات الدولية التي تعالج سبل مواجهة هذه الجرائم من ناحية أخرى.

ج/ الجريمة الإلكترونية صعبة الاكتشاف والإثبات:

نظرا للطبيعة الخاصة الذي تتميز بها الجريمة الإلكترونية فإن إثباتها يحيط به كثير من الصعوبات، والتي تتمثل في صعوبة اكتشاف هذه الجرائم، لأنها لا تترك أثرا خارجيا، فالجريمة الإلكترونية لا عنف فيها وال أثر اقتحام لسرقة مثال، وا نما هي أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسوب وليس لها أي أثر خارجي مرئي، وبمعنى آخر فإن الجريمة الإلكترونية هي جرائم فنية، وهي جرائم هادئة لا تتطلب العنف، ورغم ذلك فان البعض يشبه هذه الجرائم بجرائم العنف مثل ما ذهب إليه مكتب التحقيقات الفدرالي بالواليات المتحدة الأمريكية نظرا لتماثل دوافع المتعدين على

[1] : القانون15/04 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات.

[2] : لمادة 394 مكرر 7 من القانون15/04 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات.

نظم الحاسوب الآلي مع مرتكبي العنف.فإذا تم اكتشاف الجريمة الإلكترونية، فال يكون ذلك إلا بمحض الصدفة، نظرا لعدم وجود أثر مادي لما يجري خلال تنفيذها من عمليات، حيث يتم نقل المعلومات بالنبضات الإلكترونية، ولذلك يستطيع الجاني تدمير دليل الإدانة في أقل من ثانية، إلى جانب إمكانية ارتكابها خارج الحدود الوطنية والدول والقارات وذلك باستخدام شبكات الاتصال ودون تحمل عناء الانتقال، إلى جانب تلك الرغبة في استقرار حركة المعاملات محاولة إخفاء أسلوب ارتكاب الجريمة حتى لا يتم تقليدها من جانب الآخرين.[1]

د/ وقوع الجريمة الإلكترونية في بيئة المعالجة الآلية للبيانات:

تقع الجريمة الإلكترونية أثناء المعالجة الآلية للبيانات والمعطيات الخاصة بالكمبيوتر، ويتمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث عن قيام أو عدم قيام أركان الجريمة الإلكترونية الخاصة بالتعدي على نظام معالجة البيانات، ذلك أنه في حالة تخلف هذا الشرط تنتفي الجريمة الإلكترونية.

حيث يستلزم لقيام هذه الجريمة التعامل مع بيانات مجتمعة ومجهزة للدخول للنظام المعلوماتي بعرض معالجتها إلكترونيا، بما يمكن المستخدم من امكانية كتابتها من خلال العمليات المتبعة، والتي يتوافر فيها امكانية تصحيحها أو تعديلها أو محوها أو تخزينها أو استرجاعها وطباعتها، وهذه العمليات وثيقة الصلة بارتكاب الجرائم، ولا بد من فهم الجاني لها أثناء ارتكابها في حالات التزوير والتقليد. [2]

[1] : خالد محمود إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2009، ص66.

[2] : خالدمحمود إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص67.

المبحث الثاني: التحقيق الجنائي في الجريمة الإلكترونية

نظرا لانتشار الجريمة الإلكترونية بشكل ملفت للانتباه، ولأن أجهزة التحقيق في الجرائم التقليدية لم تكن كافية للتصدي لهذا النوع من الإجرام، أنشئت أجهزة خاصة بالتحقيق فيها.

المطلب الأول: الهيئات المكلفة بالبحث والتحري عن الجرائم الإلكترونية

للتحقيق أهمية في إثبات وقوع الجرائم و إقامة الدليل على مرتكبيها بأدلة الإثبات على اختلاف أنواعها، وهو كما يدل عليه اسمه استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة، ومن يقوم بالتحقيق هم الضبطية القضائية وقضاة وفق إجراءات البحث و التحري المحددة وفقا لقانون الإجراءات الجزائية.

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

يمكن القول أن المحقق هو من يتولى التحقيق من رجال الضبطية القضائية، أو من أعضاء النيابة العامة، أو قضاة التحقيق ويلحق بالمحقق الجنائي الباحث الجنائي الذي يكون غالبا من الشرطية القضائية، الذين خول لهم القانون مهمة جمع االستدالالت عن المشتبه بهم.

وقد استحدثها المشرع الجزائري بموجب قانون رقم 09 -04[1] المؤرخ في 05 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتم تنظيم عملها بموجب المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015، ومن مهامها تفعيل التعاون القضائي والأمني الدولي وغدارة وتنسيق العمليات الوقائية والمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكاليفها

[1] : سعيد علي نعيم، آليات البحث والتحري من الجرائم المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2013، ص107.

بالقيام بخبرات قضائية في حال الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني الهيئة الوطنية تعد سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل، وتظم أساسا أعضاء من الحكومة معنيين بالموضوع، ومسؤولي مصالح الأمن، وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء .تظم الهيئة قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك والأمن الوطنيين، وفقا لأحكام قانون الإجراءات الجزائية تكلف بتجميع وتسجيل وحفظ المعلومات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية وضمان المراقبة والوقاية للاتصالات الإلكترونية، وذلك قصد الكشف عن الجرائم المنصوص عليها في قانون العقوبات أو الجرائم الأخرى تحت سلطة القاضي المختص.

للإشارة هنا تمكنت الجزائر ممثلة أساسا في أجهزتها الأمنية التابعة للدرك الوطني والأمن الوطني وبالتعاون مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من معالجة أكثر من 100 جريمة إلكترونية منها 30 %على مواقع التواصل الاجتماعي، هذا وقد سجلت مديرية الشرطة القضائية بالمديرية العامة للأمن الوطني خلال السداسي الأول من عام 2016 وجود 11 قضية متعلقة بالإرهاب الإلكتروني أغلبها خاصة بالتهديدات الإرهابية باسم تنظيم داعش الإرهابي لتسفر جهود البحث والتحري والتنسيق بين مختلف القطاعات المختصة توقيف 58 شخصا متورطا في قضايا إرهاب الكتروني تمت إحالتهم على القضاء[1].

هذا وقد استطاعت الشرطة الجزائرية المتخصصة من توقيف ما يزيد عن 160 جزائري لهم علاقة مباشرة مع تنظيم داعش في العراق، سوريا وليبيا كما تمكنت من فك

[1] :سعيد علي نعيم، آليات البحث والتحري من الجرائم المعلوماتية في القانون الجزائري، المرجع السابق، ص 108.

شفرات الرسائل المتبادلة وما يزيد عن 30 خلية تسعى لاستقطاب الشباب لتجميده عبر مواقع الانترنت ومنصات التواصل الاجتماعي خاصة الفيس بوك والتويتر لصالح التنظيمات الإرهابية نتيجة استعمالها لأنظمة تكنولوجية حديثة وتلقيها معلومات تفيد بوجود منشورات إرهابية داعمة وتدعو للمشاركة في منتديات إرهابية غلى جانب اتصالات محلية ودولية.

تنص المادة 32 من الأمر رقم 11/21 على انه[1]"تتولى الهيئة المذكورة في المادة 31خصوصا المهام التالية":

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال

ومكافحتها.

- مساعدة السلطة القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال بما في ذلك تجميع المعلومات.

- تبادل المعلومات مع نظيرتها في الخارج قصد جمع المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال وتحديد مكان تواجدهم. [2]

الفرع الثاني: الوحدات التابعة لسلك الأمن الوطني

توجد لدى مديرية الأمن الوطني و الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن والنظام العام مجموعة من الوحدات نكرها منها:

أ- الوحدات التابعة لسلك الأمن الوطني : تضع مديرية الأمن الوطني في إطار تحديد سياسة أمنية فعالة، كافة الإمكانيات البشرية والتقنية المتاحة لديهم لأجل التصدي لكل

[1] : 32 من الأمر رقم 11/21 المؤرخ في 25 أوت 2021المتضمن تعديل قانون الإجراءات الجزائية الجزائري.

[2] : سعيد علي نعيم، آليات البحث والتحري من الجرائم المعلوماتية في القانون الجزائري، المرجع السابق، ص109.

أنواع الجرائم بالخصوص تلك المستحدثة منها كالجرائم الإلكترونية، والتي تعتبر نتاج القصور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات الإعلام والاتصال، وذلك بهدف حماية المصلحة العامة وكذلك المصالح الخاصة المرتبطة باستعمال هذا النوع من التكنولوجيات .

توجد على مستوى جهاز الأمن الوطني ثلاث وحدات مكلفة بالبحث والتحقيق في الجرائم المعلوماتية وهي كالآتي:[1]

- المخبر المركزي للشرطة العلمية بالجزائر العاصمة– .
- المخبر الجهوي للشرطة العلمية بقسنطينة.

في سبيل تدعيم المصالح الولاية للشرطة القضائية قامت المديرية العامة للأمن الوطني سنة 2010 بخلق ما يقارب 23 خلية لمكافحة الجريمة المعلوماتية على مستوى ولايات الوسط، الشرق، الغرب، الجنوب، لتقوم فيما بعد بتعميم الخلايا على جميع مصالح الأمن ولايات الوطن.[2]

ب- الوحدات التابعة للقيادة العامة للدرك الوطني : يضع الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن الوطني والنظام العام ومحاربة الجريمة بكافة أنواعها، وحدات متنوعة وعديدة على مستوى القيادة العامة، أو على مستوى القيادات الجهوية والمحلية نذكر منها[3] :

- المصالح والمراكز العلمية والتقنية
- هياكل التكوين
- المصلحة المركزية للتحريات الجنائية

[1] : المرجع نفسه، ص110.

