حجية الدليل الرقمي في إثبات جريمة الابتزاز الإلكتروني في القانون الجزائري

Authentic digital evidence for proving the crime of electronic blackmail in Algerian law

د. فاطمة العرفي،[1]

[1]كلية الحقوق بدواو جامعة بومرداس، f.larfi@univ-boumerdes.dz

تاريخ الإرسال: 11 / 03 /2020 تاريخ القبول: 2020/08/31 تاريخ النشر: 2022/10/15

ملخص:

هيمنة الفضاء الرقمي من خلال المبالغة في صناعة المحتوى أدى إلى تغيير وتضييق مفهوم حق الخصوصية مما سمح بحدوث انتهاكات ذات طبيعة جنائية مثل الإبتزاز الإلكتروني التي هو جريمة تقع في مسرح إفتراضي، تحتوي سلسلة من الأفعال الجبرية تتضمن التهديد والمساومة للوصول لأهداف معنوية أو مادية أو جنسية، مما يعقد متابعة الواقعة الإجرامية لأن الإحاطة بها يقتضي الوصول للدليل الرقمي الذي تبنى عليه مسألة التجريم برمتها، وهذا الأمر ليس بالهين ويقتضى خبرة تقنية وقانونية للوصول للفعالية العملية التي تحقق العدالة وتمنع الإفلات من العقاب.

الكلمات المفتاحية: الإبتزاز الإلكتروني، العالم الإفتراضي، انتهاك الخصوصية، حماية قانونية، الدليل الرقمي.

Abstract:

The dominance of the digital space through exaggeration in the content industry led to a change and narrowing the concept of the right to privacy, which allowed for violations of a criminal nature, such as electronic extortion, which is a crime that occurs in a virtual theater, to contain a series of forced actions that include the threat and compromise to reach moral goals or Material or sexual, which complicates the follow-up of the criminal incident because surrounding it requires access to the digital evidence on which the entire

criminalization issue is based, and this is not easy and requires technical and legal expertise to reach the practical effectiveness that achieves justice and prevents impunity.

Keywords: electronic blackmail, virtual world, privacy violation, legal protection, digital directory

1- **المرسل:** فاطمة العرفي، f.larfi@univ-boumerdes.dz

مقدمة:

أصبح الفضاء الرقمي بخصائصه الهُلامية المهيمنة يشكل تهديدا بالغا على خصوصية الأشخاص التي ما فتئت تضيق في مواجهة المحتوى الإفتراضي وتقنياته ومنصاته، مما يستوجب فرض حماية قانونية للمكانة الأدبية، واعتبار المساس بها بأي طريقة جريمة بالغة الخطورة، حيث تعد جريمة الإبتزاز الإلكتروني من الجرائم الخطيرة التي تلحق أضرارا بالضحية سواء في مشاعره أو ماله أو عمله أو سمعته، كما أنها تدمر نفسيته وحياته الخاصة، من خلال صنع محتوي إلكتروني إبتزازي خاص من خلال التقاط صور أو تسجيل حوار مسموع أو مكتوب والتهديد بنشره على الملأ من خلال حساب تواصلي لأي سبب من الأسباب، مما يطرح المسؤولية القانونية عن الحساب ومحتوياته، خصوصا أن سرية الحياة الخاصة كمفهوم غامض ومستقل يتطور بذاته تبعا لتطور المجتمع، وطبيعة الأشخاص، وهي عادة تتكون من عناصر جوهرية، كالاسم والرسم والحياة الحميمية والعاطفية وكل ما يتعلق بالشرف والأخلاق[1]. وهي جوهر الحياة الخاصة للإنسان، وبهذا تتمثل بالسرية والخلوة والهدوء، فهي تستند إلى عناصر مادية ومعنوية تمثل نطاقه الذي يرغب الشخص بالاحتفاظ به منطويا أو مخفيا، والمرتبط بالشعور بالحياء الذي يمثل الفيصل في تحديد نطاق الحياة الخاصة وتنتهي الحياة العامة[2]، ومتى حدث الانتهاك في الفضاء الرقمي تتعقد متابعة الواقعة الإجرامية لأن الإحاطة بها يقتضي الوصول للدليل الرقمي الذي تبنى عليه مسألة التجريم برمتها، وهذه

مسألة في منتهى الأهمية لأنها تتعلق بمواجهة جريمة ما فتئت تنتشر في المجتمع الجزائري، مما يطرح يجعلنا نطرح الإشكالية الآتية: **ماهي حجية الدليل الرقمي قي إثبات جريمة الابتزاز الإلكتروني؟** وتتفرع عنها مجموعة من الإشكاليات الفرعية هي:

-ما هو مفهوم الحياة الخاصة وجريمة الابتزاز الإلكتروني وأركانها؟
-ماهي إجراءات الحصول على الدليل الرقمي في جريمة الابتزاز الإلكتروني؟
-ماهي محددات أنواع الحماية العقابية والمدنية للأشخاص في مواجهة جريمة الابتزاز الإلكتروني؟ وستتم دراسة هذا الموضوع من خلال منهج وصفي يعتمد التحليل والنقد من أجل إيجاد مقاربة قانونية متكاملة خصوص في ظل قلة الدراسات التي تطرقت لهذا الموضوع من المنظور التنظري في اطار القانون الجزائري، وسيتم ذلك من خلال العناصر الآتية:

1- انتهاك جريمة الإبتزاز الإلكتروني لمفهوم الخصوصية في نطاق الرقمنة.

2- **الضوابط القانونية المقررة لحماية الأشخاص من جريمة الإبتزاز الإلكتروني.**

1-انتهاك جريمة الإبتزاز الإلكتروني لمفهوم الخصوصية في نطاق الرقمنة:

الحق في الخصوصية من الحقوق الدستورية الأساسية الملازمة واللصيقة للشخص الطبيعي بصفته الانسانية كأصل عام[3]. ولو أن القانون الجزائري لا يحدد هذا المفهوم ومحدداته مما ينبئ عن تعقده وتشعب مراميه[4]. حيث يصبح الشخص معرضا للانتهاك متى تم تسجيل محتوى متعلق به في العالم الرقمي، مما يجعله غير قابل للمحو، وهذا ما سنتتطرق إليه فيما يأتي:

1-1-مفهوم حق الخصوصية: هو مفهوم تغير في ظل هيمنة الفضاء الرقمي، حيث أصبح أكثر شمولا من حماية البيانات، ليعني خصوصية المعلومات، الذي هو حق الأشخاص أو المجموعات أو المؤسسات أن يحددوا لأنفسهم حدود إطلاع الآخرين على معلوماتهم الشخصية، أو هي حق الشخص في ضبط عملية جمع المعلومات الشخصية عنه، وعملية معالجتها آليا وحفظها، وتوزيعها واستخدامها في صنع القرار الخاص به أو المؤثر فيه، لكن الملاحظ أن

المشاهير يتم تضييق مفهوم الحياة الخاصة بهم بسبب وضع أنفسهم تحت الأضواء مما يثير الفضول وحب الاستطلاع حولهم، مما يجعل جزءا كبيرا من هذه الخصوصية يفلت من نظام الحماية النوعية المفروضة قانونا.

