

القرصنة الرقمية كعائق تقني لنظام التقاضي الإلكتروني

Digital piracy as a technical obstacle to the electronic litigation system

مزوري إكرام¹

المركز الجامعي- مغنية، الجزائر

Ikram97mzouri@gmail.com

الحاج علي بدر الدين

المركز الجامعي- مغنية، الجزائر

Badro85@live.com

ملخص:

يعد التقاضي الإلكتروني نتاجا للتطور التكنولوجي و المعلوماتي ، حيث أصبح الحديث عن تقديم الخدمات والمعلومات في صورة رقمية، بعيدا عن الشكل التقليدي أي الورقي، فالتقاضي الإلكتروني يقوم على استخدام وسائل الإتصال الحديثة و يعتمد على برامج و وسائط إلكترونية لتبادل المعلومات و البيانات المتعلقة بالخصومة .

لكن قد تعترض سيرورة المحاكمة الإلكترونية عراقيل تقنية، أهم صورها القرصنة الرقمية، إذ يتم إختراق الوسائل التقنية المعتمدة في التقاضي الإلكتروني مثل : البريد الإلكتروني، و ذلك بهدف تزوير البيانات أو التشهير بسمعة أحد الخصوم و كشف أسرار الدعوى، لذلك كان من الضروري تكثيف الحماية التقنية للأنظمة المعتمدة في التقاضي الإلكتروني.

الكلمات المفتاحية : القرصنة الرقمية، التقاضي الإلكتروني، الجريمة الإلكترونية، الوسائط الإلكترونية، المحكمة الإلكترونية.

Abstract: Electronic litigation is a product of technological and information development, as it has become a matter of providing services and information in a digital form, away from the traditional form, i.e. paper. Electronic litigation is based on the use of modern means of communication and depends on programs and electronic media to exchange information and data related to litigation.

مزوري إكرام¹

However, the electronic trial process may encounter technical obstacles, the most important of which is digital piracy, as the technical means adopted in electronic litigation, such as: e-mail, are breached, with the aim of falsifying data or defaming the reputation of one of the opponents and revealing the secrets of the case, so it was necessary to intensify technical protection For the systems adopted in electronic litigation.

key words :digital piracy; electronic litigation; electronic crime; electronicmedia; electronic court.

مقدمة:

مس التطور التكنولوجي مختلف المجالات، الإجتماعية الإقتصادية و التجارية، ولم يقتصر عليها فحسب بل إمتد ليشمل حل النزاع القضائي بواسطة الطرق التقنية و الفنية.¹ وتعتبر سلبيات التقاضي التقليدي و المتمثلة في طول إجراءاته و كثرة الأعباء المالية و المصاريف، أحد دواعي إعتقاد هذا نظام التقاضي الإلكتروني، والذي يراد به: " إستخدام وسائل تقنية الإتصال المرئية و السمعية الإلكترونية في مباشرة الدعوى القضائية و حتى في الفصل في المنازعات القضائي عن بعد." ولقد حمل هذا النظام الجديد في طياته العديد من الميزات و الإيجابيات، حيث ترتب عنه إختفاء الوثائق الورقية و ظهور الوثائق الإلكترونية، الأمر الذي نجم عنه خفض التكاليف و الأعباء المالية ضف إلى ذلك تجنب ضياع و تلف الأوراق كذلك الوثائق و السندات الإلكترونية تضمن سهولة التعرف على التغيرات الطارئة عليها،² كذلك تسليم المستندات و العرائض إلكترونيا عبر شبكة الإتصال ويطلق على هذه العملية مصطلح التسليم المعنوي، أو التنزيل عن بعد كذلك سرعة إجراءات التقاضي، كما قد حلت وسائل الدفع الإلكتروني محل الدفع النقدي العادي.³

كما قد كان لجائحة كورونا دور في التطبيق الواسع لنظام التقاضي الإلكتروني، حيث قامت العديد من دول العالم من بينها الجزائر بإعتماده تماشيا مع الإجراءات التي أقرتها قوانين هذه الدول، حفاظا على الصحة العامة و حياة الأفراد. لكن إضفاء الصبغة الرقمية على مرفق القضاء، جعله عرضة لإعتداءات تمس بأنظمتها و برامجها الإلكترونية، أهمها جريمة القرصنة الرقمية .

كما أصبحت أسرار المتقاضين و معلوماتهم الشخصية محل تجسس من طرف قراصنة الرقمنة، فقد كلفت هذه الأفعال غير المشروعة خسائر مادية و معنوية فادحة تمس بالعدالة و حق الأفراد في حماية معطيات و معلوماتهم الشخصية.

ويكتسي هذا الموضوع أهمية بالغة كونه يسلط الضوء على جريمة خطيرة تستهدف نظام التقاضي الإلكتروني و تعرقل سير إجراءاته، كما تلحق ضرار بالغا بالأجهزة و البرامج المستعملة في هذا النوع من التقاضي، قد تصل في بعض الحالات إلى تخريب المنظومة المعلوماتية بشكل نهائي، كما تهدد حق المتقاضين في المحاكمة العادلة و تجعل أسرارهم الشخصية العائلية أو التجارية عرضة للتجسس و الإطلاع من طرف الغير.

كما يسعى هذا البحث إلى تبيان المقصود بالقرصنة الرقمية و التطرق للخصائص التي تميزها، كما نبين من خلاله تصنيفات قرصنة الرقمنة و سماتهم إضافة إلى صور القرصنة الرقمية التي تستهدف نظام التقاضي الإلكتروني، كما تسمح هذه الدراسة بإيجاد حلول لهذا النوع من الإجرام ، والبحث عن السبل الفنية و التكنولوجية للتصدي له و سن قوانين موضوعية و إجرائية تتماشى و خصوصية جريمة القرصنة الرقمية .

و إنطلاقا مما سبق فالإشكال المطروح يتمثل في :

- كيف يتم الإعتداء على نظام التقاضي الإلكتروني من خلال القرصنة الرقمية؟
- ماهي سبل الحماية الفنية لتأمين نظام التقاضي الإلكتروني من القرصنة الرقمية؟

و للإجابة على الإشكالية المطروحة أعلاه إتبعنا المنهج الوصفي التحليلي للتعريف بالقرصنة الرقمية و إبراز خصائصها و تصنيفات القرصان الرقمي و سماته، كذلك صور القرصنة الرقمية التي تستهدف نظام التقاضي الإلكتروني ، و إستراتيجية تأمين هذا النظام منها.ومن أجل الإجابة عن هذه الإشكالية المطروحة أعلاه نقترح الخطة الآتية:

المبحث الأول: ماهية القرصنة الرقمية.

المبحث الثاني: إستراتيجية التأمين الفني من لقرصنة الرقمية الواقعة على نظام التقاضي الإلكتروني.

