مجلة الدراسات القانونية المقارنة

EISSN:2600-6154 **المجلد 07/ العـــدد01 (2021)، ص.ص.1205-1234** **ISSN:2478-0022**

جريمة التهديد والابتزاز الإلكتروني

The crime of electronic extortion

عراب مريم

ARAB Meriem

أستاذة محاضرة صنف (ب)

كلية الحقوق والعلوم السياسية، جامعة وهران2، أحمد بن أحمد

Lecturer Class B

Faculty of Law and Political Science, University of Oran 2, Mohammed ben Ahmed

senouci_meriem@yahoo.fr

تاريخ إرسال المقال:2020/11/23 **تاريخ القبول:2021/05/05** **تاريخ النشر:2021/06/28**

ملخص:

شهد العالم منذ منتصف القرن العشرين تطورات في مجال التقنية الإلكترونية التي تعد موردا لا يقل ولا ينضب، وتعد تكنولوجيا المعلومات الحديثة وليدة الإندماج الذي حصل بين الحوسبة والاتصال، وإن استخدام أي جهاز إلكتروني يمنح العديد من المزايا التي تقابلها العديد من الجرائم التي تقع عبر وسائل تقنية المعلومات الحديثة منها ما يمس حياة الأشخاص.

تعرض هذه الدراسة جريمة التهديد بالابتزاز الإلكتروني في التشريع الجزائري، وقد تناولت هذه الجريمة كصورة من صور الجرائم الإلكترونية، فتعرضت لتعريفها وأنواعها وطرق ارتكابها، والوسائل الحديثة المستخدمة في تنفيذها، وكذا أركانها (الركن الشرعي والركن المادي والركن المعنوي).

وتعالج الدراسة أيضا الإشكاليات التي تثيرها جريمة التهديد بالابتزاز الإلكتروني من الجانب الإجرائي من إجراءات التحقيق، وخصوصيتها التي تلقي بصعوبات أمام جهات التحقيق، كما تتعرض لأهم طرق الإثبات التي تختص بها الجريمة الإكترونية وهي الدليل الرقمي، وتنتهي الدراسة بعرض دور الجهات الأمنية في الجزائر في مكافحة الجريمة المعلوماتية.

كلمات مفتاحية:

الجرائم، التهديد، الاتصالات، الأنترنت، الحاسب الآلي.

Abstract:

Since the middle of the twentieth century, the world has witnessed developments in the field of electronic technology, which is an inexhaustible

Email: senouci_meriem@yahoo.fr **المؤلف المرسل: عراب مريم**

resource: Modern information technologies is the result of the merger that occurred between measles and communication, and the use of any electronique device gives many advantages that are offset by many crimes that occur through modern information technologies means that affect the sanctity of persons life.

This study deals with the crime of electronic extortion in Algerian law. It first dealt with this crime as a form of cybercrime. It was presented to define the crime, the types of crime, the ways of committing it, and the modern means used in executing the crime. And the elements of the constituent elements of the text of the system (the legal pilar) and the physical and moral pilar, and the study addresses the problems raised by the crime of electronic by procedure terms to solve the investigation, and the specificity of these procedures, which give obstacles and difficulties to the investigation authorities.

We also present the most important methods to proof of the crime of electronic, namely the digital evidence, the study concludes with presenting the role of security agencies in Algeria in combating information crime.

Keywords:

Crime-Extortion - Communication - Internet-Computer.

المقدمة:

عرف العالم تطور هائل في المجال العلمي والتقني بسبب ظهور الأنترنت، وهذا التطور يمكن أن يكون سلاحا ذو حدين، الأمر الذي دفع بالمشرفين تنظيم هذا المجال بما يخدم حقوق الأنترنت من كل اعتداء، إلا أنه في هذا العالم الرقمي كرست مجموعة من الفئات المجرمة جهودها لاستغلال هذه التقنيات العالية وتوجيهها لتنفيذ إجرامهم وغرائزهم، حيث جعلت الطرف الأخر سلعة لاستغلالهم عن طريق التهديد عبر رسائل التواصل الاجتماعي من خلال نشر صورهم أو فيديوهاتهم أو معلومات عنهم، و قد يكون الضحية شخصا طبيعيا كما يمكن أن يكون شخصا معنويا، فقد استغل المجرمون ما أتاحه العصر الحديث من تقدم في مجال الأنترنت، لاستحداث أساليب جديدة واستخدام وسائل علمية في تهديد الأشخاص، والتي لم تتناولها النصوص القانونية بصريح العبارة و لم تجرم الاعتداء عليها.

وبالتالي فإن جريمة التهديد والابتزاز عبر الوسائط الإلكترونية يتعدى الإشكالية التقليدية التي تناولتها الدراسات الفقهية، وقلة من الدراسات من سلطت الضوء على الجرائم المعلوماتية، ولا سيما بعد انتشار مواقع الدردشة، وشبكات التواصل الاجتماعي مثل: YouTube-Facebook- Twitter والمشكلة أن الأفراد يفرطون في خصوصيتهم من خلال وضع معلومات عن أنفسهم وصور شخصية لهم ومقاطع فيديو تكون متاحة للجميع، وعرضة للمتطفلين أو الهاكرز[1] أو حتى محترفي الإجرام المعلوماتي، والأسوأ أن الكثير من المراهقين والأطفال كانوا فريسة سهلة للابتزاز تارة والتغرير بهم تارة أخرى من قبل مجرمي الإنترنت .

وقد أصبحت جريمة الابتزاز الإلكتروني وهي أحد صور الجريمة الإلكترونية ظاهرة تخترق المجتمع وتهدد دعائمه، وسبب تجريم جريمة الابتزاز الإلكتروني هو الضغط الذي يمارس المجرم على الضحية، بتهديده بإفشاء سرِه، مما يضطر معه إلى الانصياع والاذعان لرغبة الجاني، وتحقيق مطالبه المشروعة أو الغير مشروعة تحت اكراه من الخوف من الفضيحة،

المشرع الجزائري لم يتطرق لجريمة التهديد الإلكتروني ونظرا للأهمية التي بات يوليها لكل ما يتعلق بالمعلوماتية حاول بجد تطوير المنظومة القانونية، وإصدار تشريعات تواكب التطور الحاصل في المجال التكنولوجي، ومن أبرز التعديلات ما ورد في القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004[2]المتضمن "جرائم المساس بأنظمة المعالجة الألية للمعطيات"، ثم القانون رقم 09- 04ا لمؤرخ في 05 سبتمبر 2009[3]، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال".

وأخيرا إصداره للقانون رقم 18_07 بتاريخ 10 جوان 2018[4] المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الذي يعد الإطار التشريعي المنظم للمسائل المتعلقة بحماية المعطيات الشخصية في الجزائر.

وأمام الخطر الذي لا يستهان به على الحياة الخاصة من الانتهاك والتهديد في مجال المعلوماتية، تتمحور إشكالية البحث في تحديد ماهية جريمة التهديد والابتزاز الإلكتروني ؟ وهل الحماية التي جاء بها المشرع الجزائري في القانون الجنائي كافية لحماية الأشخاص من هذه الجريمة ؟ وما مدى كفاية النصوص الحالية في مكافحتها ومواجهتها؟.

وعليه سوف نعالج الموضوع وفقا لخطة مفصلة تتكون من مبحثين:

في المبحث الأول سنتطرق لمفهوم جريمة التهديد والإبتزاز الإلكتروني وأركانها وصورها ووسائل إرتكابها، أما المبحث الثاني فيتضمن الأليات القانونية لمكافحة الجريمة بتحديد اجراءات التحقيق في الجريمة وطرق إثباتها ودور الجهات الأمنية الجزائرية في مواجهتها.

وسنحاول الإجابة على الكثير من التساؤلات عن الجريمة ونقدم بعض المقترحات والتوصيات.

المبحث الأول: الإطار الموضوعي لجريمة التهديد والإبتزاز الإلكتروني

إن إرتباط الحياة الخاصة للأشخاص بالمعلوماتية في ظل الحواسيب والأنترنت، جعلهم عرضة بمختلف أشكال وصور التهديد بالإبتزاز، ولتحديد هذه الجريمة لابد من تناول هذا المبحث في مطلبين:

المطلب الأول: المقصود بجريمة التهديد والإبتزاز الإلكتروني ومدى خطورتها وأركانها

المطلب الثاني: صور جريمة التهديد والإبتزاز الإلكتروني وطرق إرتكابها

المطلب الأول: المقصود بجريمة التهديد والإبتزاز الإلكتروني ومدى خطورتها وأركانها:

لم تعرف التشريعات الجنائية جريمة التهديد والإبتزاز الإلكتروني وترك أمر ذلك لفقهاء القانون الجنائي.

الفرع الأول: تعريف جريمة التهديد والإبتزاز الإلكتروني ومدى خطورتها

يقصد بالتهديد نشر وزرع الخوف في نفسية الشخص، بالضغط على إرادته وتخويفه من أن ضررا ما سيلحق به أو سيلحق أشخاص أو أشياء له بها صلة.[5]

أولا: تعريف جريمة التهديد والإبتزاز الإلكتروني

أ: التعريف اللغوي:

التهديد في اللغة هو" الوعيد والتخويف"، يقال هدد يهدد تهديدا أي خوفه وهدده بالعقوبة.

ب: التعريف الإصطلاحي:

جريمة التهديد و الابتزاز الإلكتروني هي إحدى صور الجرائم الإلكترونية(Cyber-crimes) وهي تتكون من مقطعين هما الجريمة (Crime)، والمقطع الآخر (Cyber) وهي السيبرانية، ويستخدم مصطلح الإلكترونية لوصف فكرة أن الجريمة تتم من خلال التقنية الحديثة، أما الجريمة فهي تلك الأفعال المخالفة للقانون، وقد اصطلح على تعريف الجرائم الإلكترونية بأنها:" المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد ايذاء سمعة الضحية أو أذى مادي أو عقلي مباشر أو غير مباشر باستخدام شبكات الاتصال مثل الانترنت(غرف الدردشة، البريد الإلكتروني، والهاتف النقال، والحاسب الآلي)".

كما عرف فقهاء القانون الجنائي التهديد بأنه: " كل قول أو كتابة من شأنه إلقاء الرعب والخوف في قلب الشخص المهدد من ارتكاب الجاني للجريمة ضد النفس أو المال أو إفشاء أو نسبة أمور مخدشة للشرف، وقد يحمله التهديد تحت تأثير ذلك الخوف إلى استجابة الجاني إلى ما ابتغى متى اصطحب التهديد بطلب"، وهناك من عرفه بأنه: " تخويف المجني عليه وإلقاء حالة الرعب في نفسه وإزعاجه من ضرر معين يراد إيقاعه به". [6]

وهو" ترويع المجني عليه وإلقاء الرعب في قلبه يتوعده بإنزال شر عليه".[7]

واستنادا لكل هذه التعاريف نستخلص بأن التهديد من الجرائم التي من شأنها أن تحدث أثرا خطيرا في نفس المجني عليه، تتمثل في إلحاق حالة الرعب والقلق لما سيلحق به أو بشخص له علاقة به أو بماله أو إفشاء أمور ماسة بحياته الشخصية أو بشرفه.

ثانيا: المقصود بجريمة التهديد والابتزاز الإلكتروني

التهديد الإلكتروني هو حصول فعل التهديد باستعمال الوسائط الإلكترونية، أو هو عملية تهديد وترهيب للضحية بنشر صور وفيديوهات أو تسريب معلومات تخص الضحية، مقابل دفع هذا الأخير لمبلغ مالي أو استغلاله للقيام بأعمال غير مشروعة لصالح الجاني، وعادة ما يتم الإطاحة بالضحايا عن طريق البريد الإلكتروني أو وسائل التواصل الاجتماعي، نظرا لانتشارها الواسع واستخدامها الكبير.[8]

والمشكلة أن الأشخاص يفرطون في خصوصيتهم عبر الأنترنت مما يشكل خطرا على حياتهم من كل أشكال وصور الإعتداء عليها، في الوقت الذي لم يفرد فيه المشرع الجنائي نصوص خاصة لحماية خصوصية الأفراد عبر الأنترنت.

ثالثا: مدى خطورة جريمة التهديد الإلكتروني

بعد انتشار بنوك المعلومات أو ما يسمى بهستيريا التواصل الاجتماعي عبر شبكة الأنترنت من خلال مواقع الدردشة، إذا كثيرا من الناس كبارا أو صغارا يضعون معلومات شخصية، وصور ومقاطع فيديو خاصة بهم والتي تكون عرضة للمتطفلين أو الهاكرز أو مجرمي الأنترنت الذين احترفوا سلوكيات الاعتداء على خصوصية الأفراد عبر الوسائل الإلكترونية، خاصة الضعفاء منهم، كالنساء والمراهقين، وتكمن خطورة التهديد هنا في جعل هؤلاء الضحايا يقبلون على الانتحار أو القتل من قبل عائلاتهم .

في الوقت الذي يعرف الإحجام عن الإبلاغ ورفع قضايا على المجرمين، لأنه غالبا ما تكون مثل هذه التهديدات والابتزازات محرجة للضحايا، وفي كثير من الأحيان ما تكون مدمرة لحياة الضحية الاجتماعية، وهو ما أدى إلى عدم وجود إحصائيات إلى هذا النوع من الجرائم.[9]

وبالتالي فإن حياة الأشخاص وشعورهم بالأمان في أموالهم وعرضهم، من أهم الأمور أو الأغراض السياسية التي يجب على المجتمعات مراعاتها، بتوفير حماية قانونية فعالة تهدف إلى إيقاع من يعتدي عليها تحت طائلة القانون.