2-1: مفهوم الفضاء الرقمي وجريمة الابتزاز: الفضاء الرقمي هو فضاء إفتراضي يضم الأدوات والتقنيات والمنصات الموجودة على شبكة الأنترنت التي تسمح بإجراء أنشطة إلكترونية تتمحور حول التفاعل الرقمي فهي تمثل الإعلام الجديد أو البديل الذي يتمظهر في شكل مجتمع افتراضي تقدم خلاله خدمات عديدة.

فهي مستودعات رقمية للمعلومات والبيانات الشخصية وغير الشخصية تضم وسائل نشأت لمساعدة الأشخاص على التقارب والتشارك والتواصل، واكتشاف الأحداث المحلية والدولية، والعثور على المجموعات للانضمام إليها، أنتجت ظواهر مرضية نتيجة إساءة الاستخدام منها انتهاكها لخصوصية الأشخاص في ظل التعامل معه بتساهل وإفراط من خلال جعل الحياة الخاصة من معلومات، صور، فيديوهات عن مناسبات خاصة للشخص وأسرته وأصدقاءه متاحة في الفضاء العام[5]، وهذا يجعلها عرضة للانتهاك والمساس من قبل المتطفلين أو حتى محترفي الإجرام الإلكتروني [6]، مما يجعلها مشكلة معقدة خارجة السيطرة، ولعل أخطر الانتهاكات التي تهدث في الفضاء الرقمي جريمة الابتزاز الإلكتروني، حيث يعرف الابتزاز بشكل عام تعرف بأنه:

سلوك يتضمن مساومة الشخص للحصول على مكاسب مادية أو معنوية أو جنسية أو لمجرد الانتقام عن طريق وسائل الإكراه والقسر بتهديده بإفشاء أسرار ممكن أن تسئ له أو تلحق به ضررا به، وهو أنواع منه الإبتزاز الإلكتروني الذي يعني: التهديد والمساومة التي تقع بواسطة آلية إلكترونية، أو هو: الحصول على معلومات سرية إلكترونيا تتعلق بالمجني عليه لا يرغب وصولها للآخرين والتهديد بإفشاء السر أو نشر المعلومات إن لم تتحقق مطالبه وتنفذ، مما يؤثر على إرادة ونفسية المجني عليه، فيبستجيب لرغبات الجاني[7].

فالابتزاز في مضمونه طلب خدمة من شخص مع العلم المسبق بعدم قدرته المطلقة على قيامه بها، فهو إذا في معناه الدقيق استخدام المبتز سواء أكان

شخصا أم تنظيما أسلوب من أساليب الضغط المادي أو المعنوي لدفع الضحية لنهج سلوك معين يجلب المنفعة للجهة المبتزة، مستخدماً مثلا اتباع أسلوب التهديد بالتشهير بالضحية على أوسع نطاق، أو إبلاغ ذوي المرأة زوجاً كان أو أباً أو أخاً؛ حتى يجعل الضحية تقع تحت وطأة ضغوط المبتز ليجبرها على مجاراته وتحقيق رغباته الجنسية أو المادية، مما يعني أن محل الابتزاز خدمة تقترن الفعل المؤذي بالرضا، لذا لابد من توافر القصد الجنائي من خلال اتجاه نية المبتز لاستعمال التهديد والمساومة من أجل الحصول على الخدمة مع العلم المسبق بهدم القدرة على الدفع[8].

من هذا المنطلق يمكن اعتبار ابتزاز الأشخاص ضمن هذا المفهوم الذي ذكرته المواد 284 و286و 371 ق ع ج ، ولو أنه كان من الأفضل ذكرها في نصوص قانونية واضحة تأخذ بعين الاعتبار المستجدات التكنولوجية التي أصبحت جزء منها، وأيضا نظرا لانتشارها وخطورتها على اعتبار أن هذا النوع من المواد المسيئة أصبحت تنتج ثم تروج عبر الوسائط الرقمية، أو تنتج بشكل مباشر أمام جمهور يشاهدها، حيث يتم استغلال قوة الهوية المجهولة للجناة للإساءة للأشخاص، مثل تظاهر المتصيد بأنه صديق حتى يكتسب ثقة الشخص ومن ثم يطلب منه رقم هاتفه بغرض التواصل معه في العالم الحقيقي، لاستغلاله فعليا أو الاكتفاء بالتسجيل أو التصوير أو الدردشة ذات الطابع الإباحي ومن ثم ابتزازه فإذا رفض قام بالتشهير به[9].

ومن جهة أخرى فإن جعل المعلومات الشخصية متاحة للعموم، يشكل خطورة على الحياة الخاصة نظرا للاستعمال الهستيري لها خصوصا على الجيل الجديد الذين أصبح يبالغ في نشر أدق خصوصياته على صفحاته الخاصة في ظل غياب رقابة الأهل أو تساهلها، مما أدى لارتكاب الكثير من الجرائم[10].

وهذا يفسر الأضرار المترتبة عنها[11]، فهي تؤثر على سمعة الضحية وتضيع مستقبله الاجتماعي، فضلا عن المعاناة النفسية نتيجة الضغوط التي تتعرض لها، والعزلة وتجنب الآخرين نتيجة الشعور بالعار والخجل وانخفاض تقدير الذات وتأنيب الضمير، وأيضا الانحراف، الانتقام، الاباحية، الطلاق، التفكك الأسري كما أن تأثيرها يمتد لتهديد منظومة القيم داخل المجتمع والنظام

الأخلاقي فيه واهتزاز معايير الأخلاق الحميدة[12]. ويزداد الأمر خطورة متى استهدف الإبتزاز الإلكتروني الأطفال، وهي جرائم لا تقل بشاعة عن الاختطاف، مما يستوجب توفير حماية نوعية حقيقة لهذه الفئة الهشة.