المبحث الأول: ماهية القرصنة الرقمية

لقد إقتصر لفظ القرصنة سابقا على القرصنة البحرية التي تتم في البحار من أجل السطو على السفن خاصة المحملة بالبضائع والأمتعة من أجل سرقة حمولتها، لكن في ظل التطور الهائل للعلم والتكنولوجيا و ظهور الحاسبات الآلية وشبكة الأنترنت الأمر الذي ترتب عليه بروز نوع جديد من القرصنة أطلق عليه مصطلح القرصنة الرقمية التي تتم في بيئة إفتراضية ترتكب من طرف مجرم يدعى بالقرصان الرقمي، ونظرا لحدثة هذا النوع من الإجرام الذي ساهم في تعدد التعاريف التي حظيت بها جريمة

القرصنة الرقمية كذلك الخصائص التي تتميز بها وأصناف و سمات مرتكبيها والذي سيتم التطرق إليه في المطلب الأول، أما في المطلب الثاني فسيتم تبيان صور القرصنة الرقمية التي تستهدف نظام التقاضي الإلكتروني.

المطلب الأول: مفهوم القرصنة الرقمية

تعد القرصنة الرقمية صورة من صور الجريمة المعلوماتية التي تستهدف نظم المعلومات، و تعد من أخطر أنواع هذا الإجرام، لما فيها من إعتداء على خصوصية الأفراد و سرية المعلومات، وسيتم من خلال هذا المطلب الأول التطرق للتعريفات الممنوحة للقرصنة الرقمية و ذلك من خلال الفرع الأول، ثم بعد ذلك إبراز خصائصها في الفرع الثاني، أما الفرع الثالث سيخصص لتبيان تصنيفات القائمين بها و أهم سماتهم.

الفرع الأول: تعريف القرصنة الرقمية

مصطلح القرصنة الرقمية يتكون من كلمتين: " القرصنة والرقمية" ، القرصنة التي ظهرت منذ القدم لكن كلمة الرقمية فهي لفظ جديد نوعا ما و تقني يحتمل عدة معاني وتأويلات، ولإحاطة بتعريف مصطلح القرصنة الرقمية ينبغي تعريفها من الناحية الإصطلاحية (أولا) ثم من الجانب الفقهي (ثانيا) إضافة إلى تعريفها من الناحية القانونية (ثالثا).

أولا: التعريف الإصطلاحي للقرصنة الرقمية: يتطلب مصطلح القرصنة الرقمية تعريفا من الناحية الإصطلاحية من أجل ضبط مفهومها بشكل دقيق.

تعريف القرصنة إصطلاحا: هيكل فعل غير مشروع يرتكب ضد سفينة أو طائرة خاصة في البحار العالية أو ضد الأشخاص أو الأموال في السفينة ذاتها أو في الطائرة ذاتها بغية تحقيق منافع خاصة.

هذا هو التعريف الإصطلاحي التقليدي لجريمة القرصنة التي يتم إرتكابها في البئة التقليدية والتي تستهدف السفينة أو الطائرة أما الإصطلاح الحديث فيقصد بالقرصنة : إختراق أجهزة الحاسوب عبر شبكة الأنترنت من طرف القرصان الرقمي.

تعريف الرقمية إصطلاحا: يراد بكلمة الرقمية من الجانب الإصطلاحي : هي تقنية حديثة لتدوين وتثبيت المعلومات عن طريق تخزينها و إستعادتها بواسطة جهاز الحاسوب، فهي تعرض من خلاله وترتبط به إرتباطا وثيقا سواء على مستوى الإنتاج أو التلقي.⁴

فمن خلال تعريف كل كلمة على حدة نصل إلى التعريف الشامل لجريمة القرصنة الرقمية: يقصد بها الإستعمال الذي يتم بواسطة وسائل الإتصال وتكنولوجيات المعلومات وفق صورة غير مشروعة، والتي تستهدف أنظمة المعالجة الآلية للبيانات بغية كشف البيانات الخاصة والسرية أو القيام بتغييرها أو إتلافها.⁵

كما يصطلح على القرصنة الرقمية أو الإلكترونية باللغة الإنجليزية Hacking والتي تعني قيام أحد الأشخاص غير المصرح لهم بالدخول إلى نظام التشغيل الخاص بجهاز الحاسب الآلي بطريقة غير شرعية ولأغراض غير سوية مثل التجسس أو السرقة أو التخريب أو التدمير، حيث يتمكن الشخص (الهاكرز) من أن ينسخ أو يمسح أو يضيف ملفات أو برامج.⁶

ثانيا: التعريف الفقهي لجريمة القرصنة الرقمية: ظهرت عدة تعاريف فقهية تناولت هذه الجريمة المستحدثة، وقد ثار خلاف فيما بين هذه التعاريف والأمر راجع لحدثة هذا النوع من الإجرام، صنف إلى ذلك الاختلاف الذي طال تسمية هذه الجريمة، فهناك من يسميها بجرائم القرصنة الرقمية وهناك من ينعتها بجريمة القرصنة الإلكترونية أو المعلوماتية.

- أ- الإتجاه الأول: جانب من الفقه عرفها على أنها عملية إختراق لأجهزة الحاسوب تتم عبر شبكة الأنترنت .
- ب- الإتجاه الثاني: عرفها هذا الإتجاه بأنها ليست سوى عملية دخول غير مصرح به إلى أجهزة الغير وشبكاتهم الإلكترونية.⁷

ونتيجة لانتشار الإجرام الرقمي سارعت الدول في تجريمه وسن نصوص تتلائم وخصوصيته.

ثالثا: التعريف التشريعي لجريمة القرصنة الرقمية: تعتبر القرصنة الرقمية صورة من صور الجريمة المعلوماتية التي أفرزتها الثورة التكنولوجية وظهور وسائل إتصال جديدة لم تكن معروفة في السابق، وعد عملت معظم الدول جاهدة على وضع قانون خاص ينظم الجرائم الإلكترونية بمختلف صورها، من أجل الحد من المشاكل الناجمة عن هذه الأفعال غير المشروعة التي يعتمد في ارتكابها على أجهزة الحاسوب أو أية وسيلة من وسائل تقنية المعلومات.⁸

- أ- التشريع الفرنسي

لم يورد المشرع الفرنسي تعريفا لجريمة القرصنة الرقمية، لكنه جرم الإعتداء على أنظمة معالجة البيانات والتي تضمنها الفصل الثالث من الباب الثاني من قانون العقوبات الفرنسي و من أمثلة هذه الجرائم : إدخال أو مسح أو تغيير معلومات بطريق الغش والتي

تناولتها المادة 223-3 إضافة إلى تجريمه بعض الإعتداءات التي تستهدف البيانات و المعلومات المعالجة إلكترونيا وتمس بالمصالح العليا للدولة من المادة 411-6 إلى المادة 411-10.⁹

ب- التشريع الجزائري

من خلال إستقراء نصوص قانون العقوبات فإننا لانجد مصطلح جريمة القرصنة الرقمية، بل الأكثر من ذلك لم يستعمل المشرع الجزائري لفظ الجريمة المعلوماتية أو الإلكترونية، بل إعتد تسمية جرائم المساس بأنظمة المعالجة الآلية للمعطيات، من خلال إستحدثه للفصل السابع مكرر بموجب تعديله لقانون العقوبات بالقانون رقم 14.04¹⁰ والمعنون بالمساس بأنظمة المعالجة الآلية للمعطيات وذلك من المادة 394 مكرر إلى غاية المادة 394 مكرر 7.

