جامعة أكلي محند أولحاج – البويرة
كلية الحقوق والعلوم السياسية
قسم القانون العام

جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية

مذكرة لنيل شهادة الماستر في القانون العام

تخصص: قانون جنائي وعلوم جنائية

إعداد الطالبتين:
- بوضياف سارة
- بن تواتي صارة

إشراف الأستاذ:
د/ خليفي سمير

لجنة المناقشة

الأستاذ(ة) د/ قاسم حكيم.....رئيسا

الأستاذ(ة): د/ خليفي سمير .....مشرفا ومقررا

الأستاذ(ة): د/ نبهي محمد.....ممتحنا

السنة الجامعية: 2022/2021

شكر و تقدير

إن الشكر لله شكرا عظيما، والحمد لله حمدا كثيرا الذي أعاننا في إنجاز هذا العمل حمدا يليق بجلال وجهه وعظيم سلطانه .

عملا بقوله **صلى الله عليه و سلم:** << من لا يشكر الناس لا يشكر الله >> .

أولا نتقدم بجزيل الشكر والامتنان إلى الذي يصب مثل النهر على طلبته بالعلم " **الدكتور خليفي سمير**"، الذي أشرف على مذكرتنا ولم يبخل علينا يوما بالنصائح فكان لنا السراج الذي ينير الطريق؛ لن ولم تكن الحروف في وقت ما كافية للبوح بما يحمله القلب من امتنان فجزاك الله عنا كل خير .

كما نتقدم بالشكر الجزيل إلى أعضاء لجنة المناقشة قبولهم مناقشة مذكرتنا وتكبدهم عناء قراءتها وتقييمها.

دون أن ننسى تقديم أسمى عبارات الشكر و التقدير إلى الذين مهدوا لنا طريق العلم والمعرفة، إلى جميع أساتذة كلية الحقوق والعلوم السياسية لجامعة البويرة.

إهداء

أهدي ثمرة جهدي إلى :

من قال فيهما ذو الجلال و الاكرام: << و قضى ربك ألا تعبدوا إلا إياه و بالوالدين إحسانا إما يبلغن عندك الكبر أحدهما أو كلاهما فلا تقل لهما أف و لا تنهرهما و قل لهم قولا كريما>>. *سورة الإسراء .*

إلى ليث بيتنا الذي عمل بكد في سبيلي و علمني الكفاح و أوصلني إلى ما أنا عليه، إلى أغلى شخص في هذا الوجود الذي ليس له مثيل .

*" **أبي الغالي** " أطال الله في عمره .*

إلى التي لا يمكن للكلمات أن توفي حقها و لا للأرقام أن تحصي فضائلها، إلى التي أمسكت بيدي و أخذتني عند نهر العلم و فارقتني عند الضفة و أخفت دموع خوفها، إلى من جعل الجنة تحت قدميها .

*" **أمي الغالية** " أطال الله في عمرها .*

إلى منبع المحبة و الحنان .

*" **أخواتي** " كل باسمها .*

إلى من أسند بهما أزري .

*" **إخواني** " عادل، عبد العالي .*

إلى روح عمي رحمه الله و أسكنه فسيح جنانه .

إلى من يحمل معنى كاد المعلم أن يكون رسولا .

*" **معلمي** " لك مني خالص الدعاء .*

إلى صديقتي و زميلتي في هذا العمل .

*" **بن تواتي صارة** "*

إلى كل من له معزة في قلبي : *" أبناء أخواتي كل باسمه ، أزواج أخواتي، صديقاتي المقربات كل باسمها" .*

بوضياف سارة .

إهداء

الحمد لله الذي بنعمته تتم الصالحات والصلاة على الحبيب المصطفى وأهله .

الحمد لله الذي وفقنا لتثمين هذه الخطوة في مسيرتنا الدراسية بمذكرتنا، فهذه ثمرة الجهد والنجاح بفضله تعالى .

إلهي لا يطيب الليل إلا بشكرك ولا يطيب النهار إلا بطاعتك، ولا تطيب الآخرة إلا بعفوك.

إلى ملاكي في الحياة...إلى معنى الحب والحنان والتفاني...إلى بسمة الحياة و سر الوجود إلى من كان دعاؤها سر نجاحي، إلى أغلى الحبايب

" أمي الحبيبة "

إلى من كلله الله بالهيبة والوقار إلى من علمني العطاء بدون انتظار، إلى من خطى لي المبادئ والأخلاق

" أبي الغالي"

إلى من نشأت وترعرعت بينهم إخوتي وأخواتي سندي في الحياة حفظم الله وأنار دربهم.

إلى رفيق دربي... إلى من أحمل اسمه بكل افتخار

" زوجي الغالي"

إلى قرة عيني، إلى اللذان لا أستطيع العيش من دونهما أولادي

*" **وسيم**"، "**أمير**" أنار الله خطاهم و حفظهم.*

إلى جميع الأصدقاء والأهل والأحبة .

بن تواتي صارة

مقدمة

عرفت البشرية عبر تاريخها الطويل تطورات متلاحقة وتحولات كبيرة في طرق وأساليب الحياة، ويعود الفضل في ذلك للثورة التكنولوجية أو الثورة الرقمية التي عرفتها خلال العقود الأخيرة من القرن العشرين في مجال الاتصالات الالكترونية وتكنولوجيا المعلومات والتي شملت معظم نواحي الحياة انطلاقا من قدرتها على دفع المجتمعات الإنسانية إلى حيز متطور قائم على محورية المعلومات المعرفة وصولا إلى الهيمنة العنيفة للعلوم والتكنولوجيا باعتبار من يملك المعلومات يمتلك مفاتيح المستقبل.

جاءت هذه الثورة نتيجة التقدم الهائل في وسائل الاتصال المعلوماتية، ومن بين وسائلها الكثيرة أجهزة الحاسب الآلي والهاتف النقال باعتبار الحاسب الآلي أداة للتحكم بالمعلومات وتجميعها ومعالجتها واختزانها واسترجاعها ونقلها. أما الهواتف النقالة أو المحمولة فهي أحد أشكال أدوات الاتصال اللاسلكي عن طريق شبكة من أبراج البث وأصبحت بديلا لأجهزة الحاسب من حيث البرامج والتطبيقات الخاصة بالهواتف.

وفي ظل المعطيات الحديثة للمجتمعات المعاصرة التي تشهد انفتاحا وهو ما جعلها مجالا مفتوحا تهدده أخطار جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية، فقد أفرز تزايد استعمال شبكات الاتصال الحديثة والأنظمة المعلوماتية إشكالات قانونية هامة، فظهرت أنماط جديدة من الجرائم لم تكن معهودة في السابق يتم تنفيذها عبر معدات أو أجهزة إلكترونية أو تبث عبر شبكة الانترنت أو محتوياتها تلحق أضرارا وهي من أثار الممارسات السيئة لثورة تكنولوجيا المعلومات.

وتشكل جرائم الاعتداء على الأشخاص ذروة الإجرام لما تمثله من اعتداء على حياة الآخرين وإهدار لحقهم في الحياة والسلامة الجسدية لا يجادل أحد في أن حق الإنسان في الحيلة وفي سلامته الجسدية هما من أسمى الحقوق الطبيعية التي يتمتع بها هذا الأخير وفي الحفاظ عليها حفاظا على حقه في الولوج والبقاء وصيانة الجسم امتداد طبيعي لصيانة الحياة. لذا كانت من أهداف القوانين الجنائية حماية هذا الحق عبر تجريم كل الأنشطة التي من شأنها أن تصيب الأشخاص في حياتهم أو في جسدهم.

لما كان الأمر كذلك في إطار الجرائم العادية فإنه عندما يتعلق الأمر بالجريمة المرتكبة عبر الوسائط الإلكترونية وما يتبع ذلك من وقوع الكثير من الضحايا نتيجة للعمليات الممنهجة التي يتخذها المجرمون المعلوماتيون.

أدى ظهور هذا النوع من الجرائم الذي عرف بمصطلح "الجريمة الإلكترونية" والتي سماها المشرع الجزائري بجرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات الجزائري، وهي أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية. ويوما بعد يوم توج التطور المتلاحق في تقنية المعلومات إلى خلق بيئة افتراضية تتحقق فيها المعلومات والاتصالات عبر الحدود ما يؤدي إلى الاعتداء على حق الإنسان في سمعته وشرفه و اعتباره؛ كما هو الحال في جريمتي القذف والسب وكذا التحرش الجنسي عبر الوسائط الإلكترونية، فهي جرائم متطورة ومستحدثة تستوجب الذكاء الإجرامي مما أدى إلى تطوير البنية التشريعية على المستوى القانوني وأخذ إشكالات عديدة في تنظيم قواعد إجرائية لمواجهة مثل هذه الجرائم وهذا نظرا للخطورة التي بلغتها الجرائم المرتكبة عبر الوسائط الإلكترونية، فقد جندت كل القوانين والتشريعات لتجريم وردع مثل هذا النوع من الجرائم.

حاول المشرع الجزائري قدر الإمكان التصدي لجرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية بسن قوانين لمواجهة الجريمة الإلكترونية بموجب قانون العقوبات وقانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[1]، وقانون الإجراءات الجزائية، حيث عرف هذا الأخير تعديلا في إجراءات التحقيق والمتابعة في الجرائم الإلكترونية، فأنشأ لها قطب جزائي وطني مختص في مكافحة الجرائم

[1] قانون **رقم 09-04** المؤرخ في 14 شعبان 1430، الموافق ل 05 غشت 2009، يتضمن القواعد الخاصة من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج. ر، العدد 47، الصادر بتاريخ 16 غشت 2009.

المتصلة بتكنولوجيات الإعلام والاتصال وهذا وفقا للأمر رقم 11/21 المتمم لقانون الإجراءات الجزائية[1]، ورغبة منه في مسايرة ومواكبة الاتفاقيات على الصعيد العربي والدولي.

أهمية الموضوع:

يكتسي موضوع دراسة جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية جانبا كبيرا من الأهمية يتمثل في كونه يضم أهم وأخطر الجرائم التي عرفها المجتمع والتي تؤدي إلى زعزعة المجتمع بأكمله وليس الفرد فقط، وأنه ومع التطور العلمي تتزايد نسبة ارتفاع الجرائم المرتكبة عبر الوسائط الإلكترونية لأن مرتكبيها دائما ما ينشطون في تطوير أدواتهم مستفيدين من التقدم الحاصل في استخدام التكنولوجيا، الأمر الذي يترتب عليه بالضرورة العمل على مكافحة هذه الجرائم على النحو الذي يؤدي إلى الحد منها إن لم يكن القضاء عليها. كما تكمن أهمية هذا الموضوع كون الجريمة المعلوماتية من الموضوعات الحديثة التي فرضت نفسها بقوة على المستوى الوطني والدولي والتي تفرض على المشرع الجزائري ضرورة مواجهتها بترسانة قانونية حاسمة ورادعة لمكافحة ومعاقبة مرتكبيها.