[2] : قدري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة ماجستير ، جامعة قاصدي مرباح، ورقلة ، كلية الحقوق والعلوم السياسية ، قسم الحقوق، 2013، ص179.

[3] : المرجع نفسه، ص180.

- المعهد الوطني لعلم الإجرام

يوجد بالعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع لقيادة العلمية للدرك الوطني قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، حيث يقوم بتحليل الأدلة الانجاز ات الخاصة بالجرائم الإلكترونية، وذلك بتحليل الدعامات الإلكترونية، والمقاربات الهاتفية، وتحسين التسجيلات الصوتية والفيديو والصورة وذلك لتسهيل استغلالها بالإضافة إلى مراكز الرقابة من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومية للدرك الوطني وهو قيد الإنشاء .

المطلب الثاني: وسائل الإثبات في الجرائم الإلكترونية

الفرع الأول: مفهوم الدليل الإلكتروني

يعرف الدليل الذي يجد أساسا له في العالم الافتراضي ويقود إلى الجريمة وهو كدليل بيانات يمكن إعدادها أو تخزينها بشكل إلكتروني، وعرف كذلك بأنه معلومات يقبلها العقل والمنطق ويعتمدها العلم، يتم الحصول عليها بإجراءات علمية وقانونية، بترجمة المعلومات والبيانات المخزنة في الحاسوب وملحقاته وشبكات الاتصال ويمكن استخدامها في أي مرحلة من مراحل التحقيق والمحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة.

وكذلك عرفه الفقه بأنه الدليل الذي يتم الحصول عليه بواسطة التقنية الإلكترونية من الحاسوب وشبكة الانترنت، والأجهزة الإلكترونية الملحقة والمتصلة به، وشبكات الاتصال من خلال إجراءات قانونية، لتقديمها للقضاء كدليل إلكتروني جنائي يصلح لإثبات الجريمة [1]

[1] : قادري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، المرجع السابق، ص181.

والذي يلاحظ على هذا التعريف أنه يقصر مفهوم الدليل الرقمي على ذلك الذي يتم استخراجه من الحاسب الآلي، ولاشك أن ذلك فيه تضييف لدائرة الأدلة الرقمية، فهي كما يمكن أن تستمد من الحاسب الآلي، فمن الممكن أن يُ تحصل عليها من أية آلة رقمية أخرى، فالهاتف و ألآت التصوير وغيرها من الأجهزة التي تعتمد التقنية الرقمية في تشغيلها يمكن أن تكون مصدرا ً للدليل الرقمي، فضلاً عن ذلك فإن هذا التعريف يخلط بين الدليل الرقمي ومسألة استخلاصه، حيث عر َّف بأنه الدليل المأخوذ من الكمبيوتر.... الخ .[1]

وهذا يعني أن الدليل الرقمي لا تثبت له هذه الصفة إلا إذا تم أخذه أو استخلاصه من مصدره، وهذا حسب رأيي المتواضع؛ إذا من شأن التسليم بذلك القول إن تلك المجالات المغناطيسية أو الكهربائية قبل فصلها عن مصدرها بواسطة الوسائل الفنية لا تصلح لأن توصف بالدليل الرقمي، أي أن مخرجات الآلة الرقمية لا تكون لها قيمة إثباتية مادامت في الوسط الافتراضي الذي نشأت فيه أو بواسطته، وهذا غير دقيق كما سنبين ذلك في محله، وهو ما يصم هذا التعريف بالقصور لكونه لا يعطى تعريفاً جامعاً للدليل الرقمي .[2]

الفرع الثاني: أشكال الدليل الإلكتروني

ليس للدليل الرقمي صورة واحدة بل يوجد له العديد من الصور والأشكال نذكر منها على سبيل المثال: [3]

1- الصورة الرقمية:

[1] : صغير يوسف، الجريمة المرتكبة عبر الانترنت، رسالة ماجستير ، جامعة مولود معمري ، تيزي وزو ، كلية الحقوق والعلوم السياسية ، 2013، ص87.

[2] : المرجع نفسه، ص88.

[3] : محمد الأمين البشري، التحقيق في الجرائم المستحدثة، الطبعة الأولى، دار الجامعة ، عمان، 2015، ص117.

هي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفي العادة تقدم الصورة في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية والصورة الرقمية تمثل تكنولوجيا بديل للصورة التقليدية".[1]

2- النصوص المكتوبة:

وتشمل الأوراق التحضيرية التي يتم إ عدادها بخط اليد كمسودة أو تصور العملية التي يتم برمجتها، وكذلك نصوص أساسية وقانونية محفوظة في الملفات العادية وتكون لها علاقة بالجريمة.

3- التسجيلات الصوتية:

وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية، وتشمل المحادثات

الصوتية على الأنترنت.[2]

[1] : المرجع نفسه، ص118.

[2] : محمد الأمين البشري، التحقيق في الجرائم المستحدثة، المرجع السابق، ص119.

خلاصة الفصل:

الجريمة الإلكترونية لا حدود جغرافية لها هذا ما يكسبها طابعا دوليا ،وتعد هذه السمة نقطة هامة تستحق الوقوف عندها وبحثها باستفاضة باعتبار جرائم المعلوماتية جرائم عابرة للحدود، وترجع تسميتها بالعاملين إلى مزاولة الأنشطة الإجرامية فيها على مستوى عالمي وعبر الدول حول الحدود، نتيجة للتقدم المذهل في وسائل الاتصالات والمواصلات، فهذا النوع من الإجرامية أصبح ظاهرة تؤرق العديد من دول العالم لما لها من آثار خطيرة على وضع ومكانة هذه الدول، وتعتبر من المواضيع الحديثة والخطيرة التي تشغل اهتمامات رجال القانون والفقهاء.

الفصل الثاني

آليات حماية الجريمة الإلكترونية في التشريع الجزائري

تمهيد:

إن الحديث عن الجرائم الناشئة عن الاستخدام غير المشروع للكمبيوتر كأداة لارتكاب الأفعال غير المشروعة وشبكة الانترنت المرتبطة به التي ساهمت إلى حد كبير إلى انتشار الجريمة بمختلف أشكالها لنذهب بالقول أننا أمام عولمة الجريمة، وا ٍن كان في نطاق تطبيق نصوص القانون الجنائي، إلا أنه يجب أن نعترف أننا بصدد ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي، سواء من حيث محل الجريمة أو أسباب ارتكابها أوصفات المجرم المعلوماتي فالجريمة هنا جريمة معلوماتية تتعلق بالتقنية المعتمدة على المعالجة الالكترونية للمعلومات والبيانات وقبل الدخول في الحديث عن مختلف الإشكالات التي ثارت في خصوص هذا الموضوع من خلال إخضاعها لقانون العقوبات وبعض القوانين التقليدية والخاصة.

المبحث الأول: إجراءات الحماية الموضوعية

لابد من الاعتراف أن الإسهام في اقتراح حلول للإشكالات التي يطرحها موضوع الحماية الجزائية للإلكترونية مهمة تعترضها صعوبة منهجية كبرى مصدرها اتساع وتشعب الجوانب التي تتعلق بالإلكترونية ، لذلك سوف نتعرض في هذا المبحث للحماية الجزائية للإلكترونية من جانبه الموضوعي، من خلال قانون العقوبات ونصوص الملكية الفكرية والصناعية باعتبار المعلوماتية نتاج فكروا إبداع.

المطلب الأول: الحماية في قانون العقوبات وقانون الملكية الفكرية

الفرع الأول: الحماية في قانون العقوبات

أولا: جريمة المساس بأنظمة المعالجة الآلية للمعطيات

جريمة المساس بأنظمة المعالجة الآلية للمعطيات أو جريمة الغش المعلوماتي وهو الفعل المنصوص والمعاقب عليه في المواد[1]394 مكرر إلى المادة394مكرر7ونجد أن المشرع الجزائري لم يعرف لنا نظام المعالجة الآلية للمعطيات، بالرجوع إلى الاتفاقية الدولية الخاصة بالإجرام المعلوماتي قدمت تعريفا للنظام المعلوماتي في مادتها الثانية[1].

وبالعودة إلى قانون العقوبات الجزائري، نجد أن الغش المعلوماتي يأخذ صورتين أساسيتان وهما:

- الدخول في منظومة معلوماتية
- المساس بمنظومة معلوماتية
- صور أخرى من الغش المعلوماتي.

[1] : المواد394 مكرر إلى المادة394مكرر7 من قانون العقوبات المعدل والمتمم بالقانون09/01 المؤرخ في26 يونيو 2001.

أ- الدخول في منظومة معلوماتية.

ويشمل فعلين هما: الدخول والبقاء.

1_جريمة الدخول غير المشروع

تنص المادة394 مكرر من قانون العقوبات الجزائري والتي تقابلها المادة1/323 قانون عقوبات فرنسي على معاقبة كل من يدخل عن طريق الغش في كل جزء.