الفرع الثاني: أركان جريمة التهديد والابتزاز الإلكتروني

وفقا للنموذج الإجرامي فإن الجريمة حتى تقع يجب أن يكون هناك ركنان أحدهما مادي والأخر معنوي، وجريمة التهديد مثل كل الجرائم يتطلب لقيامها هذين الركنين:

أولا: الركن المادي لجريمة التهديد والابتزاز الإلكتروني

يعتبر الركن المادي للجريمة السلوك الذي يظهر إلى حيز الوجود، فهو يبرز الجريمة ويجعلها تخرج إلى العالم الخارجي، ولا تختلف جريمة التهديد الإلكتروني في أركانها عن جريمة التهديد التقليدي، فهي تتطلبسلوك إجرامي يصدر من الجاني سواء بالقول أو الكتابة أو أي فعل أخر يتمثل في القيام بفعل التهديد بنشر البيانات أو الصور أو مقاطع فيديو للضحية، ولا يهم من أين حصل عليها، فيمكن أن يكون قد حصل عليها باختراق حساب الضحية أو أنه عثر عليها في جهاز الضحية المسروق أو المعثور عليه، كما لا يشترط أن يتم التهديد بطريقة معينة، فيمكن أن يتم عن طريق غرف الدردشة أو عن طريق البريد الإلكتروني أو بتسجيل صوتي، كما لا يهم إن كان الابتزاز لمصلحة المبتز المشروعة أو غير المشروعة، فالعبرة في استخدام الضغط والإكراه المقترن بالتهديد لإرغام المجني عليه للقيام بذلك الفعل.

وبالتالي فعناصر الركن المادي للجريمة ثلاثة: الفعل أو النشاط الإجرامي والنتيجة والعلاقة السببية بينهما.

فهي تتطلب سلوك إجرامي يتم عبر وسائل التواصل الاجتماعي أو الحاسب الألي ويعتبر تهديدا كل قول أو كتابة أو رموز أو صور أو شعارات من شأنه إلقاء الرعب والخوف في قلب الشخص المهدد، ولا يهم إن كان الجاني ينوي تنفيذ الأمر المهدد به أم لا، فقط يشترط أن يكون جديا وليس مجرد هزل.

ثانيا: الركن المعنوي لجريمة التهديد والابتزاز الإلكتروني

المسؤولية لا تقرر لمجرد وقوع الفعل المادي للجريمة فلابد لدور الإرادة في الجريمة، أو ما يسمى بالقصد الجنائي، الذي يتخذ صورتين القصد الجنائي العام والقصد الجنائي الخاص.

أي لابد أن يعلم الجاني بنتيجة السلوك الذي يرتكبه، والوقائع التي تتصل بها، والتي تعد من عناصر الجريمة والعلم بموضوع الجريمة، فيجب أن ينصب علمه على أن ما يقوم به من الحصول على صور فاضحة لحد الأشخاص وتهديده بهذه الصور مقابل الحصول على منفعة جريمة يعاقب عليها القانون، هنا يتحقق العلم وتكتمل أركان الجريمة، كما ينبغي ان يعلم أن فعله يلحق ضررا بالمجني عليه، ولا عبرة في قيام القصد ان انصرفت الإرادة إلى هذه النتيجة إذ يكفي توقعها.

ولكي تقوم المسؤولية الجنائية يجب اثبات ان إرادة الفاعل اتجهت إلى القيام بهذا الفعل، وذلك دون أن تقع ارادته في عيب من عيوب الإرادة، كأن يكون مدركا أنه يحصل على معلومات وصور سرية وخاصة بالضحية من مستودع

اسرار الأخير، فإن كان مكرها فلا يوجد قصد جنائي، ولا تقوم مسؤولية الفاعل المكره، كما أنه لابد أن يتحقق القسم الثاني من الإرادة وهو إرادة النتيجة فلابد أن تتجه إرادة الجاني إلى تحقق النتيجة الاجرامية من فعله بالحصول على المنفعة المادية أو المعنوية أو اللاأخلاقية، ويجب أن يكون التهديد جدي بدرجة كافية للتأثير في نفسية المجني عليه.

ثالثا: الركن الشرعي لجريمة التهديد

الركن الشرعي في الجريمة هو نص التجريم أو التحريم والعقاب، فهو النص الذي نستند اليه لتجريم فعل والعقاب عليه، وأن يكون هذا النص ساريا من حيث الزمان والمكان والأشخاص على مرتكب الفعل الإجرامي، ومن هذا ظهرت القاعدة القانونية الأشهر وهي" لا جريمة ولا عقوبة بغير نص" وهو ما يعرف بمبدأ الشرعية الجنائية.

إن النتيجة الحتمية لمبدأ الشرعية الجنائية تتمثل في انحصار مصادر التجريم والعقاب في فكرة التشريع لأنه لا جريمة ولا عقوبة إلا بنص خاص، وهذا يعتبر ضمانا للمجرم بحيث لا توقع عليه أي عقوبة غير تلك المنصوص عليها، وبالتالي وأمام التزايد المستمر للجرائم المعلوماتية، باشرت معظم الدول أليات قانونية تمثلت في المواجهة التشريعية للإجرام على الصعيد الوطني، وذلك بمساهمة كل دولة بتشريعها الداخلي بإيجاد النصوص القانونية الكفيلة بمكافحة الجريمة وقمعها والردع لمرتكبيها، وذلك بحسب قدراتها وظروفها ومصالحها، فالبعض سارع لمواجهة الجريمة بسن تشريع مستقل، والبعض الأخر اكتفى بتطبيق النصوص التقليدية.

لقد استقر الفكر القانوني على ضرورة وجود نصوص خاصة لمواجهة الجريمة المعلوماتية، خاصة مع ظهور شبكة الأنترنت التي ساهمت بشكل خطير في تفشي هذه الجريمة، فقامت الدول بتبني نصوص عقابية خاصة بالجريمة المعلوماتية وقد ترددت في اختيار التقنية التشريعية المناسبة، فمنها من قام بإدماج نصوص خاصة بالإجرام المعلوماتي في قانون العقوبات التقليدي ومنها من وضع قانون جنائي مستقل للمعلوماتية.

فالركن الشرعي في الجرائم المعلوماتية هو نص التجريم الواجب التطبيق على الفعل والعقوبة المقررة له، ومعظم الدول التي تستعمل تكنولوجيا الإعلام والاتصال سنت تشريع جنائي تجرم السلوك الذي يرتكبه المجرم باستخدام وسائل تكنولوجيا الإعلام والاتصال يضر بمصلحة الأشخاص.

وبالرجوع للقانون الجزائري فنجد أن جريمة التهديد الإلكترونية بصفة عامة لم تنل حضها في قانون العقوبات، وبالرجوع للقواعد التقليدية الخاصة بجريمة التهديد وفق المواد من 284 إلى 287 من قانون العقوبات الجزائري، فقدعاقبت المادة 284 كل من هدد بإرتكاب جرائم القتل أو السجن أو أي إعتداء أخر على الأشخاص مما يعاقب عليها بالإعدام أو السجن المؤبد وكان ذلك بمحرر موقع أو غير موقع عليه أو بصور أو رموز أو شعارات يعاقب بالحبس من سنتين إلى عشر سنوات وبغرامة من 20 000 إلى 100 000 دج إذا كان التهديد مصحوبا بأمر بإيداع مبلغ من النقود في مكان معين أو بتنفيذ أي شرط أخر.

وقد يكون التهديد كتابة أو شفاهة، فالمادة 287 من قانون العقوبات الجزائري تتضمن في فحواها بأنه: يعاقب بالحبس من ثلاث أشهر إلى سنة، وبغرامة من 20.000 إلى 100.000 دج، إذا كان ومصحوبا بأمر أو شرط التهديد بالعنف أو القتل.

المطلب الثاني: صور جريمة التهديد والابتزاز الإلكتروني وطرق ارتكابها:

إن تطور الحواسيب الرقمية وتكنولوجيا المعلومات أتاح نقل النشاط الاجتماعي والتفافي والسياسي والاقتصادي من العالم المادي إلى العالم الافتراضي، وهذا التطور رافقه خطر حقيقي تتمثل في إمكانية جمع المعلومات وتخزينها والاتصال بها، والوصول إليها بعدة طرق غير مشروعة وقانونية بدون علم ومعرفة صاحبها، وهذا ما يشكل إعتداء على حياة الأشخاص.

الفرع الأول: صور التهديد والابتزاز الإلكتروني

تعتبر جريمة التهديد بالابتزاز الإلكتروني من الجرائم ذات الأنواع والصور المختلفة والمتشعبة، حيث أن هذه الصور تتنوع تارة بالنظر إلى الضحية المستهدفة من الجريمة، وتارة أخرى بالنظر إلى الهدف المرتقب من الجريمة أو المرجو تنفيذه أو المنفعة التي تعود على المجرم.

أولا: بالنظر إلى شخص الضحية.

تتعدد جرائم التهديد والابتزاز الإلكتروني تبعاً لشخصية المجني عليه المحتمل كضحية للجريمة:

أ: الشخصيات الاعتبارية.

هناك نوع من جرائم الابتزاز الإلكتروني تكون فيها الفئة المستهدفة كضحية هي الحكومات والشركات والمؤسسات ذات الشخصية المعنوية، وذلك حيث تتم جريمة الابتزاز عن طريق الحصول على معلومات سرية خاصة بالضحية كمؤسسة أو شركة، والتهديد بالإعلان عن هذه المعلومات ونشرها للآخرين، وقد تبدأ جريمة الابتزاز بمتطفل أو دخيل على مواقع مهمة، ثم تتمحور شكل الجريمة ليكون التهديد بنشر هذه المعلومات حتى عن طريق السطو على موقع الشخص المعنوي ضحية الجريمة وابتزازه[10]، لا سيما وأن المجرم لديه يقين بالجانب المالي للضحية.

ب: الأحداث.

تختلف التشريعات والأنظمة في تعريفها للأحداث، وذلك يرجع إلى اختلاف تحديد سن التمييز وسن الرشد، بسبب العوامل الطبيعية والاجتماعية والثقافية الخاصة بكل مجتمع وتفرده.

وتكثر جرائم ابتزاز الأحداث وذلك حيث يقوم المبتز بالضغط على الحدث بتهديده بنشر صور أو تسجيل مرئي أو محادثات على مواقع الدردشة، عن واقعة أو وقائع يكون من شأنها تحقير للمجني عليه عند أهله ومحيطه الاجتماعي[11]، كما أن الحدث ضحية سهلة لجرائم الابتزاز الإلكتروني، وذلك لسهولة انزلاقه في الجريمة ولقلة خبرته وصغر سنه، فالأحداث من أكثر الفئات اتصالاً بالتكنولوجيا ووسائل التواصل الاجتماعي وأكثر ولعاً بها، حيث باتت تشكل حيزا كبيرا من يومهم. مما يسهل إدراجهم في الجريمة.

ج: النساء.

يعد ابتزاز النساء أكثر أنواع الابتزاز الإلكتروني شهرة وانتشاراً، حيث أن جرائم الابتزاز الإلكتروني للنساء تعتبر النموذج المثالي للجريمة، سيما ما إذا كان المبتز رجلاً وضحية الجريمة امرأة، وذلك يرجع إلى أنه غالباً ما يكون تهديد المبتز للمرأة هنا أدواته فيها صوراً فاضحة أو محادثات خادشه للحياء، أو عرضاً مرئياً لعلاقة غير شرعية جمعت ما بين المبتز

وضحيته، والمبتز قد يكون خطط لجريمته منذ البداية، وقد تزرع الفكرة في رأسه بعد أن تتوطد أواصر العلاقة بينه وبين ضحية جريمة ابتزازه المرتقبة، فقد تبدأ العلاقة العاطفية وما أن يحصل الجاني على صور أو مستندات للضحية، حتى يقوم بتهديد وابتزاز الضحية بطلب مبالغ مالية، مما يجعل الفتاة تضطر للإذعان لهذه الطلبات.

وقد تجتمع في ضحية الابتزاز الإلكتروني كونها امرأة وايضاً من الأحداث، حيث تتضاعف فرصة المبتز في هذه الحالة في ارتكاب جريمته، والوصول إلى مآربه بالضغط على الضحية، والتي غالباً ما تتجاوب بسبب العار.

د: الرجال

يقع الرجل مجنياً عليه في جريمة الابتزاز الإلكتروني للعديد من الأسباب، فقد يكون ميسور الحال وعرضة للابتزاز من بعض النساء محترفات بيع الهوى على المواقع الإلكترونية، وتهدده بإذاعة صور أو مقاطع مصورة لتهدد مركزه، كما يكون الرجل عرضة لجرائم الابتزاز بشكل عام بسبب أسرار في مجال عمله أو عائلته، أو أي معلومات بشكل عام يرى الرجل الضحية أن الإفصاح عنها ونشرها يؤذي شرفه وسمعته.

ثانيا: صور الابتزاز الإلكتروني بالنظر إلى الهدف المرجو من المجرم.