1-1-3:أركان جريمة الإبتزاز الإلكتروني: الإبتزاز الإلكتروني يعني الحصول على معلومات سرية إلكترونية للشخص لا يرغب في إذاعتها في الفضاء العام سواء بواسطة الاختراق والسرقة أو عن طريق استغلال الثقة والأمان [13]. ثم التهديد والمساومة بجعل المنشور مقترحا للعامة مقابل الحصول على مكاسب مادية أو معنوية أو جنسية أو ارتكاب جريمة، وما يمثله ذلك من ضغط على إرادة الضحية وتخويفه بالفضيحة والتشهير بأي وسيلة رقمية، فهذه الجريمة تمر بعدة مراحل:

-الحصول على معلومات وبيانات سرية متعلقة بالحياة الخاصة للضحية سواء عن طريق الثقة أو عن طريق توريطها في جريمة أو قضية أخلاقية ممكن تحدث بلبلة في الرأي العام أو عن طريق اختراق جهازها وسرقة محتوياته أو الغش والتجسس الإلكتروني من صور وفيديوهات وتسجيلات ودردشات، أو عن طريق صناعة محتوى رقمي ملفق للضحية أو استرجاعه من هاتف أو لوح إلكتروني مبيع...إلخ.

-مرحلة الابتزاز عن طريق الضغط والتهديد بنشر تلك المعلومات التي لا ترغب الضحية في إذاعتها، وهي مرحلة تتعلق بارغام الضحية على شراء سكوت الجاني من تنفيذ تهديداته، فهي مرحلة السيطرة على الضحية حتى تصبح معدومة الاختيار فلا يكون أمامها غير الرضوخ لطلبات المبتز وإلا تعرضت للأذى النفسي والجسدي[14].

-أن يكون التهديد بأي وسيلة تقنية، كتابة، صوتا عن طريق التسجيل أو بواسطة، بقصد الحصول مكسب مادي أو معنوي أو جنسي أو أي شئ آخر دون وجه حق، ولا يهم كون الشئ المتزع ملكا للضحية أو لغيرها أو كون الانتزاع لصالح الغير.

-في حال تعنت الضحية ورفضها تلبية مطالب المبتز مهما كان نوعها مادية أو أو معنوية أو جنسية، تأتي مرحلة التشهير عن طريق نشر الأسرار الخاصة علانية بواسطة منصة رقمية مثل الفاسبوك أو انسناجرام أو سنابشات أو

اليوتيوب وغيرها، سواء في صفحة الضحية المخترقة أو في صفحة الجاني، أو في صفحة باسم الضحية أو باسم مستعارمجهول الهوية.

وتزداد خطورة هذا الفعل متى تم التلاعب في الصورة عن طريق (الفوتوشوب) وفي الفيديوهات عن طريق(المونتاج) أو تعديل الصوت عن طريق برامج وتطبيقات رقمية متطورة، مما يعطي انطباع فيه مغالطة عن الضحية ويصورها كأنها فاسقة خارج عن الأخلاق.

1-الركن المادي: السلوك الإجرامي في هذه الجريمة يتمظهر في الحصول على منتوج رقمي خاص للضحية ثم تهديده بنشره في البيئة الرقمية، مما يعني أن مسرح الجريمة هو منصات رقمية واسعة الاستخدام، سواء تمظهرت في شكل صور أو فيديوهات أو رسائل صوتية أو رسائل دردشة مكتوبة، مما يخيف الضحية ويدفعها للرضوخ لطلبات المبتز. فالناحية الأساسية للعنصر المادي في مجال الابتزاز هو أن الشخص الواقع تحت طائلة الابتزاز يكون في حالة استحالة مطلقة عن دفع الأمر المهدد به في حالة عدم استجابته لرغبات المبتز، فالانسان يكون في حالة اعسار، بحيث تنعدم لديه القدرة على دفع الخطر، ولا يوجد من يضمن سلامته في حال رفضه طلبات المُبتز[15].

-النتيجة الإجرامية: التهديد بنشر المنتوج الرقمي يشكل ضغطا على إرادة الضحية ويدفعه للرضوخ لمطالب المبتز دون رضاه منعا لحدوث التشهير والفضيحة في الفضاء الرقمي وبالتالي خسارته لرأسماله الاعتباري أو الرمزي.

-العلاقة السببية: من الصعوبة بمكان تحديد العلاقة السببية في هذه الجريمة بسبب التعقيدات المتعلقة بها باعتبارها تقع في بيئة افتراضية، وما يرافق ذلك من تداخل والمراحل التي تمر بها الجريمة من الدخول عبر الكومبيوتر والأوامر المدخلة والنتيجة المراد الحصول عليها، وهل تحققت بالفعل أم لا، من هذا المنطلق فالعلاقة السببية في جريمة الإبتزاز تكمن في خوف ورضوخ الضحية وتلبيته لطلبات الجاني نتيجة تهديد الجاني للضحية بالنشر والعلانية في الفضاء الرقمي لأسرار ومعلومات وبيانات تتعلق بخصوصيته.

2-الركن المعنوي: الابتزاز جريمة قصدية تستوجب اتجاه نية المبتز نحو الضغط على إرادة الشخص من أجل ارضاخه لرغباته مهما كان نوعها. حيث يشترط في الشخص القائم بالابتزاز، توافر عنصري العلم والإرادة؛

-العلم: يشترط علم الجاني أن تهديده بنشرمعلومات تتعلق بالحياة الخاصة للضحية علانية هو جريمة معاقب عليها قانونا. كما يعلم كل عناصر الجريمة من أول أخذ معلوماتها الخاصة وصورها وتسجيلاتها واتصالاتها سواء تحصل عليها بنفسه أو عن طريق الغير ومهما كانت وسيلة الحصول عليها.

-الإرادة: أن تتجه نية الجاني السيئة اتجاه مساومة الضحية وتهديده بإذاعة منشور إلكتروني، مع علمه الأكيد بكون ذلك يسبب له أذى معنويا جسيما. طبيعة المنشورات التي تنشر على موقع الفايسبوك تستلزم وجود النية والتحضير وتوافر إحاطة المجني عليه وإلمامه بنشاطه، وكذلك توافر إرادته نحو تحقيق العناصر المادية للجريمة بتعديل إعداد الخصوصية قبل الضغط على زر"النشر"

فالقصد الجنائي يعني اتجاه الإرادة الواعية إلى الجريمة في كل أركانها وعناصرها علما نافيا للجهالة[16]، وأن يكون الجاني وهو يبتز ضحيته عالما بأنه يؤذيه ويغتصب ما لا حق له فيه ولا لغيره ولا أهمية بعد ذلك بالبواعث التي تكون قد دفعت الجاني إلى ارتكاب الجريمة.

2-الضوابط القانونية المقررة لحماية الأشخاص من جريمة الإبتزاز الإلكتروني: خصوصية ضبط الجاني في جريمة الإبتزاز الإلكتروني تتبني على الحصول على دليل رقمي في البيئة الرقمية لأنه يمثل أساس بناء دعوى جزائية مؤسسة، من هذا المنطلق سيتم التطرق للإجراءات الخاصة ومن ثم الحماية الموضوعية للأشخاص من جريمة الابتزاز الإلكتروني.