2_جريمة البقاء غير المشروع:

نص المشرع الجزائري على هذه الجريمة في المادة394مكرر من قانون العقوبات الجزائري ويقصد بالبقاء الدخول الشرعي أكثر من الوقت المحدد وذلك بغية عدم أتاء إتاوة، وتقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل بعد،كما يجرم البقاء حتى ولو تم بصفة عرضية.[1]

ب- المساس بمنظومة معلوماتية.

تنص المادة394 مكرر1 قانون العقوبات الجزائري ن "كل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".[2]

- **صور أخرى للغش المعلوماتي:**

جاء نص المادة 394 مكرر 2من قانون العقوبات الجزائري بتجريم الأعمال التالية:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي السالفة الذكر.

[1]: أحسن بوسقيعة، الوجيز في القانون الجزائي،الطبعة6، دار هومة، الجزائر، ص445.

[2]: مرزوق نسيمة، جرائم الانترنت مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر ،2006_2009، ص10.

- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى جرائم الغش المعلوماتي.

كما نصت المادة 6 من اتفاقية بودابست على جريمة الاستخدام غير المشروع للمعطيات على معاقبة كل من يقوم عمدا بإنتاج أو استعمال أو استيراد أو توزيع برنامج حاسوب بغرض ارتكاب أو كلمة سر أو رمز وصول أو بيانات مماثلة بغرض ارتكاب الجرائم المنصوص عليها في المواد2 إلى5، ولا يشترط اجتماع تلك الجرائم بل يكفي توافر إحدى تلك الجرائم. [1]

ثانيا: جريمة التزوير المعلوماتي

إن التعديل أو التغيير الذي يقع على المعطيات أو البرامج من شأنه أن يشكل جريمة تزوير والتي تقوم على تغيير الحقيقة بقصد الغش تغييرا يترتب عليه إلحاق الضرر بالغير، ويلاحظ أن المشرع الفرنسي بعد تعديل قانون العقوبات لسنة1988 وصدور قانون العقوبات لسنة1994 عدل المادة1/441لكي تستوعب بجانب التزوير العادي جريمة التزوير المعلوماتي، حيث نصت بعد تعديلها على :

"إن كل تغيير للحقيقة بطريق الغش ....في محرر مكتوب أو في أي دعامة أخرى تحتوي تعبير عن الفكر"، فالمشرع فصل بذلك بين التزوير في البيانات المسجلة في ذاكرة الكمبيوتر وبين التزوير في محررات نظام المعالجة الآلية للمعلومات، حيث أفرد نص خاص، للصورة الأولى بينما احتوى الصورة الثانية في النص العام لجريمة التزوير.[2]

وقد تناولت المادة7 من اتفاقية بودابست جريمة التزوير المتصلة بالحاسوب واعتبرت أن الواقعـــة تعتبر تزويرا إذا تضمنت خلق أو تعديل لبيانات أو برامج غير مرخص بإنشائها أو تعديلها، حـــيث تصبح لها قيمة مختلفة في الإثبات فيما يتعلق

[1]: قربوز حليمة ،الجريمة المعلوماتية في التشريع الجزائري والقانون المقارن، مرجع سبق ذكره، ص 62.

[2]: المرجع نفسه، ص63.

بالمعاملات القانونية التي تقوم على الثقة في المعلومات القائمة على تلك البيانات التي تعرضت للتزوير.

ونجد المشرع الجزائري لم ينص عن التزوير المعلوماتي لذلك سنتطرق إلى تحديد جريمة التزوير المعلوماتي(الفقرة الأولى) وموقف المشرع الجزائري من التزوير المعلوماتي(الفقرة الثانـــــية).[1]

إن موضوع التزوير هو المحرر، الذي لا بد من توافر شروط فيه، تتمثل في الكتابة من قبل شخص وأن ينتج أثاره القانونية هذه من الناحية التقليدية لجريمة التزوير، لكن في مجال المعلوماتية فالأمر يختلف فجريمة التزوير المعلوماتي تقع على المستندات المعلوماتية.

كما أن الغاية من تجريم أفعال التزوير هو حماية الثقة العامة، التي تنشأ من تعامل الأفراد بالمحررات بمفهومها التقليدي، ووضع نص خاص بالتزوير المعلوماتي يحقق الحماية للنظام المعلوماتي فقط دون الحفاظ على الثقة العامة، وبذلك فإن المحررات المعلوماتية تخرج من المفهوم التقليدي للمحرر مما ينقص من ثقة المتعاملين بها، لذلك فإن إلغاء النص يخضع المحررات المعلوماتية إلى النصوص التقليدية الخاصة بالتزوير، بالمفهوم الجديد للمحررات. [2]

إن النشاط الإجرامي المكون لجريمة التزوير المعلوماتي يتمثل في فعل تغيير الحقيقة ويعني استبدالها بما يخالفها وا ٍذا انتفى هذا التغيير انتفى التزوير وا ٍن تحوير البرنامج أو قواعد البيانات لا يعد تزويرا بل يقع تحت طائلة نصوص قانون حقوق المؤلف والحقوق المجاورة.[3]

---

[1]: نهلة القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الثانية، 2009، ص 37.

[2]: سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجيستير، جامعة الحاج لخضر، باتنة، 2013، ص 55.

[3]: نهلة القادر المومني، الجرائم المعلوماتية، مرجع سبق ذكره، ص 38.

إن قانون العقوبات الجزائري لم يستحدث نصا خاصا بالتزوير المعلوماتي، الذي يعتبر من اخطر صور الغش المعلوماتي نظرا للدور الهام والخطير الذي أصبح يقوم به الحاسوب الآن.

ونجد أن المشرع الجزائري نص على التزوير الخاص بالمحررات في القسم الثالث والرابع والخامس من الفصل السابع من الباب الأول من الكتاب الثالث من قانون العقوبات في المواد214الى229التي تشترط المحرر لتطبيق جريمة التزوير، ولم يتخذ أي موقف لتوسيع مفهوم المحرر من اجل إدماج المستندات المعلوماتية ضمن المحررات محل جريمة التزوير. [1]

الفرع الثاني: الحماية في نصوص الملكية الفكرية

أولا:الاعتداءات الواردة على برامج الكمبيوتر

حماية لحقوق المؤلف لم تخلو اغلب التشريعات الخاصة بحماية حق المؤلف من نصوص تجــريم الاعتداء على حق المؤلف، ومن تلك التشريعات التشريع الجزائري الذي جرم الاعتداء على حقوق المؤلف بما فيها حقوق مؤلفي البرامج، وذلك في المواد155،154،151،من الأمر05/03 المتعلق بحقوق المؤلف والحقوق المجاورة، أما المشرع الفرنسي فنص عليها في المادة02/335 من الأمر657/01 المتعلق بحقوق المؤلف والحقوق المجاورة، أما المشرع المصري فنص عليها في نص المادة 47من القانون38/92.

وأما بالنسبة للاتفاقيات الدولية كاتفاقية برن لعام 1979 فإنها أقرت مبادئ وأسس تحكم الجانب الجزائي للمساس بحق المؤلف، ولم تجرم بصفة صريحة تصرفات معينة لتترك أمر تحديد جرائم الاعتداء على حقوق المؤلف إلى التشريعات الداخلية للدول.

[1] : سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سبق ذكره، ص57.

ويلاحظ أن المشرع أدخل جميع جرائم الاعتداء على حقوق المؤلف بما فيهم مؤلفي البرامج تحت وصف جنحة التقليد وا ٍن كان لا يصدق عليها جميعها ذلك الوصف.[1]

ثانيا: الجزاءات المقررة لجرائم الاعتداء على برامج الكمبيوتر

لقد قرر المشرع الجزائري بموجب المواد:159،158،157،156،153من الأمر 05/03المتعلق بحقوق المؤلف والحقوق المجاورة الجزاءات المقررة على كل من يعتدي على حقوق المؤلف.

غير أن الشروع أو المحاولة الذي يمكن تصوره بالنسبة لهذه الجرائم غير معاقب عليه بنص خاص، لان العقوبة المقررة لهذه الجرائم عقوبة جنحة والقاعدة تقضي بأن لا يعاقب على الشروع في الجنح إلا بنص خاص. [2]

1_العقوبات الأصلية

حدد المشرع الجزائري في المادة153من الأمر05/03 عقوبة تتمثل في الحبس من 3اشهر إلى3سنوات وغرامة من 000.500دج إلى1.000.000دج سواء كان النشر قد حصل في الجزائر أو خارجها.

2_ العقوبات التكميلية وتدابير الأمن

تتمثل العقوبات التكميلية في التشريع الجزائري في المصادرة ونشر الحكم حيث نص على المصادرة في المادة157من الأمر05/03 التي نصت على انه تقرر الجهة القضائية المختصة مصادرة المبالغ التي تساوي مبلغ الإيرادات أو أقساط الإيرادات الناتجة عن الاستغلال غير الشرعي للمصنف ومصادرة العتاد المخصص لمباشرة النشاط أو المشروع والنسخ.

---

[1]: أسامة أمحمد المناعسة، جلال محمد الزغبي، جرائم الحاسب الآلي ، دار وائل للنشر،الأردن،2004،ص44.

[2] : المرجع نفسه، ص45.