إضافة إلى قانون العقوبات نص المشرع الجزائري على الجرائم التي ترتكب في بيئة رقمية من خلال القانون رقم 04.09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بالضبط المادة 2 منه حيث أطلق عليها تسمية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، فقد عرفتها المادة السالفة الذكر على أنها : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية.

ففي هذا القانون إستخدم المشرع لفظ مغاير عن اللفظ الذي إعتده في قانون العقوبات، فمن خلال المادة 2 من القانون رقم 04.09 يلاحظ أن المشرع لم يحصر الجرائم الرقمية، بل فتح المجال أمام أي جريمة ذات طابع تقني رقمي يتم أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

تمتاز القرصنة الرقمية بجملة من الخصائص والتي سيتم التطرق إليها في الفرع الثاني.

الفرع الثاني: خصائص القرصنة الرقمية

طالما أن جريمة القرصنة الرقمية ليست إلا صورة من صور الجريمة الإلكترونية، فهي تتميز بذات الخصائص التي تتسم بها هذه الأخيرة.

أولا : الحاسب الآلي أداة لإرتكاب الجريمة: القرصان الرقمي يرتكب جريمته بواسطة احاسب الآلي، والذي يكون موصولا بشبكة الأنترنت فيقوم بالإعتداء بواسطته على برامج وبيانات ومعلومات الحاسب الآلي أو مايصطلح عليه بالكمبيوتر.

ثانيا : صعوبة إكتشاف جريمة القرصنة الرقمية: أهم مايميز هذه الجريمة هو صعوبة إكتشافها، وذلك لعدة أسباب منها: عدم إنتباه الضحية أصلا لوقوع الجريمة عليه، كون الجاني يمتلك مهارات تقنية عالية، فينفذ الجريمة بكل دقة مثال ذلك : مثال ذلك إرسال فيروسات و سرقة المال المعلوماتي.¹¹

ثالثا : جريمة القرصنة الرقمية جريمة عابرة للحدود: تتصف هذه الجريمة بكونها ذات طابع دولي، فهي لا تنحصر في مكان أو دولة معينة، فقد تقع هذه الجريمة والجاني يتواجد بدولة والمجني عليه يقيم بدولة أخرى ، بمعنى القرصان الرقمي يرتكب فعله غير المشروع في دولة والمتمثل في فعل القرصنة والإختراق لنظم المعالجة الآلية للمعطيات، لكن النتيجة الإجرامية المترتبة عن فعله المجرم تتحقق في دولة أخرى.

رابعا: جريمة القرصنة الرقمية صعبة الإثبات: ترجع صعوبة إثبات هذه الجريمة إلى عدة أسباب منها مايتعلق بطبيعة الوسائل المستعملة لإرتكاب القرصنة الرقمية، فالقرصان الرقمي يتصف بالهدوء واللاعنف، فلا يستعمل السلاح لإتكاب جريمته بل يعتمد في ذلك على برامج رقمية وأدوات إلكترونية لهذا سميتم بالجريمة الناعمة، خلافا للجريمة التقليدية التي يتسم فيها الجاني بالعنف و إستخدام السلاح لتحقيق أهدافه الإجرامية.

ومن بين أسباب صعوبة إكتشاف هذه الجريمة هو تستر المجني عليه عن الفعل المجرم الواقع عليه خوفا من الإبتزاز والتشهير أو عدم تغطنه للجريمة أصلا، ضف إلى ذلك طبيعة الجريمة إذ يقع الفعل غير المشروع في مكان وتحقق النتيجة الإجرامية في مكان آخر.

الفرع الثالث : تصنيفات وسمات قرصنة الرقمنة

يطلق على مرتكب جريمة القرصنة الرقمية إسم القرصان الرقمي، والذي يمكن تعريفه على أنه شخص له القدرة على التعامل من أنظمة الحاسب الآلي والشبكات بحيث تكون له القدرة على تخطي أي إجراءات أو أنظمة الحماية التي أتخذت لحماية تلك الحاسبات أو الشبكات.¹² كما يصنف هذا الأخير إلى فئات و أصناف (أولا) ونظرا لخصوصية الإجرام الرقمي الأمر الذي إنعكس على الجاني حيث يتصف بميزات تجعله مختلفا عن المجرم التقليدي (ثانيا).

أولا: تصنيف قرصنة الرقمنة: يمكن تصنيف الجناة الذين يرتكبون جريمة القرصنة الرقمية إلى فئتين أساسيتين، لكن هذا لا يمنع من وجود طوائف أخرى كون أن الإجرام الرقمي يتميز بالتطور و التغير المستمر.

أ- الفئة الأولى : الهاكرز (Hachers)

كما يصطلح عليهم بالهواة العابثون، وهم القراصنة الذين يخترقون أنظمة وبرامج الحاسوب بدافع التسلية والشغف من أجل إثبات الذات، فهم لا يملكون نوايا سيئة مثل القراصنة المحترفون (Crachers).

ب- الفئة الثانية: القراصنة المحترفون (Crachers)

هذه الفئة تعكس إعتداءاتهم ميولا إجرامية خطيرة تنبئ عن رغبتها في إحداث التخريب، ويتميز هؤلاء بقدراتهم التقنية الواسعة وخبرتهم في مجال أنظمة الحاسوب والشبكات وهم أكثر خطورة من الصنف الأول فقد يحدثون أضرارا كبيرة.¹³

لكن هذا فيما يتعلق بالتصنيف العام للقراصنة في البيئة الرقمية، أما فيما يتعلق بجريمة القرصنة الرقمية التي تستهدف نظام التقاضي الإلكتروني، فالأمر يختلف فعادة يكون القائم بهذا الفعل الإجرامي أحد أطراف الدعوى الذي يسعى لتحقيق مصلحة غير مشروعة من خلال إختراقه للأنظمة المعتمدة في المحاكمة الإلكترونية، إذ يتمتع هذا الأخير بقدر من الذكاء و الخبرة التي يستطيع من خلالها تنفيذ جريمته أو قد يعهد أحد الخصوم بالقيام بهذه الجريمة لأحد الأشخاص ذوو الخبرة في المجال المعلوماتي و التقني، فيقوم القرصان الرقمي في هذه الحالة بتنفيذ ماطلب منه سواء تعلق الأمر بتزوير البيانات و التواقيع الإلكترونية و إحداث تغيرات في المعلومات المقدمة من الطرف الآخر أو حذفها نهائا.