2-1-1: طرق إثبات جريمة الإبتزاز الإلكتروني: خصوصية متابعة جريمة الابتزاز الإلكتروني تكمن في صعوبة اثباتها لأنها تتم عن طريق وسائل تقنية معقدة وتتم في مسرح رقمي وكل هذا ينعكس على مدى حجية الدليل الرقمي المتحصل عليه من سلسلة اجراءات التحري والاستدلال وهل تكفي لتكوين قناعة تسمح بتحريك دعوى عمومية ضد الجاني ومن ثم التحقيق معه.

وبالرجوع للدليل الرقمي المأخوذ من منظومة معلوماتية نجده يكون في شكل مجالات أو نبضات مغناطسية أو تطبيقات تكنولوجية خاصة ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأشكال والرسوم، وذلك من أجل الربط بين الجريمة والمجرم والضحية وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون[17].

فالدليل الرقمي يشمل جميع البيانات الرقمية التي بدورها تدل على وجود الجريمة وحقيقة ارتكابها، ومن ثم الربط بينها وبين الجاني والمجني عليه، ويمكن استخدامها في أي مرحلة من مراحل التحقيق لإثبات واقعة قانونية[18]، حيث يستطيع مزود الخدمة معرفة المستخدم ومعرفة كل المواقع التي زارها ومنتديات الحوار والاتصالات التي قام بها، مهما اتصل بهوية مستعارة أو إمايل مزيف[19]. فالحصول على الدليل الرقمي، يقتضي وجود خبير تقني يقوم بالفحص والمعاينة من خلال:

-المعاينة: يقصد بها رؤية أماكن ارتكاب الوقائع الجنائية وإثبات محتوياتها في البيئة الافتراضية، الذي هو مسرح جريمة الإبتزاز الإلكتروني، وهي تتطلب قيام المحقق بالانتقال إلى محل الواقعة أو أي محل آخر توجد بها أشياء، أو آثار يرى المحقق أن لها ارتباطا بالجريمة وتساهم في كشف الجريمة [20].

وتتم المعاينة بعد تلقي البلاغ عن ارتكاب إحدى الجرائم المعلوماتية، حيث يتم التأكد من البيانات المطلوبة في البلاغ، ثم يجري الانتقال إلى مسرح المعاينة، والذي هو مسرح افتراضي، حيث يجب مراعاة الضوابط الآتية عند القيام بالمعاينة في جريمة الابتزاز الإلكتروني:

-إصدار إذن من النيابة العامة يجيز تفتيش أنظمة المعلوماتية، ومن ثم تكليف خبير أو فريق من الخبراء، من أجل وضع خطة التفتيش الإلكتروني.

-جمع معلومات مسبقة عن مكان وقوع جريمة الإبتزاز الإكتروني، مع تحديد عدد أجهزة الحاسوب المطلوب معاينتها وفحصها.

-تحديد مكان تواجد وقوع جريمة الإبتزاز الإلكتروني بدقة من خلال تحديد الصفحة واسم المستخدم وكلمة المرور السرية، ويتم ذلك من طرف موظف

متخصص، أو فريق عمل إذا كانت المهمة معقدة، وأن تتم المعاينة وفق مبدأ إجراءات التقاضي المتعارف عليها ومبدأ الشرعية.

- المحافظة على مسرح الجريمة بحيث تتم حماية البصمات ومنع استخدام أي حاسب آلي في مسرح الجريمة، مع ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات الحاسب الآلي، وضمان العثور على الخادم بشبكة الاتصال لحماية الأدلة من التخريب، مع تأمين عدم انقطاع التيار الكهربائي عن مكان المعاينة لضمان التعامل الايجابي مع الأدلة الرقمية، وخشية ضياعها مع انقطاع التيار الكهربائي، ووضع حراسة على العتاد حتى لا يتم تحريكه أو سرقته أو إخفاءه، مع وضعها في حالة عدم اتصال OFF.

-قطع الاتصال الهاتفي عن أجهزة الحاسب الآلي الموجودة في مسرح الجريمة، حتى لا يمكن الوصول إليها من قبل الجاني أو غيره.

- الاستعانة بالوسائل الفنية التي تستخدم في بنية نظم المعلومات، من خلال معرفة الطريقة المعد بها النظام المعلوماتي والآثار التي يخلفها، ومعرفة السجلات الالكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز المتصل وبرتوكولات الاتصال عبر الأنترنت والمعروفة بالاختصار(IP)، (INTERNET PROTOCOL ADDREES) ويعرف هذا الأخير على أنه وسيلة تراسل حزم البيانات يتكون من أربعة أجزاء وكل جزء يتكون من أربعة خانات، يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات الآلية المرتبطة، والرابع يحدد الحاسب الآلي الذي تم الاتصال منه.

وأيضا البروكسي: الذي هو وسيلة تعمل كوسيط بين الشبكة ومستخدميها تضمن الشركات المقدمة لخدمة الاتصال بالشبكات قدرتها لادارة الشبكة، وضمان الأمن وتوفير خدمات الذاكرة الجاهزة وبرامج التتبع التي تقوم بالتعرف على محاولات الاختراق وتقدم بيانا شاملا عن المستخدم الذي تم اختراق جهازه، بالإضافة لفحص الخوادم وسائل مستخدمة في استرجاع المعلومات من الأقراص التالفة وبرامج كسر كلمات المرور، وبرامج البحث عن الملفات العادية والمخفية وبرامج تشغيل الحاسب وبرامج مسح البيانات.

-أدوات فحص الشبكات: من خلال فحص برتوكولIP و TC لمعرفة ما قد يصيب الشبكة من مشاكل ومعرفة العمليات التي قد تتعرض لها.
- ويستخدم لتحديد هوية كل جهاز يتصل بالأنترنت، حيث عندما يتصل المستخدم بالأنترنت فإنه يترك آثارا لكل موقع يزوره مع إمكانية معرفة نوع الكومبيوتر والمتصفح والبريد الالكتروني ومعلوماته الشخصية.
-التحفظ على محتويات سلة المهملات وما فيها من أوراق وشرائط وأقراص ممغنطة، ورفع البصمات.
-الحرص على عدم نقل المواد المعلوماتية خارج مسرح الجريمة إلا بعد خلو المحيط الخارجي للحاسب الآلي من مجال مغناطيسي قوي، حيث تتسبب الممرات المغناطيسية في محو البيانات ولا يتم ذلك إلا من قبل خبراء الحاسب الآلي.
-التفتيش: ويكون لـ: -المسرح التقليدي: ويكون خارج العالم الافتراضي وينصب على الأشياء المادية المحسوسة في المكان الذي وقعت فيه الجريمة، ويترك الجاني فيها آثارا عديدة كالبصمات والمتعلقات الشخصية أو وسائط التخزين أو أوراق الطابعة.
-والمسرح الافتراضي: وهو المسرح الذي يقع داخل جهاز التليفون أو اللوح الرقمي أو الحاسب الآلي، ويتكون من البيانات الرقمية الموجودة داخل جهاز الحاسب وشبكاته والأقراص الصلبة، ويكون التعامل مع هذه الأدلة من قبل الخبراء المتخصصين بالحاسب الآلي للتعامل مع هذا النوع من الأدلة[21].