يختلف الهدف الذي يرجوه المبتز من جريمته باختلاف كل جريمة، وذلك على النحو التالي:

أ: هـدف مادي:

من أهم وأكثر الأهداف التي يسعى المبتز إلى تحقيقها من ارتكابه جريمة الابتزاز هي تحقيق منفعة مادية، وذلك بطلب مبالغ مالية أو عينية ذات قيمة من المجني عليه، وذلك مقابل ألا يقوم المبتز بنشر الأسرار التي يخشى المجني عليه نشرها على المجتمع وتختلف القيمة المادية التي تطلب من المجني عليه بحسب يساره وملاءته، وبحسب ما إذا كان شخصية اعتبارية كشركة تجارية، أو إذا كان المجني عليه فرد سواء كان رجل أو امرأة.

ب: هـدف جنسي:

هذا الهدف يبدو واضحاً وشائعاً حينما تكون الضحية امرأة أو حدث، وأكثر شيوعاً حينما تجمع الضحية بين كونها امرأة وحدث في نفس الوقت، ويتحقق هدف المبتز الجنسي حينما يكون المقابل الذي يطلبه لعدم افشاء أسرار الضحية، وقد يكون الهدف تهديد المجني عليه للقيام بهذه الممارسات مع شخص آخر غير المبتز، ويكون الابتزاز بطلب المقابل مرة واحدة، أو مرات بحسب ظروف كل جريمة، وإن كان أغلب ضحايا الابتزاز الجنسي من النساء.

ج: هدف نفعي.

يحقق المبتز هدفه من ارتكاب جريمة الابتزاز الإلكتروني، بقيامه بتهديد الضحية بإفشاء اسراره ونشرها للملأ، وذلك إذا لم يقم بتحقيق طلب أو مصلحة للمبتز، وقد تكون المنفعة الأمر بتنفيذ سرقة لصالح المبتز، أو ترويج مخدرات، أو التوسط لدى شخص لإتمام عمل سواء كان هذا العمل مشروعاً أم غير مشروع – طالما كان العمل ضد إرادة المجني عليه– فقد تحققت جريمة الابتزاز.

ثالثا: صور الابتزاز الإلكتروني بالنظر إلى وسائله.

أ: ابتزاز مادي

وهو أن يقوم الجاني بتهديد المجني عليه المرتقب بوسائل مادية ملموسة كالصور والمقاطع المرئية والمستندات، ويكون التهديد مادي إلكتروني عن طريق الاتصالات الإلكترونية وهي كل المراسلات والإرسالات التي تقع سواء في شكل علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات، يتم تبادلها أو إرسالها بطريق الكتروني عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية[12].

ب: ابتزاز معنوي

وهو تهديد بوسائل غير ملموسة وذلك باستخدام عبارات شديدة للتهديد والوعيد بفضح أمر الضحية حتى يغلب على ظن الأخير أن المبتز منفذ لتهديده ولا محالة في ذلك.

الفرع الثاني: طرق جريمة التهديد والابتزاز الإلكتروني ووسائل إرتكابها.

لكل جريمة خصوصية معينة وطرقا مختلفة لتنفيذها، وحينما يختار الجاني الطريقة المناسبة التي سيسلكها لارتكاب جريمته، فإن لكل طريقة وسيلة مختلفة، وبناء عليه سوف نتعرض لبعض طرق ووسائل التهديد بالابتزاز الإلكتروني:

أولا: طرق التهديد والابتـزاز الإلكتروني.

تتعدد طرق التهديد والابتزاز الإلكتروني على حسب، كل مجرم وتخطيط جريمته واحتياجاتها، وذلك على النحو التالي:

أ: الحاسب الآلي وملحقاته وبرامجه:

يعرف جهاز الحاسب الألي بأنه:" عبارة عن جهاز إلكتروني كيميائي بصري أو جهاز إعداد معلومات ذات سرعة عالية يؤدي وظائف منطقية حسابية أو تخزينية، ويشتمل على أي تسهيل لتخزين المعلومات أو تسهيل الاتصالات مباشرة سواء المختزنة أو التي تعمل بالاختزان مع هذا الجهاز".[13]

وعرفه البعض الأخر بأنه: " مجموعة متداخلة من الأجزاء لديها هدف مشترك من خلال أداء التعليمات المخزنة، وهو ألة حاسبة إلكترونية ذات سرعة عالية ودقة كبيرة يمكنها قبول البيانات وتخزينها ومعالجتها للحصول على النتائج المطلوبة."

وكمثال على استخدام الحاسب كأداة في ارتكاب جريمة التهديد بالابتزاز الإلكتروني حيث يقوم أحد الموظفين بالدخول على الحاسب الآلي التابع للشركة، ثم يقوم بالدخول إلى المستند الخاص بمعلومات وبيانات الموظفين، فيقوم بالحصول على بيانات ومعلومات سرية عن الموظفين ويبتزهم.

بً: الانتـرنت.

تعتبر الأنترنت شبكة الاتصالات الدولية – والتي ربطت بين الملايين من أجهزة الحاسب الألي على مستوى العالم– من أهم التطورات في تاريخ البشرية، وهي تعتبر أضخم شبكة كمبيوتر على مستوى العالم، وهي ثمرة الاندماج بين تكنولوجيا الحاسب وتكنولوجيا الاتصالات[14].

فالأنترنت هي تلك الشبكة (العنكبوتية) التي تربط بين كم هائل من الحاسبات، مستعملة في عملية الربط هذه مختلف وسائل الاتصالات السلكية واللاسلكية، مثل الخطوط الهاتفية العامة أو الخطوط الخاصة أو الأقمار الصناعية أو الكوابل والألياف البصرية، وغيرها من وسائل الاتصالات الحديثة وفائقة السرعة، وتمتد هذه الشبكة حول العالم لتؤلف شبكة دولية هائلة لتبادل المعلومات، بحيث يمكن لمستعملها الدخول إليها في أي وقت ومن أي مكان في العالم على أن يكون معه حاسوب مجهز بوسائط الاتصال بالشبكة لتلقي وإرسال البيانات عبر مزود الخدمة[15].

1- البريد الإلكتروني

يعمل البريد الإلكتروني على تبادل الرسائل الإلكترونية بما فيها النصوص والمقاطع الصوتية والصور، وقد وفرت هذه الخدمة كثيراً من الوقت بحيث تصل الرسائل في نفس اللحظة إلى أي مكان في العالم.

2-خدمة الدردشة

هو برنامج يسمح بتجمع عدد من الأشخاص في جميع أنحاء العالم للتواصل مع بعضهم إما كتابة أو صوتاً أو عن طريق الفيديو.

3 – الهواتف النقالة وملحقاتها وبرامجها.

يُستخدم الهاتف النقال بواسطة المجرم الإلكتروني باعتباره أداة لارتكاب الجريمة، وذلك عندما يستخدم الإنترنت في برامج التواصل، كأن يقوم بالتجسس على الآخرين، بالاستعمال غير المشروع لتكنولوجيا الاتصالات والمعلومات الخاصة بالهاتف النقال والذي من شأنه الإضرار بمصلحة الغير أو تعريضها للخطر، أما ملحقات الهاتف فهي الكاميرا والبلوتوث وآلات التسجيل، أما البرامج فهناك أيضا مجموعة من البرامج الخاصة بالهاتف المحمول.

ثـــــانيا: وسائل التهديد والابتـزاز الإلكتروني.

هناك العديد من الوسائل التي يستخدمها المبتز في سبيل وصوله لهدفه من الجريمة، وهذه الوسائل من ضمن الأسباب الرئيسية التي تجعل المجني عليه يذعن لرغبات المجرم ملبياً إياها، وتتنوع بدءا من صورة أو تسجيل صوتي للضحية، وقد تكون الوسيلة تجمع ما بين الصورة والصوت في تسجيل مرئي، وقد تكون الوسيلة ايضاً الحصول على اسرار تمس الحياة الخاصة للضحية عن طريق وثائق وبيانات، وهناك وسيلة استخدام الالفاظ والعبارات ذات الوعيد.

كما أن هناك حالات أخرى كاختراق الحسابات الإلكترونية كمواقع التواصل الاجتماعي مثل "فيسبوك" و"ماسنجر" فيحصل الجاني على معلومات وصور خاصة للضحية ثم يقوم المحتال بابتزاز الضحية وطلب مبالغ طائلة منه أو فضحه.

المبحث الثـاني: الأليات القانونية لمكافحة جريمة التهديد بالابتزاز الإلكتروني

جريمة التهديد الإلكتروني مثل غيرها من الجرائم لها أركانها وعناصرها، وتسير الدعوى الجنائية بالنسبة لها بذات المراحل التي تسير فيها الدعوى الجنائية في الجرائم العادية (التقليدية).

وكما هو الحال في القصور التشريعي لتحديد كل جريمة معلوماتية على حدى، لإزالة كل غموض يحيط بها، فإن مظاهر الفراغ التشريعي تظهر أيضا في المجال الإجرائي الذي يواجه الطبيعة الخاصة للجريمة المعلوماتية بصفة عامة وجريمة التهديد الإلكتروني بصفة خاصة.

وبالرغم من قيام الكثير من الدول بسن تشريعات جديدة، أو تعديل تشريعاتها القائمة لمواجهة الجريمة المعلوماتية، إلا أنها لم تتوصل إلى تدارك كل ما يحيط بالجريمة من الجانب الإجرائي، كذلك بالنسبة للمشرع في الدول العربية لم يتدخل جديا لمواجهة هذا النوع من الجرائم بنصوص إجرائية خاصة، وأمام هذا القصور التشريعي تبرز مسألة صعوبة جمع الأدلة في مجال الجريمة المعلوماتية من جهة، ومن جهة أخرى صعوبة في تطبيق الإجراءات الجنائية التقليدية.

والمشرع الجزائري وإن كان قد تطرق للجريمة المعلوماتية في 2004 بموجب القانون 04-15، وتدارك بعض الإشكاليات بإصداره قانون 09-04[16]، فقد خص الجانب الإجرائي من أجل الوقاية والمكافحة من الجريمة المعلوماتية بإهتمام بدليل أنه أفرد له نصوص قانونية خاصة به، والذي تبنى بموجبها صراحة إجراءات خاصة تميز هذا النمط من الجريمة عن غيرها من الجرائم التقليدية، وفي ذلك مسايرة منه لما تنص عليه الاتفاقيات الدولية في هذا الشأن وهذا بموجب القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004، المعدل للأمر 156/66 المتضمن قانون الإجراءات الجزائية، والمرسوم التنفيذي رقم 06-348 المؤرخ في 05 أكتوبر 2006، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، إلا أن هناك إشكالات تطرح أمام رجال القانون حول كيفية ملاحقة المجرمين ومسألة الاختصاص، مرورا بأعمال الاستدلال والتحقيق وانتهاء بقضية الإثبات.

المطلب الأول: التحقيق والإثبات في جريمة التهديد والابتزاز الإلكتروني.

تمر هذه الجريمة كغيرها من الجرائم بعد وقوعها، في مرحلة الاستدلال والتحقيق الجنائي، والذي يهدف إلى الوصول إلى اكتشاف الجريمة وفاعلها، والوقوف على كل الوقائع والملابسات التي مرت بها، ومرتكبها إن كان فاعلا وحيدا للجريمة أم كانوا فاعلين لها، وكل هذا البحث والتحقيق يكون من أهم أهدافه الوصول إلى الحقيقة، والحقيقة القانونية تحتاج إلى دليل تتأكد معه نسبة التهمة إلى المتهم بها، أو نفي الجريمة عنه، ولعله لكي تكتمل خصوصية هذه الجريمة، كان لنا أن نقر بأن الدليل في الجريمة الإلكترونية، وبالأخص في جريمة الابتزاز الإلكتروني دليل غير تقليدي، دليل يرتبط بالحواسيب وأجهزة الهواتف النقالة وملحقاتها والبرامج والتطبيقات التكنولوجية، فجرائم التقنية تمتاز بالتباعد الجغرافي بين الجاني والمجني عليه، ويرتكب المجرم المعلوماتي جريمته بعد تخطيط مسبق باستعمال قدراته الفنية والعقلية، ويحيط نفسه بتدابير أمنية ووقائية تزيد من صعوبة الكشف عنه وعن مخططاته، لذا فهو يلجأ للتمويه باستخدام التشفير وكلمات السر أو استخدام أسماء مستعارة، بالإضافة إلى سهولة محو كل دليل والتلاعب فيه، أمام كل هذا تبرز صعوبة الاكتشاف في الجرائم المعلوماتية.

وبالتالي سنتناول في هذا الفرع المتمثل في التحقيق والإثبات في جريمة التهديد بالابتزاز الإلكتروني، والصعوبات التي تواجه السلطات في التحقيق والإثبات، كما نتناول العقوبات المقررة للجريمة:

الفرع الأول: التحقيق في جريمة التهديد بالابتزاز الإلكتروني والصعوبات التي تواجه المحقق

رغم اختلاف الجرائم الإلكترونية بشكل عام عن الجرائم التقليدية، وهو ما يلقي بعبء على سلطات التحقيق، من ضرورة تطوير اجراءات التحقيق لكي تتناسب مع التحقيق في الجرائم الإلكترونية بصفة عامة، وفي الابتزاز الإلكتروني بصفة خاصة، فأيضا يظل نظام الإجراءات الجزائية في قواعد التحقيق هو السائد، مع ضرورة اعتبار الفوارق الموضوعية في التحقيق، حيث أن هناك صعوبات تثار اثناء التحقيق تنبع من طبيعة جريمة التهديد بالابتزاز الإلكتروني.