ثانيا: مميزات قرصنة الرقمنة: يتسم القرصان الرقمي بعدة سمات تميزه عن المجرم في البيئة التقليدية والتي سيتم التطريق إليها كالتالي:

أ-القرصان الرقمي مجرم ذكي ومحترف:المجرم يقترب جريمته بأسلوب هدائي، مما يجعل هذه الجرائم تصنف ضمن تقنيات التدمير الناعمة،فهو يقوم بحو البيانات و المعلومات وتعطيلها من دون عنف.¹⁴

ب-القرصان الرقمي مجرم عائد إلى الإجرام: يتميز القرصان الرقمي بنزعتة للعودة إلى الإجرام، بهدف سد الثغرات التي أدت إلى إكتشاف أمره وزجه في السجن، حيث يستفيد من أخطائه من أجل تطوير قدراته وإمكاناته الفنية والتقنية.¹⁵

ج-القرصان الرقمي مجرم متخصص:من خلال بعض القضايا تم التوصل إلى أن العديد من المجرمين متخصصين في الجريمة المعلوماتية دون غيرها من الجرائم دون غيرها من الجرائم.¹⁶

د-القرصان الرقمي يبرر إرتكاب جريمته: إذ يرى أن أفعاله مشروعة لأنه قام بها بدافع التسلية و حب المغامرة والتحدي، وأن إختراقه للأنظمة المعلوماتية أمر عادي بالنسبة له ولا يكيف على أنه جريمة رقمية.

المطلب الثاني: صور القرصنة الرقمية الواقعة على نظام التقاضي الإلكتروني

يقوم نظام التقاضي الإلكتروني على مجموعة من المقومات، منها القانونية و المقصود بها الإطار التشريعي و التنظيمي لهذا النظام الجديد، كذلك المقومات البشرية و تتمثل في الأشخاص المتخصصين في المجال القانوني و الفني و التقني، فهم من يقومون بتطبيق نظام التقاضي عن بعد، إذ يتوجب على هذا الطاقم البشري من قضاة و أمناء ضبط و محامين الإلمام بكيفيات إستعمال الوسائل الإلكترونية و حسن إستخدامها، لضمان التطبيق الجيد لهذا النظام.

ضف إلى ذلك المقومات المادية و التي نعني بها العتاد و المتطلبات الفنية للتقاضي الإلكتروني، وهي الحواسيب، شبكة الحاسب الآلي كذلك شبكة الأنترنت و البرامج الإلكترونية ، إذ تعد هذه المقومات الأخيرة محل جريمة القرصنة، إذ يتم الإعتداء على برامج الخاسوب و البرامج الإلكترونية المعتمدة في نظام التقاضي الإلكتروني،¹⁷ حيث سيتم من خلال هذا المطلب، تبيان أشكال القرصنة الرقمية التي تستهدف هذا النظام منها الإختراق و مايتفرع عنه من أفعال مجرمة و قد خصصنا له الفرع الأول، أما الفرع الثاني سأتطرق من خلاله إلى ثاني صورة و المتمثلة في التجسس المعلوماتي.

الفرع الأول: الإختراق.(Pentration)

هو القدرة على الوصول لهدف معين بطريقة غير مشروعة، عن طريق ثغرات في نظام الحماية الخاص بجهاز الحاسب الآلي المستهدف،¹⁸ وقد إستعمل المشرع الجزائري عبارة جريمة الدخول و البقاء عن طريق الغش إلى النظام المعلوماتي للدلالة على عملية الإختراق وذلك في المادة 394 مكرر¹⁹ من قانون العقوبات الجزائري. والجريمة السالفة الذكر تنقسم بدورها إلى نوعين:

النوع الأول: جريمة الدخول عن طريق الغش إلى النظام المعلوماتي

إذ يتحقق الركن المادي للجريمة من خلال عميلة الدخول إلى النظام المعلوماتي أو جزء منه،²⁰ وذلك من خلال تجاوز أنظمة الحماية الفنية، كما يلاحظ أن المشرع الجزائري لا يعاقب على الجريمة التامة فقط بل حتى على مجرد الشروع و هذا ما دلت عليه عبارة " أو يحاول ذلك" وهذا ما أكدته أيضا الماد 394 مكرر²¹ من ذات القانون،

كما يلاحظ من خلال نص المادة السالفة الذكر أن المشرع لم يشترط أن يكون النظام المعلوماتي محمي بواسطة أنظمة الحماية الفنية لتقوم الجريمة.

وبما أن نظام التقاضي الإلكتروني يعتمد على الحواسيب و شبكة الأنترنت و البرامج الإلكترونية لتبادل البيانات و الوثائق الخاصة بأطراف الخصومة، مثال ذلك البريد الإلكتروني فقد يتعرض للإختراق، بهدف الإطلاع على المعلومات و المستندات و العرائض، كما قد تستهدف عملية الإختراق نظام تبادل البيانات إلكترونيا و الذي عرفه قانون الأونسترال النموذجي بشأن التجارة الإلكترونية في المادة 2 فقرة ب: " نقل المعلومات إلكترونيا من حاسوب إلى حاسوب آخر بإستخدام معيار متفق عليه لتكوين المعلومات."

فقد يتم إختراق هذا النظام الذي تتم من خلاله المراسلات بين القاضي و أمناء الضبط و بين النيابة العامة و المحامين. كما نص المشرع على طرفين مشددين للعقوبة و المتمثلين في: إذا نجم عن الإختراق حذف أو تغيير لمعطيات المنظومة المعلوماتية أو متى ترتب عن هذا الفعل غير المشروع تخريب نظام إستغلال هذه المظومة و هو مانصت عليه المادة 394 مكرر فقرة 2 و 3 من قانون العقوبات.

النوع الثاني: جريمة البقاء غير المصرح به في النظام المعلوماتي

قد لا يكتفي القرصان الرقمي بمجرد الإختراق و الدخول إلى النظم المعلوماتية، بل يمكنه داخل هذا النظام بالرغم من علمه بعدم أحقيته في الدخول إليه و هو ما يستنتج من خلال عبارة " عن طريق الغش" الواردة في المدة السالفة الذكر، كما قد يقوم الجاني بإحداث تغييرات في معطيات المنظومة أو القيام بحذف البيانات و المعلومات الخاصة بها فتشدد العقوبة ف هذه الحالة وفقا لما تم الإشارة إليه سابقا.