وقد نص القانون رقم 09-04، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على إجراءات التفتيش الإلكتروني في حالة الجرائم المرتكبة بواسطة نظم المعلوماتية في (م5) منه[22]، وطبعا يكون ذلك بإذن مسبب من طرف النيابة العامة وإلا وقع باطلا، كما تنص الفقرة 3 من المادة نفسها على توسيع نطاق التفتيش خارج الإقليم الوطني، وذلك عن طريق المساعدة الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل[23].

-سماع شهادة الشهود: الشاهد في جريمة الإبتزاز الإلكتروني هو الخبير المتخصص في تقنيات الحاسب الآلي والشبكات، والتي يحوز على معلومات جوهرية ولازمة للدخول في نظام المعالجة الآلية للبيانات، ويطلق عليه الشاهد المعلوماتي، ومهمته أنه يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا عن أدلة الجريمة بداخله[24].

2-1-2-صعوبات تحصيل الدليل الرقمي: رغم تطور اجراءات الاستدلال والتحري والتحقيق في الجرائم الإلكترونية ومن ضمنها الابتزاز الإلكتروني، إلا أن هناك الكثير من المعوقات التي تمنع الحصول على أدلة رقمية قوية نظرا لسهولة محو الأدلة التي تمكن من الاستدلال على هوية الجاني والتلاعب فيها، فهي جريمة هلامية تستوجب خبرة وتقنيات متطورة جدا، وتتمثل الصعوبات في:

-محددات الخصوصية التي هي حقوق لصيقة بالشخصية محمية دستوريا، وأي انتهاك من أجل مقتضيات التحقيق يستوجب الاذن المسبب قانونيا.

-ديناميكية هكذا نوع من الجرائم وتطوراتها السريعة بالموازاة مع جمود التشريعات وضعف خبرة موظفي تطبيق القوانين يصعب عمليات الحصول على الأدلة الرقمية.

-تنازع القوانين والاختصاص مع عدم أو ضعف التنسيق بين الدول يعصعب عملية الحصول على الأدلة الرقمية من حيث الضبط والتفتيش، خصوصا متى كانت عناصر جريمة الابتزاز الإلكتروني موزعة بين عدة دول.

-سهولة محو الأدلة مما يحول دون تعقب الجناة، وذلك لتضليل الجهات الأمنية، حيث يتم التلاعب في الأدلة ومسحها والعبث فيها للافلات من العقاب، خصوصا في ظل احتراف الجناة لعمليات التشفير والترميز.

-نقص الخبرة مما يؤثر على عملية التحقيق برمتها من حيث ضبط الأدلة، حمايتها واحرازها حتى لا يتم إتلافها وضياعها، مثل اتلاف القرص الصلب أو الأقراص الممغنطة أو أوعية المعلومات التي تخزن فيها البيانات.

-إحجام الضحية عن الإبلاغ خوفا من الجاني ومن الفضيحة والتشهير، خصوصا إذا كان المحتوى الابتزازي حساس وحميمي ومحرج.
-ضخامة البيانات المعلوماتية التي تحتاج إلى فحص والتفتيش للبحث عن الأدلة الرقمية بداخلها لإدانة الجاني في جريمة الابتزاز الإلكتروني[25].

2-2: **الحماية العقابية والمدنية للأشخاص من جريمة الإبتزاز الإلكتروني:**
تزايد اساءة الاستخدام للفضاء الرقمي دفع دول عديدة في العالم إلى تعديل التشريعات الجزائية وإصدار قوانين تتضمن أحكاما عقابية رادعة بحق مرتكبي الجرائم عن طريق الانترنت، باعتبارها أصبحت مشكلة خارجة عن السيطرة، فتجاهلها أو منعها تماما ليس حلا واقعيا ذكيا[26]. بل يجب تحديد هوية المجرم وتتبعه من أجل توقيف المشروع الإبتزازي حتى لا يصل لمرحلة النشر.

2-2-1-عقوبات جريمة الابتزاز الإلكتروني: المشرع الجزائري لم يضع موضوع مستقل لجريمة الإبتزاز الإلكتروني وعليه هذه الجريمة تأخذ حكم الإبتزاز عموما في المواد سابقة الذكر، وخصوصيتها أنها تقع في النطاق الافتراضي، حيث تم تجريم أفعال استغلال منتوج التجسس على حرمة الحياة الخاصة، في المادة 303 مكرر ق ع ج وهو نص مأخوذ من قانون العقوبات الفرنسي الجديد لسنة 1992 في المادة 226-2 ق ع فرنسي، تشير إلى أن القاضي الجزائي يهتم على وجه الخصوص بالعناصر المكونة لجنح أفعال التجسس على الحياة الخاصة واستغلاله، ويتجلى ذلك في إعتنائه بعنصر المكان الخاص الذي يعتبره أكثر أهمية من شرط:" المساس بحرمة الحياة الخاصة"[27].

فالمادة 303 مكرر أشارت صراحة إلى السرية من خلال عبارة (أحاديث خاصة أو سرية) كما يشير إلى السكينة من خلال عبارة(المكان الخاص)، وهو المجال الذي يطمئن إليه الشخص وتتحقق له فيه السكينة والهدوء فتتولد له بهما حرمة الحياة الخاصة التي يمنع المساس بها[28].

فالتجريم وارد على من يستعمل التسجيل أو الصورة أو المستند طبقا للشروط المحددة بالنص العقابي سواء تم ذلك الاستعمال في علانية أو في غيرها، فيكون مرتكبا للجريمة الشخص الذي يستخدم محتوى التجسس الذي تم الحصول عليه بطريق غير مشروع طبقا لمقتضيات المادة 303 مكرر ق ع ج،

في الفضاء الرقمي، وهي الوثائق التي يتم الاحتفاظ بها أو وضعها في متناول الجمهور أو الغير أو السماح بذلك أو استعمالها بأية وسيلة كانت[29].