أولا: التحقيق في جريمة التهديد بالابتزاز الإلكتروني.

نصت المادة 40 الفقرة الأولى من قانون الإجراءات الجزائية المعدل بموجب القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004، والمرسوم التنفيذي رقم 06-348 المؤرخ في 2006/10/05[17] والمتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق على أن اختصاص قاضي التحقيق المحلي يتحدد بمكان وقوع الجريمة أو محل إقامة أحد المشتبه في مساهمتهم في اقترافها، أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب أخر.

أما فيما يخص ضباط الشرطة القضائية طبقا للمادة 1/16 من قانون الإجراءات الجزائية فإنهم يمارسون اختصاصهم المحلي في حدود الدائرة التي يباشرون فيها وظائفهم المعتادة، وفي حالات الاستعجال لهم مباشرة مهامهم في كافة اختصاص المجلس القضائي الملحقين به، أو كافة الإقليم الوطني بناء على أمر من القاضي المختص وبعد إطلاع وكيل الجمهورية التابعين له.

ثانيا: الصعوبات التي تواجه المحقق أمام

يعتبر التحقيق في جرائم الابتزاز الإلكتروني، أمر ليس بالهين بسبب الصعوبات التي تواجه المحقق أمام جريمة ما زالت غامضة، حتى ان عدم التمكن من السيطرة على مجريات التحقيق، قد يؤدي إلى فقدان الثقة في المجتمع وزيادة نسبة الجريمة، وتتمثل هذه الصعوبات في:

أ: حق الانسان في الخصوصية.

كثير من التشريعات في الدول جرمت التعدي على حياة الانسان الخاصة باستخدام شبكة الانترنت، وقد نص عليها ميثاق الأمم المتحدة سنة 1948م، ومنها المادة 15 " لا يعرض أي شخص لتدخل تعسفي في حياته الخاصة، أو أسرته، أو مسكنه، أو رسائله أو شن حملات على شرفه وسمعته، ولكل شخص الحق في طلب حماية القانون له من مثل هذه التدخلات أو تلك الحملات".

وكل الإعلانات العالمية لحقوق الانسان اكدت حرصها على حماية الخصوصية والحياة الخاصة، وسايرت الدساتير والأنظمة العربية ما ذهبت اليه هذه الإعلانات.

ب: نقص خبرة العاملين بجهات التحقيق.

مازالت جهات التحقيق تعاني من قلة الخبرة الفنية وقلة التدريب على التعامل مع الأدلة الرقمية، وكيفية البحث عنها، وكيفية الحصول على هذا الدليل، كما أن خبرة التحقيق مع مجرم ذكي له طبيعة خاصة، سيما وان هذا المجرم يراوغ ويحاول الهرب من جرمه، ربما بإغراق المحقق في تفاصيل لا يعلمها جيدا، حيث ان المحقق الجنائي في جرائم التهديد

بالابتزاز الإلكتروني يجب أن يكون له تكوين تقني، فيجب ان يجمع بين مهارة استخدام التقنية الحديثة، وكذلك مهارة تقييم الجريمة الإلكترونية ومدى الخطورة الاجرامية لمرتكبها، وكذلك مهارة التعرف على المكونات المادية للأجهزة وعلى ملحقاتها من طابعات وماسحات ضوئية وكاميرات، وذلك للتأكد من ارتباطها بالجهاز الأصلي من عدمه، وتقييم الوسائط الخاصة بتخزين الأدلة الرقمية لتحديد مدى ارتباطها بالإنترنت وما إذا كانت جزء من أدوات الجريمة من عدمه.

ج: تنازع الاختصاص

من المعلوم أن الشبكة العنكبوتية لا تستأثر بها دولة معينة ويتسنى لمستخدميها ولوجها من أي مكان في العالم من خلال جهاز حاسب ألي يكون متصلا بها، فهي بطبيعتها لا تحدها حدود وهي خارجة عن أي رقابة أو سيطرة من أية جهة وبالتالي عدم خضوعها لأي سلطة قانون جنائي معين، وعملا بمبدأ إقليمية القوانين فإن كل دولة تمارس سيادتها على إقليمها بتطبيق قوانينها على إقليمها بصرف النظر عن جنسية مرتكب الجريمة.

ولما كانت الجريمة الإلكترونية ذات طبيعة خاصة وتتميز بخصوصيات متعددة، منها أنها جريمة عابرة للحدود خلافا للجرائم التقليدية، الأمر الذي يجعلها في كثير من الأحيان تستعصي الخضوع للقوالب التي تحكم مسألة الاختصاص المكاني، إلا أن الاتجاه الغالب اليوم لحل مشكلة الاختصاص القضائي في العالم الافتراضي، هو تطبيق المبادئ ذاتها المعمول بها لحل مشكلة الاختصاص الجزائي الدولي في الجرائم التقليدية، وعلى رأسها مبدأ إقليمية القوانين، أي تطبيق القانون الجزائي على جميع الجرائم التي ترتكب في إقليم الدولة أيا كانت جنسية مرتكب الجريمة.

إلا أن طريقة تبني هذا الحل اختلفت من دولة إلى أخرى فبعضها ساير الاجتهاد الفقهي، والبعض الأخر ساير الاجتهاد القضائي، وبعضها الأخر تبنى تشريعات تتعلق بالجرائم المعلوماتية، كما أن هناك دول أخرى تبنت الحل عن طريق الاتفاقيات الدولية.

أما فيما يخص موقف المشرع الجزائري من مسألة الاختصاص القضائي المحلي، فقد حدد المشرع الجزائري معايير الاختصاص المحلي للجرائم المعلوماتية في قانون الإجراءات الجزائية في المواد 37،40،329، ونجد بأنه تخطى مشكلة امتداد التفتيش خارج الإقليم الوطني بموجب ما رسمه القانون.

لكن مشكلة الاختصاص القضائي وملائمة القانون الواجب التطبيق تظل قائمة في مجال الجرائم المعلوماتية، حتى وان بادر المشرع الجزائري بتعديل قانون الإجراءات الجزائية بموجب القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004، حيث عدل المادة 329 من قانون الإجراءات الجزائية وذلك بجواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة...." وقد جاء عقب ذلك المرسوم التنفيذي رقم 06-348المؤرخ في 2006/10/05 والمتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ليجسد فعليا بموجب المادة الأولى منه مجال اختصاص بعض المحاكم في إطار الجرائم الماسة بأنظمة المعالجة الألية للمعطيات...".

الفرع الثاني: الإثبات في جريمة التهديد بالابتــزاز الإلكتروني.

نظم المشرع استخلاص الدليل في الجرائم عن طريق قواعد إجرائية معينة، ومما لاشك فيه أن هذه القواعد عامة النطاق تطبق في جميع الجرائم تقليدية كانت أو مستحدثة.

وبما أنه من خصائص الجريمة الإلكترونية أنها صعبة الإثبات والاكتشاف، نظرا لارتكابها من قبل جناة محترفون، يملكون مهارات فنية عالية يحيطونها بسرية تامة، لذا فإنه تصعب مهمة المحققين من ضباط شرطة وقضاة في جمع أدلة الإثبات، كما أن ارتباط الجرائم محل الدراسة بالحاسب الألي، يتطلب الإحاطة بمكونات هذا الأخير وبنظام المعالجة الألية للمعطيات والشبكات وبطرق الدخول إليها، وكل ما يتعلق بهذه الجرائم من تقنيات وهذا ما يحتاج إلى دراية ومعرفة فنية، فضلا عن المعرفة القانونية.

وتجدر الإشارة إلى أن مجموع القواعد المتعلقة بطرق الإثبات لا اختلاف فيها بين الجرائم التقليدية والجرائم الإلكترونية، إلا أن الطابع الخاص الذي تتميز به الجرائم الإلكترونية هو أن محل أو موضوع بعضها يكون غير مادي، وبالتالي إذا استطاع الجناة تطوير طرق الإجرام على هذا النحو من التقنية العالية في بيئة تكنولوجيا المعلومات، كان من الضروري تطوير وسائل الإثبات بما يواكب التطور في وسائل الإجرام الإلكتروني، وأصبح متطلبا من أجهزة العدالة الجنائية أن تتعامل مع أشكال مستحدثة من الأدلة في مجال الإثبات الجنائي خاصة مسألة حجية الدليل الإلكتروني[18].

وبالتالي هل تكفي القواعد الإجرائية المقررة لإثبات الجرائم التقليدية لكي تسري على إثبات الجرائم الإلكترونية بصفة عامة وجريمة التهديد والابتزاز الإلكتروني بصفة خاصة؟

أولا: دور طرق الإثبات التقليدية في إثبات جريمة التهديد والابتزاز الإلكتروني:

تتمثل طرق الإثبات التقليدية في القانون الجزائري في إثبات الجرائم بصفة عامة فيما يلي:

1.الشهادة

يجوز طبقا للمادة 88 من قانون الإجراءات الجزائية الجزائري لقاضي التحقيق سماع كل شخص يرى فائدة من سماع شهادته سواء كان شاهد نفي أو إثبات، ويعتبر أداء الشهادة إجراء من إجراءات التحقيق، ويقصد به الإدلاء بمعلومات تتعلق بالجريمة أمام سلطة التحقيق بالشروط التي حددها القانون، فهو إقرار من الشاهد بأمر رآه أو سمعه أو أدركه بأية حاسة من حواسه.

ولا تقل الشهادة أهمية في الجريمة الإلكترونية عن باقي الإجراءات في الحصول على الدليل الإلكتروني، فالقاعدة العامة تقتضي أن يلتزم الشاهد بالإفصاح بما يعلمه من معلومات بخصوص واقعة الجريمة والفاعلين فيها، والإدلاء بكل ما يكشف الحقيقة.

للمحقق في الجرائم المعلوماتية أن يسمع الشهود وهم الأشخاص الذين كانوا في مسرح الجريمة أو لديهم معلومات تقنية تفيذ الكشف عن الجريمة، وغالبا ما يكون الشاهد المعلوماتي من أصحاب الخبرة، والمتخصصون في مجال تكنولوجيا الإعلام والاتصال، والذين لهم المعرفة الكافية بنظام المعالجة الألية للبيانات.

فالشاهد في الجريمة المعلوماتية صاحب الخبرة والتخصص في تقنية وعلوم الحاسوب الذي تكون لديه معلومات جوهرية هامة للولوج إلى نظام المعالجة الألية للبيانات، إذا كانت مصلحة التحقيق تقتضي ذلك، ويطلق على هذا النوع من الشهود مصطلح (الشاهد المعلوماتي)، تمييزا له عن الشاهد التقليدي.

ويرى الفقه أن الشاهد المعلوماتي يشمل الفئات التالية:

– القائم على تشغيل الحاسوب والمعدات المتصلة به واستخدام لوحة المفاتيح في ادخال البيانات، وإدخال البرامج.

– خبراء البرمجة الذين يتمكنون من كتابة أوامر البرامج، والذين يقومون بتخطيط واختبار وتعديل وتصحيح برامج الحاسب وادخال التعديلات واضافتها.

– المحلل، وهو الذي يقوم بتحليل خطوات البرامج وتجميع البيانات لنظام معين ودراستها ثم تحليل هذا النظام وتقسيمه إلى وحدات منفصلة واستنتاج العلاقات الوظيفية بين هذه الوحدات.

– مدير النظام، وهو الذي يوكل إليه أعمال الإدارة في النظم المعلوماتية ويدخل ضمن هذه الطائفة مدخل البيانات والمعلومات.[19].

كما يوجد نوع أخر من الشهادة وهو الشهادة عبر الأنترنت وتفترض هذه النوعية من الشهادة حصولها في مرحلة التحقيق النهائي أمام محكمة الموضوع، حيث يكون الشاهد غير حاضر ماديا أو جسديا أمام المحكمة، وإنما يتم سماع شهادته عبر الأنترنت بشكل سمعي ومرئي، والشاهد هنا يبرز في هيئته الكاملة، فيبدو كما لوكان حاضرا حيث تظهر للمحكمة ردود أفعاله الطبيعية عندما توجه له الأسئلة، الأمر الذي يتيح للمحكمة تقدير قيمة هذه الشهادة[20].

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الألية للبيانات.

2. القرائن

القرينة مأخوذة من كلمة مقارنة وتعرف بأنها:" استنتاج الواقعة المطلوب إثباتها من واقعة أخرى قام عليها دليل إثبات"، أي يقصد بها دلالة واقعة قام الدليل عليها على واقعة أخرى لم يقم عليها دليل بطريق الاستنتاج المنطقي، فالقرينة على هذا النحو تعتبر دليل إثبات غير مباشر وهي بذلك تتميز عن باقي الأدلة كالشهادة والاعتراف التي تعتبر أدلة مباشرة على الواقعة المراد إثباتها.

القاعدة أن القرائن والدلائل لا ترقى إلى مرتبة الأدلة ولا يجوز الاستناد إليها منفردة في الحكم إلا إلى جانب دليل أو أدلة متنوعة، فدورها هو تدعيم الأدلة التي طرحت.