-الإعتداء على المعطيات الداخلية للنظام المعلوماتي:

لقد نص المشرع على هذه الجريمة في المادة 394 مكرر 21²² من قانون العقوبات و يطلق على هذه الجريمة مصطلح الإتلاف المعلوماتي، وتعد هذه الجريمة من بين أخطر أنواع الجرائم الخاصة بالمعالجة الآلية للمعطيات، لاسيما بعد ظهور المحررات و الوثائق الإلكترونية كبديل للمستندات و المحررات الورقية،²³ فقد يقوم القرصان الرقمي متعمدا إحداث تغييرات في البيانات و المعلومات التي يحتويها النظام المعلوماتي إما بتعديلها أو إدخال معطيات إليها أو حذفها و إلتهائها نهائيا، ومثال ذلك قيام الجاني بتغيير المعلومات الموجودة في العريضة بإضافة وقائع لم تتضمنها هذه الأخيرة أو حذف وقائع كانت موجودة فعلا في العريضة، أو القيام بحذف الوثائق و المستندات التي يعتمد عليها أحد الأطراف لتدعيم مطالبه و كسب حقه، كما قد يعمد القرصان الرقمي بالتلاعب

بتواريخ الجلسات من خلال إختراقه لحاسوب أو البردي الإلكتروني الخاص بأمين الضبط.

مايجب الإشارة إليه أن المشرع الجزائري لم ينص على التزوير المعلوماتي للمحررات الرسمية أو العرفية الإلكترونية ، فقد نصت المادة 216 من قانون العقوبات على جريمة تزوير المحررات الرسمية أو العمومية من طرف الأشخاص العاديين، والتي تتم ما بتقليد أو بتزييف الكتابة أو بإصطناع إتفاقات أو نصوص أو إلتزامات أو مخالصات أو بإدراجها في هذه المحررات فيما بعد، كما تتحقق جريمة التزوير إذا تم إضافة أو إسقاط أو تزييف الشروط أو الإقرارات أو الوقائع التي أعدت هذه المحررات لتلقيها و إثباتها، وأيضا إنتحال شخصية الغير أو الحلول محلها.

فقد إكتفى المشرع بتجريم التزوير للمحررات العمومية و الرسمية في البيئة التقليدية، وهذا ما يحدث فراغا تشريعا، متى تعلق الأمر بالمحررات الرسمية الإلكترونية، التي يتم تحريرها و إرسالها و تبادلها وفقا لدعامة إلكترونية.

كذلك نفس الأمر فيما يخص جريمة تزوير التوقيع الإلكتروني²⁴، فبالرغم من أن المشرع الجزائري سن القانون رقم 04.15²⁵ المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، كما نص في القانون المدني على الإثبات بواسطة المستندات الموقعة إلكترونيا، إلا أنه لم ينص على جريمة تزوير التوقيع الإلكتروني، وفي هذه الحالة لا يمكن إسقاط القواعد التي تحكم جريمة تزوير التوقيع التقليدي، لأن ذلك يتنافى و مبدأ الشرعية، و كذلك لإختلاف محل الجريمة، كمل لايمكن تطبيق نصوص جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وذلك راجع لإختلاف المصلحة المحمية، بين الجريمتين فجريمة تزوير التوقيع الإلكتروني تهدف إلى حماية الثقة العامة في الوثيقة، أما الجريمة الثانية، فتسعى إلى الحفاظ على سرية المعلومات و سلامة سير النظام المعلوماتي.²⁶

كما قد يتم الإعتداء على التوقيع الإلكتروني ، من خلال أعمال القرصنة الرقمية، إذ يقوم القرصان الرقمي بإختراق النظام المعلوماتي وإكتشاف التوقيع و فك رموزه أو الإستلاء عليه و إستعماله دون موافقة صاحبه و بدون علمه، ويتم ذلك وفق طريقتين، إما: بالسيطرة على النظام المعلوماتي للموقع، فيوقع الجاني بإستخدام المفتاح الخاص أو الرقم السري لصاحبه، وقد نصت المادة 6 من القانون رقم 03.15 على إثبات العلاقة بين معطيات التحقق و صاحب التوقيع و ذلك بواسطة شهادة إلكترونية موصوفة تصدرها وزارة العدل، معناه أنه هناك إمكانية الإعتداء على التوقيع الإلكتروني، أما الطريقة الثانية فتتمثل في : السيطرة على النظام المعلوماتي لجهة التصديق الإلكتروني وذلك طبقا للمادة 394 مكرر من قانون العقوبات.²⁷

-الإعتداء على المعطيات الخارجية للنظام المعلوماتي :

نصت على هذه الجريمة المادة 394 مكرر 2²⁸ من قانون العقوبات، فيكون محل الجريمة في هذه الحالة فقد كرس المشرع من خلال هذه المادة الحماية الجنائية للمعطيات الخارجية للنظام المعلوماتي، فيقصد المعطيات المخزنة تلك التي تحفظ في أقراص مضغوطة أو بطاقات الذاكرة، أو المخزنة داخل النظام ذاته كذاكرته أو قرصه الصلب، أما المعطيات المرسلّة عن طريق منظومة معلوماتية نعني بها تبادل إرسال المعلومات بين أجهزة المنظومة المعلوماتية.²⁹

الفرع الثاني: التجسس المعلوماتي

قد لا يوجد فرق بين الإختراق و التجسس المعلوماتي إلا من حيث الهدف، فالأساليب المتبعة في التجسس المعلوماتي هي ذاتها التي تتبع لتنفيذ عملية الإختراق، وعليه يمكن تعريف التجسس في المجال الرقمي على أنه : إختراق يسعى من خلاله إلى التعرف على ما يحتويه جهاز الكمبيوتر الذي يستهدفه دون نية الإضرار بالمحتوى المعلوماتي كما قد عرفه بعض الفقه على أنه: الإطلاع على معلومات خاصة بالغير محفوظة على جهاز إلكتروني و ليس مسموحا لغير المخولين بالإطلاع عليها.³⁰

فلا فرق بين التجسس الرقمي أو الإلكتروني والتجسس التقليدي، إلا أن النوع الأول يتم في بيئة إفتراضية بواسطة تكنولوجيا المعلومات وعن طريق أجهزة و أدوات إلكترونية.³¹ والجدير بالذكر أن أغلبية جرائم التجسس تتم بإستخدام فيروسات يتم نقلها إلى الحاسوب المستهدف من أجل نقل و إرسال نسخ من المعلومات و البيانات التي يحتويها جهاز الحاسب الآلي محل الجريمة.³² قد يقيم الجاني بإرسال فيروسات إلى الحواسيب المعتمدة في التقاضي عن بعد أو حاسوب أحد المتقاضين، من أجل الإطلاع على أسرار الدعوى، والمعلومات المهمة و السرية.

بل الأكثر من ذلك قد يتم التجسس من خلال إختراق البرنامج المعتمد للمحادثة المرئية عن بعد، إذ نص القانون رقم 03.15³³ على إمكانية الإعتماد على المحادثة المرئية عن بعد لسماع و إستجواب الأطراف، وقد أكد المشرع على ضرورة أن تتضمن الوسيلة المستعملة سرية الإرسال و أمانته و ذلك في نص المادة 14 من القانون السالف الذكر.

