حجية الدليل الإلكتروني في إثبات الإعتداءات المنصوص عليها في المواد 394 مكرر إلى 394 مكرر2 من قانون العقوبات الجزائري.

The proof of the electronic evidence in proving the assaults stipulated in articles 394 bis to 394 bis 2 of the Algerian code.

خليفي فتيحة
كلية الحقوق جامعة عين تموشنت
مخبر الأسواق، التشغيل، التشريع
والمحاكاة في الدول المغاربية
fatiha.khelifi@univ-temouchent.edu.dz

مهداوي محمد صالح
كلية الحقوق جامعة عين تموشنت
مخبر الأسواق، التشغيل، التشريع
والمحاكاة في الدول المغاربية
mohammed.mehdaoui@univ-temouchent.edu.dz

تاريخ الاستلام: 2023/05/22 تاريخ القبول : 2024/12/06 ؛ تاريخ النشر :ديسمبر 2024

ملخص:

رغم الخدمات الجليلة التي قدمها التطور التكنولوجي للإنسان إلا أن هناك من إستغل الجانب السلبي من ذلك التطور لتجسيد أفعاله الإجرامية، والتي من ضمنها الإعتداء على النظم المعلوماتية سواء بالدخول أو البقاء فيها غشا، أو عن طريق المساس بمعطياتها أو إساءة إستخدامها، الأمر الذي ترتب عنه أضرار بالغة الخطورة، إلا أن المشرع الجزائري كان حريصا أشد الحرص على مكافحة هذه الإعتداءات إذ سارع إلى النص على تجريمها من خلال القانون 04-05 المعدل لقانون العقوبات، ونظرا للطابع الإفتراضي والتقني الذي تتميز به تلك الإعتداءات كان من الصعب إثباتها بأدلة تقليدية لعدم إتفاق طبيعتهما، لذلك إستوجب الأمر البحث عن دليل آخر ذو طابع تقني.

الكلمات المفتاحية: الدليل الإلكتروني؛ النظام المعلوماتي؛ إعتداءات؛ معطيات؛ إثبات.

Abstract :

Despite the great services provided by the technological development to man, there are those who exploited the negative side of that development to carry out their criminal acts, which include assaulting information systems, whether by entering or remaining in them fraudulently, or by compromising or misusing their data, which resulted in extremely dangerous damages, but the Algerian legislator was very keen to combat these attacks, as he/ she was quick to criminalizing them through law 04-05 amending the penal code, and given the hypothetical and technical nature that characterizes these attacks, it was difficult to prove them with traditional evidence because they do not match, therefore, the matter necessitated the search for other for evidence of a technical nature.

Keywords : electronic directory; information system; assaults; data; proof.

المؤلف المرسل: خليفي فتيحة .

مقدمة:

إجتاح العالم في السنوات الأخيرة تطورا منقطع النظير في مجال تكنولوجيا المعلومات والإتصال التي تحققت معها رفاهية الإنسان ورقيه فغيرت بذلك من نمط حياته فأصبح يعتمد إعتمادا شبه كامل على ما تقدمه هذه التكنولوجيا في جل الميادين وفي مختلف التعاملات التي يقوم بها.

ويعد جهاز الحاسوب أهم ثورة أفرزها ذلك التطور إذ أصبح الركيزة الأساسية والتي لا غنى عنها نظرا لخدماته الجليلة وإمكانياته الإستثائية في تخزين المعلومات وتنظيمها بل وحتى في عملية إسترجاعها، إذ لا يتطلب الأمر في ذلك سوى كبسة واحدة على أحد أزراره فاستبدلت الملفات الورقية بالرقمية، وتعززت أهمية هذا الجهاز أكثر بظهور شبكة الأنترنت التي تيسرت معها عملية تداول تلك المعلومات المخزنة من شخص لآخر ومن دولة لأخرى بل ومن قارة لقارة.

لكن من جهة أخرى، تم إستغلال ذلك الجهاز في شن إعتداءات على المعطيات المخزنة فيه من طرف جناة واكبوا التطور التكنولوجي لتجسيد نشاطهم الإجرامي، فتمخض عن ذلك ميلاد نوع جديد من الجرائم تسمى بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، إستهدفت النظام المعلوماتي الذي تتمثل وظيفته الأساسية في معالجة البيانات والإحتفاظ بها.

ونظرا لأهمية هذا النظام ومن أجل حمايته فقد سارع المشرع الجزائري إلى تجريم ما يقع عليه من إعتداءات وذلك بموجب القانون 04-15 المعدل لقانون العقوبات حيث تضمنت مواده من 394 مكرر إلى 394 مكرر 2 صور الجرائم القائمة بسبب تلك الإعتداءات، والتي تتسم بطابع تقني معقد نظرا للبيئة التي ترتكب فيها، الأمر الذي ترتب عنه صعوبة في عملية إثباتها بالأدلة التقليدية والتي لم تفض إلى أية نتيجة نظرا لكونها لا تتفق بشكل كامل مع الوسط الذي ترتكب فيه تلك الإعتداءات.

ومن أجل مواجهتها وحتى لا يتم إفلات الجناة منها كان من اللازم التطوير من الأساليب التقليدية للبحث عن الدليل المناسب لإثباتها، وإخراجها في شكل معطيات رقمية إفتراضية فكان بذلك ما يعرف بالدليل الإلكتروني، باعتبار أن الدليل أثر يولد وحقيقة تنبعث من الجريمة المرتكبة.

وتبرز أهمية دراسة موضوع إثبات الإعتداءات التي تستهدف النظام المعلوماتي في التعرف على دور الدليل الإلكتروني والمكانة التي يحتلها في عملية الإثبات، نظرا لحداثته النسبية وطابعه التقني الذي ميز من خصوصية التعامل معه الأمر الذي يستدعي في بعض الأحيان الإستعانة بخبراء في المجال التقني من أجل فهم هذا الدليل،ولمعالجة هذا الموضوع نطرح الإشكالية التالية:

إلى أي مدى يمكن للدليل الإلكتروني أن يثبت الإعتداءات الواقعة على النظام المعلوماتي؟ وبعبارة أخرى هل للدليل الإلكتروني الحجية الكافية لإثبات صور الإعتداءات التي تستهدف النظام المعلوماتي؟

وللإجابة على الإشكالية المطروحة وإثرائها بالتحليل والنقاش إرتأينا الإعتماد على المنهج الوصفي باعتباره الأنسب في عملية وصف الإعتداءات التي يتعرض لها النظام المعلوماتي مما يساعد في عملية التعرف طابعها الخاص، بالإضافة إلى المنهج التحليلي والذي يمكننا من خلاله مناقشة القيمة القانونية التي يتمتع بها الدليل الإلكتروني ومدى قوته وحجيته في عملية الإثبات حتى يستند إليه القاضي ويبني على أساسه إقتناعه.

في هذا الإطار إعتمدنا على خطة من مبحثين رئيسيين بحيث خصصنا المبحث الأول لصور الإعتداءات المنصوص عليها في المواد394 مكرر إلى 394 مكرر2، في حين خصصنا المبحث الثاني للدليل الإلكتروني كآلية لإثبات الإعتداءات المنصوص عليها في المواد 394مكرر إلى 394 مكرر2.