أما عن عقوبة نشر الحكم فنص عليها المشرع الجزائري في المادة158من الأمر رقم05/03 والتي تقضي أنه يمكن للجهة القاضية المختصة بطلب من الطرف المدني، أن تأمر بنشر أحكام الإدانة كاملة أو مجزئة في الصحف التي تعينها وتعليق هذه الأحكام في الأماكن التي تحددها ومن ضمن ذلك على باب المسكن الخاص بالمحكوم عليه وكل مؤسسة أو قاعة حفلات يملكها على أن يكون ذلك على نفقة هذا الأخير شريطة أن لا تتعدى هذه المصاريف الغرامة المحكوم بها.

ويقصد بهذه العقوبة التشهير بالمحكوم عليه والتأثير على شخصيته الأدبية والمالية، وهي بذلك عقوبة ماسة بشرف الاعتبار.[1]

إن قانون الملكية الفكرية يشمل عدة مجالات منها: العلامات التجارية براءة الاختراع، الرسوم والنماذج، تسمية المنشأ، وما يهمنا بصدد حماية برامج الكمبيوتر هو حمايتها من خلال براءة الاختراع. [2]

أولا: الشروط الواجب توافرها في براءة الاختراع

بصدور الأمر 07/03 المؤرخ في: 2003[3]/07/19 المتضمن براءة الاختراع وبالعودة إلى نصوصه نجد المادة الثانية منه عرفت الاختراع بأنه:»فكرة المخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية«، وبشأن الشروط الواجب توافرها في الاختراع كي تطبق عليه أحكام المادة الثالثة من ذات الأمر التي تنص على ما يلي: "يمكن إن تقع تحت براءة الاختراع الجديدة الناتجة عن نشاط الاختراعي والقابلة للتطبيق صناعيا".

[1] : أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، مرجع سبق ذكره، ص75.

[2] :سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة لنيل شهادة الماجيستير في الحقوق، قانون جنائي، جامعة محمد خيضر، بسكرة، 2013، ص 51.

[3] : الأمر 07/03 المؤرخ في: 2003/07/19 المتضمن براءة الاختراع.

ثانيا/مدى تطبيق نصوص براءة الاختراع على برامج الكمبيوتر.

حسبما يراه المختصون في الميدان فأنه من الصعب توفير حماية ناجحة للبرمجيات بالرجوع إلى قانون الملكية الصناعية، ويتعلق الأمر خاصة بشرطين لابد من توفرهما في العمل الإبداعي لكي يظفر صاحبه بالبراءة:

- ✓ *الجدية.
- ✓ القابلية لاستغلال الصناعي.[1]

المبحث الثاني: إجراءات التحقيق في الجرائم الإلكترونية في التشريع الجزائري

إجراءات التحقيق الابتدائي هي مجموعة من الأعمال التي تباشرها سلطة مختصة للتحقيق في مدى صحة الاتهام الموجه من طرف النيابة العامة بشان واقعة جنائية معروضة عليها وذلك بالبحث عن الأدلة المثبتة لذلك، والتحقيق مرحلة لاحقة لإجراءات جمع الاستدلال وتسبق مرحلة المحاكمة التي تقوم بها جهة الحكم، وعليه فإن التحقيق يهدف إلى تمهيد الطريق أمام قضاء الحكم باتخاذ جميع الإجراءات الضرورية للكشف عن الحقيقة.

يهدف التحقيق الابتدائي إلى الكشف عن الحقيقة للوصول إلى هذا الغرض يلجا المحقق إلى مجموعة إجراءات بعضها يهدف للحصول على الدليل، وتسمى إجراءات جمع الدليل كالتفتيش والضبط والمعاينة والشهادة والخبرة، وبعضها الأخر يمهد للدليل ويؤدي إليه وتعرف بالإجراءات الاحتياطية ضد المتهم كالقبض والحبس المؤقت.

[1] : سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مرجع سبق ذكره، ص 52.

المطلب الأول: جمع الأدلة التقليدية للتحقيق في الجرائم الإلكترونية

الفرع الأول: التفتيش وضبط الأدلة في الجريمة الإلكترونية

أولا: التفتيش في الجريمة الإلكترونية

لقد تعددت التعريفات التي أضافها الفقه على التفتيش، إلى أنها تجتمع على أن التفتيش عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل وذلك من اجل إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات القانونية المقررة، وقد أحاط القانون التفتيش بضمانات عديدة لأنه قد يقتضي البحث في محل له حرمة خاصة.وا ٍذا كان التفتيش للأشياء المادية بما فيها المكونات المادية للحاسوب لا يثير إشكالية، فما مدى خضوع البرامج والمعلومات كمكونات معنوية للحاسوب للتفتيش؟ وما هي ضوابط تفتيش نظم الحاسوب؟[1]

1_مدى قابلية نظم الحاسوب للتفتيش:

يتكون الحاسوب من مكونات مادية ومكونات معنوية، ولا تثار أدنى صعوبة إذا كان محل جرائم الحاسوب الآلي مكونات مادية حيث ينطبق بصددها القواعد التقليدية دون صعوبة، فالواقع أن ولوج المكونات المادية للحاسوب بأوعيتها المختلفة بحثا عن شيء يتصل بجريمة معلوماتية قد وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها، وأنه يدخل في نطاق التفتيش طالما تم وفقا للإجراءات القانونية المقررة، بمعنى أن حكم تفتيش تلك المكونات يتوقف على طبيعة المكان الموجود فيه وهل هو من الأماكن العامة أو الأماكن الخاصة إذ أن لصفة المكان أهمية خاصة في مجال التفتيش.

[1] : الملتقى الوطني حول الجريمة الالكترونية، جريدة الأمة العربية، وهران 2013/02/01 .

2_ ضوابط تفتيش نظم الحاسب الآلي:

إذا كان الوصول إلى الحقيقة يمثل الغاية من الإجراءات، بيد أن تحقيق تلك الغاية لا يكون بأي ثمن، ففي كل الحالات فإن الغاية لا تبرر الوسيلة، فالبحث عن الحقيقة القضائية لا ينبغي أن يكون طليقا من كل قيد، بل إن ذلك يخضع لضوابط معينة، ومن هذا المنطلق يجب أن يخضع التفتيش لضوابط يمكن تقسيمها إلى ضوابط موضوعية وضوابط شكلية.

ثانيا: ضبط الأدلة في الجريمة الإلكترونية

هو ضبط الأدلة أو الأشياء التي تفيد في ظهور الحقيقة في الجريمة التي وقعت، فالضبط إن لم يكن في اغلب الأحيان هو غرض التفتيش وله السبب الوحيد، فقد يتم الضبط استنادا لأسباب أخرى غير التفتيش من ذلك المعاينة، وما يقدم المتهم والشهود لمأموري الضبط القضائي، لذا يرى جانب من الفقه أن الضبط ليس من إجراءات التحري بل من إجراءات الاستدلال خاصة إذا تم في مكان يجوز لسلطات الضبط دخوله مثل الأشياء التي يتم العثور عليها خارج المساكن أو في الطريق العام أو في الحقول أو غيرها.[1]

والضبط لا يخرج من كونه وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، سواء في ذلك أن يكون هذا الشيء عقارا أو منقولا الضبط حسب الأصل لا يراد إلا على أشياء مادية فلا صعوبة بالتالي بضبط الأدلة في الجريمة الواقعة على المكونات المادية للكومبيوتر، كرفع البصمات مثلا عنها وكذلك لا صعوبة أيضا في ضبط الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في نسخة غير مشروع أو إتلافه بوسائل تقليدية كالكسر، الحرق، ل كن تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف البرامج مثل الفيروس وفي ضبط البيانات الكمبيوتر

[1] : سميرة معاشي، ماهية الجريمة الالكترونية ..مجلة المنتدى القانوني، العدد السابع جامعة بسكرة، 2012، ص311.

لعدم وجود أي دليل مرئي في هذه الحالات، ولسهولة تدمير الدليل في ثواني معدودات ولعدم معرفة كلمة السر أو ثغرات المرور أو ترميز البيانات.[1]

الفرع الثاني: المعاينة وندب الخبراء في الجريمة الإلكترونية

أولا: المعاينة في الجريمة الإلكترونية

ولقد أشارت قوانين الإجراءات الجنائية إلى إجراء المعاينة باعتباره إجراء من نص إجراءات التي تمتلكها السلطات التحقيقية بمختلف فئاتها وطوائفها، وهذا ما ورد في المادة 79 من قانون الإجراءات الجزائية الجزائري [2]" يجوز لقاضي التحقيق الانتقال إلى 5 أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها المعاينة هي إثبات حالة الأماكن والأشياء والأشخاص وكل ما يعتبر في كشف الحقيقة فهي بهذا المعنى تستلزم الانتقال إلى محل الواقعة أو أي محل آخر توجد به آثار يرى المحقق أن لها صلة بالجريمة والأصل أن إجراء المعاينة متروك لتقدير المحقق لا يقوم بها إلا إذا كان هناك فائدة من ورائها، كما أن هناك حالات يوجب فيها القانون على النيابة الانتقال فورا إلى مسرح الجريمة وهي حالة إخطارها بجناية متلبس به[3]".....

يرى البعض أن أهمية المعاينة تتضاءل في الجريمة الإلكترونية وذلك لندرة تخلف الآثار المادية عند ارتكاب الجريمة الإلكترونية، كما أن طول الفترة بين وقوع الجريمة أو ارتكابها وبين اكتشافها يكون له التأثير السلبي على الآثار الناجمة عنها بسبب العبث أو المحو أو التلف لتلك الآثار، فعند تلقي بلاغ عن وقوع إحدى الجرائم الإلكترونية وهذا بعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته.