فيمكن لقاضي التحقيق اللجوء إلى المحادثة المرئية عن بعد، من أجل إستجواب أو سماع شخص أو إجراء مواجهات بين عدة أشخاص، كما مكن ذلك للقاضي و ذلك بغية سماع الشهود و الأطراف المدنية و الخبراء، أو الإستماع إلى تصريحات المتهم المحبوس حيث تتم المحادثة في المؤسسة العقابية التي يتواجد فيها.

فقد اخترق الجاني النظام الإلكتروني المعتمد في المحادثة المرئية عن بعد، دون أن تتفطن الجهة القائمة بها بذلك، فيتجاوز نظم الحماية الفنية، و يتنصت و يتجسس على الأقوال و التصريحات المدلى بها من قبل المتهمين أو الشهود و الخبراء و الضحايا.

المبحث الثاني: إستراتيجية التأمين الفني من القرصنة الرقمية الواقعة على نظام التقاضي الإلكتروني

إن الأمر الأهم من تجريم القرصنة الرقمية هو إيجاد حلول و طريق للتأمين منها، بهدف حماية نظام التقاضي الإلكتروني من هذه التجاوزات التي من شأنها، أن تهدر حقوق المتقاضين وتمس بهيبة و مكانة مرفق القضاء، فقد تم العمل على إيجاد سبل فنية و إجراءات تقنية تقل التصدي لهذه الجريمة و هو ماسيتم معالجته من خلال هذا المبحث.

فقد خصصنا المطلب الأول للتطرق إلى إجراء فني و نظام حماية تقني يتمثل في تأمين خطوط الدفاع الأمامية بإستخدام تطبيقات الجدران النارية، أما المطلب الثاني سآبين من خلاله نظام حماية آخر يتمثل في تشفير المعلومات المنقولة و المحفوظة.

المطلب الأول: تأمين خطوط الدفاع الأمامية بإستخدام تطبيقات الجدران النارية

تقوم هذه البرمجيات -تطبيقات الجدران النارية- مقام المصفاة إذ تقوم بمنع وصول الطلبات المشبوهة إلى الأجهزة المزودة، من خلال الإعتماد على مجموعة البيانات التي يحدد بموجبها مدراء الشبكة طبيعة المعلومات، التي يتم السماح للعاملين داخل المؤسسة بالولوج إليها،³⁴ و هذه الجدران النارية صنفان، يتمثل الصنف الأول في الجدران النارية المؤسسية وهو ماسيتم التطرق له في الفرع الأول، أما الفرع الثاني سأعالج من خلاله صنف آخر من خطوط الدفاع الأمامية و هو مايصطلح عليه بالجدران النارية الشخصية.

الفرع الأول: الجدران النارية المؤسسية

وهي تطبيقات الحماية المرتبطة بأجهزة المؤسسات حيث تقوم بحماية محتوياتها، مادامت متصلة بشبكة الأنترنت،³⁵ ومنه يتوجب على المحكمة أو المجلس القضائي أو المحكمة العليا، التي تعتمد نظام التقاضي الإلكتروني بتزويد حواسيبها بهذه الأنظمة الفنية للتصدي للإعتداءات من قرصنة رقمية وغيرها من الجرائم المعلوماتية.

الفرع الثاني: الجدران النارية الشخصية.

نظرا لإنتشار الأجهزة الإلكترونية المحمولة كالهاتف النقال و الحاسوب المحمول أو حتى الثابت في المنزل، عمل مدراء المعلوماتية بتثبيت تطبيقات الحماية الشخصية على

هذه الأجهزة،³⁶ فالجدران النارية المؤسسية لا تكفي لمجابهة القرصنة الرقمية، التي تعرقل سير التقاضي عن بعد بل يجب أن يكون كل جهاز إلكتروني مزود بتطبيق الحماية الشخصية، سواء للمتقاضين أو غيرهم.

تطبيقات الجدران النارية لم تحقق الحماية الكاملة لبرامج وبيانات الحاسوب، ونظرا لقصورها تم البحث عن سبل أخرى للتأمين من بينها تأمين حسابات المستخدمين ونظم التحقق من الهوية، و قد خصصنا المطلب الثاني لتوضيح هذه الأنظمة الفنية.

المطلب الثاني: تشفير المعلومات المنقولة و المحفوظة

يعد التشفير أهم أساليب مواجهة القرنة الرقمية بمختلف صورها، و يراد بهذا المصطلح: " تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من إطلاع الغير عليها أو من تعديلها أو تغييرها."³⁷

وتعتمد تقنية التشفير الحديثة على نظرية تتمثل في: تمتلك كل جهة أو فرد مفتاحين لتشفير و فك تشفير البيانات، المفتاح الأول و هو المفتاح الخاص و يكون فقط بحوزة الجهة المخولة، و المفتاح الثاني هو المفتاح العام و الذي يتم نشره على شبكة الأنترنت من أجل إستخدامه من قبل الجهات الأخرى لتشفير الملفات و المعلومات المراد إيصالها إلى الطرف الآخر.³⁸

إذ يتوجب على المحاكم إستخدام هذه التقنية، في تعاملاتها مع الجهات القضائية الأخرى و كذلك مع المتقاضين.

الخاتمة:

تعد القرصنة الرقمية من بين العراقيل التقنية و الفنية التي تقف عائقا أما التطبيق الحسن لنظام التقاضي الإلكتروني، ومن خلال هذه الدراسة، خلصت إلى مجموعة من النتائج، إضافة إلى بعض تقديم التوصيات من باب إثراء الموضوع.

أولا: النتائج.

-إعتمد المشرع الجزائري مصطلح جرائم المساس بأنظمة المعالجة الآلية للمعطيات للدلالة على الجرائم الإلكترونية، و جريمة الدخول أو البقاء عن طريق الغش إلى المظومة المعلوماتية للدلالة على القرصنة الرقمية دون أن يورد تعريفا لها.

-تمتاز القرصنة الرقمية بمجموعة من الخصائص، التي تشترك فيها مع الجريمة الإلكترونية كونها أحد صورها من بينها يعد الحاسب الآلي أداة لإرتكابها، كما تتميز بصعوبة إكتشافها و إثباتها .

-يندرج القرصان الرقمي ضمن فئتين أساسيتين هما : الفئة الأولى الهاكرز و الفئة الثانية الكراكرز.

-يمتاز القرصان الرقمي بجملة من الخصائص أهمها: القرصان الرقمي مجرم ذكي ومحترف، القرصان الرقمي مجرم متخصص.

-يعد الاختراق و التجسس صورتين القرصنة الرقمية التي تستهدف نظام التقاضي الإلكتروني.

-لم ينص المشرع الجزائري على تزوير المحررات الرسمية او العمومية الإلكترونية، كما لم ينص على جريمة تزوير التوقيع الإلكتروني.

-قد يهدف التجسس المحادثة المرئية عن بعد، و المعتمدة في إجراء التحقيق لإستجواب وسماع الأشخاص.