وتجدر الإشارة إلى أن الدليل الرقمي يعد من فئة القرائن القضائية التي يعود تقدير قيمتها إلى قاضي الموضوع فمعرفة عنوان الأنترنت الرقمي مثلا " IPadresse" يشير إلى الحاسوب الذي ارتكبت بواسطته الجريمة فقط، ولا يؤدي إلى معرفة الفاعل بدقة، وذلك بخلاف الدليل العلمي الذي يحدد بصمة الأصبع مثلا وغيرها من الأدلة التي تشير إلى الفاعل الحقيقي بدقة متناهية[21].

3. الاعتراف أو الإقرار بالجريمة

الاعتراف في القانون هو:"إقرار المدعى عليه على نفسه بصدور الواقعة الجرمية عنه"

والأصل أن يكون للاعتراف دور حاسم في الدعوى الجزائية، عندما يصدر عن شخص لم يجد أمامه إلا الاعتراف إلى العدالة بحقيقة ما اقترف، إلا أن الاعتراف قد يكون كاذبا في بعض الأحيان لعدة اعتبارات إشباعا لنزوات المدعى عليه، كمن يعترف بارتكابه لجريمة خطيرة اهتم بها الرأي العام كي تتحدث عنه وسائل الإعلام، وقد يصدر الاعتراف نتيجة وهم المدعى عليه، وقد يصدر بدافع إنقاذ المجرم الحقيقي كأن يعترف الابن بارتكابه الجريمة كي ينقذ والده من العقوبة.

الاعتراف هو وسيلة من وسائل الإثبات، وحجيته تخضع للسلطة التقديرية للقاضي، وفي الجرائم المعلوماتية يمكن للقاضي الاستعانة بخبير لتقييم هذا الاعتراف لأنه اعتراف من شخص يملك مهارات تقنية في مجال التكنولوجيا.

4. الخبرة

تقدم الخبرة عونا ثمينا لجهة التحقيق والقضاء ولسائر السلطات المختصة بالدعوى الجنائية، فبدونها يتعذر الوصول إلى الرأي السديد بشأن المسائل الفنية التي يكون على ضوئها كشف جوانب الحقيقة المبنية على الأصول والحقائق العلمية.

وإذا كان للخبرة أهمية في الجرائم التقليدية فإن أهميتها تزداد وتصبح ضرورية بل وحتمية في اشتقاق الأدلة الإلكترونية لإثبات الجرائم المعلوماتية، حيث تتعلق بمسائل فنية معقدة ومحل الجريمة فيها غير مادي والتطور في أساليب ارتكابها سريع ومتلاحق، ولا يكشف غموضها إلا متخصص وعلى درجة من التمييز، ولذا يجب الاستعانة بالخبرة التقنية في مجال الجريمة الإلكترونية.

تعد الخبرة التقنية في جريمة التهديد عبر الأنترنت من أكثر طرق الإثبات أهمية، إذ أنها تؤدي دورا هاما في التحقيق الأولي أو الابتدائي والنهائي، حيث أصبح يعرف في الفقه المقارن بمصطلح المعلوماتية الشرعية والتي يقصد بها " استخدام الطرق العلمية لجمع وتعريف وتحليل وتفسير الدليل الرقمي المأخوذ من مصادر رقمية والاحتفاظ به وتوثيقه، على نحو يسهل بناء الحوادث التي تؤدي إلى اكتشاف الجريمة.

ويقصد بالخبرة المعلوماتية الشرعية عملية البحث التي يقوم بها الخبير المعلوماتي من أجل الحصول على الدليل الرقمي، بغية إعادة بناء مجريات القضية وتوضيحها للمحكمة وهذه العملية تشبه تشريح الجثة في الطب الشرعي.

5. المعاينة

المعاينة قد تكون إجراء تحقيق أو استدلال، وهي جوازية شأنها شأن سائر إجراءات التحقيق، ولا تتمتع في مجال كشفها غموض الجريمة المعلوماتية نفس درجة الأهمية التي تلعبها في مجال الجريمة التقليدية وذلك لإعتباربن هما: الجرائم التي تقع على نظم المعلومات والشبكات قلما أن يترتب على ارتكابها أثار مادية، بالإضافة إلى أن عددا كبيرا من الناس قد يتردد على مسرح الجريمة خلال الفترة الزمنية التي تتوسط ارتكاب الجريمة واكتشافها، مما يتيح الفرصة لإحداث تغيير أو إتلاف أو عبث بالأثار المادية.

6. التفتيش في البيئة المعلوماتية

التفتيش من أخطر الإجراءات الجنائية التي تمس حريات الناس، فهو بحث في مستودع أسرارهم التي يحرصون على الاحتفاظ بها لأنفسهم، فالتفتيش هو البحث عن شيء يتصل بالجريمة ويفيد في الكشف عن الحقيقة، لذا يعتبر من أهم

إجراءات التحقيق في كشف الحقيقة لأنه غالبا ما يسفر عن أدلة مادية تؤيد نسبة الجرائم إلى المتهم، والتفتيش في الجريمة الإلكترونية يشمل جميع وسائل التكنولوجيا والاتصال التي استعملت في ارتكاب الجريمة، وتفتيش البيانات المخزنة فيها، والاطلاع على البريد الإلكتروني واسندت مهمة التفتيش للمحققين مع توسيع صلاحياتهم في مجال الكشف عن الجريمة الإلكترونية.

ومن المعروف أن نظم المعالجة الألية تتكون من مكونات مادية وأخرى مكونات منطقية أو معنوية، ترتبط بغيرها بشبكات اتصال بعدية سلكية ولاسلكية سواء على المستوى المحلي أو المستوى الدولي، فهل تخضع هذه المكونات للتفتيش؟

يخضع الولوج في المكونات المادية للحاسب بحثا عن شيء يتصل بجريمة معلوماتية وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، وهناك تشريعات قلة تنص صراحة على تفتيش مكونات الحاسب الألي،[22] بمعنى أن حكم تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه، سواء الأماكن العامة أو الأماكن الخاصة، وسواء كان مسكن المتهم أو الغير وفي أي ساعة، وبصفة عامة إن لصفة المكان أهمية خاصة في مجال التفتيش، وبنفس الضمانات المقررة قانونا في أغلب التشريعات الجزائية كالقانون الجزائري، حيث نصت المادة (64) من ق.إ.ج على أنه:" لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، إلا أنه وإذا كان المشرع الجزائري قد أورد القاعدة في المادة (64)، رجع وأورد عليها استثناء بموجب الفقرة الثالثة من نفس المادة، حيث استثنى المشرع تطبيق هذه الضمانات على طائفة من الجرائم محيلا في ذلك إلى أحكام المادة (47) في فقرتها الثالثة التي تنص " وعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الألية للمعطيات وجرائم تبييض الأموال والإرهاب وكذلك الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز اجراء التفتيش والمعاينة والحجز في كل محل سكني في كل ساعة من ساعات النهار أو الليل بناء على اذن مسبق من وكيل الجمهورية المختص".

ثار الخلاف الفقهي بشأن جواز تفتيش المكونات المعنوية للحواسيب تمهيدا لضبط الأدلة الإلكترونية، لأنه يحتوي على معنويات وليس ماديات، وانقسموا في ذلك لاتجاهين:فمنهم من ذهب إلى القول بعدم صلاحية إجراء التفتيش والضبط على برامج وبيانات الحاسب الآلي باعتباره وسيلة للإثبات المادي، يهدف لضبط أدلة مادية تتعلق بالجريمة وتفيد في كشف الحقيقة، وهذا يتنافى مع الطبيعة غير المادية لبرامج وبيانات الحاسب الآلي ويمثل هذا الرأي جانب من الفقه الفرنسي الذي يرى أن النبضات أو الإشارات الإلكترونية المغنطة لا تعد من قبيل الأشياء المادية المحسوسة التي يمكن تفتيشها وضبطها.[23]

ورأى جانب أخر أن المعلومات التي لا تعد شيئا ماديا وإنما ذات طبيعة معنوية، والتي في الأصل هي مجرد ذبذبات ونبضات إلكترونية أو إشارات أو موجات كهرومغناطيسية، إلا أنها قابلة لأن تُخزَّن في أوعية ووسائط مادية كالأقراص والأشرطة المغنطة، وبالتالي فهي ليست شيئا معنويا كالحقوق والآراء والأفكار، بل هي أشياء مادية محسوسة لها وجود ملموس في العالم الخارجي، ومن ثم يصح أن يرد عليها التفتيش والضبط.

أما فيما يخص مدى خضوع شبكات الحاسوب للتفتيش عن بعد، فبالرجوع لقانون الإجراءات الجزائية الجزائري فقد ورد نص على حالة وجود الحاسوب الثاني المتصل بالأول المراد تفتيشه موجود على التراب الجزائري، أجاز ذلك شرط أن يكون قد صدر أمر من وكيل الجمهورية أو قاضي التحقيق بتفتيش مفتوح يمتد على مستوى التراب الوطني بكامله طبقا للمادة 47 من قانون الإجراءات الجزائية في فقرتها الأخيرة.

لكن الإشكال يطرح هو عندما يكون الحاسوب المراد تفتيشه في دولة أخرى، لأن التفتيش هنا يتعارض مع تمسك كل دولة في سيادتها وحدودها الإقليمية، وهذا ما يواجه سلطات التحقيق من مشاكل لجمع الأدلة الإلكترونية[24].

ونتيجة لذلك أدخلت بعض الدول تعديلات في قانون الإجراءات الجزائية لتجيز تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج إقليم الدولة، ومن ذلك المشرع الجزائري الذي أجاز تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج اقليم الدولة، حيث أجازت الفقرة 3 من المادة 5 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها لسنة 2009 الحصول على المعطيات المبحوث عنها والمخزنة في الأنظمة المتصلة الواقعة خارج الإقليم الوطني والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى وذلك بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل.

7. الضبط في مجال الجريمة المعلوماتية

مما لاشك فيه أن النتيجة الحتمية التي ينتهي إليها التفتيش هي ضبط الأدلة التي يتم الحصول عليها أثناءه، ويقصد بالضبط في قانون الإجراءات الجنائية، وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، والقاعدة أن الضبط لا يرد إلا على الأشياء المادية أما الأشياء المعنوية فلا تصلح بطبيعتها أن تكون محلا للضبط، كما يشترط في الضبط أن يكون الشيء مفيدا في كشف الحقيقة، والأدلة المادية التي يجوز ضبطها في الجريمة المعلوماتية والتي لها قيمة خاصة في إثبات الجرائم ونسبتها إلى المتهم هي: الأوراق والمستندات الرسمية سواء كانت تحضيرية أو أصلية، أساسية أو قانونية، أيضا جهاز الحاسب الألي وملحقاته أقراص الليزر، الشرائط الممغنطة، البطاقات الممغنطة وبطاقات الائتمان...إلخ

أما فيما يخص ضبط المكونات المعنوية للحاسب الآلي من معلومات وبرامج، وما تحتويه صناديق البريد الإلكترونية من رسائل وصور وبيانات، وكيف يتم المحافظة على هذه الأدلة من التلف، تجدر الإشارة إلى أن الجدل لا يزال قائما إلى يومنا هذا بين المؤيد والرافض لإمكانية ضبط البيانات المعالجة إلكترونيا منفصلة عن دعامتها المادية، كتلك التي يتم عرضها على شاشة الحاسب الآلي، فذهب اتجاه إلى أنه من غير الممكن ضبط البيانات إلكترونيا لانتفاء الطابع المادي لهذه البيانات، ذلك أن بيانات الحاسب الآلي ليست كمثل الأشياء المحسوسة، وذهب اتجاه ثان إلى أنه وإن كانت الغاية من التفتيش هو ضبط الأدلة المادية، إلا أن هذا المفهوم يمكن أن يمتد ليشمل بيانات المعالجة الإلكترونية المجردة، لأنه من الممكن ضبطها إذا أصبح لها كيان مادي، كضبط القطعة الصلبة كأداة تخزينية للدليل، والمعلومات والبيانات المراد ضبطها على ورق أو تسجيلها في أشرطة أو أقراص أو نسخها في ملفات، إذ في هذه الحالة تتحول المكونات المعنوية للحاسب الآلي إلى أشياء مرئية ومقروءة وتكتسب كيانا ماديا، والقول نفسه يطبق بشأن الرسائل

الالكترونية، فللمحقق أن يضبط الرسائل المخزنة بالبريد الالكتروني عن طريق طباعة الرسالة التي يريد ضبطها أو تسجيلها في ملف أو قرص.

أما بالرجوع إلى التشريع الجزائري فقد تدخل بموجب المادة 6 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والإيصال ومكافحتها لسنة 2009، حيث تنص على أنه " عندما تكشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز، والوضع في أحراز وفقا للقواعد المقررة في ق.إ.ج".

ثانيا: طرق الإثبات المستحدثة في جريمة التهديد الإلكترونية

لم تسلم طرق الإثبات من تأثيرات ثورة المعلومات والتكنولوجيا، فقد أفرزت إلى حيز الوجود نوعا جديدا من الأدلة يتماشى مع طبيعة جرائم الأنترنت، وهو ما يعرف بالدليل الرقمي، أي الدليل الناتج عن فحص المكونات المعنوية أو البرمجية للحواسيب وشبكة الأنترنت، وهذا الدليل تبنته معظم التشريعات وذلك بتحديد الشروط التي يجب توافرها في الدليل الرقمي حتى يمكن قبوله من قبل القضاء الجزائي.