إن البحث في موضوع جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية هو بحث في قضية من قضايا الواقع، وإشكال من إشكالاته .

أسباب اختيار الموضوع:

تكمن دواعي اختيار موضوع جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية لكونه موضوع مستحدث تزامن مع التطور التكنولوجي لوسائل الاتصال والإعلام هذا من جهة، ومن جهة أخرى كونه من بين الجرائم الأكثر تعقيدا، وتتمثل دواعي اختيارنا له فيما هو ذاتي وآخر موضوعي.

[1] **أمر رقم 21-11** المؤرخ في 16 محرم 1443 الموافق ل 25 غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق ل 08 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج.ر، عدد65، الصادر بتاريخ 26 أوت، 2021.

الأسباب الذاتية:

قمنا باختيار هذا الموضوع نظرا لاهتمامنا الكبير بالمجال المعلوماتي من الناحية التقنية مما دفع بنا إلى دراسة الجانب القانوني العقابي، وحداثة هذا الموضوع لفت انتباهنا كباحثين مما أورد إلينا حب الاطلاع عليه ورغبتنا في التعمق في دراسة هذه الجرائم المستحدثة والإلمام بجوانبها المختلفة والتطلع على المستجدات الحاصلة بها وإثراء النقاش القانوني حول هذا الموضوع الهام بتناوله بشقيه الموضوعي والإجرائي، ورغبة منا في معرفة مواجهة المشرع الجزائري لمثل هذه الجرائم، إضافة إلى دواعي موضوعية.

الأسباب الموضوعية:

محاولة التعرف أكثر على تقنيات التواصل الحديثة لمواكبة الجرائم الصادرة عنها و اتخاذ الإجراءات المناسبة للحد منها، ومعرفة القفزات السريعة التي عرفتها مختلف الوسائط الإلكترونية خاصة منها شبكة الانترنت و الهاتف المحمول بعد أن أدخل عليهما أحدث تقنيات نقل المعلومات، ، و محاولة الوقوف على الجهود المبذولة من طرف المشرع الجزائري و ما إذا كانت كافية للحد من هذا النوع من الجرائم أم لا.

أهداف الدراسة:

إن دراسة موضوع جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية يهدف إلى:

*-معرفة ما توصلت إليه التشريعات من سنها للقوانين وتبنيها للاتفاقيات لردع هذه الجريمة.

*-تسليط الضوء على أدلة الإثبات في الجريمة المعلوماتية من أجل التعرف عليها وعلى الخصوصيات التي تميزها عن باقي أدلة الجرائم التقليدية، وتسليط الضوء على وسائل الاتصال الحديثة.

*-تقييم مدى مواكبة القضاء لهذا النوع من الجرائم الحديثة.

وانطلاقا مما سبق ذكره فإن موضوع دراستنا حول جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية يثير التساؤل التالي:

فيما تتمثل جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية وماهي الاجراءات القانونية المقررة لإثباتها ؟

على هذا الأساس اعتمدنا على منهجين يتماشى وموضوع بحثنا وهما المنهج الوصفي والمنهج التحليلي.

إذ اعتمدنا المنهج الوصفي نظرا لقيامنا بوصف الجرائم والانتهاكات التي تطال الأشخاص عبر الوسائط الإلكترونية، وهذا من أجل تشخيص الجانب المفاهيمي لموضوع الدراسة. أما اعتمادنا على المنهج التحليلي راجع إلى قيامنا بتحليل الجرائم المرتكبة على الأشخاص عبر الوسائط الإلكترونية باعتبار أن الموضوع مستقى ومستمد من النصوص القانونية وبيان مدى تكاملها وتناسبها وتحقيق الغرض من تشريعها.

وحتى نتمكن من معالجة الإشكالية المطروحة ارتأينا إلى تقسيم الخطة إلى فصلين معتمدين على التقسيم الثنائي للخطة، حيث تطرقنا إلى توضيح الإطار المفاهيمي لجرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية وذلك من خلال تبيان ماهية جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية، ومن ثم التطرق إلى صور جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية (**الفصل الأول**). ليصل بنا الحديث إلى توضيح الإطار التنظيمي عبر الوسائط الإلكترونية، إذ تناولنا القواعد الإجرائية لجرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية، ومن ثم تبيان صعوبات و آليات مكافحة الجريمة الإلكترونية (**الفصل الثاني**).

الفصل الأول:

الإطار المفاهيمي لجرائم الإعتداء على الأشخاص عبر الوسائط الإلكترونية

الفصل الأول:

الإطار المفاهيمي لجرائم الإعتداء على الأشخاص عبر الوسائط الإلكترونية

نتجت عن الثورة المعلوماتية جرائم إلكترونية مختلفة ومتنوعة وبدرجة خطورة إجرامية عالية عن الجرائم التقليدية فظهرت إلى الوجود مصطلحات جديدة للدلالة على الجرائم التي تقع في البيئة الإلكترونية، وقد تنوعت هذه الجرائم في هذا الوسط الإجرامي كجرائم الاعتداء على الأشخاص وبالأخص عبر الوسائط الإلكترونية، حيث اعتمدت على وسائل إلكترونية حديثة ومتنوعة على حسب الخدمة التي يقدمها والغرض الذي يستعمل لأجله في البيئة الرقمية لاستعمالها في وسائل إجرامية التي ترتبط ارتباطا وطيدا بالشبكة العنكبوتية. وباختلاف وسائل ارتكابها ومرتكبيها اختلفت كذلك صور الاعتداء عليها بصورة تقنية جديدة غير مشروعة.

ويتم تناول هذا الفصل من خلال تقسيمه إلى مبحثين؛ نستهل دراستنا بماهية جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية(**المبحث الأول**)، ثم التطرق إلى صور جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية(**المبحث الثاني**).

المبحث الأول

ماهية جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية

لا شك أن الثورة الإلكترونية التي عرفها العالم اليوم تؤرخ لحقبة جديدة من تاريخ البشرية، حيث قدمت الوسائط الإلكترونية (الحاسب الآلي–الانترنت–الهاتف...) للبشرية الرقي في جميع المجالات فأصبحت هذه الأخيرة وسيلة العالم نحو الرقي الحضاري ومصدر للثروة، هذا التطور المذهل واكبه من جهة أخرى تميز في انحراف العقل البشري عن مسار الأخلاق والقانون إلى إفراز أنواع جديدة من السلوك الإجرامي تمثلت في الجرائم المرتكبة عبر الوسائط الإلكترونية[1].

ولعل أبرز ما يميز هذه المرحلة التي نعيشها اليوم، هو التآزر الغير المسبوق في تكنولوجيا الاتصال بين النواقل والحاسبات. ومن منظور اتصالي يمكن القول أن تكنولوجيا الاتصال هي مجموع التقنيات والأدوات والوسائل والنظم المختلفة التي يتم توظيفها لمعالجة المحتوى الذي يراد توصيله من خلال عملية الاتصال الجماهيري والشخصي وغير ذلك من أنواع الاتصال، ومن هنا جاءت تسمية هذه المرحلة بمرحلة تكنولوجيا الاتصال المتعدد الوسائط.

وقبل التطرق إلى ماهية جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية، سنتطرق إلى مفهوم الوسائط الإلكترونية **(المطلب الأول)**، بالإضافة إلى وسائل ارتكاب جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية **(المطلب الثاني)**.

[1] **مراد يتار**، الجرائم المرتكبة عبر الوسائط الإلكترونية، رسالة لنيل شهادة الماستر في القانون الخاص، تخصص العلوم الجنائية والأمنية، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة القاضي عياض مراكش، 2017-2018، ص01.

المطلب الأول

مفهوم الوسائط الالكترونية

قد تقدم التكنولوجيا للباحثين في مجال المعرفة خيارات جديدة للحصول على ما يريدون من المعلومات والأشكال والصور. لكن اشترطت بالضرورة أن يقتضي في منتجي تلك المعرفة سلوكيات لم تكن ضرورية في السابق؛ أي وفق الوسائل التقليدية[1].

ظهر مفهوم الوسائط الالكترونية أو ما يسمى بالوسائط المتعددة متزامنا مع تطور الحاسب الآلي خاصة في أجياله الحديثة، وتمثل تقنيات الوسائط الالكترونية المتعددة ابرز مظاهر الثورة الرقمية حيث أتاحت تقنيات الحاسوب والانترنت تقديم المواد المقروءة والمسموعة والمرئية في أن واحد على شاشة الحاسوب، إذ يمكن مثلا قراءة نص روائي والاستماع إلى نص موسيقي، ومشاهدة صور ثابتة وفيديوهات تعبر عن الموضوع نفسه، فهذه التقنية تخاطب جميع حواس الإنسان ومداركه العقلية. وقد نضجت تلك التقنيات بشكل منقطع في السنوات الأخيرة وهي في طريقها للاندماج في حياتنا اليومية وبالأخص في مجالات الإعلام والتعليم والترفيه والأنشطة الاقتصادية والاجتماعية[2].

ولعل أبرز ما يميز هذه المرحلة التي نعيشها اليوم هو التآزر غير المسبوق في تكنولوجيا الاتصال بين النواقل والحاسبات، ومن منظور اتصالي يمكن القول بأن تكنولوجيا الاتصال هي مجموع التقنيات والوسائل والنظم المختلفة التي يتم توظيفها لمعالجة المضمون أو المحتوى الذي يراد توصيله من خلال عملية الاتصال الجماهيري أو الشخصي وغير ذلك من أنواع الاتصال والتي يتم من خلالها جمع المعلومات والبيانات في الوقت المناسب، وهذه

---

[1] **عباس ناجي حسن**، الوسائط المتعددة في الإعلام الالكتروني دراسة مقارنة، الطبعة الأولى، دار صفاء للطباعة والنشر والتوزيع، المملكة الأردنية الهاشمية، عمان، 2016، ص130.

[2] **محمد جاسم فلحي**، النشر الالكتروني الطباعة والصحافة الالكترونية والوسائط المتعددة، د.ط، دار المناهج للنشر والتوزيع، عمان، 2005، ص97.

المرحلة الراهنة تتسم بصفة أساسية هي المزج بين أكثر من تكنولوجيا اتصالية تمثلها أكثر من وسيلة لتحقيق هدف نهائي وهو توصيل الرسالة للجمهور المستهدف ومن هنا جاءت تسمية هذه المرحلة بمرحلة تكنولوجيا الاتصال المتعدد الوسائط[1].

واليوم تمكنت الوسائط المتعددة أن تدخل مجالات كثيرة منها؛ المواقع الالكترونية الإخبارية، الاختبارات، البرامج الترفيهية التعليمية، حيث تصنف الوسائط الالكترونية المتعددة إلى عدة تصنيفات حسب استخداماتها الحسية أو المستفيدين ومستوى التكنولوجيا[2].