-يتم التصدي للقرصنة الرقمية من خلال إجراءات فنية و تقنية تحول دون المساس بالأنظمة المعلوماتية.

ثانيا: التوصيات.

-العمل على تطوير النظم المعلوماتية لقاعدة بيانات السلطة القضائية، طبقا لأحدث نظم البرمجة المعتمدة دوليا والقابلة للتطوير.

-تعديل قانون العقوبات و قانون الإجراءات المدنية و الإدارية و كذلك القانون المتعلق بعصرنة العدالة من أجل ضمان التطبيق الفعال لنظام التقاضي الإلكتروني، و حمايته من الاعتداءات.

-تكريس الحماية الفنية و التكنولوجية للنظم المعلوماتية سواء التابعة لمرافق القضاء أو للأشخاص العاديين لحمايتهم من القرصنة الرقمية.

-العمل على إجراء دورات تدريبية و تكوينية دورية في مجال القضاء الإلكتروني لكل العاملين في مجال القضاء من قضاة ومحامين وأمناء ضبط من أجل مواكبة التطورات المتواصلة في مجال التقنية العلمية من جهة وتحقيق حماية أكبر للدعوى الإلكترونية من خطر الاختراق حفاظا على سرية المعلومات والمعاملات القضائية.

الهوامش:

1 - عصماني ليلي، نظام التقاضي الإلكتروني آلية لإنجاح الخطط التنموية، مجلة المفكر، العدد 13، كلية الحقوق و العلوم السياسية، جامعة حمه لخضر، بسكرة، فيفري، 2016، ص.216.

- 2 ترجمان سمية، آلية التقاضي الإلكتروني في البيئة الرقمية، مجلة الدراسات القانونية، المجلد 5، العدد 2، مخبر السيادة و العولمة، جامعة يحيى فارس، المدينة، جوان 2019، ص. 124.
- 3 - عصماني ليلى، المرجع السابق، ص. 217، 218.
- 4 - معمري سومية، المرجع السابق، ص. 7.
- 5 - خالد حسن أحمد، جرائم الأنترنت بين القرصنة الإلكترونية و جرائم الإبتزاز الإلكتروني- دراسة مقارنة، د.ط، دار الفكر الجامعي، مصر، 2019، ص. 61.
- 6 - أشرف السعيد أحمد، القرصنة الإلكترونية، د.ط، د.د.ن، د.ب.ن، 2013، ص. 12.
- 7 - المرجع نفسه، ص. 63، 62.
- 8 - لورنس سعيد الحوامة، الجريمة المعلوماتية أركانها و آلية مكافحتها، مجلة الميزان للدراسات الإسلامية و القانونية جامعة العلوم الإسلامية العالمية، السعودية، د.م، د.ع، 2016-2017، ص. 8.
- 9 - فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة ماجستير، تخصص قانون عام، كلية الحقوق و العلوم السياسية، جامعة أبي بر بلقاي، تلمسان، 2011-2012، ص. 94.
- 10 - القانون رقم 14.04 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 يتضمن تعديل قانون العقوبات، ج.ر.ج، العدد 71 الصادرة في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004.
- 11 - رحموني محمد، خصائص الجريمة الإلكترونية و مجالات إستخدامها، مجلة الحقيقة، المجلد 17، العدد 41، جامعة أحمد دراية، أدرار، 2018، ص. 441.
- 12 - خالد حسن أحمد لطفي، جرائم الأنترنت بين القرصنة الإلكترونية و جرائم الإبتزاز الإلكتروني: (دراسة مقارنة)، دار الفكر الجامعي، 2019، ص. 64.
- 13 - نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر و التوزيع، الأردن، 2008، ص. 8.
- 14 - مليكة عطوي، لجريمة المعلوماتية، حوليات جامعة الجزائر 1، العدد 21، جامعة الجزائر بن يوسف بن خدة، جوان 2012، ص. 12.
- 15 - أحمد خالد حسن، جرائم الأنترنت بين القرصنة الإلكترونية و جرائم الإبتزاز الإلكتروني، دار الفكر الجامعي، مصر، 2019، ص. 79.
- 16 - غادة نصار، الإرهاب و الجريمة الإلكترونية، العربي للنشر و التوزيع، مصر، 2017، ص. 49.
- 17 - بن عيرد عبد الغني، بضيايف هاجر، التقاضي الإلكتروني على ضوء أحدث التعديلات بين التطلعات و التحديات، مجلة الدراسات و البحوث القانونية، المجلد 6، العدد 2، مخبر الدراسات و البحوث في القانون و الأسرة و التنمية الإدارية، جامعة المسيلة، 2021، ص. 16.
- 18 - أشرف السعيد أحمد، المرجع السابق، ص. 16.
- 19 - المادة 394 مكرر من قانون العقوبات: "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) و بغرامة من 50.000 دج على 200.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك."
- 20 - ناجية شيخ، حول مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم القانونية و السياسية، المجلد 9، العدد 2، كلية الحقوق و العلوم السياسية، جامعة الشهيد حمدة لخضر، الوادي، جوان 2018، ص. 690.
- 21 - المادة 394 مكرر 7 من قانون العقوبات: "يعاقب على الشروع في ارتكاب الجرح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنة ذاتها."
- 22 - المادة 394 مكرر 1 من ق.ع.ج: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.00 دج إلى 4.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها."
- 23 - عز الدين عثمان، "صور الركن المادي في الجرائم الماسة بأنظمة العالجة الآلية للمعطيات"، مجلة العلوم القانونية و السياسية، المجلد 09، العدد 03، كلية الحقوق و العلوم السياسية، جامعة الشهيد حمدة لخضر، الوادي، ص. 618.
- 24 - التوقيع الإلكتروني عرفته المادة 2 فقرة 1 من القانون رقم 04.15: "بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق."
- 25 - القانون رقم 04.15 المؤرخ في 11 ربيع الثاني عام 1436 هـ الموافق أول فبراير سنة 2015م ج.ر.ج.ج العدد 6 الصادرة في 20 ربيع الثاني 1436 هـ الموافق 10 فبراير 2015 م.
- 26 - راضية مشري، جريمة تزوير التوقيع الإلكتروني في التشريع الجزائري، حوليات جامعة قالملة للعلوم الإجتماعية و الإنسانية، العدد 20، جامعة قالملة، جوان 2017، ص. 136.
- 27 - بن سالم احمد عبد الرحمن، مزوري إكرام، التوقيع الإلكتروني كأداة لضمان أمن للدفع الإلكتروني، الملتقى الوطني الأول: الصيرفة الإلكترونية بين الواقع و المأمول، كلية الحقوق و العلوم السياسية، جامعة المسيلة، 2020، ص. 8.