أما بالنسبة للمشرع الجزائري فهو ليس في منأى عن هذا التطور الحاصل في مفهوم الجريمة المعلوماتية وفي سبيل الوقاية منها بالطرق المستحدثة، لذا أورد أساليب التحري الخاصة في التعديل رقم 22/06 المؤرخ في 2006/12/20 المعدل والمتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية،والتي نص فيها على إجراء التسرب واعتراض المراسلات والأصوات، وحصر مجال تطبيقها على سبعة فئات من الجرائم منها الجرائم الماسة بأنظمة المعالجة الألية للمعطيات.

1. الدليل الرقمي

يعرف الدليل الرقمي بأنه الدليل المأخوذ من أجهزة الكمبيوتر، ويكون في شكل مجالات مغناطيسية أو نبضات كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء، ويتطلب البحث في ماهية الدليل الرقمي التعرض لتعريفه، ثم التعرف على حجيته.

هناك عدة تعريفات للدليل الرقمي، تباينت بين التوسع والتضييق، نذكر منها:

. هو " أية بيانات مخزنة أو منقولة بواسطة الحاسوب، تدعم أية نظرية حول كيفية ارتكاب الجريمة، وتتعلق بعناصر هامة في الجريمة ".

. وهو " المعلومات والبيانات ذات القيمة الاستقصائية والمخزنة أو المنقولة عبر جهاز إلكتروني "

ويعود السبب في تسميته بالدليل الرقمي، هو أن البيانات داخل العالم الافتراضي، بجميع صورها سواء أكانت صورا أو تسجيلات أو نصوصا، تأخذ شكل أرقام، ومن ثم يتم تحويل هذه الأرقام عند عرضها إلى صورة أو تسجيل أو نص.

يتميز الدليل الرقمي بخصائص تميزه عن الدليل المادي تتمثل في صعوبة محوه أو تحطيمه، وحتى في إصدار أمر الغاءه يمكن إعادة اظهاره من خلال ذاكرة الألة التي تحتوي على ذلك الدليل،كما يمكن للسلطات المختصة من إخضاعه لبعض البرامج والتطبيقات للتعرف إذا ما كان هذا الدليل قد تعرض للعبث أو التخريب.[25]

وتجدر الإشارة إلى أنه لا تقف الصعوبات التي تواجه الدليل الرقمي عند حد كيفية الحصول عليه وإجراءات حفظه، بل تمتد إلى مدى القوة الثبوتية التي يتمتع بها هذا الدليل، ومدى حرية قاضي الموضوع بالإقتناع به، لذلك حاول المشرع والقضاء والفقه المقارن التصدي لهذه المسألة، وذلك بتحديد الشروط التي يجب توفرها في الدليل الرقمي أو في مخرجات الحاسوب، حتى يمكن قبوله من قبل القاضي الجزائي[26].

إن طبيعة الدليل الرقمي تأثر على اقتناع القاضي، حيث أصبح القاضي الجنائي يستند عليه في إثبات الجرائم المعلوماتية، كما أن الدليل الرقمي لا يقتصر دوره على إثبات الجرائم التي تدخل في إطار النظام المعلوماتي فحسب بل يتعدى ذلك الدور إلى الجرائم في نطاق النصوص العقابية التقليدية، ومنها جرائم التهديد والخطف والقتل والمخدرات التي تستخدم فيها التكنولوجيا الرقمية كأداة لتسهيل تنفيذ الجرائم بسرعة وكفاءة، حيث يعتقد المجرمون أن هذه التقنية منفصلة تماما عن العالم المادي مما يجعلهم يشعرون بالأمان.

وتجب الإشارة إلى أن الأدلة الرقمية تتمتع بحجية قاطعة في الدلالة على الوقائع التي يتضمنها، ويمكن التغلب على مشكلة الشك في مصداقيتها من خلال إخضاعها لاختبارات تمكن من التأكد من صحتها.

إلا أنه نتيجة تردد الفقه والقضاء حيال مشروعية الأدلة المتحصلة من الوسائل الإلكترونية كمخرجات الحاسب الآلي بأنواعها المختلفة، خشية أن تكون قد تعرضت للتغيير في فحواها، خاصة أن معظمها يمس مساسا مباشرا بحقوق الأفراد الأساسية وحرياتهم، لهذا وضعت شروط ينبغي توافرها في كل دليل مقدم أمام القضاء الجنائي كأن يكون الدليل مشروعا أي أن يكون وليد إجراءات صحيحة.

– أن يتم تحديد هوية الشخص أو الجهة المنسوب إليه المخرجات بصورة قاطعة.

– أن يتم أيضا استخلاص المعلومات المخزنة إلكترونيا وحفظها بصورتها الأصلية التي أنشئت عليها وبصورة تضمن عدم تعرضها لأي شكل من أشكال العبث أو التلف وهذا الشرط يتطلب اتخاذ بعض الإجراءات التي من أهمها : التحقق من سلامة الحاسب الآلي ودقته في عرض المعلومات المخزنة، وحفظ مخرجات الحاسب الآلي وتخزينها في بيئة مناسبة، وكفاءة ونزاهة القائمين على جمع الأدلة وتخزينها، أي تكون الأدلة التي تم استخراجها غير قابلة للشك.

– أن يتم الحصول عليه بصورة مشروعة وغير مخالفة لأحكام القانون الجنائي، وإلا تعد باطلة.

– أن تكون الأدلة المتحصل عليها من الحاسوب أو الأنترنت قابلة للمناقشة من قبل الخصوم وأطراف الدعوى سواء كانت مطبوعة أو بيانات تم عرضها على شاشة الحاسوب، أو أشرطة أو أقراص ممغنطة أو ضوئية أو مصغرات فيلمية[27].

2. التسرب

من بين الإجراءات التي اتخذها المشرع الجزائري لمكافحة الجرائم المستحدثة عملية التسرب، وقد كان ذلك بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون

الإجراءات الجزائية، والذي أفرد الفصل الخامس منه تحت عنوان " في التسرب"، وقد تم تنظيم هذا الإجراء وفق ثمانية مواد (من 65 مكرر11 إلى 65 مكرر 18) وتناول من خلالها تحديد مفهوم التسرب وشروط إجراءها وأثارها.

عرف المشرع الجزائري التسرب في المادة 65مكرر 12 من قانون الإجراءات الجزائية بقوله: " يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم "، وقد حدد المشرع الجزائري نطاق هذا الإجراء بالجرائم المذكورة في المادة 65 مكرر من ق.إ.ج على سبيل الحصر وهي: الجرائم الماسة بأنظمة المعالجة الألية للمعطيات، جرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف.

ويعرفه البعض بأنه: " تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون شرطة قضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط شرطة قضائية أخر مكلف بتنسيق عملية التسرب، بهذف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، وذلك بخفاء الهوية الحقيقية، وبتقديم المتسرب نفسه على أنه فاعل أو شريك".

ويمكن تجسيد هذه العملية في الجرائم المعلوماتية كاشتراط ضابط أو عون الشرطة القضائية في محادثات غرف الدردشة أو حلقات النقاش، فيتخذ المتسرب أسماء مستعارة ويظهر بمظهر طبيعي كما لو كان فاعل مثلهم ويحاول الاستفادة من معرفتهم حول كيفية ارتكابهم الجرائم، وقد أسند المشرع الجزائري مهمة إصدار إذن التسرب إلى وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية، و تنص المادة 65 مكرر11 أنه:" إذا اقتضت ضرورات التحري أو التحقيق في إحدى الجرائم المنصوص عليها المادة 65 مكرر5 يجوز لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته بمباشرة عملية التسرب".

وبما أن التسرب كممارسة غير عادية للضابط أو عون الشرطة القضائية، بل يعد من أخر الإجراءات مساسا بحرمة الحياة الخاصة للمتهم، لذا اشترط المشرع ضمانات معينة يتعين مراعاتها عند اللجوء إلى هذا الإجراء ويتمثل ذلك فيما يلي:

— صدور التسرب من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية.

– أن يكون الإذن مكتوبا مع احتوائه على الأسباب التي تبرر صدوره.

–أن يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء، وهوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته.

– يحدد في الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة أشهر، ويمكن أن تتحدد حسب مقتضيات التحري أو التحقيق، ضمن نفس الشروط الشكلية والزمنية، وفي نفس الوقت أجاز القانون للقاضي الذي رخص بإجرائها أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة[28].

وتجدر الإشارة إلى أن المشرع الجزائري اشترط احاطة عملية التسرب بالسرية التامة وذلك لتحقيق الأهداف المتوخاة منها، ولذلك قرر المشرع جزاءات عقابية مشددة في حالة اظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية.

3. اعتراض المراسلات وتسجيل الأصوات والتقاط الصور (المراقبة الإلكترونية)

أورد المشرع الجزائري هذه الأساليب بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، والذي أفرد الفصل الرابع منه تحت عنوان " اعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور"، في المواد من 65 مكرر5 إلى غاية 65 مكرر10.

لم يعرف المشرع الجزائري المراقبة الإلكترونية لا في مواد قانون الإجراءات الجزائية ولا في القانون رقم 09/04 المتعلق بقواعد مكافحة جرائم تكنولوجيا الإعلام والإتصال والوقاية منها، وبالرجوع لتعريف الفقهاء فقد اختلفوا في ذلك، فذهب اتجاه للقول بأنها:" إجراء تحقيق يباشر خلسة وينتهك سرية الأحاديث الخاصة تأمر به السلطة القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي لجريمة تحقق وقوعها ويتضمن من ناحية استراق السمع ومن ناحية أخرى حفاظه على الأشرطة عن طريق أجهزة مخصصة لهذا الغرض".[29]

واكتفى المشرع الجزائري بوضع تعريف للاتصالات الإلكترونية في الفصل الأول من القانون 09/04 المتعلق بالوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والإيصال ومكافحتها وبالتحديد المادة 2 منه والتي نصت على:" أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"، وبالتالي فالمشرع الجزائري قد أعطى مفهوما واسعا للاتصالات الإلكترونية لتشمل كل اتصال يقوم به الشخص أيا كانت الوسيلة الإلكترونية المستعملة في ذلك.

اعتراض المراسلات

يعرف بعض الفقهاء اعتراض المراسلات بأنها:" عملية مراقبة سرية المراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو في مشاركتهم في ارتكاب الجريمة". وتتم المراقبة عن طريق الاعتراض أو التسجيل أو النسخ للمراسلات، والتي هي عبارة عن بيانات قابلة للإنتاج أو التوزيع أو التخزين أو الاستقبال أو العرض[30].

وتجدر الإشارة إلى أن اتخاذ هذا الأسلوب دون علم أصحابه بقدر ما يفيد في كشف الجريمة إلا أنه يمس بحرمة الحياة الخاصة للأفراد، واعتداء على سرية مراسلاتهم واتصالاتهم، لذا فقد أحاط المشرع الجزائري استعماله بمجموعة من الضمانات القانونية تتمثل في:

- شرط أن تكون السلطة المختصة بإصدار هذا الإذن من طرف السلطة القضائية، أي بإذن من وكيل الجمهورية أو قاضي التحقيق، وهذا ضمانا لمشروعية اعتراض المراسلات السلكية واللاسلكية طبقا لنص المادة 65 مكرر5 من قانون الإجراءات الجزائية.

– يجب أن يكون الاعتراض في الجرائم التي نص عليها القانون بنص صريح منها الجرائم المعلوماتية، طبقا لنص المادة 65 مكرر5، وأن تكون مدة الإجراء أربعة أشهر قابلة للتجديد، حسب تقدير السلطة مصدرة الأمر وفقا لمقتضيات التحقيق والتحري، وذلك بموجب المادة 65مكرر5 فقرة 2.

تسجيل الأصوات والتقاط الصور

يتجلى أسلوب تسجيل الأصوات في وضع الترتيبات التقنية دون موافقة المعنيين من أجل إلتقاط وتثبيت وبث تسجيل الكلام المتفوه به من قبل شخص أو عدة أشخاص في أماكن عامة أو خاصة.

وأيضا بالنسبة لالتقاط الصور تكون دون موافقة المعنيين لشخص أو عدة أشخاص متواجدين في مكان ما.

وتجدر الإشارة إلى أن المشرع الجزائري مكن ضابط الشرطة القضائية من إجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، ولكن باحترام مجموعة من الشروط الواردة في نص المادة 65 مكرر5 من ق إ ج وهي:

– أن تتم هذه الإجراءات بمناسبة جرائم محددة على سبيل الحصر ومن بينها الجرائم الماسة بأنظمة المعالجة الألية للمعطيات.

– يجب أن تتم هذه الإجراءات بمناسبة جريمة في حالة تلبس أو بمناسبة التحقيق الابتدائي الذي يجريه قاضي التحقيق.

– يجب أن تتم هذه الإجراءات بناء على إذن مكتوب من وكيل الجمهورية المختص إقليميا، وفي حالة فتح تحقيق تتم بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة.

– يجب أن يتضمن هذا الإذن كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة (سكنية أو غيرها...) والجريمة التي تبرر اللجوء إلى هذه الإجراءات ومدتها.

– يجب أن يكون الإذن محدد لمدة أقصاها أربعة أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق، وتجدر الملاحظة أن المشرع لم يحدد عدد المرات مما يجعل المجال مفتوحا.

– يجب على ضابط الشرطة القضائية أن يحرر محضرا عن كل إجراء من الإجراءات المذكورة، ويحدد فيه تاريخ بداية وانتهاء هذا الإجراء أو هذه الإجراءات.