ويكمن توضيح مفهوم الوسائط الإلكترونية من خلال التطرق إلى تعريف الوسائط الإلكترونية **(الفرع الأول)**، بالإضافة إلى خصائص الوسائط الإلكترونية **(الفرع الثاني)**.

الفرع الأول: تعريف الوسائط الإلكترونية

يشير مصطلح الوسائط الالكترونية أو ما يسمى بالوسائط المتعددة إلى مفاهيم وتطبيقات مختلفة عند مجموعة القطاعات التي تتعامل معها مباشرة، ويحمل التعبير مفاهيم أخرى مثل الوسائط الأحادية والوسائط المندمجة، والوسائط النهائية.

ونستعرض مجموعة من التعريفات التي تؤخذ وتعتبر مداخل لفهم الوسائط الالكترونية المتعددة منها:

"هي مصطلح لوصف اتحاد البرامج والأجهزة التي تمكن المستخدم من الاستفادة من النص والصور والصوت والعروض والصور المتحركة ومقاطع الفيديو"[3].

[1] **محي الدين تيتاوي**، النشر الالكتروني والآخراج الصحفي، شركة مطابع السودان للعملة، الخرطوم، 2004، ص119.

[2] **حسن حسين زيتون**، تصميم التدريس رؤية منظومية، الطبعة الثانية، عالم الكتب، 2001، ص456-457.

[3] **عباس مصطفى صادق**، الإعلام الجديد المفاهيم والوسائل والتطبيقات، الطبعة الأولى، دار الشروق للنشر والتوزيع، رام الله، فلسطين، 2008، ص128.

وتعرفها المنظمة العربية على أنها "التكامل بين أكثر من وسيلة واحدة تكمل بعضها البعض عند العرض أو التدريس ومن أمثلة ذلك: مطبوعات الفيديو، الشرائح، التسجيلات الصوتية، كمبيوتر[1].

كما تعرف الوسائط الالكترونية بأنها تزامن وتوافق في استعمال أكثر من وسيط إعلامي إلكتروني للحاسوب، والأنواع الأساسية المتاحة في الوسائط الالكترونية هي؛ النص المكتوب والتصوير والرسم والصوت والفيديو، ونقل هذه الوسائل على أقراص مدمجة يجعلها وسيلة إعلامية يمكن مشاهدتها على شاشة الحاسوب. وبمعنى آخر هو قدرة المستعمل على الخلط أو التفاعل مع أنواع متعددة كالنص المكتوب والصور والأصوات والرسومات والفيديو في الحاسوب.

و بعبارة أخرى الوسائط الالكترونية المتعددة تعني الاستعمال المختلط بين أكثر من وسيلة رقمية مختلطة أو مندرجة، وربما يكون الجانب الفريد في الوسائط الالكترونية هو الاندماج أكثر من رسالة فضلا عن قدرة المستعمل في التحكم في تدفق المعلومات وصياغتها، وذلك ما يميز الوسائط الالكترونية الحاسوبية عن التلفزيون أي الاتجاه الواحد[2].

ويعرفها عبد الحميد بسيوني بأنها: تعبر عن دمج أنظمة مختلفة (كمبيوتر، ونصوص ومرئيات ساكنة ومتحركة، وصوتيات واتصالات) في نظام واحد يضع في متناول الإنسان في منزله أو عمله أو إشعاله بمجموعة أدوات وتقنيات تتيح له استعمال إمكانات متعددة في نظام متكامل ومتسع ومتفاعل يوسع آفاق الاستخدام من بيئة صغيرة محدودة إلى بيئة متعددة الخدمات غير مرتبطة بالمكان مستفيدة من التطورات الحديثة بأسلوب سهل ونظام عمل ميسر.

[1] **عباس ناجي حسن**، المرجع السابق، ص132.

[2] **محمد جاسم فلحي**، النشر الالكتروني في الطباعة والصحافة الالكترونية والوسائط المتعددة، دار المناهج للنشر والتوزيع، عمان، 2006، ص99.

ويمكن القول بأن الوسائط الالكترونية جاءت بداية لغرض الجمع بين العديد من المعدات لتوظف قدراتها وتحقق الاتصال بينها عن طريق ربط مركزي محوري تعمل من خلاله، وهذا الرابط المحوري هو جهاز الحاسب الذي يقوم بوظائفه المعتادة[1]. إن تعامل الحاسب مع الأرقام حسابا ومع البيانات الرقمية والحرفية فرزا وتبويبا وتصنيفا يختلف عن تعامله مع صور المرئيات عرضا وتحريكا وتسجيلا، ومع الأصوات حفاظا وسماعا وغيرها فالاختلافات كثيرة، لكن أهم شيء في هذه الاختلافات هي:

- المقدرة على المعالجة وسرعتها.
- سعة الذاكرة التي تستخدم وتتعامل مع الصور والأصوات.
- قدرة البرامج على إدارة مهام الاتصالات بين الأجهزة والمعدات.
- مقدار التطور الذي يحدث كل يوم ومدى توافقية النظم القديمة مع الأحداث.

الفرع الثاني: خصائص الوسائط الإلكترونية

إن تقنية الوسائط المتعددة لا يشترط فيها أن تكون متفاعلة دائما لكي يطلق عليها اسم ملتميديا، حيث أن المستخدمين يستطيعون أن يجلسوا ويراقبوا الملتيميديا كما يفعلون مع التلفزيون أو في السينما، ولكن عندما يعطي للمستخدمين حرية السيطرة والإبحار والتجوال من خلال متطلباتهم وإرادتهم فإن الملتميديا تصبح متفاعلة.

والوسائط المتعددة كتقنية قد تغلغلت في حياتنا وأفادت كافة قطاعات المجتمعات، ومع تزايد التنافس أصبح من الضروري تقديم خدمات أفضل وتوفير معلومات حديثة بشكل متواصل[2].

وهذا ما توفره تقنية الوسائط المتعددة التي تتميز بعدة خصائص أهمها:

[1] **عبد الحميد بسيوني**، الوسائط المتعددة، الطبعة الأولى، دار النشر للجامعات، القاهرة، 2002، ص08.

[2] **المرجع نفسه**، ص12.

أولا- التفاعلية:

التفاعلية في تعريفها هي قيام المستخدمة بمشاركة نشطة في عملية الاستخدام في صورة استجابات نحو مصدر الاستخدام مما يؤدي إلى استمرار هذا الاستخدام، كذلك تعني الحوار بين طرفي الموقف الاتصالي المستخدم التي يجب أن تكون سهلة حتى تجذب انتباه المستخدم فيسير في المحتوى ويتلقى التغذية الراجعة ويبحر في العرض ليكتشف ويتوصل بنفسه للمعلومات التي يرغبها[1].

التفاعل موجود في كل نواحي الحياة فنحن نتفاعل مع كل الأشياء في حياتنا ونتفاعل مع أشكال عديدة من الوسائط (النصوص والصوت والمرئيات) في حياتنا اليومية، فقراءة جريدة وانتقاء مقالات معينة منها الإطلاع عليها هو تفاعل مع محتويات الصحيفة وعند اختيار برنامج أو مباراة من برامج التلفزيون وتسجيله لمشاهدته فيما بعد هو نوع من أنواع التفاعل كما أن تسجيل الأغاني والاستماع إليها في وقت لاحق هو نوع من أنواع التفاعل أيضا، لكن هذه الأنواع تكون قاصرة على أفعال معينة قد تزيد أو تنقص، ويعد الحاسب أكثر تفاعلية لما له من مميزات التخزين الضخم والعرض الاختياري والبحث في محتوياته الكبيرة من المعلومات[2].

ثانيا- التنوعية:

توفر الوسائل المتعددة بيئة استخدام وتعلم متنوعة يجد فيها كل مستخدم ما يناسبه ويتحقق ذلك إجرائيا عن طريق توفير مجموعة من بدائل وخيارات الاستخدام أمام المستخدم، وتتمثل هذه الخيارات في تقديم الأنشطة الترفيهية والثقافية والتعليمية وغيرها، كما تتمثل في تعدد مستويات المحتوى وتعدد أساليب الاستخدام[3].

[1] **لؤي الزغبي**، الوسائط المتعددة، د.ط، منشورات الجامعة الافتراضية السورية، 2020، ص113.

[2] **عبد الحميد بسيوني**، المرجع السابق، ص14.

[3] **لؤي الزغبي**، المرجع السابق، ص115.

كما تعمل الوسائط المتعددة الالكترونية على توفير مجموعة من العناصر التي تساعد على توضيح المعلومات والمعارف، فاقتراب محتوى الوسائط الالكترونية من بعض على الموقع الواحد سواء كان من مواقع صحافة الشبكات أو مواقع المعلومات أو مواقع التعليق و المشاركة في ذلك فإنها تتفق في تقديم خدمة واحدة من الأخبار والمعلومات والأفكار، وهذا هو السبب الأساسي لاستخدام أكثر من وسيلة لتأكيد المعنى والدلالة وتلبية حاجات المتلقين في التعرض لاهتماماتهم بخصائص المحتوى، ويعتمد استخدام الوسائط المتعددة على استخدام الملفات الجاهزة(صوت، صور، فيديو) لتدعيم المعني والعمليات المعرفية، وذلك من خلال دعم النصوص بالصوت أو الصور أما في مجال الإعلام فإن الاستخدام الحي للوسائل قبل اللقاءات الصوتية أو الصور الفيديو في مواقع الأحداث يكون الأساس هو في بناء مفهوم الوسائط الإلكترونية المتعددة[1].

ثالثا- التكاملية:

تعتمد قوة عروض الوسائل المتعددة على تكامل العناصر التي تشملها، فلا يمكن أن يدخل عنصر من عناصر الوسائل المتعددة في برنامج ما عشوائيا دون أن تكون له وظيفة معينة ودون أن يكون هذا العنصر مشاركا مع العناصر الأخرى في تحقيق الهدف النهائي من العرض، وتوصيل محتوى الرسالة المطلوبة إلى المتعلم، واختيار هذه العناصر يعتمد على خصائص المستخدمين و لاسيما المتعلمين ومحتوى المادة المعروضة، إلا أنها في النهاية لابد أن تكمل بعضها البعض وإلا سوف يؤثر ذلك على جودة العرض وبالتالي سوف يؤثر ذلك على درجة التفاعل بين المتعلم والعرض[2].

[1] **رحيمة الطيب عيساني**، الوسائط التقنية الحديثة وأثرها على الإعلام المرئي والمسموع، د.ط، الرياض، 2010، ص55.

[2] **لؤي الزغبي**، المرجع السابق، ص116.

رابعا– التزامنية:

الوسائل المتعددة عرض متكامل تتداخل فيه العناصر كلا حسب دوره في العرض في الوقت المناسب، ولذلك فعملية التزامن تعني تزامن الحركة في الرسوم والصور المتحركة لكي تتناسب مع سرعة العرض وأيضا تتوافق مع إمكانيات المستخدم وخاصة المتعلمين، كما أنه لابد وأن تتوافق سرعة الصورة مع الصوت الصادر والمصاحب لهذه الصورة[1].