ومسرح الجريمة الإلكترونية يختلف عن مسرح الجريمة التقليدية كالقتل والسرقة فالجريمة الإلكترونية قد تكون جريمة مستمرة كما في حالة الجرائم الاقتصادية – السرقة

---

[1] : المرجع نفسه، ص312.

[2] : المادة 79 من الأمر رقم 66-155المؤر خ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية.

[3] : نهلا عبد القادر المومني،الجرائم المعلوماتية ، دار الثقافة،الأردن،ط1 ، 2008.، ص143.

والاحتيال وقد يكون مسرحها كالجرائم الأخرى كما في التزوير وا ٍتلاف البرامج وتفجير المباني والمنشآت، ففي حالة الجريمة المستمرة ذات الأهداف الاقتصادية تكون المعاينة هدفها المداهمة وضبط الأدلة على الطبيعة، وفي الحالة الثانية وبعد وقوع الجريمة فالأمر متوقف على اعترافات المتهمين متى تم القبض عليهم وكذلك شهادة الشهود والقرائن، وعند إجراء المعاينة بعد وقوع الجريمة في المجال الإلكتروني فيجب مراعاة الإجراءات التالية عند الانتقال إلى مسرح الجريمة [1]:

ضرورة وجود معلومات مسبقة عن مكان الجريمة، من حيث الأجهزة المطلوب معاينتها وشبكاتها مع وجود خريطة تبين الموقع المراد معاينته، تحديد الأجهزة المحتمل تورطها في الجريمة الإلكترونية حتى يتم تحديد كيفية التعامل معها فنيا قبل المعاينة، سواء من الضبط أو التأمين أو حفظ الأوراق، كما يجب على القائمين بالمعاينة، تأمين الأجهزة والمعدات التي يتم الاستعانة بها خلال إجراء المعاينة، وبما أن الجريمة الإلكترونية تعتمد على التقنية الحديثة فيجب إعداد فريق من الخبراء مختص في مجال التقنية الحديثة، وا ٍخطاره مسبقا حتى يستعد من الناحية الفنية والعملية ويعد خطة مناسبة للمعاينة، وأكيد قبل كل شيء يجب مراعاة ما جاء في القوانين الجنائية حول المعاينة وذلك تحقيقا لمبدأ 2الشرعية.[2]

ثانيا: ندب الخبراء في الجريمة لإلكترونية

الخبرة هي الوسيلة لتحديد التفسير الفني للأدلة أو الدلائل بالاستعانة بالمعلومات، فهي في الحقيقة ليست دليلا مستقلا عن القولي أو الدليل المادي، إنما هي تقييم فني لهذا الدليل والعنصر المميز للخبرة عن غيرها من إجراءات الإثبات كالمعاينة، الشهادة والتفتيش.

[1] :نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنيت،دار الفكر الجامعي الإسكندرية، .،2007ط1، ص49.

[2] : نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنيت، المرجع السابق، ص50.

من المعلوم أن هناك حاجة دائمة إلى خبراء وفنيين عند وقوع الجريمة الإلكترونية ويمتد عملهم ليشمل المراجعة والتدقيق على العمليات الآلية للبيانات، وكذلك إعداد البرمجيات وتشغيل الحاسب الآلي وعلومه، وان نجاح الاستدلالات وأعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة وتخص هؤلاء الخبراء، وكذا يجب على المحقق الجنائي أن يحدد للخبير الإلكتروني دوره في المسالة الانتداب فيها على وجه الدقة، وبالنظر إلى أن الجريمة الإلكترونية لها الخصوصية التي تتعلق بها فإن الخبير الإلكتروني قد يكون من الجناة الذين سبق لهم ارتكاب مثل هذه الجرائم وتم تذويبهم داخل المؤسسات الإلكترونية للاستفادة من قدراتهم فضلا عن تأهيلهم كمواطنين صالحين[1] .

المطلب الثاني: جمع الأدلة المستحدثة للتحقيق في الجرائم الإلكترونية

الفرع الأول: حجية الدليل المستحدث في الكشف عن الجريمة الإلكترونية

تعرف المادة 65 مكرر 12 من القانون الإجراءات الجزائية الجزائري[2] التسرب على :انه "قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية مراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم انه فاعل انطلاقا من هذا التعريف، يتبين أن التسرب عملية معقدة جدا تتطلب معهم أو شريك أو خاف"أحيانا من العون أو ضابط الشرطة القضائية المساهمة المباشرة في نشاط الخلية الإجرامية التي تم التسرب إليها وارتكاب أفعال محظورة قصد تحقيق الهدف النهائي من العملية، بل أحيانا يكون القيام بتلك الأفعال ضرورة لقبوله في الخلية

لذلك اعتبار لهذه الضرورة تفطن المشرع الجزائري وجرد الضابط أو العون المتسرب من المسؤولية الجنائية عن كافة الأفعال غير المشروعة التي قد يقدم على ارتكابها أثناء عملية التسرب.

[1] :نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنيت، المرجع السابق، ص51.

[2]: المادة 65 مكرر 12 من الأمر رقم 66-155 المؤرخ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية.

ليس هذا فحسب، بل أحاط المشرع المسرب كذلك بعدة ضمانات من أجل حمايته وحماية أسرته أثناء عملية التسرب وبعد انقضائها، منها ما ورد في المادة 65 مكرر 16[1] من قانون الإجراءات الجزائية بأنه" لا يجوز إظهار الهوية الحقيقية لضابط أو أعوان الشرطة القضائية الذين يباشرون عملية التسرب تحت هوية مستعارة في أية مرحلة من مراحل الإجراء " .

وما تضمنته كذلك المادة 65 مكرر 17 من[2] القانون نفسه بأنه " إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في الرخصة للتسرب، وفي حالة عدم تمديدها، يمكن العون المتسرب واصلة النشاطات المذكورة في المادة 65 مكرر14[3] أعلاه للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسئولا جزائية، على لا أن يتجاوز ذلك 4 أشهر. "

وعلى هدى ذلك، لا يجوز اللجوء لعملية التسرب إلا في بعض الجرائم البالغة الخطورة والتي حددها المشرع الجزائري على سبيل الحصر في المادة 65[4] مكرر وهي جرائم : المخدرات الجريمة المنظمة العابرة للحدود جرائم، تبييض الأموال و جرائم التخريب والإرهاب، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

ويمكن تصور عملية التسرب في جرائم الفضاء الرقمي في ولوج ضابط أو عون الشرطة القضائية إلى العالم الافتراضي ومشاركته في محادثات غرف الدردشة أو حلقات النقاش المباشر حول تقنيات اختراق شبكات الاتصال أو بث الفيروسات أو أنه طهرا في مجموعات أو نوادي الهاكر، فيها بمظهر طبيعي كما لو كان واحد مستخدما

[1]: المادة 65 مكرر 16 من الأمر رقم 66-155 المؤرخ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية.
[2]: المادة 65 مكرر 17 من الأمر رقم 66-155 المؤرخ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية.
[3]: المادة 65 مكرر 14 من الأمر رقم 66-155 المؤرخ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية.
[4]: المادة 65 مكرر من الأمر رقم 66-155 المؤرخ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية.

في ذلك أسماء وصفات مستعارة وهمية ظاهرا مثلهم قصد إستدارجهم والكشف عنهم وعن أعمالهم الإجرامية.[1]

نظرا المشرع بجملة من الشروط والضوابط الواجب مراعاتها قبل وأثناء مباشرته وهي كالتالي:[2]

أولا-**الضوابط الإجرائية**: تتلخص الضوابط الإجرائية للتسرب الالكتروني في الإذن القضائي وكل ما يجب أن يتضمنه من أحكام، لا إذ يجوز للضابط أو عون الشرطة القضائية الغوص في عملية التسرب من تلقاء نفسه دون الحصول على إذن مسبق من طرف الجهات القضائية المختصة والمتمثلة حسب أحكام المادة 65 مكرر 11 ق، إ، ج[3] في وكيل الجمهورية قبل افتتاح التحقيق أو قاضي التحقيق بعد افتتاحه على أن تتم العملية تحت الرقابة المباشرة للجهة الصادرة للإذن حسب الحالة لت فادي حدوث تجاوزات وتعسفات في استعمال هذا الحق .

ولا يكفي أن يصدر الإذن بالتسرب من الجهة المختصة فحسب، بل لابد أن يكون مكتوبا وا ٍن كان هذا الإجراء باطلا، لأن الأصل في العمل الإجرائي الكتابة، وهو ما أكدته المادة 65 مكرر 15 ق، إ، ج[4] بنصها " يجب أن يكون الإذن المسلم طبقا تحت طائلة البطلان."

كما يشترط أن يتضمن الإذن بالتسرب جملة من البيانات التي يتوقف على تحديدها صحة الإجراء ذاته، كذكر نوع الجريمة محل عملية التسرب واسم ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، وتحديد المدة المطلوبة لهذه العملية، والتي يجب ألا تتجاوز أربعة أشهر قابلة للتجديد حسب مقتضيات التحري

[1]:بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، مرجع سبق ذكره، ص92.

[2]: المرجع نفسه، ص93.

[3]: المادة 65 مكرر 11 من الأمر رقم 66-155 المؤرخ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية.

[4]: المادة 65 مكرر 15 من الأمر رقم 66-155 المؤرخ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية.