4. الإجراءات التحفظية

نصت المادة 40 مكرر5 من قانون الإجراءات الجزائية على "أنه يجوز لقاضي التحقيق تلقائيا أو بناء على طلب النيابة العامة طوال مدة التحقيق أن يأمر باتخاذ كل إجراء تحفظي أو تدبير أمن زيادة على حجز الأموال المتحصل عليها من الجريمة أو التي استعملت في ارتكابها".

كما نصت المواد 40مكرر 2و3 والمادة 44 و47 من قانون الإجراءات الجزائية، على جواز إجراء حجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص، كما يمكن لقاضي التحقيق القيام بذلك على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك.

حفظ المعطيات المتعلقة بحركة السير أو التزامات مقدمي الخدمات

يتميز الدليل التقني بأنه مرن لأن طبيعة العالم الافتراضي تفرض ذلك، وبالتالي يستطيع الجاني إزالته عن بعد باستخدام التقنية ذاتها، من هنا استلزم الأمر وضع إطار قانوني لحفظ المعطيات الإلكترونية المتعلقة بالتحقيقات الجنائية، وهذا ما تضمنه قرار الجمعية العامة للأمم المتحدة رقم 63/55 المؤرخ في 2001/01/22 في الفقرة المادة 1 منه، والتي ألزمت الدول أن تسمح بحفظ المعطيات الإلكترونية المتعلقة بالتحقيقات الجنائية.

كما تعد اتفاقية بودابست المتعلقة بمحاربة الإجرام المعلوماتي من أول النصوص التي اعتبرت أنه يمكن الاعتماد على مساعدة مقدمي الخدمات في مجال مكافحة الجرائم المعلوماتية[31]، وهو ما أكده المشرع الجزائري بموجب المادة 10 من الفصل الرابع من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها تحت عنوان " التزامات مقدمي الخدمات"، كما يلي: "...يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية..."

أورد المشرع الجزائري تعريفا لمقدمي الخدمات أو موفر الخدمة في نص المادة 08 في فقرتها الثامنة من القانون 03/2000 بأنه:"كل شخص طبيعي أو معنوي يقدم خدمات مستعملا وسائل المواصلات السلكية واللاسلكية"[32]، وقد عرفت المادة 08 من نفس القانون في فقرتها 21 المواصلات السلكية واللاسلكية بأنها:"كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطيسية"

وقد تبنى المشرع الجزائري تعريفا أخر لمزودي الخدمات بموجب الفقرة (د) من المادة 2 من القانون رقم 09-04 وهو تعريف استمده من مضمون اتفاقية بودابست، وهو تعريف أوسع من الذي تبناه بموجب المادة 08 من القانون رقم 03/2000، لأنه لم يحصر الخدمة المقدمة في نطاق خدمة الاتصالات السلكية واللاسلكية فقط وإنما يمتد ليشمل خدمة الاتصال ككل مهما كانت طبيعتها، بشرط أن تتم بواسطة المنظومة المعلوماتية أو نظام للاتصالات، فجاء التعريف كما يلي:

" 1- أي كيان عام أو خاص يقدم لمستعملي خدماته، ضمانة القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات.

2- وأي كيان أخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها"

يلتزم مقدمي الخدمات بتقديم يد المساعدة للسلطات القضائية المختصة، ونصت المادة 10 من القانون رقم 04/09 (السالف الذكر) على هذا الالتزام بما يلي:

- الالتزام بجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها: والتي يتم تبادلها عن طريق خدمات الأنترنت المختلفة سواء الويب أو الإيميل...وغيرها من الخدمات.
- الالتزام بوضع المعطيات المراد حفظها تحت تصرف السلطات: وقد حددت المادة 11 من القانون السالف الذكر طريقة حفظ، ومدة الحفظ والتي تقدر بسنة من تاريخ التسجيل.

- الالتزام بحفظ السر المهني: عند القيام بجمع أو تسجيل المعطيات أو عند قيامهم بحفظها، وهذا ما نصت عليه الفقرة 3 من المادة 10 من القانون رقم 04/09.

وبناء على ما تقدم، فإن المراسلة بالبريد الإلكتروني والتي يتم استقبالها بواسطة مزود الخدمة الخاص بالمرسل اليه والتي لم يطلع عليها بعد فإنها تستقر في حالة تخزين الكتروني لدى مزود الخدمة، الذي إما أن يقوم بمسح تلك الرسالة أو يقوم بتخزينها.[33]

الالتزامات الخاصة بمقدمي خدمة الأنترنت

قد خص المشرع الجزائري مقدمي خدمة الأنترنت طبقا للقانون رقم 04/09 (السالف الذكر) بالتزامين، نص عليهما بموجب المادة 12 كمايلي:

التدخل الفوري لسحب المحتويات التي يتيح الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول على الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

المطلب الثاني: دور الجهات الأمنية الجزائرية في متابعة الجريمة المعلوماتية

إن الوقاية المثلى والفعالة من الجريمة المعلوماتية وما تفرضه من تحديات تتجاوز الوسائل التقليدية إلى وسائل أكثر جرأة، جعلت الجزائر تتخذ كل السبل الكفيلة للحيلولة من تفشي واستفحال هذه الجريمة، بالاعتماد على جهازي الأمن والدرك الوطني كأهم ألية للوقاية والمكافحة في مجال الجريمة المعلوماتية.

الفرع الأول: دور جهازي الأمن والدرك الوطني في متابعة الجريمة المعلوماتية

لقد سعت الجزائر لتفعيل جهازي الأمن والدرك الوطني كألية فعالة يتم الاعتماد عليها من أجل الوقاية ومكافحة الجريمة المعلوماتية، فجهاز الشرطة هو المكلف بالتحري عن الجرائم وضبطها وتلقي البلاغات وإجراء التحقيقات الأولية بشأنها، وتقديمها للجهات القضائية المختصة لمباشرة الدعوى الجزائية[34]، لذا كرست المديرية العامة للأمن الوطني استراتيجية عمل تضمن الجانب المتعلق بتكوين ضباط الشرطة القضائية لمكافحة هذا النوع المستجد من الإجرام الإلكتروني، بالإضافة إلى استحداث مخابر الشرطة العلمية والتقنية والتي يكمن دورها في المساعدة إلى الوصول إلى الحقيقة باستغلال الأجهزة الإلكترونية التي يشتبه باستعمالها في ارتكاب الجريمة، وذلك باستخراج المعطيات المخزنة بداخلها والتي من شأنها مساعدة السلطة المكلفة بالتحقيق.

أما على مستوى جهاز الدرك الوطني فقد تم إعادة تنظيم مصالح الدرك حسب الاختصاص والصلاحيات وطبيعة الجريمة، ثم بموجب المرسوم الرئاسي رقم 183/04 المؤرخ في 26 يونيو 2004 تم إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام، والذي يعد بمثابة هيئة مختصة في إجراء الخبرة والمعاينة في الجرائم المعلوماتية، كما قامت قيادة الدرك الوطني باستحداث مشروع إنشاء مركز لمحاربة جرائم الإعلام الألي يساهم في تقديم المساعدة التقنية، بتقديم أسماء الخبراء المختصين المنتمين للمعهد الوطني للأدلة الجنائية وعلم الإجرام، على مستوى كافة المحاكم والمجالس القضائية لتسخيرهم

والاستفادة من خبراتهم في مجال الإعلام الألي والأنترنت، حتى يسهل عمل القضاة في فهم الأدلة التقنية المترتبة عن الجرائم المعلوماتية[35].

الفرع الثاني: دور الهيئة الوطنية للوقاية من جرائم الإعلام والاتصال ومكافحتها

من بين الأليات التي أوجدها المشرع الجزائري في مجال الوقاية والمكافحة من الجريمة المعلوماتية إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته بموجب القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها في نص المادة 13 منه، التي تنص على:"تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته.

تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم"

كما نصت المادة 14 من نفس القانون على مجموعة من المهام المسندة لهذه الهيئة:

" – تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته.

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والإتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

– تبادل المعلومات مع نظيرتها في الخارج قصد جمع المعلومات المفيدة ف التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وتحديد مكان تواجدهم".

خاتمة:

تعتبر جريمة التهديد والابتزاز الإلكتروني من الجرائم الإلكترونية المستحدثة، ويطلق عليها في علم الجريمة الجرائم الناعمة، التي تخلو من العنف، وهي أحد صور الجريمة الإلكترونية، و التهديد بالابتزاز الإلكتروني هو الوجه الآخر لجريمة التهديد بالابتزاز التقليدية التي تنشأ وترتكب في عالم مادي، وفي مسرح جريمة تقليدي، حيث يترك الجاني أثاره، أما التهديد والابتزاز الإلكتروني فيتم في عالم افتراضي ملئ بالرموز والشفرات، وشبكات المعلومات و الأجهزة الحديثة وتطبيقاته.

وتجدر الإشارة إلى أن جريمة التهديد بالابتزاز قد تتسبب في حدوث جرائم بعدها، كالقتل أو أي جريمة عنف أو إعتداء أخرى أو سرقة، لذا لابد من ضرورة نشر الوعي داخل المجتمع بأخطار جريمة التهديد بالابتزاز الإلكتروني، وتشجيع من يتعرض للابتزاز بالإبلاغ عن الجريمة.

كما أن الخضوع للمجرم ومطالبه من شأنه أن يزيد في هيمنته وتعنته، لذا يجب التحرك في الإبلاغ عن الجريمة للتخلص منها دون إبلاغ المجرم عن نية التحرك، فالتصرف بحكمة يمكن من إيقاع المجرم في شباك القضاء.

لقد ألقى التطور التكنولوجي مسؤولية كبيرة على عاتق المشرع الجنائي لمواجهة الجرائم المعلوماتية الناشئة عن إساءة استخدام الأنظمة المعلوماتية خاصة في ظل قصور نصوص قانون العقوبات عن الإحاطة بهذه الجرائم، وما يصاحبه من مخاطر جمة و جرائم جديدة وارتكاب جرائم تقليدية بطرق مستحدث، فالأنترنت قدمت مزايا كثيرة في سرعة إنتشار الأخبار والمعلومات التي ساهمت من جهة أخرى في انتشار جرائم التهديد لحياة الأشخاص مع عدم إمكانية وسيلة

الأنترنت من توفير أمان وسرية لكل ما ينقل عبرها، وكل ما يستخدم من تقنيات عبرها، وهذا ما أدى إلى عجز النصوص التقليدية للتصدي لهذا النوع المستحدث للإجرام.

وموضوع التهديد والابتزاز الإلكتروني من الموضوعات التي لا تزال حديثة، والتي لم تنل حظها بنص تشريعي خاص مثل ما هو الحال في الجزائر، وبالتالي كان لزاما علينا مواجهة الجريمة بالنص التجريمي القديم وهو المواد من 284 إلى 287 من قانون العقوبات الجزائري.

وأمام كل التحديات التي تواجه المشرع من صعوبة تحديد هوية المجرم المعلوماتي واستحالة التوصل إلى أدلة مادية ملموسة، والامتداد الجغرافي للجريمة فهي عابرة الحدود، فإنه تبين لنا من خلال الدراسة قصور قواعد القانون الجنائي في مواجهة تهديد حياة الأشخاص عبر الوسائط الإلكترونية، ولذا لابد من تعديل قانون العقوبات وتحديد كل جريمة معلوماتية على حدى بكل صورها بصفة عامة وجريمة التهديد الإلكتروني على وجه الخصوص بتحديد صوره، لأنه لا يكفي التوسع من نطاق تطبيق النصوص التقليدية، حتى لا يصطدم القاضي الجنائي بمبدأ الشرعية الجنائي.

بالإضافة إلى ضرورة استحداث نصوص قانونية إجرائية تتلائم مع مجال الضبط والتحقيق في المجال الافتراضي، لأننا نتوقع أن تكون جريمة التهديد عبر الوسائط الإلكترونية أكثر تطورا مستقبلا، وستكون الأجيال القادمة أكثر خبرة، فالجاني المعلوماتي يتمتع بنوع عالي من الذكاء، والاعتماد بشكل كبير على أساليب تقنية كأنظمة الحاسب الألي والأنترنت والهواتف الذكية، وكل أشكال الأجهزة الإلكترونية.

قائمة المراجع

أولا: المراجع باللغة العربية:

I. النصوص القانونية:

1. المرسوم التنفيذي رقم 98-257 المؤرخ في 25 أوت 1998، المتعلق بشروط وضبط كيفيات إقامة خدمات الأنترنت وإستغلاله، ج.ر،عدد 63.

2. القانون رقم 2000-03 المؤرخ في 5 أوت 2000، يحدد القواعد المتعلقة بالبريد والمراسلات السلكية واللاسلكية، ج.ر، عدد 48 الصادرة بالتاريخ 6 أوت 2000.

3. القانون رقم 04-15المؤرخ في10نوفمبر 2004 المعدل والمتمم للأمر 66-156،المؤرخ في 1966/06/08 المتضمن قانون العقوبات، ج.ر عدد 71 المؤرخ في2004/11/10.

4. المرسوم التنفيذي رقم 06-348 المؤرخ في 2006/10/05 ج.ر رقم 63 الصادرة بتاريخ 2006/11/08.