ويلاحظ أيضا أن النص مرن من عبارة(بأي تقنية أو وسيلة تمس بالشخص)، عند ارتكاب الأفعال عن طريق الصحافة، وللقاض السلطة التقديرية في تحديد ذلك، فالنت وما تحتويه من منصات وتقنيات وسيلة إعلام واتصال.

والملاحظ أن القانون الجزائري يعاقب على جنحة استغلال منتوج التجسس متى تحقق النشاط الإجرامي من خلال اجتماع في وقت واحد كل من الشرط المسبق المتمثل في ارتكاب جنحة المادة 303 مكرر، وكذا توافر عناصر أخرى تميز جنحة المادى 303 مكرر1، وذلك كما يأتي:

-شرط وجوب ارتكاب جنحة المادة 303 مكرر بصفة مسبقة: يعني قيام جنحة الحصول على منتوج التجسس سواء أكان صورا أم تسجيلات سمعية أو كتابية، ومن ثم إفشاؤها.

-توافر عناصر خاصة هي: استغلال الوثائق المتحصل عليها بكيفية غير قانونية من خلال: الاحتفاظ بمنتوج التجسس سواء للاستعمال الشخصي أو للغير، استعماله، إفشاؤه. لكن يثور التساؤل حول ما إذا كان كل من قام بفعل الإفشاء مغاير عن فعل الحصول على منتوج التجسس.

وتتم متابعة مرتكب الالتقاط على أساس المادة 303 مكرر باعتباره فاعلا أصليا، وعلى أساس المادة 303 مكرر1 على أساس أنه شريك بتهمة تقديم الدعم والمساعدة لاستغلال منتوج التجسس. كما متابعة مرتكب الالتقاط باعتباره مصدر الانتهاكات كلها طبقا للمادة 303 مكرر لأنه تنازل عن منتوج التجسس، كما تتم متابعة المحتفظ والمستعمل والناشر لمنتوج التجسس بشرط معرفة ليمكن نسبة الجريمة له[30].

وبالنسبة للعقوبات الأصلية فهي مشددة وتتمثل في الحبس والغرامة، بالإضافة إلى العقوبات التكميلية المذكورة في المادة 303 مكرر2 ق ع ج [31].

2-2-2: المسؤولية المدنية عن جريمة الابتزاز الإلكتروني: قد أورد المشرع المدني نصا عاما يحمي الحقوق اللصيقة بشخصية الإنسان، حيث يمكن بمقتضاه أدرج الحياة الخاصة ضمن تلك الحقوق من خلال المادة 47 من القانون المدني،

هذا بالنسبة للأشخاص غير المعرضين للأضواء يكون التصور واسع جدا لحرمة الحياة الخاصة، عكس الأشخاص الذين المعرضين للأضواء الذين يضيق لهم مفهوم الحياة الخاصة، بسبب وضعهم أنفسهم تحت الأضواء مما يثير الفضول وحب الاستطلاع حولهم، فحماية حرمة الحياة الخاصة من كل الانتهاكات خصوصا من جريمة الابتزاز الإلكتروني تمكن الشخص من المطالبة بالتعويض عن الأضرار التي لحقت بالشخص المضرور بناء على المادة (47) ق مدني ج[32]، حيث يكفي المضرور إثبات الخطأ أو الاعتداء بأي صورة كان، فيكون له الحق في التعويض إلى جانب المتابعة الجزائية، وللقاضي السلطة التقديرية في تأكيد الضرر أو نفيه، وتقدير مقداره متى أثبت عنده فهو مفترض بمجرد المساس بالحق في الحياة الخاصة وقد يكون الضرر ماديا أو معنويا، (المادة182مكرر) ق مدني ج [33]. و(المادة3) ق إ ج ج التي نصت على قبول دعوى المسؤولية المدنية عن كافة أوجه الضرر سواء كانت مادية أو جثمانية أو أدبية ناجمة عن الوقائع موضوع الدعوى الجزائية .

وعليه فكل اعتداء على هذا الحق بأي صورة كانت ينشئ للمضرور الحق في رفع دعوى للمطالبة بالتعويض المناسب من أجل إزالة الضرر أو التقليل منه بطريقة مناسبة، ويعود للسلطة التقديرية للقاضي، لأنه يمس عناصر لا تقبل التقويم المالي، إذ لابد أن يتلاءم مع الضرر الذي يلحق بالضحية. وذلك بالرجوع إلى نصوص القانون المدني من المواد 131 إلى 134 والمواد 181 و182 مكرر، ويكون التعويض عينيا أو نقديا أو غير نقدي مثل رد الاعتبار عن طريق الاعتذار العلني.

خاتمة:

إن الحق في حرمة الحياة الخاصة من الحقوق الملازمة للشخصية التي تستوجب تكريس حماية دستورية وجنائية وإجرائية ومدنية من أجل عدم انتهاك خصوصا من الإبتزاز الإلكتروني ، من خلال:

-تحديد مفهوم الحياة الخاصة وحدودها وعناصرها بعيدا عن التضييق والغموض من خلال توسيع نطاقها، مما يوفر حماية أكبر لها ضد شتى أنواع الانتهاك خاصة الابتزاز الإلكتروني.

-اعتبار التهديد بإفشاء أمور خادشة للشرف وتوجيه عبارات فضائحية تمس سمعة الضحية جريمة ابتزاز، ويكفي للعقاب بموجبها أن يكون الجاني قد أعد رسالة التهديد لتصل إلى علم المراد تهديده سواء أرسلها إليه مباشرة أم أبلغ بها.
-وجوب النص صراحة على تجريم الإبتزاز الإلكتروني والذي يتضمن التهديد والمساومة بمنتوج رقمي للحصول على مزيا مادية أو معنوية أو جنسية. مع تشديد العقوبات أو اعتبار النت ظرف مشدد للعقوبة، لأن تطبيق القانون التقليدي غير كاف ودائما تكون عقوبته أخف.
-أخذ تدابير الحيطة والحذر من خلال تقوية الحسابات الافتراضية عن طريق تفعيل إجراءات الخصوصية اختيار كلمات سرية قوية وتغييرها دوريا.
-عدم جعل الأسرار الشخصية متاحة بتفاصيلها للعامة، مع التعامل بحذر مع الغرباء في العالم الإفتراضي، والقيام بحظر كل شخص مشبوه أو تبدو نواياه الإجرامية.
-للقاض سلطة تقديرية في تكييف قضايا الابتزاز وتشديد العقوبة لها، أو تخفيفها وذلك حسب الظروف التي ارتكبت في نطاقها وطبيعة الشخص الذي ارتكبها فيما إذا كان مجرم محترف أو لديه سوابق قضائية، أو مجرد هاوي أو للتسلية.
-الخضوع لمطالب لمجرم أو الخوف منه أو استفزازه من شأنه أن يزيد في هيمنته وتعنته، لهذا من الواجب الإسراع للتشكي عليه دون إعلامه بذلك حتى لا يأخذ احتياطاته، أي التصرف بحكمة وتريث لاستدرجه للوقوع في أيدي قوات الأمن. وإذا كان المجرم من دولة أخرى غير التي يتواجد فيها الضحية أو الشخص الواقع عليه التشهير، ففي هذه الحالة يجب إبلاغ سفارة الدولة التي يتواجد بها المجرم أو الاتصال بمحامي مختص من تلك الدولة، حيث يتم تقديم كافة المعلومات المتوفرة عن الجاني مما يساعد على تحديد هويته .
-تدريب موظفي تطبيق القوانين على خصائص المنصات الرقمية للتعاطي مع الإشكاليات العملية أثناء نظرها هذا النوع من القضايا، مثل إعدادات الخصوصية التي يستخدمها الأشخاص.