ومعناها تتناسب توقيتات تداخل العناصر المختلفة والموجودة في البرنامج زمنيا مع سرعة العرض وقدرات المستخدم، بحيث يحدث توافق بين جميع عناصر الوسائط المتعددة كعنصر الصوت مع عنصر النص المكتوب والكلام المنطوق[2].

خامسا– الرقمنة الإلكترونية:

في عروض الوسائل المتعددة يتم أخذ الصوت أو الفيديو من مصدر خارجي مثل مسجل الصوت أو الميكروفون أو كاميرا الفيديو أو مشغل شرائط الفيديو إلى بطاقة الرقمنة في الكمبيوتر، حيث تقوم بعض البطاقات بوظيفة الرقمنة للفيديو والصوت معا وباستعمال عملية تسمى أخذ العينات يقوم محور الإشارات التناظرية في البطاقة بمعالجة إشارات الصوت والفيديو وتحويلها إلى سيل متدفق من البيانات الرقمية[3].

ونعني بالرقمنة إمكانية تحويل العناصر المكونة للوسائل المتعددة إلى الشكل الرقمي الذي يمكن تخزينه ومعالجته وتقديمه بالكمبيوتر، كما تعني الإلكترونية اعتماد الوسائط المتعددة في إنتاجها وتنفيذها على العديد من الأجهزة الإلكترونية، وكذلك أنظمة شبكات المعلومات بهدف توفير الجهد والوقت والتكلفة واستخدام أحدث الأجهزة[4].

---

[1] **لؤي الزغبي**، المرجع السابق، ص117.

[2] **رحيمة الطيب عيساني**، المرجع السابق، ص55.

[3] **لؤي الزغبي**، المرجع السابق، ص118.

[4] **رحيمة الطيب عيساني**، المرجع السابق، ص56.

سادسا– المرونة:

تعتبر المرونة من الخصائص المهمة التي تتوفر في عروض الوسائل المتعددة، وتعني المرونة التحكم في عناصر الوسائل المتعددة بحيث يمكن إجراء أي تعديلات على عروض الوسائل المتعددة سواء خلال عملية التصميم أو الإنتاج أو بعد عملية الانتهاء من إنتاج العرض، وذلك بالإضافة أو الحذف في نظام عرض بعض العناصر وذلك طبقا لما يتطلبه العرض والهدف منه وخصائص المستخدمين[1].

المطلب الثاني

وسائل ارتكاب جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية

ظهرت وسائل متعددة ومتنوعة أصبحت أداة إجرامية خطيرة يعتمد عليها المجرم المعلوماتي ولذلك سوف نذكر أهمها وهي الوسائل المادية **(الفرع الأول)**، إضافة إلى الوسائل التقنية **(الفرع الثاني)**.

الفرع الأول: الوسائل المادية

تتعدد الوسائل المادية الإلكترونية التي تستخدم كأداة في ارتكاب الجرائم ضد الأشخاص، نحاول ذكر أهمها والأكثر استعمالا لها في الوسط الإجرامي.

أولا–جهاز الحاسوب:

دراسة الجريمة المعلوماتية تقتضي التطرق إلى الجانب الفني والتقني لفهم طبيعة عمل هذه التقنية الحديثة ومعرفة مكوناتها المادية والمعنوية[2].

[1] **لؤي الزغبي**، المرجع السابق، ص118.

[2] **نهلا عبد القادر المومني**، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان-الأردن، 2008، ص20.

1)تعريف جهاز الحاسوب:

يعرف الحاسوب بأنه عبارة عن جهاز إلكتروني مصنوع من مكونات يتم ربطها وتوجيهها باستخدام أوامر خاصة لمعالجة إدارة المعلومات بطريقة ما، وذلك بتنفيذ ثلاث عمليات أساسية وهي:

استقبال البيانات المدخلة (الحصول على الحقائق المجردة)، ومعالجة البيانات إلى معلومات (إجراء الحسابات والمقارنات ومعالجة المدخلات)، وإظهار المعلومات المخرجة (الحصول على النتائج)[1].

ويعرف أيضا على أنه مجموعة من الأجهزة المتكاملة مع بعضها البعض بهدف تشغيل مجموعة من البيانات الداخلية وفقا لبرامج موضوعة مسبقا للحصول على النتائج المطلوبة[2].

ونظام الحاسوب يمكن تعريفه أنه مجموعة من الأجهزة المترابطة والتي تعمل معا من خلال مجموعة من الأوامر والبيانات لتحقيق حل لمسألة معينة، أو أنه مجموعة من أجهزة إلكترونية تقوم بصورة أوتوماتيكية لاستقبال البيانات وخزنها ومعالجتها واستخراج النتائج تحت سيطرة تعليمات مخزنة فيها[3].

2)مكونات جهاز الحاسوب:

يتكون نظام الحاسوب من قسمين رئيسيين هما:

أ. **المكونات المادية للحاسوب:** وتمثل هذه المكونات الهيكل المادي أو الجسم المادي لنظام الحاسوب، ويتكون هذا الهيكل من الوحدات الرئيسية التالية:

[1] **نهلا عبد القادر المومني**، المرجع السابق، ص20.

[2] **محمد أمين الرومي**، جرائم الكمبيوتر والانترنت، د.ط، دار المطبوعات الجامعية، الاسكندرية، 2004 ، ص13.

[3] **نهلا عبد القادر المومني**، المرجع السابق، ص20.

أ/1- وحدات الإدخال: وتستعمل هذه الوحدات لإدخال المعلومات أو المعطيات أو البرامج المراد معالجتها من الوسط الموجود عليه إلى ذاكرة الحاسوب[1]. وتشمل وحدات الإدخال و لوحة المفاتيح ، الفأرة وعصا اللعب، والقلم الضوئي والماسح الضوئي والكاميرا[2].

وبالتالي يمكن تقسيمها إلى نوعين؛ وسائل تسمح بالاتصال المباشر بين الإنسان وبين وحدة المعالجة المركزية مثل لوحة المفاتيح، ووسائل تسمح بإدخال المعلومات بصورة غير مباشرة ويتم بهذه الوسائل تهيئة المعلومات المراد إدخالها على وسائط معينة ومحددة بمعزل عن الحاسوب أو الأمر، ثم تتم عملية الإدخال من خلال عملية وحدة المعالجة المركزية وتشمل وحدات الإدخال مثلا الفأرة ومشغلات الأقراص والماسح[3].

أ/2- وحدة المعالجة المركزية: تعتبر بمثابة العقل المدبر والمسيطر والمتحكم بكافة مهام الحاسب الآلي ويندرج ضمن هذه الوحدات إضافية أولى مساعدة ومتخصصة، وهي وحدات التحكم، وحدات الحاسب والمنطق، وحدات التخزين (التخزين الداخلي والتخزين الخارجي) إضافة إلى ذلك وحدة الذاكرة[4]، وتتكون هذه الوحدة من وحدتين رئيسيتين هي: وحدة التحكم والسيطرة، و وحدة الحساب والمنطق.

أ/3- وحدة الذاكرة: وهي الوحدة التي تتم فيها عمليات تخزين المعلومات الواردة للجهاز أو تخزين النتائج الآتية من وحدة المعالجة المركزية[5].

أ/4-وحدة الإخراج: هي عبارة عن مجموعة من الأدوات التي تعمل على إدخال البيانات إلى الحاسب الآلي وتختلف باختلاف نوع من الأداة التي تستخدم في الحصول على نوع معين من

---

[1] **نهلا عبد القادر المومني**، المرجع السابق، ص25.

[2] **محمد أمين الرومي**، المرجع السابق، ص15.

[3] **نهلا عبد القادر المومني**، المرجع السابق، ص25.

[4] **أسامة أحمد المناعسة، جلال محمد الزغبي**، جرائم تقنية نظم المعلومات الالكترونية-دراسة مقارنة، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، 2014، ص29.

[5] **نهلا عبد القادر المومني**، المرجع السابق، ص26.

المعلومات ومنها؛ لوحة المفاتيح والماسحة الضوئية والمايك بالإضافة إلى الشاشة والطابعة وسماعات الإخراج الصوتي[1].

أ/5-وحدة التخزين: وهي المسؤولة عن حفظ وتخزين المعلومات والبيانات والأوامر داخل الحاسب الآلي ضمن أماكن وحيز معين مفترض وذلك على صورتين (حفظ دائم وحفظ مؤقت)، أو التخزين الخارجي وفيه تستخدم أدوات منفصلة عن جهاز الحاسب الآلي ذاته، ومن أمثلتها؛ الأقراص المرنة والاسطوانات.

ب. المكونات المنطقية للحاسوب:

وتتمثل هذه المكونات المنطقية بالتطبيقات العملية التي تجري داخل الكيان المادي للحاسب، والمكونات المنطقية تشمل بالإضافة المعلومات والبيانات والبرمجيات وهذه الأخيرة هي بمثابة العمود الفقري وعصب عمل الحاسب الآلي حيث لا يمكن للفرد أن يقوم بأي عملية أيا كان نوعها على الجهاز بدونها ويمكن من خلالها الاستفادة من تشغيل الحاسب بشكل كبير عن طريق الإمكانيات والسرية التي يقدمها في انجاز المهام التي تتطلب منه، وتنقسم البرمجيات إلى أنظمة التشغيل والتطبيقات[2].

ثانيا: الهاتف الذكي.

لدراسة الجريمة المعلوماتية يقتضي التطرق إلى الجانب الفني والتقني لجهاز الهاتف الذكي، ولفهم طبيعة عمل هذه التقنية ومعرفة خدماتها يتطلب منا توضيح هذه التقنية من خلال التطرق إلى تعريف هذا الجهاز ومعرفة خدماته وأنظمته.

[1] **محمد أمين الرومي**، المرجع السابق، ص15.

[2] **فؤاد حسين العزيزي**، الجرائم المعلوماتية-دراسة مقارنة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2014، ص40.

1) تعريف الهاتف الذكي:

الهاتف الذكي النقال هو جهاز الهاتف الخلوي الذي يوفر استخدامات أساسية مثل القدرة على إجراء مكالمات واستقبال وإرسال رسائل بالإضافة إلى ذلك لديه القدرة على الاتصال بشبكة الانترنت وتلقي وإرسال البريد الالكتروني، وهو يعمل بشكل عام على نظام تشغيل خاص به والذي يسمح بإضافة تطبيقات محددة، وله القدرة أيضا على الاتصال مع جهاز الحاسوب مما يتيح نقل المعلومات والوثائق المهمة وحفظها على الحاسوب أو العكس[1].

2) خدمات الهاتف الذكي:

يقدم الهاتف الذكي العديد من الخدمات من أهمها[2]:

- الرسائل القصيرة، رسائل الوسائط المتعددة.
- تطبيقات التصوير وخدمات نقل البيانات.
- البلوتوث، تطبيقات الويب وتطبيقات التسلية.