5. القانون رقم 09-04 المؤرخ في 05أوت 2009، المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والإتصال ومكافحتها، ج.ر عدد 47، مؤرخة في 16 أوت 2009.

6. القانون رقم 18-07 المؤرخ بتاريخ 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر عدد 34 المؤرخة في 10 جوان 2018.

II. الكتب:

1. **الشوا محمد**، ثورة المعلومات وإنعكاساتها على قانون العقوبات، طبعة 2، دار النهضة العربية.

2. **الدرة ماهر عبد شويش**، شرح قانون العقوبات، القانون الخاص، طبعة 2، شركة العاتك لصناعة الكتاب.

3. **الغالبي رامي أحمد**، جريمة الإبتزاز الإلكتروني وألية مكافحتها في جمهورية العراق، ضمن مؤلف الابتزاز الإلكتروني جريمة العصر الحديث، دار الكتب والوثائق، بغداد.

4. **المطبري طارق عبد الرزاق**، الأحكام الخاصة بجريمة الإبتزاز المقررة في نظام مكافحة الجرائم المعلوماتية السعودي، رسالة ماجيستير، جامعة الإمام محمد بن سعود الإسلامية، الرياض، سنة 2010.

5. **أمير فرج يوسف**، حقوق الملكية الفكرية الإلكترونية، **حقوق الملكية الفكرية الإلكترونية، الطبعة الأولى، مكتبة الوفاء القانونية للنشر ،مصر**، سنة 2016.

6. **أسامة أحمد المناعسة وجلال محمد الزغبي**، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع،الطبعة الثانية، الأردن، سنة 2014.

7. **الزريق خليفة بن علي بن محمد**، ابتزاز الأحداث وعقوبته في النظام السعودي (دراسة تأصيلية مقارنة تطبيقية)، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2015.

8. **عفيفي كامل عفيفي**، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الأولى، سنة 2003.

9. **عبد المهين سالم بكر**، الوسيط في شرح قانون الجزاء الكويتي، القسم الخاص، الكويت، بدون سنة نشر.

10. عبد الفتاح محمود كيلاني، المسؤولية المدنية الناشئة عن المعاملات الإلكترونية عبر الأنترنت، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، سنة 2011.

11. **محمد طارق عبد الرؤوف الحق**،جريمة الإحتيال عبر الأنترنت، الأحكام الموضوعية والأحكام الإجرائية، منشورات الحلبي الحقوقية.

12. **طالب مصدق عادل**، جريمة الإبتزاز الإلكتروني في التشريع العراقي، ضمن مؤلف الإبتزاز الإلكتروني جريمة العصر الحديث، دار الكتب والوثائق، بغداد.

13. **ضياء مصطفى عثمان**، السرقة الإلكترنية، دراسة فقهية، دار النفائس للنشر والتوزيع، الطبعة الأولى 2011.

14. **صايل فاضل الهواوشة**، جرائم الحاسوب والأنترنت، دراسة تحليلية مقارنة، الأردن، سنة 2001.

15. **رشيدة بوكر**، جرائم الإعتداء على نظم المعالجة الألية في التشريع الجزائري المقارن، منشورات الحلبي، الطبعة الأولى، 2012.

16. **ياسر أمير الفاروق**، مراقبة الأحاديث الخاصة في الإجراءات الجزائية، دار المطبوعات الجامعية، الطبعة الأولى، سنة 2009.

III. المذكرات:

1. **بوخبزة عائشة**، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجيستير تخصص قانون جنائي، سنة 2013/2012،ص 247و248.

IV. المقالات:

1. **بن زحاف فيصل**، مقال قانوني بعنوان الحماية الجنائية للحكومة الإلكترونية، مجلة القانون، المجتمع والسلطة، العدد رقم 03-2014.
2. **المسند صالح بن محمد، المهيني، عبد الرحمن بن راشد**، جرائم الحاسب الآلي: الخطر الحقيقي فيعصر المعلومات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 15، العدد 29، الرياض، 2015.

قائمة الهوامش

[1] يصنف مجرموا الأنترنت إلى

أ- الهاكر: أو ما يسمى بقراصنة الكمبيوتر نوعان: -الهاكر الأمن : يقصد به من يستخدم الحاسوب وشبكة الأنترنت لإختراق نظم الأمن والشبكات، بغرض الدخول غير المصرح به، ورغم قدرته الفائقة على الإختراق، إلا أنه غير مؤذ، فهو لا يقوم بالتخريب وإنما فقط يشعره عالم الأنترنت بالحرية، إضافة إلى الفضول ودافع التحدي وإثبات المقدرة.

le terme « hacher » provient du verbe. to hack ; qui signifie la pénétration à l'interieur d'un système informatique ou un ordinateur.

الهاكر الخبيث أو الكراكر: يقصد به المخترق ذي النوايا الإجرامية، يقوم بما هو سيء كالإتلاف والتخريب أو الإرهاب أو الإبتزاز أو العدوان على الأموال بالسرقة والإحتيال وغيرها.

Le terme « cracker » provient du verbe « to crack » qui signifie « s'écraser ». le cracker la personne qui pénétre à l'interieur d'un système informatique et détruit ses éléments par plaisir.

ب- المحترفون: تتميز هذه الطائفة بسعة الخبرة والإدراك الواسع للمهارات التقنية، كما تتميز بالتنظيم والتخطيط للأنشطة الإجرامية، وتعد هذه الطائفة من بين أخطر مجرمي التقنية، حيث تهذف إعتداءاتهم إلى تحقيق الكسب المادي لهم، أو للجهات التي كلفتهم وسخرتهم لإرتكاب جرائم الحاسوب، كما تهذف إعتداءات بعضهم إلى تحقيق أغراض سياسية، أو التعبير عن موقف فكري أو فلسفي.

ج- الحاقدون:هؤلاء الطائفة لا يسعون لإثبات مقدراتهم التقنية ولا إلى تحقيق مكاسب مادية أو سياسية وإنما يحركهم الثأر والرغبة بالإنتقام، كالإنتقام لصاحب العمل مثلا، وتغلب على أنشطتهم من الناحية التقنية استخدام تقنية زرع الفيروسات والبرامج الضارة.

د- طائفة صغار السن: أو صغار نوابغ المعلوماتية،هم صغار السن مولعون بالحوسبة والإتصالات، ويثير مجرموا هذه الفئة جدلا واسعا لتقدير مدى خطورتهم، فهناك من الفقه من يرى لا يجب إسباغ أي صفة جرمية على سلوكاتهم، وهناك من الفقه من يرى بأنهم يقدمون خدمة لأمن المعلومات، لأن لهم الفضل في كشف الثغرات الأمنية في تكنولوجيا المعلومات، هناك إتجاه ثالث يصنف هؤلاء الصغار ضمن طائفة مجرمي الحواسيب كغيرهم دون تمييز. أنظر محمد طارق عبد الرؤوف الحق، جريمة الإحتيال عبر الأنترنت، الأحكام الموضوعية والأحكام الإجرائية، منشورات الحلبي الحقوقية، ص من 184-188.

[2] القانون 04-15 (المعدل والمتمم للأمر رقم 156/66 المؤرخ في 08جوان 1966 المتضمن قانون العقوبات،ج.ر عدد 71 الصادرة بتاريخ 2004/11/10،)، تضمن المواد من 394 مكرر إلى394 مكرر7 والذي تم من خلاله إدماج أحكام خاصة بالإجرام المعلوماتي في صلب قانون العقوبات لمسايرة التشريع للتطورات التكنولوجية، وهي جرائم تستهذف الأنظمة المعلوماتية من خلال الدخول غير الشرعي في النظام المعلوماتي لشخص معين أو دولة معينة والعمل على تعطيل النظام أو إزالته أو التجارة به، مثل القرصنة...إلخ.

[3] القانون رقم 09-04،(المعدل لقانون العقوبات المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها. ج ر، عدد47، الصادرة بتاريخ 16سبتمبر 2009)، جاء لتعزيز الحماية الجزائية للأنظمة المعلوماتية والذي مس المادة 303 وإقراره المواد من 303 مكرر إلى 303مكرر 3، حاول المشرع الجزائري بموجبه حماية خصوصية الأفراد تحسبا للإستخدام السيء للوسائل التكنولوجية الحديثة عن طريق الكمبيوتر أو الهاتف النقال، وما يرتبط بها من تقنيات في نظام الإتصالات الإلكترونية. مثل ما يسمى بالبلوتوث وغيره.

[4]القانون رقم 18_07 بتاريخ 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر عدد 34 المؤرخة في 10 جوان 2018،ص 11.

[5]الشوا محمد، ثورة المعلومات وإنعكاساتها على قانون العقوبات، طبعة 2، دار النهضة العربية، ص 7.

[6]عبد المهين سالم بكر، الوسيط في شرح قانون الجزاء الكويتي، القسم الخاص، الكويت، بدون سنة نشر،ص 221.

[7]الدرة ماهر عبد شويش، شرح قانون العقوبات، القانون الخاص، طبعة 2، شركة العاتك لصناعة الكتاب، ص 223.

[8]الغالبي رامي أحمد، جريمة الإبتزاز الإلكتروني وألية مكافحتها في جمهورية العراق، ضمن مؤلف الإبتزاز الإلكتروني جريمة العصر الحديث، دار الكتب والوثائق، بغداد، ص 29.

[9]طالب مصدق عادل، جريمة الإبتزاز الإلكتروني في التشريع العراقي، ضمن مؤلف الإبتزاز الإلكتروني جريمة العصر الحديث، دار الكتب والوثائق، بغداد، ص 55.

[10]المسند صالح بن محمد، المهيني، عبد الرحمن بن راشد، جرائم الحاسب الآلي: الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 15، العدد 29، الرياض، 2015، ص 181.

[11]الزريق خليفة بن علي بن محمد، ابتزاز الأحداث وعقوبته في النظام السعودي (دراسة تأصيلية مقارنة تطبيقية)، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2015، ص 72و 73

[12]هذا التعريف ورد في المادة 3 فقرة 11 من قانون 18: 07 ونفس التعريف تضمنه القانون 18:04 المتعلق بالبريد والإتصالات الإلكترونية، وكذا في القانون 09:04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.

[13]أسامة أحمد المناعسة، وجلال محمد الزغبي، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، الأردن 2014، ص 27

[14]عبد الفتاح محمود كيلاني، المسؤولية المدنية الناشئة عن المعاملات الإلكترونية عبر الأنترنت، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، سنة 2011،ص16و17.

[15]ضياء مصطفى عثمان، السرقة الإلكترنية، دراسة فقهية، دار النفائس للنشر والتوزيع، الطبعة الأولى 2011. ص 25.

[16]القانون رقم 04-15المؤرخ في 10نوفمبر 2004 المعدل والمتمم للأمر 66-156،المؤرخ في 1966/06/08 المتضمن قانون العقوبات، ج.ر عدد 71 المؤرخ في2004/11/10.والقانون رقم 09-04 المؤرخ في 2009/08/5 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة ب تكنولوجيا الإعلام والإتصال ومكافحتها، ج.ر عدد47 المؤرخة في2009/08/06.

[17]المرسوم التنفيذي رقم 06-348 المؤرخ في 05 نوفمبر2006، ج.ر رقم 63 الصادرة بتاريخ 08 نوفمبر2006.

[18]بن زحاف فيصل، مقال قانوني بعنوان الحماية الجنائية للحكومة الإلكترونية، مجلة القانون، المجتمع والسلطة، العدد رقم 03-2014، ص 82.

[19]أمير فرج يوسف، حقوق الملكية الفكرية الإلكترونية والمساس بها بإعتبارها جريمة الكترونية، الطبعة الأولى، مكتبة الوفاء القانونية،مصر، سنة 2016، ص 350.

[20]أمير فرج يوسف، حقوق الملكية الفكرية الإلكترونية، المرجع السابق، ص 350.

[21]محمد طارق عبد الرؤوف الحق، المرجع السابق، ص 310.

[22]صايل فاضل الهواوشة، جرائم الحاسوب والأنترنت، دراسة تحليلية مقارنة، الأردن، سنة 2001،ص 264.

[23]رشيدة بوكر، جرائم الإعتداء على نظم المعالجة الألية في التشريع الجزائري المقارن، منشورات الحلبي، الطبعة الأولى، 2012، ص 397.

[24]رشيدة بوكر، المرجع السابق، ص 398

[25]رشيدة بوكر، المرجع نفسه، ص 398

[26]أمير فرج يوسف، حقوق الملكية الفكرية الإلكترونية، المرجع السابق،ص 388.

[27]أمير فرج يوسف، حقوق الملكية الفكرية الإلكترونية، المرجع نفسه،ص 390و392.

[28]المادة 65 مكرر 16 من قانون الاجراءات الجزائية، راجع أيضا رشيدة بوكر، المرجع السابق،ص 439

[29]ياسر أمير الفاروق، مراقبة الأحاديث الخاصة في الإجراءات الجزائية، دار المطبوعات الجامعية، الطبعة الأولى، سنة 2009.ص 139.

[30]شيدة بوكر، المرجع السابق، ص 444و445.

[31]رشيدة بوكر، المرجع نفسه، ص 446و447.

[32]رشيدة بوكر، المرجع نفسه، ص 446و447.

[33]عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الأولى، سنة 2003، ص 327.

[34]بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماجيستير تخصص قانون جنائي، سنة 2013/2012، ص247و248.