-الاتصال فورا بالجهة المختصة لأنها الأقدر للتعامل مع الجاني، مع عدم مسح المحتوى محل الابتزاز مهما كان جد حميمي وحساس ومحرج، وتسليمه للجهات الأمنية لأنه يشكل دليل إدانة الجاني.
-ضرورة عدم بقاء الضحية لوحدها والاسراع بطلب الدعم المادي والمعنوي من شخص موثوق فيه حتى يتم تجاوز المحنة.
-ضرورة تعاون كل فعاليات المجتمع من أجل نشر التوعية بمخاطر العالم الرقمي خصوصا على النشء مع اتخاذ كل الاجراءات الاحترازية للحيلولة دون وقوع الأشخاص ضحايا للابتزاز الإلكتروني من ذوي الميول الإجرامية.
-القيام بالتخلص من محتويات الهواتف والألواح الذكية والحواسيب قبل بيعها، والتأكد من ذلك بالطرق التقنية المتطورة المناسبة.

الهوامش

(1)-مغبغب، نعيم (2008) مخاطر المعلوماتية والأنترنت، المخاطر على الحياة الخاصة وحمايتها، دراسة في القانون المقارن، بيروت، منشورات الحلبي الحقوقية، ط2، ص 121.
(2)-الزغبي، علي أحمد (2006) حق الخصوصية في القانون الجنائي، دراسة مقارنة، طرابلس، لبنان، المؤسسة الحديثة للكتاب، دط، 129-136.
(3)-حيث نصت المادة 46 من الدستور الجزائري على أنه:"لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، يحميها القانون.
سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.
لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية، ويعاقب القانون على انتهاك هذا الحكم.
حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه". القانون رقم 16-01 المؤرخ في 26 جمادى الأولى عام 1437 الموافق لـ6 مارس 2016، المتضمن التعديل الدستوري، ج ر 53، ع 14، الإثنين 27 جمادى الأولى عام 1437 الموافق لـ7 مارس 2016.
(4)-نويري عبد العزيز، (2016)الحماية الجزائية للحياة الخاصة في القانونين الجزائري والفرنسي، دراسة مقارنة، الجزائر، دار هومة، ط2، ص 60.

(5)-بركات، وجدي محمد و توفيق، توفيق عبد المنعم (2009) الأطفال والعوالم الافتراضية- مؤتمر الطفولة في عالم متغير، 18-19 ماي، البحرين، مملكة البحرين، الجمعية البحرينية لتنمية الطفولة، ص2.

(6)-الأستاذ، سوزان عدنان(2013)، انتهاك الحياة الخاصة عبر الأنترنت، دراسة مقارنة، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، دمشق جامعة دمشق، كلية الحقوق،- قسم القانون الجنائي، مج 29، ع 3 ، ص423-424.

(7)-نجاء المطيري، سامي مرزوق(2015)، المسؤولية الجنائية عن الإبتزاز الإلكتروني في النظام السعودي دراسة مقارنة، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في الشريعة والقانون، إشراف: عبد الفتاح باباه باباه، الرياض، أكاديمية نايف العربية للعلوم الأمنية، كلية العدالة الجنائية، قسم الشريعة والقانون، ص13.

(8)-العنزي، ممدوح رشيد مشرف الرشيد،(1439-2017)«الحماية الجنائية للمجني عليه»، المجلة العربية للدراسات الأمنية، الرياض، أكاديمية نايف العربية للعلوم الأمنية، مج 33، ع 70، ص 193-220.

(9)-حمد، أمل كاظم (د ت)، إدمان الاطفال والمراهقين على الأنترنت وعلاقته بالإنحراف، مجلة العلوم النفسية، جامعة بغداد، كلية التربية ابن الهيثم، قسم التربية وعلم النفس، ع19، ص 113.

(10)-سوزان عدنان الأستاذ، مرجع سابق، ص433-434.

(11)-تقرير السلامة على الأنترنت، (2015)، دراسة بحثية حول سلوك الشباب العربي على الأنترنت والمخاطر التي يتعرضون لها، ICDL arabia، ص 25.

(12)-البداينة، ذياب (1424 ه)، جرائم الحاسب الآلي والأنترنت، بحث منشور في ندوة الظواهر الإجرامية المستحدثة وسبل مواجهتها، الرياض، أكاديمية نايف العربية للعلوم الأمنية، ، ص 112.

(13)-سامي مرزوق نجاء المطيري، مرجع سابق، ص 13-22.

(14)-العنزي، ممدوح رشيد مشرف الرشيد، مرجع سابق، ص 193-220.

(15)-الداحي، محمد، (2006)، جريمتا السرقة والابتزاز، دراسة مقارنة، عين مليلة، دار الهدى، دط، ص 45.

(16)-سامي مرزوف نجاء المطيري، مرجع سابق، ص40-43.

(17)-عبد المطلب ممدوح (2006)، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والأنترنت، مصر، دار الكتب القانونية، دط، ص 88.