1- صور الإعتداءات المنصوص عليها في المواد394 مكرر إلى 394 مكرر2.

تمخض عن التطور التكنولوجي العديد من الجرائم الإلكترونية التي إتخذت من العالم الإفتراضي مسرحا لها، ومن بين تلك الجرائم الإعتداءات التي تستهدف النظام المعلوماتي[1]، وقد تكفل المشرع الجزائري بمعالجتها من خلال تعديل قانون العقوبات بموجب القانون رقم 04-15[2] من المادة 393 مكرر إلى المادة 394 مكرر2، حيث خصص لذلك القسم السابع منه تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" وفي هذا المبحث نتطرق إلى صور تلك الإعتداءات والتي تتمثل في الدخول أو البقاء غشا في النظام المعلوماتي وكذا الإعتداءات على معطيات النظام المعلوماتي.

1-1: الدخول أو البقاء غشا في أنظمة المعالجة الآلية للمعلومات.

تم النص على هذه الصورة في المادة 394 مكرر من القانون 04-15 والتي جاء فيها" يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000دج إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة تكون العقوبة الحبس نت ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000دج إلى 150.000دج"

من خلال إستقراء نص هذه المادة يتضح لنا بأن هذا الإعتداء له صورتان، تتمثل الصورة الأولى في الدخول أو البقاء غشا في النظام المعلوماتي دون التأثير عليه والصورة الثانية تتمثل في الدخول أو البقاء غشا في النظام المعلوماتي مع التأثير عليه.

1-1-1 الدخول أو البقاء غشا في النظام المعلوماتي دون التأثير عليه.

أي أن الإعتداء في هذه الحالة يتخذ صورة بسيطة أو عادية ولا تترتب عليه أية نتيجة، هذه الصورة تضمنتها الفقرة الأولى من المادة 394 مكرر، ولقيام هذه الجريمة يستلزم الأمر قيام كل من الركن المادي والمعنوي.

أولا: الركن المادي:

يتمثل في كل من فعل الدخول أو البقاء داخل النظام المعلوماتي، وفعل الدخول يعني جميع الأفعال التي تسمح بالولوج إليه حيث يتحقق ذلك من خلال الوصول إلى البيانات والمعلومات المخزنة في النظام[3]، وينبغي علينا أن نشير إلى أن الدخول لا يقصد به التواجد المادي كالدخول مثلا إلى غرفة يوجد بها جهاز الحاسوب، وإنما المقصود من ذلك هو التواجد المنطقي المعنوي، أي أن عملية الدخول تقترن بنشاط ذهني يمكن الجاني من النفاذ إلى النظام المعلوماتي بحث يمكن تشبيه الدخول إليه بالدخول إلى ذاكرة الإنسان.

ويتحقق فعل الدخول غشا متى تم إرتكابه دون الحصول على ترخيص أو إذن من الشخص الذي له سلطة على النظام المعلوماتي، كما يتحقق كذلك في حالة وجود ترخيص بالدخول إلى جزء فقط من النظام غير أن الجاني يتجاوز ذلك الجزء ويدخل إلى باقي الإجزاء الأخرى.

أما فعل البقاء غشا فيعني وصول الجاني إلى النظام المعالجة الآلية للمعطيات مع إحتفاظه بالبقاء فيه وعدم مغادرته رغم إدراكه بعدم مشروعية ما يقوم به كونه يتصرف دون وجه حق،[4] لذلك يندرج فعل البقاء غير المشروع ضمن جرائم الإمتناع كون أن الجاني إمتنع عن قطع الإتصال، كما يتحقق فعل البقاء سواء كان مستقلا عن فعل الدخول كأن يتم الدخول صدفة أو عن طريق الخطأ وعند إدراك الجاني ذلك يبقى داخل النظام ولا يقطع الإتصال ففي هذه الحالة يعاقب على جريمة البقاء كجريمة مستقلة، كما يتحقق فعل البقاء في حالة ما إذا إقترن بفعل الدخول كأن يتم الدخول إلى النظام عن طريق الغش وبقائه فيه حيث يتابع الفاعل عن تهمتين على أساس التعدد الفعلي للجرائم،[5] والمشرع الجزائري أكد على إستقلال الفعلين كجريمتين منفصلتين لكل جريمة سلوكها الخاص بها، وذلك من خلال إستعماله لعبارة "أو يبقى" فحرف "أو" يفيد التعدد.

ثانيا: الركن المعنوي:

جريمة الدخول أو البقاء غشا في النظام المعلوماتي تأخذ صورة العمد أي أنها جريمة عمدية، يقوم الركن المعنوي فيها على القصد الجنائي العام بعنصريه العلم والإرادة، أي إدراك الجاني لكافة العناصر التي يرتكز عليها كيان هذه الجريمة،[6] وكذا إتجاه إرادته إلى تحقيق فعل الدخول أو البقاء في النظام،[7] أي أن الجاني يكون على علم بأنه لا يملك حق الدخول إلى النظام المعلوماتي أو البقاء فيه إلا أن إرادته تتجه إلى تحقيق ذلك.

وبما أن جريمة الدخول أو البقاء غشا تعتبر من الجرائم الشكلية في التشريع الجزائري، فإن إرادة الجاني فيها تقتصر على السلوك الإجرامي لتستغرقه بكل مقوماته ولا تمتد إلى النتيجة،[8] ولا عبرة للباعث فيها مهما كان سواء لتحقيق الربح، الإنتقام أو قهر النظام، لذلك فالمشرع الجزائري لم يشترط أن يتوفر فيها القصد الخاص.

1-1-2 جريمة الدخول أو البقاء غشا في النظام المعلوماتي مع التأثير عليها.

فالإعتداء في هذه الجريمة يتخذ صورة مشددة، وقد تم النص عليها في الفقرة الثانية والثالثة من المادة 394 مكرر، حيث تضمنتا هاتين الفقرتين ظرفين مشددين تضاعف على أساسهما العقوبة وهما:

-حذف أو تغيير لمعطيات المنظومة.

-تخريب نظام إشتغال المنظومة.

أولا: الركن المادي:

الركن المادي للصورة المشددة يتطلب إضافة إلى فعل الدخول أو البقاء غشا ترتب نتيجة والمتمثلة في:

أ-حذف أو تغيير لمعطيات المنظومة: وعملية الحذف المقصود منها إزالة المعطيات التي يحتويها النظام،[9] ولا يشترط أن تشمل عملية الحذف جميع المعطيات الموجودة فيه وإنما يكفي إزالة جزء منها فقط، أما التغيير فيعني تعديل المعطيات من خلال عملية إستبدالها بمعطيات أخرى،[10] مما يترتب عليه تغيير معناها تماما عما كانت عليه.

ب- تخريب نظام إشتغال المنظومة: ويعني تشويه أداء عمل النظام بشكل طبيعي وإعاقته مما يترتب عليه عدم صلاحيته للإستعمال ولا يشترط أن تمس الإعاقة النظام بصورة كلية بل يكفي إعاقته

بصفة جزئية،[11] وللإشارة فإن المشرع لم يحدد نوع الوسيلة التي يعتمد عليها في إعاقة النظام المعلوماتي.