والتحقيق ضمن الشروط نفسها، وفي الوقت ذاته يجوز للقاضي الذي أذن بهذا الإجراء أن يأمر بوقفه في أي حين قبل انقضاء الآجال المحددة.[1]

ثانيا-الضوابط الموضوعية :إلى جانب الضوابط الإجرائية المذكورة أعلاه أحاط المشرع عملية التسرب بضوابط أخرى موضوعية يمكن إيجازها في عنصرين أساسين :هما

-**العنصر الأول** : هو عنصر التسبيب، تضمنته المادة 65 مكرر 15 ق، إ، ج، ويتمثل في المبررات والحجج التي أقنعت الجهات القضائية المختصة لمنح الإذن بإجراء التسرب،وكذا الدوافع والأسباب التي جعلت ضابط الشرطة القضائية يلجأ إلى هذه العملية المتمثلة عادة في ضرورة التحقيق والتي تكون ضمن موضوع طلبه الإذن.

- **أما العنصر الثاني**: فيتعلق بتحديد نوع الجريمة التي ينصب عليها الإذن بالتسرب والتي يجب 65 مكرر5على سبيل الحصر، و ألا تخرج عن نطاق الجرائم السبع التي حددتها المادة إليها أعلاه.

ثانيا: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

قد عرف المشرع الجزائري الاعتراض بالتفصيل في المادة 65 مكرر5 من قانون الإجراءات الجزائية[2]، إذ اعتبر عملية مراقبة المراسلات بأنها " اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهذه المراسلات عبارة عن بيانات قابلة للانتاج والتوزيع، التخزين، الاستقبال والعرض ".

نلاحظ أن المشرع الجزائري حدد المراسلات التي تصلح أن تكون محلا للاعتراض بتلك المراسلات التي تتم بواسطة وسائل الاتصال السلكية واللاسلكية دون أن يشير إلى طبيعة هذه المراسلات، مما يفتح المجال لمختلف الرسائل المكتوبة، بغض النظر عن شكلها (كتابة، رموز، أشكال، صور أو) الدعامة التي تنصب عليها (ورقية

[1]:بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، مرجع سبق ذكره، ص94.

[2]: المادة 65 مكرر 5 من الأمر رقم 66-155 المؤرخ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية.

أو رقمية أو ،) الوسيلة المستعملة لإرسالها سلكية كانت (كالفكس أو تليغرام)، أم لاسلكية(البريد الالكتروني، الهاتف النقال ،) باستثناء الكتب والمجلات والرسائل والحوليات .[1]

و التي تعد مراسلات خاصة، وهذا ما أكدته المادة 02 فقرة " 6 من القانون رقم04 - 09[2] التي عرفت الاتصالات الالكترونية بأنها " أو سل إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أية وسيلة وبغض الكترونية "النظر عن طبيعة المراسلات السلكية واللاسلكية فعملية الاعتراض أو المراقبة تتم بواسطة ترتيبات تقنية سرية يتم وضعها دون أو علم موافقة المعنيين، وذلك لغرض التصنت، والتقاط وتثبيت وبث وتسجيل البيانات المرسلة أو المحادثات التي أجراها المشتبه فيه بصفة خاصة أو سرية في أماكن خاصة أو عمومية، ومن ثم استعمالها كدليل المواجهة المتهم.

ولعل من أهم المراسلات الالكترونية التي يهتم القائمين بالتحقيق بإخضاعها لعملية الاعتراض غنيا لأدلة إثبات جرائم الفضاء الرقمي، المراسلات عبر البريد والمراقبة والتي تمثل المصدر الالكتروني، كون هذه التقنية من أكثر الوسائل الحديثة استخداما للاتصال عبر الانترنت ومجالا خصبا للربط بين الأشخاص في مختلف أنحاء العالم بسرعة فائقة ودون حواجز.[3]

فهو بمثابة نظام تبادل الرسائل والصور وغيرها من المواد القابلة للإدخال الرقمي في صندوق الرسالة، أو القابلة للتحميل الرقمي بصفتها ملحقات بالرسالة، كما يستخدم

---

[1]:بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، مرجع سبق ذكره، ص95.

[2]:المادة 02 الفقرة 06 من القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3]: محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مرجع سبق ذكره، ص23.

كمستودع لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقميا في صندوق خاص وشخصي المستخدم، ولا يمكن الدخول إليه بسهولة لأنه محاط بحماي فنية.[1]

ثالثا: الحفظ و الإفشاء العاجلان للمعطيات المتعلقة بالسير

يعد الحفظ والإفشاء العاجلان للمعطيات المعلوماتية من الإجراءات المستحدثة و الوقائية التي بما ارتأت له أغلبية الدول فرضت بموجب القانون على مزودي خدمة الانترنت و هذا استنشادا الغربية لمتابعة الجريمة الإلكترونية و توقيع العقاب على الجاني، واسترشادا بذلك تضمن القانون الجزائري رقم04 -09[2] الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وبالتحديد في المادة (10) عددا من الالتزامات تفرض على مزودي خدمات الانترنت بتقديم المساعدة بخصوص العمليات التي ينجزونها للسلطات المكلفة بالبحث والاستدلال لأغراض التحقيق من بينها :حفظ المعطيات المعلوماتية المتعلقة بالسير ووضعها تحت تصرف القائمين بعملية التحقيق.

1. مفهوم الحفظ العاجل لمعطيات السير:

اعتماد على ما سبق ذكره يمكن اعتبار الحفظ على المعطيات الالكترونية بأنه قيام مزودي خدمات الاتصال بتجميع المعطيات المعلوماتية التي تسمح بالتعرف على مستعملي الخدمة وحفظها وحيازتها في أرشيف، وذلك بوضعها في ترتيب معين

[1]: 25 مارس 2017، طرابلس .

[2]: المادة 10 من القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

والاحتفاظ بها في المستقبل قصد تمكين جهات الاستدلال من الاستفادة منها واستعمالها لأغراض التحري و التحقيق .[1]

فعملية الحفظ إذا هي من مهام مقدمي الخدمات، الغرض منها حماية المعطيات التي سبق وجودها في شكل مخزن من ما كل يمكن أن يتسبب في إتلافها أو تجريدها من صفتها أو حالتها الأصلية، ولا تهم الطريقة التي يتم من خلالها الحفظ على المعطيات الالكترونية ولا الوسيلة القانونية المقررة لذلك، فالأمر متروك لكل دولة لتقدير النماذج التي رأتها ملائمة لوضع عملية الحفظ موضع التنفيذ، وينبغي التنويه في هذا الإطار إلى أن عملية الحفظ لا هنا تخص كل المعطيات الالكترونية بمختلف نماذجها، إنما تخص معطيات المرور فقط أو كما يسميها البعض حركة السير، التي عرف ها المشرع الجزائري في المادة (02)الفقرة الأخيرة من القانون رقم 04 -09[2] بأنها " أية معطيات متعلقة بالاتصالات عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الاتصالات، مصدر الاتصال، الوجهة المرسلة إليها، والطريق الذي يسلكه، ووقت و تاريخ و حجم و مدة الاتصال و نوع الخدمة".

إلا أنه بالنظر إلى نص المادة 10فقرة1من القانون04-09[3] فإن المشرع قد سمح بتسجيل المعطيات المتعلقة بمحتوى الاتصالات بشرط أن يكون في حينه ، وهو إجراء تسخير من طرف السلطات القضائية لمقدمي الخدمات المعنيين لجمع وتسجيل المعطيات المتعلق بمحتوى اتصالات أيا كانت (محادثات هاتفية أو مكالمات فيديو عبر مواقع الانترنت أو مراسلات كتابية على شكل SMS-MMS .[4]

---

[1]: قادري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مرجع سبق ذكره، ص 39.

[2]: الفقرة الأخيرة من المادة 02 من القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3]: الفقرة الأولى من المادة 10 من القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[4]: قادري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مرجع سبق ذكره، ص 40.

ومن ضمن معطيات المرور التي يتعين على مقدمي الخدمات التحفظ عليها بطلب من السلطات القضائية المختصة لأغراض التحقيق، تلك التي حددها المشرع الجزائري في المادة11من القانون04-09على النحو التالي:[1]

_المعطيات التي تسمح بالتعرف على مستعملي الخدمة

_المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال (كرقم التسلسلي لجهاز الاتصال و نوعه).

_الخصائص التقنية وكذا تاريخ و وقت و مدة الاتصال .

_المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها .

_المعطيات التي تسمح بالتعرف على المرسل والمرسل إليهم (كأرقام الهاتف مثلا أو عناوين بروتوكول الانترنت ، تحديد مكانهم)...

وا ٍذا كان تحديد معطيات المرور قد يبدو أمرا سهلا عندما تكون تلك المعطيات مرتبطة بمقدم خدمة واحد، فالأمر غير ذلك عندما ترتبط بأكثر من مقدم خدمة، فغالبا ما يساهم عدد من مقدمي خدمات في نقل اتصال معين، ويحتفظ كل واحد منهم بجزء من معطيات المرور أو بعض أجزاء اللغز، مما يجعل تحديد مصدر هذا الاتصال ومنتهاه أم لا وهذه الأجزاء ضمها بعضها إلى البعض و اختبارها.