3) أنظمة الهواتف الذكية:

تتنوع الأنظمة التي تقوم بتشغيل الهواتف الذكية منها[3]:

- هواتف تعمل بنظام الأندرويد .
- هواتف تعمل بنظام الويندوز موبايل.
- هواتف تعمل بنظام سمبيان.

[1] **محمد بركات الحجار**، أثر الإعلان التجاري على السلوك الشرائي لمستخدمين خدمات الهواتف الذكية المحمولة في مدينة عمان، مذكرة مقدمة لنيل درجة الماجستير، كلية الأعمال، جامعة الشرق الأوسط، 2011، ص29.

[2] **مريم ماضوي**، تأثيرات الهاتف النقال على أنماط الاتصال الاجتماعي لدى الطالب الجامعي، مذكرة لنيل شهادة الماجستير، كلية العلوم الإنسانية والاجتماعية والعلوم الإسلامية، جامعة الحاج لخضر، باتنة، 2012-2013، ص105.

[3] **محمد بركات الحجار**، المرجع السابق، ص29-30.

4) مكونات الهاتف الذكي:

جهاز الهاتف المحمول هو أحد الأجهزة الذكية التي تدار بواسطة أحد البرامج المعلوماتية، وبدون هذا البرنامج (الكيان المنطقي للنظام المعلوماتي للهاتف) تصير المكونات المادية لهذا الجهاز والعدم سواء، فالتشابه واضح بين النظام المعلوماتي لجهاز الهاتف الذكي ونظام الحاسوب، وقد ظهرت بعض الأجهزة التي يصعب حاليا على وجه الدقة تصنيفها في إحدى الطائفتين، وهو ما سنوضحه على النحو التالي[1]:

أ. الأجزاء المادية (الكيان المادي) للهاتف الذكي:

يتشابه التكوين المادي لمختلف الهواتف المحمولة أيا كان الجيل أو الطراز الذي تنتمي إليه، إذ تنقسم هذه الأجزاء إلى قسمين:

- **الأجزاء الخارجية:** والتي يمكن رؤيتها ومعاينتها بمجرد النظر للجهاز، ويرتبط مظهرها بطراز الهاتف والجيل الذي ينتمي إليه ونوعية المستهلك للجهاز، وأبرز هذه الأجزاء؛ الغطاء الخارجي للهاتف وشاشة العرض الخاصة بالجهاز[2].
- **الأجزاء الداخلية:** أبرزها لوحة المعالجة الرئيسية جزء من الفايبر المضغوط الذي يحتوي على جميع المقاومات والمكثفات وغيرها من الدوائر اللازمة لعمل نظام الهاتف كدائرة الصوت، ودائرة الذاكرة ويأتي بعدها في المرتبة لوحة المفاتيح الداخلية للهاتف والسماعة، ويضاف إلى الهواتف الذكية مكان خاص ببطاقة الذاكرة الإضافية وكاميرا التصوير الفوتوغرافي والفيديو.

ب. الأجزاء الغير مادية:

المعلومات المعالجة آليا سواء تمثلت في برامج تشغيل الهاتف أو برامج التطبيقات التي تخدم مستخدمه وتفعل خدماته كبرامج الصوت والألعاب ،سواء أعدت خصيصا من أجلهم كانت إحدى برامج تطبيقات الحاسوب القابلة للتشغيل بواسطة الهواتف الذكية، وتعد جزء من

[1] **طارق عفيفي، صادق أحمد**، الجرائم الإلكترونية-جرائم الهاتف المحمول، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2015، ص15.

[2] **المرجع نفسه**، ص16.

مكونات الهاتف الذكي وهي مظهر من مظاهر الانتفاع لهذا الجهاز ومن ذلك رسائل البريد الإلكتروني أو البريد النصي التي ترد أو ترسل من الهاتف الذكي والصور الذكية والصور الرقمية ومقاطع الفيديو المخزنة على ذاكرة الهاتف، وبوجه عام هي كل ما يمكن استخدامه أو تسجيله أو بثه أو تخزينه بصيغة رقمية على الوسيط المادي، وبالتالي فإن قيمة هذه المعلومات تختلف بحسب نوعها وأهميتها لدى المستخدم[1].

الفرع الثاني: الوسائل التقنية

تتعدد الوسائل الإلكترونية التي تستخدم كأداة في ارتكاب الجرائم ضد الأشخاص، ومن أهم هذه الوسائل التقنية "شبكة الانترنت".

أولا- الانترنت:

كان لظهور الانترنت أثر كبير في انتقال المعلومات وتداولها والاستفادة منها في وقت قياسي في أي مكان في العالم، فالانترنت ساهم بشكل لا نظير له في صناعة المعلومات وثورتها فهو أحد العناصر الرئيسية التي ترتكز عليها تكنولوجيا المعلومات[2].

وللوقوف على الجانب التقني لشبكة الانترنت، سوف نتناول ماهية الانترنت، وطرق استخدام الشبكة في ارتكاب جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية.

1) تعريف الانترنت:

هي الترابط بين الشبكات لكونها تضم عددا كبيرا من الشبكات المترابطة في جميع أنحاء العالم ومن ثم يمكن أن يطلق عليها الشبكات المعلوماتية، ولقد اختلفت التسميات التي أطلقت على الانترنت مابين الشبكة العالمية أو الشبكة العنكبوتية أو الطريق السريع الرقمي[1].

[1] **طارق عفيفي، صلدق أحمد**، المرجع السابق، ص17.

[2] **نهلا عبد القادر المومني**، المرجع السابق، ص34.

كما تعرف الانترنت أنها توصيلات تعاونية لعدد من شبكات الحاسبات الآلية، وهي مكونة من كلمتين هما Internet connexion أو Net work، وهذا يعني أن مئات الشبكات المربوطة مع بضها البعض بطريقة بسيطة وسهلة بحيث تبدو وكأنها قطعة واحدة أو نظام واحد دون إحساس أي من الأطراف أنه يختلف فنيا عن الآخر[2].

2) **مخاطر الانترنت:**

رغم النجاح الذي تحققه الانترنت ورغم الخدمات المتعددة فهذا لا يعني أنها لا تخلو من السلبيات قد تكون خطيرة التأثير على مستعمليها، ونوجز أهم هذه المخاطر فيما يلي[3]:

-استغلال الانترنت في نشر الرذيلة والفساد الأخلاقي بين الصغار والشباب والمراهقين.

- اعتزال الشباب المشترك في الانترنت عن المجتمع، وهذه الظاهرة متواجدة بكثرة في الدول الأوروبية، حيث أقيمت دراسات على 93 عائلة أجراها فريق الباحث "روبرت كروث" وهو مختص في علم النفس الاجتماعي، وأثبتت هذه الدراسات أن الانترنت تؤثر على الحياة الاجتماعية للفرد وعلى راحته النفسية.

- السرقة الإلكترونية أو ما يعرف بالقرصنة الإلكترونية وتتمثل في سرقة المعلومات وكذلك زرع الفيروسات مما يسبب خلل في النظام أو الشبكة، كما حدث هذا حديثا بفيروس «I Love you».

-كثرة السرقات وإمكانية تزييف الوقائع أو تغيير الأحداث.

- كما يمكن أن تكون محل تهديد لأمن بعض الأفراد أو الدولة[1].

---

[1] **رصاع فتيحة**، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2011-2012، ص07.

[2] **عبد الفتاح بيومي حجازي**، الإثبات الجنائي في جرائم الانترنت، د.ط، دار الكتب القانونية، مصر، 2007، ص27.

[3] **طيبي محمد**، ثقافة الانترنت – دراسة ميدانية لاستعمالات الشبكة بمدينة تيهرت، رسالة ماجستير مقدمة لقسم علم المكتبات والعلوم الوثائقية، كلية العلوم الإنسانية والحضارة الإسلامية، جامعة وهران، 2009-2010، ص72.

ثانيا- استخدامات الانترنت:

تقدم شبكة الانترنت خدمات جليلة لكل المستخدمين[2]، يمكن إجمالها فيما يلي:

- البريد الإلكتروني مع كل أنحاء العالم، والحصول على الرسائل العلمية والكتب والمعلومات الخاصة بالعلوم وملخصاتها والتي قد لا تتوافر في المكتبات العامة.
- قراءة الصحف اليومية والمجلات الأسبوعية، ونشر ثقافات الشعوب والدول.
- نقل التكنولوجيا من دولة إلى أخرى.

ونعرض بصورة موجزة بعض الخدمات الشائعة لشبكة الانترنت على النحو التالي:

1-البريد الإلكتروني:

البريد الإلكتروني عبارة عن رسالة عادية لكن بطريقة إلكترونية، يكتبها شخص بطريقة عادية جدا على جهاز الحاسب الآلي الخاص به، وذلك أن يفتح الصفحة الخاصة ببريده الإلكتروني والتي لها رقم سري، واسم المستخدم، ولا يمكن لغيره الدخول إليه. وبعد أن يتم الكتابة يقوم بالضغط على أمر معين في الصفحة وهو "send" أي أرسل وفي حالة نجاح وصول الرسالة للعنوان المطلوب على جهاز حاسب آلي أخر له علامة (Ok) بما يفيد تمام وإرسال الرسالة، وإذا كان هناك خطأ ما في إرسالها يظهر للمرسل رسالة موجزة تشير إلى موضوع الخطأ ويتولى هو تصحيحه ثم يعيد إرسالها مرة أخرى[3].

2- شبكة العنكبوت العملاقة:

المعروفة ب (w.w.w) التي تتيح للمستخدم تصفح مواقع (sites) المعلومات، وهذه الخدمة تجمع النصوص والصور والأصوات والأفلام المتحركة، مما يتيح للمستخدم الحصول على المعلومات التي يريدها في أسرع وقت[4].

---

[1] **طيبي محمد**، المرجع السابق، ص72.

[2] **عبد الفتاح بيومي حجازي**، المرجع السابق، ص 31.

[3] **المرجع نفسه**، ص31.

[4] **نهلا عبد القادر المومني**، المرجع السابق، ص40.

3-محركات البحث:

هي عبارة عن برامج تساعد في الحصول على المعلومات فكما هو معروف هناك كم هائل من المعلومات في شبكة الانترنت، يرغب المستخدم في معرفة المواقع التي تمكنه من الوصول إلى مبتغاه، فيتم في هذه الحالة إخبار خدمة البحث باسم الموضوع الذي يهم المستخدم ومن ثم يتم تزويده لقائمة المواقع التي تتطابق مع المعلومات التي يرغب في الحصول عليها وهناك عدة محركات بحث كل منها يستخدم طريقة معينة أو خاصة في إجراء عملية البحث.