[18]-البشري، محمد الأمين(2004)، التحقيق في الجرائم المستحدثة، الرياض، أكاديمية نايف العربية للعلوم الأمنية، ط1، ص234.
[19]-سلمان، عودة يوسف (دت)، الجرائم الماسة بحرمة الحياة الخاصة التي تقع عبر وسائل تقنية المعلومات الحديثة، العراق، كلية الرافدين، قسم القانون، ص 9.
[20]-المرجع نفسه، ص 71.
[21]-العبيدي، أسامة بن غانم (دت)، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب، الرياض، أكاديمية نايف العربية للعلوم الأمنية، مج 29، ع 58، ص115-120.
[22]–قانون رقم 09-04 مؤرخ في 14 شعبان 1430الموافق لـ5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر مؤرخة بتاريخ 25 شعبان عام 1430 الموافق لـ16 غشت 2009، ع 47.
[23]–كما تنص الفقرة 4 من المادة نفسها على أنه يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.
[24]-على أحمد الزغبي، مرجع سابق، ص 315.
[25]-سامي مرزوق نجاء المطيري، مرجع سابق، ص 85-88.
[26]-أمل كاظم حمد، مرجه سابق، ص 113-114.
[27]-نويري عبد العزيز، مرجع سابق، ص121.
[28]-بن ذياب، عبد المالك، (2013/2012)، حق الخصوصية في التشريع العقابي الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، إشراف: زرارة صالحي الواسعة، باتنة، جامعة الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم الحقوق، ص281.
[29]-المرجع نفسه، ص 123-124.
[30]-نويري عبد العزيز، مرجع سابق، ص293-301.
[31]-القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، ج ر 84، ص23.
[32] – التي جاء فيها: « لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته، أن يطلب وفق هذا الاعتداء والتعويض، عما قد يكون لحقه من ضرر". الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق لـ26 سبتمبر عام 1975 المتضمن القانون المدني المعدل والمتمم.

[33] – التي جاء فيها:" يشمل التعويض عن الضرر المعنوي كل مساس بالحرية أو الشرف أو السمعة". مضافة بموجب القانون رقم 10/05 المؤرخ في 20 يونيو 2005، ج ر 5 ص 24.

قائمة المراجع

أولا-القوانين

[1]-القانون رقم 16-01 المؤرخ في 26 جمادى الأولى عام 1437 الموافق لـ6 مارس 2016، المتضمن التعديل الدستوري، ج ر 53، ع 14، الإثنين 27 جمادى الأولى عام 1437 الموافق لـ7 مارس 2016.

[2]-الأمر رقم 66-156، المؤرخ في 18 صفر 1386، الموافق لـ8 جوان 1966 المتضمن قانون العقوبات، المعدل والمتمم بالأمر رقم 75-47 المؤرخ في 17 يونيو 1975، ج ر 53، ص 755، والقانون رقم 82-04 المؤرخ في 13 فيفري 1982، ج ر 7 ص327، والقانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، ج ر 84، ص23. والقانون رقم 14-01 المؤرخ في 4 فيفري 2014 المعدل والمتمم لقانون العقوبات الجزائري، ج ر رقم 07.

[3] – الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق لـ26 سبتمبر عام 1975 المتضمن القانون المدني المعدل والمتمم بموجب القانون رقم 10/05 المؤرخ في 20 يونيو 2005، ج ر 5 ص 24.

[4]–قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق لـ5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر مؤرخة بتاريخ 25 شعبان1430 الموافق لـ16 غشت سنة 2009، ع 47.

ثانيا-الكتب

[1]-البشري، محمد الأمين(2004)، التحقيق في الجرائم المستحدثة، الرياض، أكاديمية نايف العربية للعلوم الأمنية، ط1.

[2]-الداحي، محمد، (2006)جريمتا السرقة والابتزاز، دراسة مقارنة، عين مليلة، دار الهدى، دط.

[3]- الزغبي، علي أحمد (2006) حق الخصوصية في القانون الجنائي، دراسة مقارنة، طرابلس، لبنان، المؤسسة الحديثة للكتاب، دط.

[4]- عبد الحميد، عبد المطلب ممدوح (2006)، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والأنترنت، مصر، دار الكتب القانونية، دط.
[5]- مغبغب، نعيم (2008) مخاطر المعلوماتية والأنترنت، المخاطر على الحياة الخاصة وحمايتها، دراسة في القانون المقارن، بيروت، منشورات الحلبي الحقوقية، ط2.
[6]- نويري عبد العزيز، (2016)الحماية الجزائية للحياة الخاصة في القانونين الجزائري والفرنسي، دراسة مقارنة، الجزائر، دار هومة، ط2.

ثالثا-مقالات ومذكرات ومؤتمرات علمية

[1]-الأستاذ، سوزان عدنان(2013)، انتهاك الحياة الخاصة عبر الأنترنت، دراسة مقارنة، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، دمشق جامعة دمشق، كلية الحقوق قسم القانون الجنائي، مج 29، ع 3.
[2]-البداينة، ذياب (1424هـ)، جرائم الحاسب الآلي والأنترنت، بحث منشور في ندوة الظواهر الإجرامية المستحدثة وسبل مواجهتها، الرياض، أكاديمية نايف العربية للعلوم الأمنية.
[3]-بركات، وجدي محمد وتوفيق، توفيق عبد المنعم (2009) الأطفال والعوالم الافتراضية- مؤتمر الطفولة في عالم متغير، 18-19 ماي، البحرين، مملكة البحرين، الجمعية البحرينية لتنمية الطفولة.
[4]-حمد، أمل كاظم (د ت)، إدمان الاطفال والمراهقين على الأنترنت وعلاقته بالإنحراف، مجلة العلوم النفسية، جامعة بغداد، كلية التربية ابن الهيثم، قسم التربية وعلم النفس، ع19.
[5]-بن ذياب، عبد المالك،(2013/2012)، حق الخصوصية في التشريع العقابي الجزائري، مذكرة مقدمة لنيل شهادة الماجستير تخصص علوم جنائية، إشراف: زرارة صالحي الواسعة، باتنة، جامعة الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم الحقوق.
[6]-سلمان، عودة يوسف (دت)، الجرائم الماسة بحرمة الحياة الخاصة التي تقع عبر وسائل تقنية المعلومات الحديثة، العراق، كلية الرافدين، قسم القانون.
[33]-العبيدي، أسامة بن غانم (دت)، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب، الرياض، أكاديمية نايف العربية للعلوم الأمنية، مج 29، ع 58.

[7]-العنزي، ممدوح رشيد مشرف الرشيد،(2017)، الحماية الجنائية للمجني عليه، المجلة العربية للدراسات الأمنية، الرياض، أكاديمية نايف العربية للعلوم الأمنية، مج 33، ع 70.

[8]-نجاء المطيري، سامي مرزوق(2015)، المسؤولية الجنائية عن الإبتزاز الإلكتروني في النظام السعودي دراسة مقارنة، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في الشريعة والقانون، إشراف: عبد الفتاح باباه باباه، الرياض، أكاديمية نايف العربية للعلوم الأمنية، كلية العدالة الجنائية، قسم الشريعة والقانون.

رابعا-مراجع إلكترونية

[1]-تقرير السلامة على الأنترنت، (2015)، دراسة بحثية حول سلوك الشباب العربي على الأنترنت والمخاطر التي يتعرضون لها، ICDL Arabia