لذلك عندما ترتبط معطيات المرور بأكثر من مقدم خدمة فالحفظ العاجل لهذه المعطيات يتم من خلالهم جميعا، سواء بناء على أمر منفصل لكل مقدم خدمة على انفراد أمر واحد يشملهم جميعا يتم إخطارهم به بالتعاقب، أو بناء على أمر يضم كل

[1]: المادة 11 من القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

مقدمي الخدمات، ثم يطلب من كل مقدمي خدمة يصله الأمر بالحفظ، أن يقوم بإخطار من يليه بفحوى هذا الأمر.[1]

2. الإفشاء العاجل لمعطيات السير:

يعد هذا الإجراء من الالتزامات المترتبة على مقدمي خدمات الانترنت في إطار مساعدة السلطات المكلفة بالبحث والتحقيق في جرائم الفضاء الرقمي، فهي عملية مكملة لإجراء الحفظ العاجل لمعطيات المرور، كما أوضح المشرع الجزائري إجـ ءرا الإفشاء العاجل لمعطيات السير لغرض التحقيق وجعله مازالت على عاتق كل مقدمي الخدمات، وذلك من خلال نصه في المادة (10) من القانون04 -09[2] على انه " :في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية ... و بوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة (11) أدناه، تحت تصرف السلطات المذكورة "...[3]

بناء على ما سبق فكما تلزم سلطة التحقيق مقدمي الخدمات بالحفظ العاجل على معطيات المرور فإنها تلزمهم بالإفشاء السريع لها، أو لمن تعينه من قبلها عن تلك المعطيات المهمة المتعلقة بالمرور ووضعها تحت تصرفهم لفحصها قبل أن يتم التلاعب بها، قصد الوصول إلى تحديد هوية كل مقدمي الخدمة الآخرين، والطريق الذي بمقتضاه تم الاتصال، وبهذه الطريقة يكون بمقدور السلطة المكلفة بالبحث

[1]: معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن، مرجع سبق ذكره، ص 135.

[2]: المادة 10 من القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3]: المادة 11 من القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

والتحري أن تكشف منبع الاتصال ومصبه، وهي المعلومات التي قد تقوده إلى معرفة هوية الأشخاص المتورطين في ارتكاب الجريمة.[1]

الفرع الثاني: صعوبات مكافحة الجريمة الإلكترونية

أولا: الصعوبات المتعلقة بعمل جهة البحث والتحقيق:

إن التحقيق في الجرائم المعلوماتية وملاحقة مرتكبيها جنائيا يتسم بالعديد من المعوقات التي يمكن أن تعرقل عملية التحقيق في بيئة رقمية قد تؤدي إلى وجود نتائج سلبية تنعكس على نفسية المحقق بفقده الثقة في نفسه وفي عمله، بالإضافة أنها تصعد من قيمة مكافحة هذا النوع من الجرائم.

- **عدم وجود تعاون دولي:**

في ظل الصراعات الحاصلة، يصعب إيجاد تعاون دولي حقيقي لمكافحة وكشف الجريمة الإلكترونية، فكما بينا سابقا قد يتم السلوك الإجرامي في بلد معين و تتحقق النتيجة في بلد أخر كقيام مجموعة من المجرمين بتشويه معلومات معينة و ليس بالضرورة أن ينتج هذا السلوك وأثاره في بلد المجرمين، فما هو محظور في الجزائر من الناحية الأخلاقية مباح في دول أخرى.[2]

والتطور السريع للجريمة والمعالجة البطيئة للحالات، ساعد المجرم المعلوماتي على الاستفادة من هذه العقبات للعبث والتخريب.

---

[1]: معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن، المرجع السابق، ص 136.

[2]: عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص218.

ثانيا: الصعوبات المتعلقة بجهات التحقيق ونقص في الخبرة

- **مشاكل متعلقة بجهاز التحقيق**

- قد تكون شخصية (معوقات تتعلق بالمحقق) مثل: التهيب من استخدام جهاز الكمبيوتر والتهيب من استخدام الانترنت، عدم الاهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية .

- صعوبات تتعلق بالنواحي الفنية كنقص المهارة المطلوبة للتحقيق في هذا النوع من الجرائم، نقص المهارة في استخدام الكمبيوتر والأنترنت، عدم توفر المعرفة بأساليب ارتكاب الجريمة الجرائم المعلوماتية.

- قلة الخبرة في مجال التحقيق في الجرائم المعلوماتية.[1]

- **نقص الخبرة**

إن صعوبة اكتشاف الجريمة بالدرجة الأولي مرده إلى نقص خبرة المحققين مما يضعنا أمام معادلة غير متكافئة طرفها أجهزة التحقيق بنقص خبرتها في مجال الكمبيوتر و الانترنت والطرف الآخر قراصنة محتلون و منحلون أخلاقيا يتمتعون بمهارات عالية يواكبون كل جديد في عالم المعلوماتية، وقد وصل بعض المجرمون المعلوماتيين الإطلاق على أنفسهم، ومن العوامل المساعدة اسم النخبة أما رجال الشرطة فقد أطلقوا عليهم اسم الضعفاء في نقص الخبرة في الجرائم المعلوماتية هي :[2]

- عدم تخصيص أموال من أجل التأهيل الجيد للمحققين و كذا حداثة الجريمة و خصوصيتها التي لم يعتد عليها رجال الشرطة، مما جعلهم قاصرين في مواجهتها.

- ضخامة المعلومات على الشبكة و انتشار أجهزة الكمبيوتر مما يصعب عملية التحقيق.

---

[1]: رشاد خلد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الاسكندرية، 2013، ص 58.

[2]: المرجع نفسه، ص 59.

- الإنترنت بيئة خصبة للسلوك الإجرامي .
- التطور السر يع للتقنية الحديثة و عدم وجود هيئات قضائية مختصة .
- وجود مواقع على الشبكة تسهل عملية إرسال البر يد الالكتروني دون الحاجة إلى ذكر البيانات و يميل الفقه الجنائي إلى القول بضرورة تنمية الخبرة و المهارات للمتخصصين لوضع مدروسةللتدر يب على التحقيق مع مراعاة خصوصية التطور التقنيالسر يع دون إهمال التعاون الدولي في مثل هذه الحالات.[1]

ثالثا: صعوبات متعلقة بطبيعة الجرائم المعلوماتية والجهة المتضررة

- صعوبات تتعلق بالدليل الرقمي

من الصعوبات المتعلقة بالدليل الرقمي:

- إخفاء الجريمة وغياب الدليل المرئي الممكن بالقراءة فهمه .
- افتقاد أكثر الآثار التقليدية .
- إعاقة الوصول إلى الدليل لإحاطته بوسائل الحماية كاستخدام كلمات السر .
- سهولة محو الدليل أو تدميره في زمن قصير جدا.
- صعوبة فهم الدليل الرقمي.

- صعوبات تتعلق بالجهة المتضررة

- عدم إدراك خطورة الجرائم المعلوماتية من قبل المسئولين بالمؤسسات تعد إحدى معو قات التحقيق.
- لأحجام عن الإبلاغ عن الأشخاص الميسورين أو صغار السن خوفا من المجتمع
- المحيط بهم وخشية الفضيحة بعد معوقا من معوقات التحقيق .
- عدم الإبلاغ عن الجرائم.[2]

[1]: رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 60.

[2]: جميل عبد الباقي الصغير ، أدلة الإثبات الجنائي و التكنولوجيا الحديثة، دار النهضة العربية، 2001 ، ص113.

خلاصة الفصل:

تبين لنا من خلال دراسة الفصل الثاني لهذا البحث قصور قواعد الإجراءات الجزائية في مواجهة الإجرام الإلكتروني كفشلها في مجال الضبط والتحري و التحقيق وتفتيش النظام المعلوماتيإستنباط الأدلة وا إثبات الجرائم الإلكترونية بالنظر الى طبيعة الدليل الذي يتحصل منها اذا قد يكون هذا الدليل غير مرئي وقد يسهل إخفاءه او تدميره وقد يكون متصل بدول أخرى فتكون هناك صعوبة للحصول عليه نظرا لتمسك كل دولة بسيادتها.

الخـــاتمـة

ومنه إذا كانت الجريمة الإلكترونية أثارت بعض المشكلات فيما يتعلق بالقانون الجنائي الموضوعي بحثا عن امكانية تطبيق نصوصه التقليدية على هذا النوع المستحدث من الجرائم مع احترام مبدأ الشرعية، والتفسير الضيق للنصوص الجنائية، فقد أثارت في نفس الوقت العديد من المشكلات في نطاق القانون الجنائي الإجرائي، حيث وضعت نصوص قانون الإجراءات الجنائية لتحكم الإجراءات المتعلقة بجرائم تقليدية، لا توجد صعوبات كبيرة في إثباتها أو لتحقيق فيها وجمع الأدلة المتعلقة بها، غير أن المشكلات الإجرائية في مجال الجرائم الإلكترونية بتعلقها في كثير من الأحيان ببيانات معالجة إلكترونيا، وكيانات غير ملموسة، وبالتالي يصعب من ناحية كشف هذه الجرائم ومن ناحية أخرى يصعب جمع الأدلة بشأنها.