4-التخاطب عبر الانترنت:

يقوم المستخدم في عملية التخاطب بكتابة رسالة يجري عرضها مباشرة أمام شخص أخر في أي مكان في العالم الذي يقوم بدوره بالرد مباشرة على هذه الرسالة[1].

5-المجموعات الإخبارية:

مجموعات الأخبار عبارة عن أماكن وساحات افتراضية للتحادث بين مستخدمي شبكة الانترنت من ذوي الاهتمامات المشتركة الذين يؤلفون فيما بينهم مجموعات نقاش وتبادل للبيانات والمعلومات والأفكار حول موضوع معين[2].

6-التجارة الإلكترونية:

يعكس مدلول التجارة الإلكترونية استخدام التقنيات الحديثة في المعلومات والاتصالات من أجل إبرام الصفقات وعقد المبادلات التجارية[3]،وقد أتاحت شبكة الانترنت لطرفي العقد التقابل وجها لوجه بالصوت والصورة رغم تباعدهما آلاف الأميال والاتفاق على التفصيلات

[1] **نهلا عبد القادر المومني**، المرجع السابق، ص40.

[2] **المرجع نفسه**، ص41.

[3] **الزيدي وليد**، القرصنة على الانترنت والحاسوب، الطبعة الأولى، دار أسامة للنشر ، عما ن ، ص59 .

الدقيقة بعد إبداء الإيجاب، ثم القبول بطريق الانترنت، ثم إبرام العقد والتوقيع عليه بطريق التوقيع الإلكتروني دون الحاجة لاجتماع المتعاقدين في مكان واحد.

7-كشف الجرائم وتعقب المجرمين والقبض عليهم:

في مبادرة جريئة للشرطة البريطانية أنشأت وحدة بوليسية تسمى الوحدة الوطنية لمكافحة جرائم التكنولوجيا المتطورة، وهذه الوحدة هدفها تعقب مرتكب جرائم الانترنت وقد اعترض عليها من قبل جماعات الدفاع عن الحقوق المدنية، لكن يبقى أثرها كتطبيق هام لاستخدامات الانترنت الايجابية وتأتي هذه المبادرة وغيرها في ظل نقاش بين المختصين موضوعه مدى جدوى الأساليب العلمية والإلكترونية الجديدة منها الانترنت في رفع الكفاءة اللازمة لمواجهة الجريمة[1].

8-بروتوكول نقل الملفات:

تمكن هذه الخدمة المستخدمة من نسخ الملفات من جهاز الحاسوب إلى جهاز آخر وعليه يستطيع الباحثون الحصول على أحدث الأبحاث العلمية من الجامعات ومراكز البحوث بسرعة كبيرة[2].

[1] **عبد الفتاح بيومي الحجازي**، المرجع السابق، ص32.

[2] **نهلا عبد القادر المومني**، المرجع السابق، ص42 .

المبحث الثاني

صور جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية

إن الجرائم المرتكبة ضد الأشخاص عبر الوسائط الإلكترونية ظهرت بظهور وسائل الاتصال والإعلام فهي جرائم مستحدثة بعدما كانت في الأصل جرائم تقليدية، فأصبح بإمكان المجرم المعلوماتي ارتكاب مثل هذه الجرائم التقليدية بواسطة هذه الوسائل فكل معلومة تتنقل عبر الوسائط الإلكترونية يمكن أن تكون محل الجريمة، وتجدر الإشارة إلى أنه ليست الوسائط الإلكترونية محل التجريم وإنما استعمالها بطريقة من شأنها المساس بالأشخاص في اعتبارهم أو أبدانهم أو حياتهم وسمعتهم وشرفهم.

فجرائم الاعتداء على الأشخاص جرائم تهدد بالخطر الحقوق اللصيقة بالإنسان فمنها ما يمثل اعتداء على حياة الإنسان ومنها ما يصيب الحق في شرف واعتبار الشخص، لذلك قد تطورت هذه الجرائم أكثر بعد ظهور شبكة الانترنت التي أصبحت سلاح ذو حدين رغم التسهيلات التي قدمتها المجتمعات خاصة ما تغلق بحياتهم اليومية. إلا أنها أصبحت سلاح يستعمله المجرمون، فجميع المعلومات التي تتعلق بالأفراد متداولة ومباحة وهذا ما يسهل عملية انتهاك حقوق الأفراد من قبل المجرمين.

ولتوضيح هذه الجرائم المرتكبة ضد الأشخاص عبر الوسائط الإلكترونية تناولنا صورتين من بين الجرائم الأكثر شيوعا؛ جريمتي القذف والسب عبر الوسائط الإلكترونية **(المطلب الأول)**، إضافة إلى جريمة الاستغلال الجنسي للأطفال عبر الوسائط الالكترونية **(المطلب الثاني)**.

المطلب الأول

جريمتي القذف والسب عبر الوسائط الإلكترونية

لقد كان القذف والسب لفظ سائد بصورته التقليدية إلى حاضرنا اليوم على الرغم من الترسانة القانونية سواء الوطنية أو الدولية التي سعت لمحاربتها، إلا أن التطور الذي شهدته الموجة الثالثة الثورة التكنولوجية وبالتالي ومع سرعة ظهور المعلوماتية واستخدامها وتطور جريمتي القذف والسب مواكبة التطور المعلوماتي عبر شبكة الانترنت، التي جعلت من هذا العالم قرية صغيرة أدى إلى مشاكل قانونية وأخلاقية دعت الفقه والقضاء إلى مجابهتها والبحث في ما إذا كانت القوانين كافية لمواجهتها عبر نصوص جنائية كفيلة للحد من تلك الاستخدامات السيئة لها[1]، وتعد جرائم القذف والسب الأكثر شيوعا في نطاق الشبكة، حيث يستعمل الجاني حسب القواعد العامة لجرائم القذف والسب عبارات بذيئة تمس وتخدش شرف المجني عليه[2]، وبالتطور أصبحت الانترنت إحدى هذه الوسائل إن لم نقل أكثرها رواجا فعادة ما تكون عبر البريد الالكتروني أو بالعديد من الوسائل .

وللتوضيح أكثر لجريمة القذف عبر الوسائط الإلكترونية لابد من التطرق إلى تعريف جريمتي القذف والسب عبر الوسائط الإلكترونية **(الفرع الأول)**، إضافة إلى تبيان أركان هذه الجريمة **(الفرع الثاني)**، إلى جانب توضيح أساليب ارتكاب جريمتي القذف والسب عبر الوسائط الإلكترونية والجزاءات المقررة لها **(الفرع الثالث)**.

[1] **محمد الألفي**، جرائم النشر الإلكتروني، دون طبعة، مركز تطويق الإدارة والتنمية، مصر، 2008، ص07.

[2] **شلاخ لطيفة، قريشي الحاج العربي إبراهيم**، انتشار الجريمة الإلكترونية الماسة بالأشخاص في البيئة الجزائيةٌ دراسة ميدانية لبعض مستخدمي مقاهي النت في مدينة مسيلة، مذكرة لنيل شهادة ماستر في علوم الإعلام والاتصال، كلية العلوم الإنسانية والاجتماعية، قسم العلوم والاتصال، جامعة محمد بوضياف- المسيلة، 2017، ص18.

الفرع الأول: تعريف جريمتي القذف والسب عبر الوسائط الإلكترونية

للتطرق إلى تعريف جريمتي القذف والسب عبر الوسائط الإلكترونية لا بد من تعريفها كل على حدى، لذلك سوف نتناول تعريف جريمتي القذف عبر الوسائط الإلكترونية **(أولا)**، ومن ثم تعريف جريمة السب عبر الوسائط الإلكترونية**(ثانيا)**.

أولا: تعريف جريمة القذف عبر الوسائط الإلكترونية

إن أقصى ما تهدف إليه التشريعات هو حماية الفرد وأمواله من اعتداءات الآخرين، غير أن ظهور الأديان أدى إلى بداية ظهور حماية الفرد من جميع الاعتداءات التي قد يتعرض لها بما فيها المساس بشرفه واعتباره[1].

وتعريف جريمة القذف له عدة أوجه :

1. **التعريف اللغوي:** هو الرمي، ويقال قذف بالشيء قذف، يقذف، قذفا، أي رمى وقذف الرجل، أي قال وقذف المحصنة أي رماها، ويقال قذف الشخص أي رماه والقذف بالقول هو التكلم من غير تدبر[2].
2. **التعريف القانوني:** طبقا لنص المادة 296 من قانون العقوبات فإنه << يعد قذفا كل ادعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيئة المدعى عليها به أو إسنادها إليهم أو إلى تلك الهيئة، ويعاقب على نشر هذا الادعاء أو ذلك الإسناد مباشرة أو بطرق إعادة النشر حتى وإن تم ذلك على وجه التشكيك أو إذا قصد به الشخص أو هيئة دون

[1] **منير محمد الجنبهي، ممدوح الجنبهي**، التبادل الالكتروني المعلوماتي، دار الفكر الجامعي، مصر، 2004، ص10.

[2] **هروال هبة نبيلة**، جرائم الانترنت دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد- تلمسان، 2013-2014، ص75.

ذكر الاسم لكن كان من الممكن تحديدها من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الاعلانات موضوع الجريمة>>[1].

وعليه القذف في لغة القانون هو جريمة قوامها فعل الإسناد أو الادعاء ينصب على واقعة محددة من شأنها المساس بشرف واعتبار المجني عليه.

3. **تعريف جريمة القذف بالوسائل الإلكترونية:** إن جريمة القذف بالوسائل الإلكترونية تختلف في الغالب عن جريمة القذف التقليدية استنادا للقواعد العامة وذلك لاختلاف وسيلة ارتكابها بحيث أن الاولى ترتكب بوسيلة الكترونية [2].

يمكن تعريف جريمة القذف المعلوماتي بأنها: إسناد واقعة معينة إلى الغير بإحدى وسائل المعلوماتية من شأنها لو كانت صادقة لأوجبت عقاب من أسندت إليه أو احتقاره عند أهل وطنه[3].

وعلى ذلك فإن جريمة القذف عن طريق الانترنت هي جريمة يلازم وصفها طبيعة فعل النشر وهي تبدأ وتنتهي بارتكاب هذا الفعل، فهي جريمة وقتية[4].

ثانيا: تعريف جريمة السب عبر الوسائط الالكترونية

له عدة أوجه منها:

1. **التعريف اللغوي:** هو الشتم سواء كان بإطلاق اللفظ الدال عليه أو المعارض التي تدل عليه.

---

[1] راجع **المادة 296** من الأمر رقم 66-156 المؤرخ في 08 جوان 1966 يتضمن قانون العقوبات، ج.ر، عدد 71، الصادر بتاريخ 11 جوان 1966، المعدل والمتمم.

[2] **هناء إسحاق، عبد الرحيم الشيباني**، المسؤولية الجزائية عن جريمتي السب والقذف بالوسائل الالكترونية، أطروحة ماجستير، جامعة الإمارات العربية المتحدة، كلية القانون العام، 2018، ص 08.