- 28 - المادة 394 مكرر 2 من قانون العقوبات: "يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات و بغرامة من 1.000.000 دج إلى 10.000.000 دج، كل من يقوم عمداً أو عن طريق الغش بما يأتي:
- 1- تصميم أو بحث أو تجميع، أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلّة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
 - 2- حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من إحدى هذه الجرائم المنصوص عليها في هذا القسم."
- 29 - ناجية شيخ، المرجع السابق، ص.693.
- 30 - أشرف السعيد أحمد، المرجع السابق، ص.17.
- 31 - عبد الحليم، بن بادة، محمد سعد، بوحادة جريمة التجسس الإلكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة- دراسة سياسية قانونية، الملتقى الدولي الأول: أمن المعلومات في الفضاء الإلكتروني الرهانات و التحديات في شمال إفريقيا، جامعة غرداية، الجزائر، 17- 18 فيفري 2020، ص.5.
- 32 - أشرف السعيد أحمد، المرجع السابق، ص.17.
- 33- القانون رقم 03.15 المؤرخ في 11 ربي الانى 1436 هـ الموافق أول فبراير سنة 2015 م
- 34- خالد الداودي، الجريمة المعلوماتية، الطبعة الأولى، دار الإعمار العلمي للنشر و التوزيع، 2017-2018، الأردن، ص.87.
- 35- المرجع نفسه، ص.88.
- 36- خالد الداودي، المرجع السابق، ص.88.
- 37- هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية، مصر، 2012، ص.73.
- 38- ليتيم فتيحة، ليتيم نادية، الأمن المعلوماتي للحكومة الإلكترونية و إرهاب القرصنة، مجلة المفكر، العدد 12، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر، بسكرة، 2018، 216.

قائمة المصادر و المراجع:

- أولاً: القوانين.
- القانون رقم 14.04 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 يتضمن تعديل قانون العقوبات، ج.ر.ج، العدد 71 الصادرة في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004 .
- القانون رقم 03.15 المؤرخ في 11 ربيع الثاني 1436 هـ الموافق أول فبراير سنة 2015 م و المتعلق بعصنة العدالة ج.ر.ج.ج العدد 6 الصادرة في 20 ربي الثاني 1436 هـ الموافق 10 فبراير 2015 م .
- القانون رقم 04.15 المؤرخ في 11 ربيع الثاني عام 1436 هـ الموافق أول فبراير سنة 2015م المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين ج.ر.ج.ج العدد 6 الصادرة في 20 ربيع الثاني 1436 هـ الموافق 10 فبراير 2015 م.
- ثانياً: الكتب.
- خالد حسن أحمد لطفي، جرائم الأنترنت بين القرصنة الإلكترونية و جرائم الإبتزاز الإلكتروني: (دراسة مقارنة)، دار الفكر الجامعي، 2019.
- خالد الداودي، الجريمة المعلوماتية، الطبعة الأولى، دار الإعمار العلمي للنشر و التوزيع، 2017-2018، الأردن.
- خالد حسن أحمد، جرائم الأنترنت بين القرصنة الإلكترونية و جرائم الإبتزاز الإلكتروني- دراسة مقارنة، دبط، دار الفكر الجامعي، مصر، 2019.
- غادة نصار، الإرهاب و الجريمة الإلكترونية، العربي للنشر و التوزيع، مصر، 2017.
- نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر و التوزيع، الأردن، 2008.
- هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية، مصر، 2012.
- ثالثاً: الأطروحات و المذكرات.
- رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة ماجستير، تخصص قانون عام، كلية الحقوق و العلوم السياسية، جامعة أبي بر بلقايد، تلمسان، 2011-2012.
- معمري سومية، الأدب الرقمي بين المفهوم و التأسيس مقارنة في تقنيات السرد الرقمي، أطروحة دكتوراه، تخصص الأدب الحديث و المعاصر، كلية الآداب و اللغات، جامعة الإخوة منوري، قسنطينة، 2016-2017.

رابعا : المقالات و المداخلات.

-بن سالم احمد عبد الرحمن، مزوري إكرام، التوقيع الإلكتروني كأداة لضمان أمن للدفع الإلكتروني، الملتقى الوطني الأول: الصيرفة الإلكترونية بين الواقع و المأمول، كلية الحقوق والعلوم السياسية، جامعة المسيلة، 2020.

-بن عيرد عبد الغني، بضياف هاجر، التقاضي الإلكتروني على ضوء أحدث التعديلات بين التطلعات و التحديات، مجلة الدراسات و البحوث القانونية، المجلد 6، العدد 2، امخبر الدراسات و البحوث في القانون و الأسرة و التنمية الإدارية، جامعة المسيلة، 2021.

-ترجمان سمية، آلية التقاضي الإلكتروني في البيئة الرقمية، مجلة الدراسات القانونية، المجلد 5، العدد 2، مخبر السيادة و العولمة، جامعة يحيى فارس، المدية، جوان 2019.

-راضية مشري، جريمة تزوير التوقيع الإلكتروني في التشريع الجزائري، حوليات جامعة قالملة للعلوم الإجتماعية و الإنسانية، العدد 20، جامعة قالملة، جوان 2017.

-رحموني محمد، خصائص الجريمة الإلكترونية و مجالات إستخدامها، مجلة الحقيقة، المجلد 17، العدد 41، جامعة أحمد دراية، أدرار، 2018.

-عبد الحليم، بن بادة، محمد سعد، بوحادة جريمة التجسس الإلكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة- دراسة سياسية قانونية-، الملتقى الدولي الأول: أمن المعلومات في الفضاء الإلكتروني الرهانات و التحديات في شمال إفريقيا، جامعة غرداية، الجزائر، 17- 18 فيفري 2020.

-عز الدين عثمان، "صور الركن المادي في الجرائم الماسة بأنظمة العالجة الآلية للمعطيات"، مجلة العلوم القانونية والسياسية، المجلد 09، العدد 03، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمة لخضر، الوادي.

-عصماني ليلي، نظام التقاضي الإلكتروني آلية لإنجاح الخطط التنموية، مجلة المفكر، العدد 13، كلية الحقوق و العلوم السياسية، جامعة حمة لخضر، بسكرة، فيفري، 2016،

-لورنس سعيد الحوامدة، الجريمة المعلوماتية أركانها و آلية مكافحتها، مجلة الميزان للدراسات الإسلامية و القانونية جامعة العلوم الإسلامية العالمية، السعودية، د.م، د.ع، 2016-2017.

-ليتيم فتيحة، ليتيم نادية، الأمن المعلوماتي للحكومة الإلكترونية و إرهاب القرصنة، مجلة المفكر، العدد 12، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر، بسكرة، 2018.

-مليكة عطوي، لجريمة المعلوماتية، حوليات جامعة الجزائر 1، العدد 21، جامعة الجزائر بن يوسف بن خدة، جوان 2012.

-ناجية شيخ، حول مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم القانونية و السياسية، المجلد 9، العدد 2، كلية الحقوق و العلوم السياسية، جامعة الشهيد حمة لخضر، الوادي، جوان 2018.