إضافة إلى ضرورة توفر علاقة سببية تربط بين فعل الدخول أو البقاء والنتيجة المحققة، ففرضا أن النتيجة حدثت بفعل آخر مثلا فهنا ينتفي الظرف المشدد ونكون أمام الصورة البسيطة لهذه الجريمة.

ثانيا: الركن المعنوي:

يكفي لقيام هذه الجريمة توفر القصد الجنائي العام (العلم والإرادة) والذي تقوم عليه الصورة البسيطة كما سبقت الإشارة إلى ذلك، أما نية الإضرار بالنظام فهي غير مطلوبة.[12]

فبالرجوع إلى نص المادة 394 مكرر نجده قد تضمن عبارة "فإذا ترتب على ذلك" مما يعني أن النتائج المتمثلة في الحذف أو التغيير أو التخريب تتحقق دون قصد إحداثها، أي عن طريق الخطأ ودون سوء نية.

2-1 الإعتداءات التي تطال معطيات النظام المعلوماتي.

بعد أن تم تجريم الإعتداء على النظام المعلوماتي بالدخول أو البقاء فيه غشا، نص المشرع كذلك على تجريم الإعتداءات التي تطال معطياته وذلك نظرا لأهميتها وقيمتها والتي أصبحت تضاهي أو تتجاوز قيمة المال المادي، ويمكن إعتبار هذه الإعتداءات كنتائج تترتب عن فعل الدخول أو البقاء في النظام لذلك سنتطرق إلى الجرائم الماسة بالمعطيات المخزنة في النظام المعلوماتي ثم جرائم إساءة إستخدام معطياته.

1-2-1 الجرائم الماسة بالمعطيات المخزنة في النظام المعلوماتي.

نصت على هذه الجريمة المادة 394 مكرر1 والتي جاء فيها " يعاقب بالحبس من ستة (6) أشهر إلى ثلاثة (3) سنوات وبغرامة من 500.000دج إلى 2.000.000دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

من خلال نص هذه المادة يتضح بأن المشرع الجزائري لم يحدد نوع المعلومات المشمولة بالحماية والتي تكون محل إعتداء، وإنما جاء النص عاما شاملا لجميع المعلومات التي يحتويها النظام المعلوماتي، وحتى تتحقق جريمة المساس بالمعطيات يتطلب الأمر قيام ركنيها المادي والمعنوي.

أولا: الركن المادي:

إنطلاقا من مضمون المادة السابقة نجد بأنها قد تضمنت الأفعال التي يتكون منها النشاط الإجرامي لهذه الجريمة والذي يكفي لتحققه فعل واحد فقط من تلك الأفعال والمتمثلة في:

أ-**فعل الإدخال**: يعرف هذا الفعل على أنه تغذية النظام المعلوماتي بالمعلومات المراد معالجتها أو بتعليمات لازمة لعملية المعالجة،[13] حيث يتحقق هذا الفعل بإضافة معلومات على الدعامة سواء كانت تلك الدعامة تتضمن معلومات من قبل أو خالية تماما منها،[14] ففعل الإدخال يقوم على الإضافة حتى لو كانت المعلومات المضافة صحيحة طالما أنها تؤثر على معطيات النظام المعلوماتي الموجود به سابقا.

ب-**فعل الإزالة:** ويعني المحو أي حذف من المعطيات التي يحتويها النظام المعلوماتي، كما يعني إقتطاع خصائص معطيات مسجلة من خلال محوها أو طمسها أو نقل جزء من تلك المعطيات وتخزينها في جزء آخر من النظام،[15]وفعل الإزالة هو عملية لاحقة لفعل الإدخال فإزالة المعطيات تقتضي أن عملية إدخالها قد تمت أولا.

ج-**فعل التعديل**: ويعني التغيير، بمعنى أن المعطيات التي يحتويها النظام المعلوماتي تستبدل بمعطيات أخرى، ويتحقق هذا الفعل عن طريق أخذ معلومات وتوضع مكانها معلومات أخرى الشيئ الذي يترتب عليه نتائج مغايرة وبعيدة تماما عن النتائج التي كانت ستتحقق لولا فعل التعديل.[16]

فالأفعال المشكلة لجريمة إساءة إستخدام المعطيات ذكرها المشرع الجزائري على سبيل الحصر لا المثال، فجميعها تمس بسلامة هذه المعطيات حتى لو لم ترتكب جميعا فأحدها كاف للمساس بالمعطيات وتغييرها تماما عن حقيقتها، وإن كان من الصعب جدا الفصل بينها فحتى يتم إجراء تعديل معطيات ما لا بد من القيام بفعل الإدخال أو الإزالة.[17]

ثانيا: الركن المعنوي:

ورد في نص المادة السالفة الذكر لفظ "بطريق الغش" مما يعني أن جريمة المساس بالمعطيات هي جريمة عمدية تتطلب قصد جنائي عام بعنصريه العلم والإرادة، بمعنى أن الجاني يكون على علم بالأفعال التي يقدم إلى إرتكابها فيها مساس بمعطيات محمية قانونا وأن فعله يشكل جريمة ويعاقب عليه ولكن رغم ذلك تتجه إرادته إلى تحقيق تلك الأفعال.

أما بالنسبة للقصد الجنائي الخاص فلا نلمحه في نص المادة ما يوحي بعدم ضرورة أن تتوفر لدى الجاني نية خاصة، أية نية إلحاق الضرر بصاحب تلك المعطيات وإنما يكفي لقيام هذه الجريمة القصد الجنائي العام فقط.

2-2-1 جريمة إساءة إستخدام معطيات النظام المعلوماتي.

حرص المشرع الجزائري على حماية المعطيات المعلوماتية كان واضحا حيث أنه لم يكتف بتجريم الدخول أو البقاء غشا في النظام المعلوماتي وكذا المساس بمعطياته، بل نجده إلى جانب ذلك قد نص على تجريم أفعال تسبق هذه الجرائم وأخرى لاحقة على إرتكابها وذلك من خلال نص المادة 394 مكرر2 والتي جاء فيها" يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000دج إلى 5.000.000دج كل من يقوم عمدا وعن طريق الغش بما يأتي:

-تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

-حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم" وتقوم هذه الجريمة كباقي الجرائم السابقة على ركن مادي وآخر معنوي.

أولا: الركن المادي:

باستقراء نص المادة يتضح لنا جليا أن الركن المادي يأخذ صورتين:

أ-التعامل في معطيات تصلح لإرتكاب جريمة معلوماتية: وهو ما تم النص عليه في الفقرة الأولى من المادة 394مكرر2 حيث تنطوي هذه الصورة على تجريم مجموعة من الأفعال والتي ذكرت على سبيل الحصر لا المثال والتي من شأنها أن تساهم في إرتكاب إجرائم إحدى المساس بالنظام المعلوماتي،ويبدو أن غاية المشرع من تجريم تلك الأفعال هي غاية وقائية ردعية الهدف منها منع وقوع جرائم أخرى.