[3] **عمار عباس الحسيني**، جرائم الحاسوب والانترنت الجرائم المعلوماتية، الطبعة الأولى، كلية القانون، زين الحقوقية و الأدبية، بيروت- لبنان، 2017، ص380.

[4] **مصطفى محمد موسى**، التحقيق الجنائي في الجرائم الالكترونية، الطبعة الاولى، مطابع الشرطة، مصر، 2008، ص430.

2. التعريف الاصطلاحي: هو خدش شرف شخص واعتباره عمدا دون أن يتضمن ذلك إسناد واقعة معينة إليه.

3. التعريف القانوني: عرفها المشرع الجزائري طبقا لنص المادة 297 من قانون العقوبات الجزائري: << يعد سبا كل تعبير مشين أو عبارة تتضمن تحقيرا أو قدحا لا ينطوي على إسناد أية واقعة >>[1].

ويتبين لنا من خلال ما جاء في المادة أعلاه أن السب يقوم أساسا على التعبير بغض النظر عما إذا كان السب قد شفويا أو كتابيا تضمن تحقيرا أو قدحا وقع بالطرق التقليدية أو بالوسائل التقنية الحديثة، فالمادة التي تشير إلى ذلك السب هو الإسناد العمدي لواقعة غير معينة إلى المجني عليه خادشة لشرفه واعتباره[2].

4. تعريف السب باستعمال الوسائل الحديثة: كل من سب غيره علنا بأن وجه له ألفاظا تمس شرفه أو كرامته عبر أي وسيلة إلكترونية .

الفرع الثاني: أركان جريمتي القذف والسب عبر الوسائط الإلكترونية

إن للجريمة بصفة عامة أركان لا بد من توافرها وجريمة القذف والسب لا يتصور قيامها إلا بتوافر هذه الأركان، لهذا سنتناول أركان كل من جريمة القذف والسب كل على حدى.

أولا- أركان جريمة القذف عبر الوسائط الإلكترونية:

إن جرائم القذف بشكل عام تقوم على الحط من مكانة الفرد الاجتماعية والإساءة المباشرة أو غير المباشرة له، وتتكون أركان جريمة القذف في القانون من الركن المادي و ركن العلانية والركن المعنوي.

[1] راجع **المادة 297** من الأمر رقم 66-156، المرجع السابق.

[2] **تومي يحي**، جرائم الاعتداء ضد الأفراد باستخدام تكنولوجيات الإعلام والاتصال، أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر1، 2017-2018، ص89.

1. **الركن المادي:** هو النشاط الإجرامي أو السلوك الآثم الذي يتمثل بفعل الإسناد والنتيجة الإجرامية بتحقيق الجاني فعلته بالحط من المكانة الأدبية أو الاجتماعية أو الوظيفية للغير، والعلاقة السببية هي الرابط بين السلوك الذي يمثل دور السبب والنتيجة التي تمثل دور الأثر المترتب على هذا السبب[1].

يقوم هذا الركن على ثلاث عناصر وهي النشاط الإجرامي الذي هو فعل الإسناد وموضوع الإسناد الذي من شأنها عقاب من تسند إليه الواقعة أو احتقاره، وعلانية هذا الإسناد.

أ. **فعل الإسناد:** لا ريب أن فعل الإسناد وموضوعه يشكلان جوهر السلوك الإجرامي للركن المادي في تلك الجريمة، كما أن القذف يعد فعل ذو طبيعة مزدوجة يتكون من فعلين متلازمين[2]. فجريمة القذف تتكون من فعل الإسناد والذي يقصد به قيام القاذف بنسبة واقعة معينة إلى المجني عليه والمقذوف سواء كان ذلك على سبيل التأكيد أو الاحتمال أو الشك من شأنها المساس بشرف واعتبار المجني عليه والتي بدورها لو صحت أن توجب عقابا جنائيا. كما ينصب فعل القذف على الواقعة المسندة إلى الشخص المعتدى عليه أو المدعى عليها، حيث نصت عليه المادة 296 من قانون العقوبات الجزائري على الإسناد وهو يفيد نسبة الأمر إلى الشخص المقذوف على سبيل التأكيد سواء كانت الوقائع مدعى بها صحيحة أو كاذبة مثلا فلان هو الذي سرق مال المؤسسة وأن هذا التعبير يفيد التأكيد والجزم.

ب. **الادعاء:** يحمل معنى الرواية عن الغير أو ذكر الخبر محتمل الصدق أو الكذب ويكون الادعاء بأية وسيلة من وسائل التعبير سواء بالقول أو الكتابة أو الإشارة ويتحقق سواء على سبيل القطع أو الشك، المهم أن يكون من شأنه أن يلقى في أذهان العامة عقيدة ولو وقتية

[1] **تميم بن عبد الله سيف التميمي**، الجرائم المعلوماتية في الاعتداء على الأشخاص (قذف- سب- تشهير) وفقا للشريعة الإسلامية والنظام السعودي والقانون القطري، الطبعة الاولى، مكتبة القانون والاقتصاد، الرياض، 2016، ص84-85.

[2] **تومي يحي**، المرجع السابق، ص41.

في صحة الإسناد أو الادعاء ويستوفي في القذف أن يسند القاذف الأمر إلى المقذوف على أنه عالم به أو يسنده إليه بطريق الرواية عن الغير أو يردده على أنه مجرد إشاعة[1].

ج. تعيين الواقعة: يشترط أن ينصب هنا الادعاء أو الإسناد واقعة محددة ومعينة كما أن يسند إلى موظف سرقته للمال الذي عاهد إليه فهنا الواقعة هي السرقة، أما إذا جاء الادعاء أو الإسناد حاليا من الواقعة فإنه يعد تجريما آخر. ويقصد بالواقعة أي أمر يتصور حدوثه سواء قد حدث فعليا أو كان محتملا الحدوث فالجريمة تكون مستحيلة التحقق إذا كانت الواقعة بدورها مستحيلة الوقوع[2].

إن الادعاء والإسناد يجب أن ينصب على واقعة محددة غير أنه لا يستلزم أن يكون هذا التحديد مطلقا وشاملا بل يكفي التحديد النسبي إن كان يدل على الظروف التي تم فيها عن قصد الجاني وسلطة التقدير ترجع إلى قاضي الموضوع، مثلا ذلك أن ينعت شخص آخر بأنه (ابن زنا) فإذا كان مسند هذه العبارة بقصد التشهير به على أنه ولد غير شرعي فهي جريمة قذف[3].

د. الواقعة من شأنها المساس بالشرف والاعتبار: الفعل الماس بالاعتبار وهو ذلك الفعل الذي له أثر مباشر على قيمة الإنسان سواء عند نفسه أو عند الغير وذلك بأن يحط من كرامته أو شخصيته، ومسألة الشرف والاعتبار يرجع تقديرها إلى قاضي الموضوع تبعا للظروف المحيطة بالواقعة المسندة مع وجوب الاسترسال بالدلالة العرفية للمتهم، هذا ما استقرت إليه المحكمة العليا[4].

---

[1] **محمد صبحي نجم**، شرح قانون العقوبات الجزائري، القسم الخاص، الطبعة الثانية، ديوان المطبوعات الجامعية، الجزائر، 1990، ص99.

[2] **عبد الحميد الشواربي**، جريمة القذف والسب في ضوء القضاء والفقه، د.ط، دار المطبوعات الجامعية، الاسكندرية مصر، 1985، ص82.

[3] **محمد صبحي نجم**، المرجع السابق، ص100.

[4] **عدلي خليل**، القذف والسب وتحريك الدعوى الجنائية عنهما، د.ط، دار الكتب القانونية، القاهرة، 1996، ص23.

و. تعيين الشخص أو الهيئة المقذوفة: طبقا لنص **المادة 296** من قانون العقوبات الجزائري فإن المقذوف أو المجني عليه إما أن يكون شخصا طبيعيا أو معنويا أو هيئة،ويجب أن يكون معينا وليس من الضروري أن يكون معينا بالاسم وإنما يكفي أن تكون العبارات موجهة على صورة يمكن معها فهم المقصود منها ومعرفة الشخص الذي يعينه القاذف وهي مسألة تفصل فيها محكمة الموضوع [1].

2. ركن العلانية:

طبقا لنص المادة 296 من قانون العقوبات السالفة الذكر فإن المشرع الجزائري لم يحدد في هذه الأخيرة بدقة ووضوح طرق العلانية حيث أشارت هذه المادة ذكر النشر وإعادة النشر دون بيان سندات النشر.

أ. تعريف العلانية:

العلانية قانونا كل ما يقع تحت نظر الكافة (الجمهور) أو يصل إلى سمعهم أو يقف عليه بمشيئتهم دون عائق يعتبر علانية فهي وسيلة علم أفراد المجتمع بعبارات القذف حيث لا يقوم القذف إلا إذا كان الإسناد علنيا ، والعلانية تقوم على عنصرين :

أ/1. العنصر المادي: هو السلوك المنتج لحدث نفسي من شأنه إيصال الفكرة أو الشعور أو الإرادة الآثمة للجمهور.

أ/2. العنصر المعنوي: وهو تعمد إيصال الفكرة أو الشعور أو الإرادة إلى الغير[2].

وبالتالي تعتبر العلانية ركنا مميزا لجنحة القذف فإذا غاب هذا الركن أصبحت الجريمة مجرد مخالفة يعاقب عليها القانون طبقا لنص المادة 363 من قانون العقوبات الجزائري تحت عنوان "السب الغير العلني".

[1] **أحسن بوسقيعة**، قانون العقوبات في ضوء الممارسات القضائية ، د.ط، منشورات بيرتي، الجزائر، 2007، ص 190.

[2] **المرجع نفسه**، ص 199.

ب. مدى تحقق ركن العلانية في جريمة القذف عبر الوسائط الإلكترونية :

نظرا لما يأخذه المجرمون مع هذا التطور والتقدم الذي آلت إليه التكنولوجيا بخدمة أنشطتهم الإجرامية في الاعتداء على الأشخاص، فجريمة القذف إذا ما وقعت باستخدام الوسائط الالكترونية تكون قد تمت في علانية و ذلك على نحو يؤدي إلى تكامل أركان الجريمة. حيث إذا تم كتابة عبارات القذف بواسطة الحاسوب الالكتروني أو الهاتف النقال ومن ثم عبر الانترنت من خلال خدماته المتاحة كمواقع الدردشة أو على الشات أو الفايسبوك أو المنتديات...الخ ، تتحقق العلانية التي بمقتضاها توقع العقوبة الجزائية المقررة لهذه الجريمة[1].

إذ يحدث وأن يكون السلوك الإجرامي عبر الاتصال الالكتروني المباشر كما قد يحدث بواسطة النشر الالكتروني، وتتحقق علانية الكلام والصراخ إذا تم نقلها عبر الانترنت أو الهواتف النقالة، أو تحميل مادة مسجلة وعرضها تحتوي عبارات القذف والسب بالصوت والصورة عبر مواقع التواصل الاجتماعي[2].