- **نتائج الدراسة:**

- لا يوجد إجماع على تعريف الجريمة الإلكترونية
- تعرف الجريمة لإلكترونية على أنها: "الجريمة التي يتم ارتكابها إذا قام شخص ما بطريقة مباشرة أو غير مباشرة في استغلال الحاسوب أو تطبيقاته بعمل غير مشروع وضار للمصلحة العامة، ومصلحة الأفراد الخاصة
- الجرائم المعلوماتية لها صور متعددة بتعدد دور التقنية المعلوماتية
- تعد الجرائم الإلكترونية من الجرائم المستحدثة التي بدأت في الانتشار بشكل واسع في الآونة الأخيرة، وذلك بسبب الاستعمال السيئ للثورة التكنولوجية
- نظرا لانتشار الجريمة الإلكترونية بشكل ملفت للانتباه، ولأن أجهزة التحقيق في الجرائم التقليدية لم تكن كافية للتصدي لهذا النوع من الإجرام، أنشئت أجهزة خاصة بالتحقيق فيها.
- لابد من الاعتراف أن الإسهام في اقتراح حلول للإشكالات التي يطرحها موضوع الحماية الجزائية للإلكترونية مهمة تعترضها صعوبة منهجية كبرى مصدرها اتساع وتشعب الجوانب التي تتعلق بالإلكترونية.

التوصيات:

- ضرورة تكثيف الجهود الدولية في مجال التعاون لمواجهة خطر انتشار الجريمة الإلكترونية دوليا
- تسخير كفاءات من ذوو الخبرة للتحقيق في مجال الجريمة الإلكترونية
- ضرورة إنشاء أقسام أو إدارات أو جهات للضبط الجنائي والتحقيق متخصصة في مجال الجريمة لإلكترونية

قائمة المصادر و المراجع

أ – باللغة العربية

أولا: الكتب

1. أحسن بوسقيعة، الوجيز في القانون الجزائي،الطبعة6، دار هومة، الجزائر.

2. أسامة أمحمد المناعسة، جلال محمد الزغبي، جرائم الحاسب الآلي ، دار وائل للنشر،الأردن،2004.

3. أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري،الطبعة الأولى، دار هومة،2012.

4. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي و التكنولوجيا الحديثة، دار النهضة العربية، 2001.

5. حسن صادق المرصفاوي – قانون العقوبات الخاص – منشأة المعارف – الإسكندرية مصر 1991.

6. خالد محمود إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2009.

7. رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الاسكندرية، 2013.

8. زيجة زيدان، الجريمة المعلوماتية في التشريع الجزائري الدولي دار الهدى الجزائري،2011.

9. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت،الطبعة الأولى، دار الفكر الجامعي، مصر.

10. محمد الأمين البشري، التحقيق في الجرائم المستحدثة، الطبعة الأولى، دار الجامعة ، عمان، 2015.

11. محمد سامي الشوا – ثورة المعلومات وانعكاساتها على قانون العقوبات – دار النهضة العربية – القاهرة 1994.

12. محمدالأمين البشري، التحقيق في الجرائم المستحدثة، الطبعة الأولى، دار الجامعة ، عمان، 2014.

13. محمود حماد مرهج الهيني، أصول البحث والتحقيق الجنائي، دار الكتاب القانونية، القاهرة، مصر، 2014.

14. محمود عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتاب القانونية، مصر، 2006.

15. محمود نجيب حسني – شرح قانون العقوبات – القسم الخاص – الجرائم المضرة بالمصلحة العامة – دار النهضة العربية - القاهرة 1972.

15. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنيت،دار الفكر الجامعي الإسكندرية، .،2007ط1.

16. نهلا عبد القادر المومني،الجرائم المعلوماتية ، دار الثقافة،الأردن،ط1 ، 2008.

17. نهلة القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الطبعة الثانية، 2009.

ثانيا: الرسائل الجامعية

1. حاجب هيام، الجريمة المعلوماتية، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء،2005-2006.

2. سعيد علي نعيم، آليات البحث والتحري من الجرائم المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2013.

3. طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير، في القانون الجنائي، جامعة الجزائر1 ، كلية الحقوق،2012-2001.

4. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجيستير، جامعة الحاج لخضر، باتنة، 2013.

5. سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة لنيل شهادة الماجيستير في الحقوق، قانون جنائي، جامعة محمد خيضر، بسكرة، 2013.

6. صغير يوسف، الجريمة المرتكبة عبر الانترنت، رسالة ماجستير ، جامعة مولود معمري ، تيزي وزو ، كلية الحقوق والعلوم السياسية ، 2013.

7. قادري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة ماجستير ، جامعة قاصدي مرباح، ورقلة ، كلية الحقوق والعلوم السياسية ، قسم الحقوق، 2013.

8. قربوز حليمة، الجريمة المعلوماتية في التشريع الجزائري والقانون المقارن، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2009_2006.

9. مرزوق نسيمة، جرائم الانترنت مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر ،2006_2009.

ثالثا: القوانين والأوامر

1. الأمر رقم 11/21 المؤرخ في 25 أوت 2011 المتضمن تعديل قانون الإجراءات الجزائية الجزائري.

2. القانون15/04 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر 156/66المؤرخ في 8 جوان1966 المتضمن قانون العقوبات (ج ر 71 بتاريخ10 /2004/11.).

3. القانون15/04 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات.

3. قانون العقوبات المعدل والمتمم بالقانون09/01 المؤرخ في26 يونيو 2001.

الأمر 07/03 المؤرخ في: 2003/07/19 المتضمن براءة الاختراع.

4. دستور الجمهورية الجزائرية الديمقراطية الشعبية المؤرخ في 30 ديسمبر 2020.

5. القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

رابعا: المجلات

1. سميرة معاشي، ماهية الجريمة الالكترونية ..مجلة المنتدى القانوني، العدد السابع جامعة بسكرة، 2012.

2. عرب يونس، جرائم الكمبيوتر والانترنت،ورقة عمل مقدمة إلى مؤتمر الأمن العربي،2002.

الملتقى الوطني حول الجريمة الالكترونية، جريدة الأمة العربية، وهران 2013/02/01 .

خامسا: المواقع الإلكترونية

WWW.Oecd.Org

ب- باللغة الأجنبية:

Vivant et autres: Informatique et droit pénal. Les biens informatiques objets de fraude.

Lamy informatique.1991.n°3445.

الفهرس

الفصل الأول: الإطار العام للجريمة الإلكترونية

تمهيد.....6

المبحث الأول: ماهية الجريمة الإلكترونية 7

المطلب الأول: مفهوم الجريمة الإلكترونية 7

الفرع الأول: التعريف الجريمة الإلكترونية 7

الفرع الثاني: صور الجريمة المعلوماتية 11

المطلب الثاني: البنيان القانوني للجريمة الإلكترونية ومميزاتها.....13

الفرع الأول: أركان الجريمة الإلكترونية.....14

الفرع الثاني: خصائص الجريمة الإلكترونية 18

المبحث الثاني: التحقيق الجنائي في الجريمة الإلكترونية 23

المطلب الأول: الهيئات المكلفة بالبحث والتحري عن الجرائم الإلكترونية.....23

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.....23

الفرع الثاني: الوحدات التابعة لسلك الأمن الوطني 25

المطلب الثاني: وسائل الإثبات في الجرائم الإلكترونية 27

الفرع الأول: مفهوم الدليل الإلكتروني 27

الفرع الثاني: أشكال الدليل الإلكتروني 28

خلاصة الفصل.....30

الفصل الثاني: آليات حماية الجريمة الإلكترونية في التشريع الجزائري.....34

تمهيد.....35

المبحث الأول: إجراءات الحماية الموضوعية.....35
المطلب الأول: الحماية في قانون العقوبات وقانون الملكية الفكرية 35
الفرع الأول: الحماية في قانون العقوبات 35
الفرع الثاني: الحماية في نصوص الملكية الفكرية 39
المبحث الثاني: إجراءات التحقيق في الجرائم الإلكترونية في التشريع الجزائري.....42
المطلب الأول: جمع الأدلة التقليدية للتحقيق في الجرائم الإلكترونية 43
الفرع الأول: التفتيش وضبط الأدلة في الجريمة الإلكترونية 43
الفرع الثاني: المعاينة وندب الخبراء في الجريمة الإلكترونية 45
المطلب الثاني: جمع الأدلة المستحدثة للتحقيق في الجرائم الإلكترونية 47
الفرع الأول: حجية الدليل المستحدث في الكشف عن الجريمة الإلكترونية 47
الفرع الثاني: صعوبات مكافحة الجريمة الإلكترونية.....56
خلاصة الفصل.....59
الخاتمة.....
61

مـلخص مذكرة الماستر

تعتبر الجريمة المعلوماتية من الجرائم التي باتت تشكل خطرا على المجتمع الجزائري، لذلك عمد إلى وضع آليات لمكافحتها عن طريق سن مختلق النصوص القانونية للتصدي لها وكذلك التعاون الدولي في مجال التحري والبحث في هذه الجريمة المنظمة العابرة للحدود الوطنية.

الكلمات المفتاحية:

1/ جريمة جمركية 2/ إدارة جمارك 3/ متابعة قضائية 4/ المشرع الجزائري 5/ قانون الجمارك.

Abstract of The master thesis

Information crime is considered one of the crimes that has become a threat to Algerian society, so it has set out mechanisms to combat it by enacting fabricated legal texts to address it, as well as international cooperation in the field of investigation and research in this transnational organized crime.

key words:

1/ Customs crime 2/ Customs administration 3 Judicial follow-up 4/ Algerian legislator 5 Customs law