فتلك الأفعال يمكنها أن تجعل المعطيات صالحة لإرتكاب جريمة بل وقابلة لأن تستعمل في ذلك من خلال مراحل تكون بدايتها بتصميم تلك المعطيات والبحث فيها ثم تجميعها إلى غاية جعلها تحت تصرف الغير وفي متناولهم عن طريق عملية نشرها وتوفيرها أو الإتجار بها[18]، والشيئ المميز في هذه الجريمة هو أن المشرع الجزائري وسع من دائرة المعطيات المشمولة بالحماية سواء كانت مخزنة أو معالجة وكذا المرسلة ولم تقتصر الحماية على المعطيات المخزنة في النظام المعلوماتي فقط.

ب-التعامل في معطيات محصلة من جريمة معلوماتية:

هذه الصورة تضمنتها الفقرة الثانية من المادة 394 مكرر2، إذ لم يكتف المشرع بتجريم التعامل في معطيات تصلح لإرتكاب جريمة بل تعدى ذلك ليجرم التعامل في معطيات تكون محصلة

من جريمة، حيث تتحقق هذه الصورة من خلال مجموعة من الأفعال والتي ذكرت هي الأخرى على سبيل الحصر كما لم يشترط أن ترتكب بصفة مجتمعة، إذ أن القيام بأحد تلك الأفعال يعد كافي لقيام الجريمة.

تتمثل تلك الأفعال في كل من فعل حيازة معلومات تكون ناتجة عن جرائم المساس بالنظام المعلوماتي أو إفشائها من خلال إعلانها للغير، أو نشرها من خلال كشف سريتها، أو باستعمالها عن طريق الإنتفاع بها بتفعيل فائدتها.[19]

وما تمت ملاحظته هو أن فعل النشر قد تم تكراره في كل من الفقرة الأولى والثانية من المادة 394 مكرر2 ليكون بذلك الفعل المشترك بين صورتي هذه الجريمة وهذا إن دل على شيئ فإنما يدل على خطورته، كما أنه وإن كان يقترب من فعل الإفشاء غير أنه أكثر خطورة وضررا منه، إذ أن الإفشاء يعني إذاعة المعلومة بين عدد معين من الأشخاص في حين أن النشر يعني إذاعتها بين أكبر عدد ممكن منهم، كما نشير إلى أن فعل الإفشاء في هذه الجريمة يختلف عن إفشاء السر المهني كون أن الجاني في هذه الحالة لا يعتبر شخصا مؤتمننا.

ثانيا: الركن المعنوي:

جريمة إساءة إستخدام معطيات النظام المعلوماتي هي جريمة عمدية تستلزم لقيامها توفر القصد الجنائي العام بعنصريه العلم والإرادة، بمعنى أن تتجه إرادة الجاني إلى إقتراف أحد الأفعال التي وردت في نص المادة 394 مكرر2 مع علمه بأنها أفعال مجرمة قانونا ومعاقب على فعلها،أما بالنسبة للقصد الجنائي الخاص فإنه يختلف بين صورة التعامل في معطيات تصلح لإرتكاب إحدى جرائم وصورة التعامل في معطيات محصلة من تلك الجرائم.

ففي الصورة الأولى لا يكفي القصد الجنائي العام بل يلزم أن يتوفر إلى جانبه القصد الجنائي الخاص، وذلك ما دلت عليه عبارة "غشا" والتي توحي بأن تتوفر لدى الجاني نية خاصة، حيث يتحقق القصد الجنائي الخاص بالتمهيد والإعداد لإستعمال تلك المعطيات في إرتكاب جرائم المساس بالنظام المعلوماتي،[20] أي إنصراف الإرادة إلى وقائع لا تندرج ضمن أركان الجريمة.

أما بالنسبة للصورة الثانية فما نستشفه من خلال عبارة "لأي غرض كان" أن الجاني يعاقب على تلك الأفعال مهما كان قصده، مما يعني أن هذه الصورة لا تتطلب قصدا خاصا وإنما يكفي لقيامها القصد العام.

2- الإثبات القانوني للإعتداءات المنصوص عليها في المواد 394مكرر إلى 394 مكرر2.

إن عملية الإثبات القانوني لأية جريمة تقوم على ركيزة أساسية تتمثل في مدى توفر الدليل الذي بمقتضاه يتم إثباتها وإدانة فاعلها أو نفيها وتبرئة المتهم، وباعتبار أن الإعتداءات المنصوص عليها في المواد394 مكرر إلى 394 مكرر2 تستهدف النظام المعلوماتي كما سبقت الإشارة إلى ذلك في المبحث الأول، فهي إعتداءات ترتكب في بيئة ذات طابع إفتراضي رقمي تختلف تماما على البيئة العادية الأمر الذي يجعلها تتطلب دليلا خاصا يتناسب وطبيعة الوسط الذي أرتكبت فيه حتى يتم إثباتها، هذا ما سنقوم بتوضيحه وذلك بالتطرق إلى الدليل الإلكتروني كآلية لإثبات الإعتداءات المنصوص عليها في المواد 394مكرر إلى 394 مكرر2 ثم حجية الدليل الإلكتروني في إثبات تلك الإعتداءات.

2-1الدليل الإلكتروني كآلية لإثبات الإعتداءات المنصوص عليها في المواد 394مكرر إلى 394 مكرر2.

نظرا للطبيعة اللامادية للإعتداءت على الأنظمة المعلوماتية فإن الدليل المناسب لإثباتها يكون مستمد من ذات طبيعتها باعتبار أن الدليل وليد الجريمة، الشيئ الذي يترتب عليه عدم كفاية طرق الإثبات التقليدية في إقامة الدليل على هذه الإعتداءات والتي أدت إلى بروز دليل جديد يعرف بالدليل الإلكتروني والذي نبرز مفهومه أولا ثم نبين قيمته القانونية في الإثبات.

2-1-1 مفهوم الدليل الإلكتروني.

إن مسألة تحديد مفهوم الدليل الإلكتروني تقتضي منا التطرق إلى تعريفه وإبراز الخصائص التي ينفرد بها عن الدليل المعتاد والمتعارف عليه المستمد من البيئة المادية.

أولا: تعريف الدليل الإلكتروني:

باعتبار أن الدليل الإلكتروني يولد في بيئة إلكترونية تشهد تطورا مستمرا لذلك كان من الصعب إحتواء هذا العالم لرقمي، الشيئ الذي أدى إلى تباين تعريفاته.

فقد عرف من قبل المنظمة الدولية لأدلة الحاسوب (IOCE) على أنه المعلومات المخزنة أو المتنقلة في شكل ثنائي والتي يمكن الإعتماد عليها أمام المحكمة،[21] أما بالنسبة للمشرع الجزائري فقد تجنب تعريفه ضمن المنظومة القانونية، بل ترك مهمة ذلك للإجتهادات الفقهية والتي لم تتفق على وضع تعريف له.

فعرف بأنه ذلك الدليل الذي يجد أساسا له في العالم الإفتراضي ويقود إلى الجريمة، إذ يتمثل في البيانات التي يمكن إعدادها وتخزينها في شكل إلكتروني بحيث يتمكن الحاسوب من إنجاز مهمة ما،[22] وعرف أيضا بأنه المعلومات أو البيانات المخزنة في الحاسوب أو التي يتم تناقلها عبر شبكات الإتصال والتي يمكن إستخدامها في إثبات أو نفي جريمة ما،[23] كما عرفه الأستاذ "كيسي" بأنه جميع البيانات الرقمية التي يمكن أن تثبت بأن هناك جريمة قد أرتكبت، أو توجد علاقة بين الجريمة والجاني أو علاقة بين الجريمة والمتضرر منها، والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات، خرائط الصوت أو الصورة.[24]

وبعد تقديم هذه التعريفات يمكننا أن نعرف بدورنا الدليل الإلكتروني بأنه الدليل الذي يكون قوامه المعلومات والبيانات التي تتخذ من جهاز الحاسوب وعاءا لها، بحيث يتم إستمادها بطريقة إلكترونية من أجل كشف واقعة إجرامية ذات طبيعة تقنية وإسنادها إلى فاعلها.

ثانيا: خصائص الدليل الإلكتروني وصوره:

يتميز الدليل الإلكتروني بجملة من الخصائص التي تجعله ينفرد عن الدليل التقليدي، حيث أن هذه الخصائص تعكس مدى إرتباطه بالبيئة الإفتراضية التي تمثل موطن ولادته، بالإضافة إلى أنه لا يوجد في نوع واحد وإنما له عدة أنواع.

أ-خصائص الدليل الإلكتروني:

-أنه دليل علمي: إذ يتطلب إستخلاصه طرقا غير تقليدية، حيث يتم إجراء تجارب علمية وتقنية على جهاز الحاسوب الذي تم إستخدامه في إرتكاب الجريمة،[25] فحتى يتم الحصول على هذا الدليل يستلزم الأمر اللجوء إلى الأساليب العلمية التي تتناسب مع التطور والتعقيد الذي تشهده البيئة الإلكترونية باعتباره مستمدا منها.

-أنه دليل تقني: هذه الخاصية هي نتيجة حتمية للخاصية الأولى فالقول بأن الدليل الإلكتروني علمي يثبت بالضرورة أنه دليل تقني.

حيث يتم اللجوء إلى تقنين وخبراء من أجل التعامل مع هذا الدليل إذ أن التقنية لا تنتج إعترافا أو بصمة مثلا، وإنما تنتج نبضات رقمية تتشكل قيمتها في إمكانية تعاملها مع القطع التي تشكل الحاسوب على أية شاكلة يكون عليها،[26] فاللجوء إلى الخبرة التقنية عندما يتعلق الأمر بالدليل الإلكتروني حتمية لا غنى عنها.

-أنه دليل يصعب التخلص منه: رغم أن الدليل الإلكتروني يتميز بسرعة زواله وإمكانية إتلافه بسهولة إلا أن ذلك لا يشكل عائقا أمام إسترجاعه مرة أخرى ويعود الفضل في ذلك إلى البرامج الحاسوبية التي تقوم باستعادة البيانات والمعلومات المحذوفة،[27] وهذا عكس الدليل العادي الذي يصعب إسترجاعه كحالة التخلص من بصمات الأصابع.

د-أنه دليل قابل للنسخ: إذ يمكن إستخراج نسخ منه تكون مطابقة تماما للأصل ولها ذات القيمة العلمية والحجية الثبوتية، وهذا ما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقدان والتلف والتغيير.[28]

ب-أنواع الدليل الإلكتروني:

خلال عملية البحث عن تقسيمات الدليل الإلكتروني صادفتنا العديد من الأنواع إلا أن التقسيم الأكثر شيوعا يتمثل في:

-أدلة إلكترونية أعدت لتكون وسيلة إثبات: وتتمثل في السجلات التي يتم إنشاؤها تلقائيا بواسطة الأجهزة التكنولوجية، كسجلات الهاتف فواتير أجهزة الحاسب الآلي بالإضافة إلى السجلات التي تحتوي على بيانات تم إدخالها إلى الجهاز وتمت معالجتها من خلال برنامج ما.[29]

-أدلة إلكترونية لم تعد لتكون وسيلة إثبات: هذا النوع يخلفه الجاني دون علم أو رغبة منه، حيث تتجسد في الآثار التي يتركها مستخدم النظام المعلوماتي القائم بمعالجة المعطيات بسبب قيامه بأي نشاط يدخل ضمن إطار المعالجة أو إرسال هذه المعطيات أو إستقبالها ويسمى هذا النوع بالبصمة الرقمية أو الآثار المعلوماتية الرقمية.[30]

2-1-2 القيمة القانونية للدليل الإلكتروني في الإثبات.

تتجلى القيمة القانونية للدليل الإلكتروني في الإثبات في مشروعيته أي أن يكون معترفا به من قبل المشرع كأساس للحكم بالإدانة، ويتحدد ذلك بناءا على نظام الإثبات السائد في الدولة، وهناك إتجهان رئيسيان نظام الإثبات الحر ونظام الإثبات المقيد.

أولا: نظام الإثبات الحر:

في ظل هذا النظام يكون الإثبات ممكنا بأية وسيلة من شأنها إقناع القاضي بما يريد إثباته،[31] بمعنى أن المشرع لا يحصر الأداة والوسائل التي يتم بها الإثبات وإنما يكون للقاضي الحرية في تأسيس حكمه وفقا لإقتناعه الشخصي،[32] وبالتالي يكون للقاضي أن يبني إقتناعه على أي دليل مطروح أمامه كما له أن يستبعد أي دليل آخر.

ونتيجة للتطور التكنولوجي الذي نتج عنه جرائم الإعتداء على النظام المعلوماتي، وجد القاضي نفسه مضطرا للتعامل مع الأدلة الإلكترونية من أجل إثبات تلك الإعتداءات، باعتبار أنه وفقا لنظام الإثبات الحر يكون للقاضي أن يعتمد على أي دليل يراه مناسبا بما في ذلك الأدلة الإلكترونية، فله أن يوجه أمر إلى مشغل النظام من أجل تقديم ما يلزم من معلومات بما فيها الثغرات السرية الخاصة بتشغيل النظام.

ثانيا: نظام الإثبات المقيد.

وهو عكس النظام السابق حيث أن الأدلة وفقا لهذا النظام يتم حصرها وتحديدها مسبقا من طرف المشرع ولا يجوز للقاضي الخروج عن تلك الأدلة المحددة،[33] رغم أن تحديد الأدلة مسبقا يفقد القاضي سلطته في الحكم، ففي كثير من الأحيان يحكم بما يخالف قناعته التي تكونت لديه بناءا على أدلة غير معترف بها في هذا النظام.[34]

ونظرا لتعارض هذا النظام مع الطابع المتطور للإعتداءات الواقعة على النظام المعلوماتي فقد لجأت العديد من الدول إلى إدخال تعديلات على تشريعاتها الجنائية حتى تتلاءم مع الطبيعة المتطورة لتلك الإعتداءات خاصة بعد أن رفض القضاء في بعض الدول الأخذ بالأدلة التي لم يتم النص عليها ضمن القانون الساري المفعول،[35] مثل بريطانيا التي أصدرت سنة 1990 قانون إساءة إستخدام الحاسوب حيث نص قانونها للإثبات على قبول الدليل الإلكتروني.[36]

أما بالنسبة للمشرع الجزائري فقد نص في المادة 212 من قانون الإجراءات الجزائية،[37]التي جاء فيها" يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عادا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لإقتناعه الشخصي" فما يستشف من نص هذه المادة هو أن المشرع أخذ بمبدأ نظام الإثبات الحر كأصل عام، وبالتالي فالإقرار بمبدأ حرية الإثبات يترتب عليه الإقرار بحجية الدليل الإلكتروني في إثبات الإعتداءات التي تستهدف النظام المعلوماتي.

كما أن المشرع الجزائري لم يفرد نصا خاصا يملي من خلاله على القاضي قبول أو رفض دليل معين بما في ذلك الدليل الإلكتروني، فالأصل هو حرية الأدلة.

2-2 حجية الدليل الإلكتروني في إثبات الإعتداءات المنوص عليها في المواد 394 مكرر إلى 394 مكرر2.

بما أن الإعتداء على النظام المعلوماتي يعد جريمة قائمة بذاتها ومثلما سبقت الإشارة فإن الأصل هو حرية الإثبات، فحتى يتم إثبات تلك الإعتداءات فإنه لا يكفي مجرد الحصول على الدليل

الإلكتروني وتقديمه للقضاء، وإنما يستلزم الأمر تمتعه بالقوة الإستدلالية لذلك ينبغي أن يتوفر على مجموعة من الشروط من أجل إثبات فعل الإعتداء على النظام المعلوماتي، كما يجب فحصه وتقييمه، وهنا تثار مسألة سلطة القاضي في تقدير هذا الدليل حتى يقتنع به أو يرفضه.

1-2-2 الشروط الواجب توفرها في الدليل الإلكتروني حتى يكتسب حجية إثبات الإعتداءات المنصوص عليها في المواد 394مكرر إلى 394 مكرر2.

حتى يعتد بالدليل الإلكتروني كأداة لإثبات الإعتداءات الواقعة على النظام المعلوماتي لا بد من توفره على جملة من الشروط والتي تتمثل في:

أولا: أن يكون الدليل الإلكتروني مشروعا.

ويقصد بذلك إجراءات جمع هذا الدليل، فإذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليه يترتب عليها بطلانه كونه غير صالح لإثبات تلك الإعتداءات،[38] ومثال ذلك اللجوء إلى الإكراه المادي والمعنوي ضد الجاني من أجل الحصول على شفرة الولوج إلى النظام المعلوماتي.

ثانيا: أن يكون الدليل الإلكتروني يقينيا.

إذ يجب أن يكون مبني على الجزم واليقين غير قابل للشك وبعيد تماما عن التخمين، وفي هذا الصدد يرى الرأي الغالب في الفقه الكندي أن مخرجات الحاسوب تتوفر على درجة عالية من اليقينية، فأفضل أدلة الإثبات هي تلك التي يتم إستخراجها من البيانات المخزنة بالحاسوب.[39]

ثالثا: إمكانية مناقشة الدليل الإلكتروني.

تنص الفقرة الثانية من المادة 212 من قانون الإجراءات الجزائية بأنه " لايسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه" فما جاء في هذه الفقرة يلزم القاضي بأن لا يبني حكمه إلا على الأدلة التي تم عرضها في الجلسة وتمت مناقشتها، ونفس الأمر ينطبق على الدليل الإلكتروني أيا كان شكله سواء في شكل بيانات مطبوعة أو يتم عرضها على شاشة الحاسوب فلا بد من عرضها في الجلسة حتى تكون محلا للمناقشة.

وذلك حتى يكون إقتناع القاضي مؤسس ولا يعتمد على رأي الغير إلا إذا كان هذا الغير من الخبراء في المجال المعلوماتي، فإذا ما قرر الإستناد إلى التقارير المعدة من طرف هؤلاء الخبراء فيكون حكمه متولد من عقيدته وليس من تقرير الخبراء.[40]

2-2-2 سلطة القاضي في قبول الدليل الإلكتروني لإثبات الإعتداءات المنصوص عليها في المواد 394 مكرر إلى 394 مكرر2.

بعد أن يتأكد القاضي من توفر الدليل الإلكتروني على الشروط التي سبقت الإشارة إليها تأتي عملية تقديره والتي تعتمد في أساسها على مبدأ الإقتناع الشخصي للقاضي، لكن الإشكال الذي يطرح نفسه في هذه النقطة هو أنه إذا كان الدليل هذا الدليل هو الأنسب والأفضل لإثبات الإعتداءات الواقعة على النظام المعلوماتي باعتباره يتناسب مع البيئة الإلكترونية، فطبيعة الدليل الإلكتروني تجعله لا يقوى على فهمه إلا الخبير المختص في المجال المعلوماتي أما القاضي فبصعب عليه فهمه وذلك يرجع بطبيعة الحال إلى نقص الخبرة والمعرفة لديه في المجال التقني فما مدى تأثير ذلك على السلطة التقديرية للقاضي في قبول هذا الدليل؟

في هذه الحالة ينبغي التمييز بين فرضين أساسيين، يتمثل الفرض الأول في القيمة العلمية للدليل الإلكتروني والتي تقوم على أسس وحقائق علمية جد دقيقة وثابتة لذلك يصعب بل يستحيل على القاضي أن يتناولها بالفحص،[41] لذلك ليس بإمكان القاضي الفصل فيها بل القول فيها لأهل الخبرة باعتبارهم أصحاب الرأي الحاسم فيها فإذا ما توفرت في الدليل الإلكتروني شروط الكفاءة والمصداقية والموثوقية العلمية فلا يكون أمام القاضي سوى قبوله ولا يمكنه رده أو التشكيك فيه كونه يمثل إخبارا صادقا عن وقوع هذه الإعتداءات.[42]

أما الفرض الثاني فيتمثل في الظروف والملابسات التي وجد فيها الدليل الإلكتروني والتي تندرج ضمن السلطة التقديرية للقاضي إذ بإمكانه طرح هذا الدليل واستبعاده إذا كان لا يستقيم مع ظروف هذه الإعتداءات،[43]لذلك مهما كانت قطعية الدليل الإلكتروني في إثبات الإعتداءات الواقعة على النظام المعلوماتي إلا أنه من الضروري إخضاعها للسلطة التقديرية للقاضي من أجل تكوين إقتناعه بها.

خاتمة:

في ختام هذه الورقة البحثية والتي تطرقنا من خلالها لموضوع يكتسي أهمية بالغة كونه يتعلق بإحدى الجرائم الواقعة ضمن بيئة المعالجة الآلية للمعطيات، حيث أنه لا ينجم عن إرتكابها أية آثار مادية يمكن الإستدلال بها لأجل إثبات أن النظام قد تعرض لإنتهاكات مست بسلامة أسراره.

وبما أن صور الإعتداء على النظام تعتبر جرائم قائمة بذاتها تم النص عليها بموجب نصوص قانونية، وحتى لا يتمكن مرتكبوها من الإفلات من دائرة العقاب تم الإعتماد على دليل إلكتروني

مناسب لها نظرا لطابعه العلمي والتقني إضافة إلى صعوبة التخلص منه وكذا إمكانية إستخراج عدة نسخ منه بنفس القوة والحجية الذي جعله الأنسب والأفضل لإثبات تلك الإعتداءات إذ بإمكان القاضي إعتماده دون حرج، أما عن جملة التوصيات التي يمكن تقديمها بشأن الموضوع فتتمثل في:

-جعل المشرع تخريب نظام إشتغال المنظومة مجرد ظرف مشدد لفعل الدخول أو البقاء غشا، مما يعني أنه في حالة ما إذا كان الدخول مصرحا به ومشروعا لا يمكن تفعيل الفقرة الثالثة من المادة 394 مكرر، الشيئ الذي يترتب عليه إفلات الإعتداءات العمدية على سير النظام من العقاب لذلك كان من الأحرى بالمشرع الجزائري أن ينص على هذا الإعتداء بصورة مستقلة، فحبذا لو يتم تدارك هذا القصور.

-بما أن الدليل الإلكتروني يخضع في تقديره للسلطة التقديرية للقاضي وحتى يتمكن هذا الأخير من فهمه بشكل فني وتقني وجب تكوين قضاة مختصين وإخضاعهم لتدريبات في المجال التقني، تمكنهم من التعامل مع تقنية المعلومات وكذا الأدلة المستخرجة من الحاسب الآلي بكل خبرة ودقة.

---

[1] هو أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المترابطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، أنظر المادة 2 من القانون 09-04 مؤرخ في 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج،رج،ج، عدد 47 الصادر في 16 غشت 2009.

[2] قانون رقم 04-15 مؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، ج،ر،ج،ج عدد 71 الصادر بتاريخ 10 نوفمبر 2004.

[3] عباس كريمة، 2017، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مجلة البيبان للدراسات القانونية والسياسية،المجلد2، العدد 4، ص122، الجزائر.

[4] Jean pradel, juin 1990, les infraction relatives à l'informatique, revue internationale de droit comparé, vol 42,N^0 2, p824.

[5] عباس كريمة، مرجع سابق، ص 123.

6 الجمادي خالد سليمان عبد الله ، 2019،جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري –دراسة مقارنة- رسالة مقدمة للحصول على درجة الماجستير، كلية الحقوق، جامعة قطر ، ص 79.

[7] الكبيجي بهاء فهمي ، 2013، مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني مع الأحكام العامة للجريمة، رسالة مقدمة للحصول على درجة الماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن، ص 34.

[8] بوكر رشيدة، 2021، الدخول أو البقاء داخل نظم معلومات المؤسسة الاقتصادية "بين عدم التصريح والحماية الجزائية" مجلة قانون العمل والتشغيل، المجلد 6، العدد 1، ص 214، الجزائر.

[9] محمد نصر محمد، 2015، الوسيط في الجرائم المعلوماتية، ط 1، مركز الدراسات العربية للنشر والتوزيع، جمهورية مصر العربية، ص 74.

[10] مطشر دلال لطيف ،2018، جريمة الإعتداء على المواقع الإلكترونية –دراسة مقارنة- مجلة جامعة بابل للعلوم الإنسانية، مجلد 26، العدد 9، ص 401، العراق.

[11] بن شهرة شول، 2010، آليات مكافحة الجريمة المعلوماتية –مواقع التجارة الإلكترونية نموذجا- مجلة دراسات، العدد 13، ص 209، الجزائر.

[12] دردور نسيم، 2012-2013، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، كلية الحقوق، جامعة منتوري قسنطينة، الجزائر، ص 33.

[13] بشان عبد النور، 2017-2018، الجوانب الموضوعية لمعالجة الجريمة المعلوماتية، أطروحة لنيل شهادة دكتوراه، كلية الحقوق، حامعة الجزائر 1، الجزائر، ص 338.

[14] حمودي ناصر، 2015، الحماية الجنائية للتجارة الإلكترونية، مذكرة لنيل شهادة الماجستير، كلية الحقوق، جامعة الجزائر1، الجزائر، ص 90.

[15] سعيداني نعيم، 2020-2021، الحماية الجنائية للحق في الخصوصية في مجال المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج لخضر، الجزائر، ص 397.

[16] بشان عبد النور، مرجع سابق، ص 340.

[17] Ibtissem Maalaoui,2011, les infractions portant atteinte à la sécurité du système informatique d'un entreprise, mémoire présenté à la faculté des études supérieures en vue de l'obtention du grade de maitrise en droit (L.L.M) option droit des affaires, université de montréal, france, p74.

[18] سعيداني نعيم، مرجع سابق، ص 402.

[19] بشان عبد النور، مرجع سابق، ص ص 348،349،350.

[20] غلاب فايز محمد راجح ، 2010-2011، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة مقدمة من أجل الحصول على شهادة دكتوراه، كلية الحقوق، جامعة الجزائر 1، الجزائر، ص 232.

[21] عبد الحميد عائشة، 2020، الدليل الرقمي كحجية للإثبات أمام القاضي الجزائي في المعاملات الإلكترونية، مجلة صوت القانون، المجلد 7، العدد 1، ص 484، الجزائر.

[22] الأسدي كريم منشد خنياب، 2019، جرائم النصب والإحتيال وعلاقتهما بالجرائم المشابهة لهما في القانون الجنائي، ط1، الآن ناشرون وموزعون، الأردن، ص 305.

[23] الرشيد عادل بن عبد العزيز بن صالح ، 2017، قرائن الجريمة الإلكترونية وأثرها في الإثبات، ط1، دار كنوز إشبيليا للنشر والتوزيع، الرياض، ص70.

[24] فلاح عبد القادر، آيت عبد المالك نادية، 2019، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، ص 1700، الجزائر.

[25] عبد العال أسامة حسين محي الدين، 2021، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية دراسة تحليلية مقارنة، مجلة البحوث القانونية والإقتصادية، العدد 76، ص 643.

[26] عادل حامد بشير، 2020-2021، الإثبات الجنائي للجريمة الإلكترونية، ط1، دار النهضة العربية، القاهرة، ص 53.

[27] محمد كمال، 2022، الإرهاب السيبراني عندما يستخدم الإرهابي الكيبورد بدلا من القنبلة ، د،ط، دار كليم للطباعة والنشر، الإمارات، ص 77.

[28] الأسدي كريم منشد خنياب ، مرجع سابق، ص 306.

[29] بلجراف سامية، 2021، سلطة القاضي الجزائي في قبول وتقدير الدليل الرقمي، مجلة الدراسات القانونية المقارنة، المجلد 7، العدد 1، ص 683، الجزائر.

[30] سعيداني نعيم، مرجع سابق، ص 436.

[31] خميس السيد إسماعيل، 2016، الإثبات أمام القضائين الإداري والعادي، ط1، دار محمود للنشر، القاهرة، ص 11.

[32] بن فردية محمد، 2014، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي –دراسة مقارنة- المجلة الأكاديمية للبحث القانوني، المجلد 9، العدد 1، ص 282، الجزائر.

[33] ضريفي نادية، دراج عبد الوهاب، 2019، سلطات القاضي الجنائي في تقدير الدليل الإلكتروني المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، ص 125، الجزائر.

[34] عبد العال أسامة حسين محي الدين ، مرجع سابق، ص 696.

[35] بدري فيصل، 2017-2018، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق، جامعة الجزائر 1، الجزائر، ص 238.

[36] مجذوب لامية ، 2019، إجراء التفتيش في التزوير الإلكتروني، مجلة التواصل في الاقتصاد والإدارة والقانون، المجلد 25، العدد 3، ص 116، الجزائر.

[37] أمر رقم 66-155 مؤرخ في 8 يونيو 1966، يتضمن قانون الإجراءات الجزائية، ج،ر،ج،ج، عدد 48، الصادر في 10 يونيو 1966.

[38] محمودي نور الهدى 2017، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، المجلد 4، العدد 11، ص 920، الجزائر.

[39] بن فردية محمد، مرجع سابق، ص 281.

[40] محمود نور الهدى ، مرجع سابق، ص 919.

[41] بن خليفة إلهام، 2015-2016، الحماية الجنائية للمحررات الإلكترونية من التزوير، أطروحة مقدمة لنيل درجة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، ص 276.

[42] سعيداني نعيم، مرجع سابق، ص 463.

[43] يعيش تمام شوقي، 2019، الجريمة المعلوماتية-دراسة تأصيلية مقارنة- ط1، مطبعة الرمال، الجزائر، ص 54.

قائمة المصادر والمراجع:

أولا: باللغة العربية.

1-النصوص القانونية:

- قانون رقم 04-15 مؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، ج،ر،ج،ج عدد 71 الصادر بتاريخ 10 نوفمبر 2004.

- أمر رقم 66-155 مؤرخ في 8 يونيو 1966، يتضمن قانون الإجراءات الجزائية، ج،ر،ج،ج، عدد 48، الصادر في 10 يونيو 1966.

2-الكتب:

- الرشيد عادل بن عبد العزيز بن صالح ، 2017، قرائن الجريمة الإلكترونية وأثرها في الإثبات، ط1، دار كنوز إشبيليا للنشر والتوزيع، الرياض.

- الأسدي كريم منشد خنياب، 2019، جرائم النصب والإحتيال وعلاقتهما بالجرائم المشابهة لهما في القانون الجنائي، ط1، الآن ناشرون وموزعون، الأردن.

- خميس السيد إسماعيل، 2016، الإثبات أمام القضائين الإداري والعادي، ط1، دار محمود للنشر، القاهرة.

- عادل حامد بشير، 2020-2021، الإثبات الجنائي للجريمة الإلكترونية، ط1، دار النهضة العربية، القاهرة.

- محمد نصر محمد، 2015، الوسيط في الجرائم المعلوماتية، ط 1، مركز الدراسات العربية للنشر والتوزيع، جمهورية مصر العربية.

- محمد كمال، 2022، الإرهاب السيبراني عندما يستخدم الإرهابي الكيبورد بدلا من القنبلة ، د,ط، دار كليم للطباعة والنشر، الإمارات.

- يعيش تمام شوقي، 2019، الجريمة المعلوماتية-دراسة تأصيلية مقارنة- ط1، مطبعة الرمال، الجزائر.

3-الرسائل الجامعية:

أ-رسائل الدكتوراه:

- بن خليفة إلهام، 2015-2016، الحماية الجنائية للمحررات الإلكترونية من التزوير، أطروحة مقدمة لنيل درجة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر.

- بشان عبد النور، 2017-2018، الجوانب الموضوعية لمعالجة الجريمة المعلوماتية، أطروحة لنيل شهادة دكتوراه، كلية الحقوق، جامعة الجزائر 1، الجزائر.

- بدري فيصل، 2017-2018، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق، جامعة الجزائر 1، الجزائر.

- سعيداني نعيم، 2020-2021، الحماية الجنائية للحق في الخصوصية في مجال المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج لخضر، الجزائر.
- غلاب فايز محمد راجح ، 2010-2011، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة مقدمة من أجل الحصول على شهادة دكتوراه، كلية الحقوق، جامعة الجزائر 1، الجزائر.

ب-رسائل الماجستير:
- الكبيجي بهاء فهمي ، 2013، مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني مع الأحكام العامة للجريمة، رسالة مقدمة للحصول على درجة الماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن.
- الجمادي خالد سليمان عبد الله ، 2019،جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري –دراسة مقارنة- رسالة مقدمة للحصول على درجة الماجستير، كلية الحقوق، جامعة قطر.
- حمودي ناصر، 2015، الحماية الجنائية للتجارة الإلكترونية، مذكرة لنيل شهادة الماجستير، كلية الحقوق، جامعة الجزائر1، الجزائر.
- دردور نسيم، 2012-2013، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، كلية الحقوق، جامعة منتوري قسنطينة، الجزائر.
4-المقالات في مجلة علمية:
- بن شهرة شول، 2010، آليات مكافحة الجريمة المعلوماتية –مواقع التجارة الإلكترونية نموذجا- مجلة دراسات، العدد 13، الجزائر.
- بن فردية محمد، 2014، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي –دراسة مقارنة- المجلة الأكاديمية للبحث القانوني، المجلد 9، العدد 1، الجزائر.
3- بوكر رشيدة، 2021، الدخول أو البقاء داخل نظم معلومات المؤسسة الاقتصادية "بين عدم التصريح والحماية الجزائية" مجلة قانون العمل والتشغيل، المجلد 6، العدد 1، الجزائر.
- بلجراف سامية، 2021، سلطة القاضي الجزائي في قبول وتقدير الدليل الرقمي، مجلة الدراسات القانونية المقارنة، المجلد 7، العدد 1، ص 683، الجزائر.

- ضريفي نادية، دراج عبد الوهاب، 2019، سلطات القاضي الجنائي في تقدير الدليل الإلكتروني المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، الجزائر.
- عباس كريمة، 2017، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مجلة البيبان للدراسات القانونية والسياسية،المجلد2، العدد 4، الجزائر.
- عبد الحميد عائشة، 2020، الدليل الرقمي كحجية للإثبات أمام القاضي الجزائي في المعاملات الإلكترونية، مجلة صوت القانون، المجلد 7، العدد 1، الجزائر.
- عبد العال أسامة حسين محي الدين، 2021، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية دراسة تحليلية مقارنة، مجلة البحوث القانونية والإقتصادية، العدد 76.
- فلاح عبد القادر، آيت عبد المالك نادية، 2019، التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، الجزائر.
- محمودي نور الهدى 2017، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، المجلد 4، العدد 11، الجزائر.
- مطشر دلال لطيف ،2018، جريمة الإعتداء على المواقع الإلكترونية –دراسة مقارنة- مجلة جامعة بابل للعلوم الإنسانية، مجلد 26، العدد 9، ص 401، العراق.
- مجذوب لامية ، 2019، إجراء التفتيش في التزوير الإلكتروني، مجلة التواصل في الاقتصاد والإدارة والقانون، المجلد 25، العدد 3، الجزائر.

ثانيا: باللغة الأجنبية.

1-Theses:
- Ibtissem Maalaoui,2011, les infractions portant atteinte à la sécurité du système informatique d'un entreprise, mémoire présenté à la faculté des études supérieures en vue de l'obtention du grade de maitrise en droit (L.L.M) option droit des affaires, université de montréal, france.

2-Articles:
- Jean pradel, juin 1990, les infraction relatives à l'informatique, revue internationale de droit comparé, vol 42,N^0 2.