3. الركن المعنوي:

باعتبار القذف جريمة عمدية يتخذ الركن المعنوي صورة القصد الجنائي العام ، وعلى ذلك يتكون من عنصرين :

العنصر الأول: هو علم الجاني بشتى عناصر الجريمة.

العنصر الثاني: انصراف إرادة الجاني إلى إتيان الفعل وتحقيق نتيجته ويتولى قاضي الموضوع تقدير هذا الركن من واقع ظروف الدعوى بشرط أن يكون استنتاجه غير مشوب بقصور[3].

---

[1] **محمد الألفي**، المرجع السابق، ص 85.

[2] **عادل عزام سقف الحيط**، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، الطبعة الاولى، دار الثقافة للنشر والتوزيع، عمان، 2011، ص212.

[3] **مصطفى محمد موسى**، المرجع السابق، ص434.

والركن المعنوي يتمثل في انصراف إرادة الفاعل إلى الفعل المادي المكون للجريمة كما وصفه القانون، ولما كان هذا الفعل هو التعبير علنا عن أمر ماس بالشرف والاعتبار فيتعين القول بتوافر القصد الجنائي أن تنصرف إرادة الجاني من جهة إلى مس الشرف والاعتبار فهذا قصد القذف وإلى العلانية في هذا المس من جهة أخرى ، وهذا هو قصد إذاعة القذف فهو جريمة عمدية في كافة حالاته[1].

وبالتالي فالركن المعنوي بصفة عامة له علاقة تربط بين ماديات الجريمة وشخصية الجاني وهذه العلاقة تكون محل لوم للقانون.

ثانيا- أركان جريمة السب عبر الوسائط الإلكترونية :

جريمة السب مثلها مثل باقي الجرائم تتكون من ركنين؛ الأول مادي تتمثل في ارتكاب الشخص السلوك المعاقب عليه والثاني معنوي يتمثل في القصد الجنائي ، وكونه يخدش شرف وكرامة الشخص فنشاطه يكون بتعبير معين يتخذ صورة القول أو الكتابة وإلصاق صفة أو عيب أو لفظ جارح قاصدا الحط من مكانة المجني عليه[2].

1. الركن المادي :

يتحقق الركن المادي لجريمة السب في إسناد صفة أو عيب أو لفظ مشين إلى شخص محدد وذلك علانية النشاط الخادش للشرف و الاعتبار بسبب فعل السب وعليه عبارة السب الأكثر عنفا هي التي تتضمن التحقير نظرا لما تحتويه من اعتداء وكلام بذيء فالتعبير المشين

[1] **نبيل صقر**، الوسيط في شرح 50 جريمة من جرائم الأشخاص، شركة دار الهدى للنشر والتوزيع، الجزائر، 2009، ص 126.

[2] **تميم بن عبد الله بن سيف التميمي**، المرجع السابق ، ص107.

هو كل ما من شأنه الحط من قدر المجني عليه والنيل من شرفه، أما القدح فهو كل تعبير قبيح يمس شرف واعتبار المجني عليه[1]. ويتكون هذا الركن من ثلاث عناصر وهي:

أ. السلوك الاجرامي :

هو النشاط أو السلوك الإجرامي الذي يرتكب باستخدام الحاسب الالكتروني وشبكة الانترنت أو الوسائط الالكترونية الأخرى وتتطلب تواجد بيئة رقمية واتصال بالشبكة المعلوماتية العالمية، وبما أن جريمة السب إحدى هذه الجرائم يقوم الركن المادي فيها على نشاط إجرامي معين يتمثل في إسناد تعبير مشين ضد شخص أو عدة أشخاص بغض النظر إذا كان الشخص طبيعيا أو معنويا بحيث ينطوي هذا التعبير على خدش لشرف المجني عليه واعتباره دون أن يتضمن إسناد واقعة معينة إليه.

كما يقع السب وجاهيا على شبكة الانترنت في حالات معينة مثل تبادل الكتابة والرسوم والتسجيلات الفيديوية ونحوها في غرف الدردشة، بحيث تتسم الدردشات بالتزامنية بين عدد المشتركين في الحوار في غرفة افتراضية واحدة ومن ثم يجمع بين مستخدمي هذه الخدمة وحدتان؛ وحدة زمنية هي وقت اجتماعهم وإن اختلف التوقيت في كل بلد، و وحدة مكانية افتراضية هي غرفة المحادثة وإن اختلف المكان المادي لمجهولية شخصية المعتدي[2].

ب. النتيجة :

هي الأثر المترتب على السلوك الإجرامي وهي التعبير الذي يحدث في العالم الخارجي، ففي مدلولها القانوني هي العدوان الذي يهدد مصلحة قدر المشرع جدارتها بالحماية الجزائية وعلى وفق ذلك النتيجة لها صورتان؛ الأولى تتمثل في الضرر والثانية تتمثل في الاعتداء[3].

---

[1] **العاقل غريب أحمد**، جرائم الإهانة والقذف والسب معلقا عليها بأحكام النقض والمحكمة الإدارية العليا، مركز معلومات النيابة الإدارية ، مصر، 1954، ص 21.

[2] **حصة راشد محمد السليطي**، جرائم القذف والسب العلني عبر الانترنت- دراسة مقارنة، المجلة القانونية والقضائية، العدد 01، قطر، 2015، ص305.

[3] **المرجع نفسه**، ص 305.

فتتحقق النتيجة الجرمية بتحقق النشاط الإجرامي المرتكب باستخدام الحاسوب أو الهاتف النقال المتصلين بالشبكة المعلوماتية، أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى المكونة لجريمة السب سواء أسند المتهم إلى المجني عليه عيبا معينا يخدش شرفه أو اعتباره .

ج. **العلاقة السببية :**

لكي يتحقق الركن المادي في هذه الجريمة يجب أن تكون الإساءة التي لحقت بكرامة المعتدى عليه من فعل الجاني وحده وللقول بتوافر العلاقة السببية بين السلوك الإجرامي (فعل السبب) الذي تم عبر الانترنت أو من خلال مواقع التواصل الاجتماعي والنتيجة الإجرامية التي مست بالمجني عليه في شرفه واعتباره أو سمعته، إذ ينبغي أن يكون التعبير المشين المتضمن عيبا ينطوي على المساس بالشرف والاعتبار موجها إلى شخص أو عدة أشخاص معينين بسبب انتمائهم إلى مجموعة عرقية أو إلى دين معين وفضلا على ذلك يستوي أن يكون الشخص طبيعيا أو معنويا، غير أنه لا يشترط تحديد الشخص المجني عليه وإنما يكفي أن يكون من السهل التعرف عليه. ولربط السبب بالنتيجة الإجرامية في جريمة السب عبر تكنولوجيات الإعلام والاتصال[1].

فلا بد أن تتوافر في واقعة السب خدش لشرف واعتبار المجني عليه عناصر منها:

- أن يكون النشاط خادش لشرف المجني عليه أو اعتباره دون أن يتضمن واقعة معينة.
- أن يكون السب عبر الوسائط الإلكترونية موجها إلى شخص معين.
- ضرورة توافر عنصر العلانية.

2. الركن المعنوي:

يتخذ الركن المعنوي أو القصد الجنائي أو القصد الجنائي في جريمة السب صورة القصد الجنائي العام إذ لا يشترط توافر القصد الجنائي الخاص ويتمثل الركن المعنوي في جريمة السب في الجهر لا بالألفاظ المشينة مع العلم أن تلك العبارات تلحق ضرر بالمجني عليه والتي

[1] **حصة راشد محمد السليطي** ، المرجع السابق ، ص306.

ترتكب عبر منظومة معلوماتية أو عبر نظام الاتصالات الإلكترونية، وتتخذ صورة القصد الجنائي العام إذ لا يتطلب القانون لقيام جريمة السب قصدا جنائيا خاصا وإنما القصد الجنائي العام الذي يتكون من عنصرين أساسيين وهما عنصر العلم والإرادة، والقصد لابد أن ينصرف إلى جميع أركان الجريمة، فيتعين أن يعلم المتهم بدلالة الواقعة التي لا يسندها إلى المجني عليه[1].

الفرع الثالث : أساليب ارتكاب جريمتي القذف والسب عبر الوسائط الإلكترونية و الجزاءات المقررة لها

تنوعت أساليب ارتكاب الجرائم الإلكترونية كالحواسيب وغيرها من الأجهزة الأخرى وهذا نتيجة تطور الثورة التكنولوجية ،وكون جريمة القذف والسب جريمة أكثر شيوعا في الفضاء الرقمي أدى بالتشريعات إلى اتخاذ خطوات إستراتيجية و وضع أحكام ونصوص عقابية تجرم هذه الجريمة.

ولتوضيح هذا سنبين أساليب ارتكاب جريمة القذف والسب عبر الوسائط الإلكترونية(أولا)، ومن ثم التطرق إلى الجزاءات المقررة لها(ثانيا).

أولا- أساليب ارتكاب جريمتي القذف والسب عبر الوسائط الالكترونية:

إن الإجرام المتواصل بالوسائط الالكترونية أدى إلى تحديات كبيرة بالنسبة لقانون العقوبات إذ يسيء استخدام شبكة الانترنت في الاعتداء على الأشخاص سواء كانوا طبيعيين أو اعتباريين في شرفهم واعتبارهم والتشهير بهم من خلال نشر رسائل تحتوي عبارات القذف والسب وغيرها، ويكون القذف والسب وجاهيا عبر وسائل الاتصال الالكترونية، السمعية

[1] **العاقل غريب أحمد**، المرجع السابق ، ص 23.

والبصرية، والكتابية والفيديوية[1]، أو يتم بث فيديو مسجل يحتوي على قذف أو سب عبر موقع youtube.

ومن بين وسائل التعبير عن الإسناد في جريمة القذف أو السب العلني يمكن التعرض لها على النحو الآتي :

1. **شبكة الويب العالمية w.w.w web** : يمكن القول أن شبكة الويب نظام فرعي من الانترنت فهو النظام الشامل بواسطة استخدام الوسائط الالكترونية المتعددة[2].

تتيح شبكة web لأي شخص كان الاطلاع على معلومات تخص جهات أخرى وأشخاص آخرين قاموا بوضعها عبر هذه الشبكة وجعلها في إطار الخدمة، وقد تكون هذه المعلومات الغاية منها الاعتداء على الأفراد والإساءة إليهم حيث يستطيع أي مستخدم للشبكة أن ينشأ لنفسه موقعا site في هذه الشبكة، وبالتالي يستطيع الجاني (القاذف) أن ينشر الكلام الذي يحتوي قذف المجني عليه في إسناده مادة معينة في موقعه فيطلع عليها كل من يدخل موقعه. كما ترتكب جريمة القذف عبر الشبكة المعلوماتية العالمية حالة قيام المعتدي بإسناد مادة معينة من القذف وبإسناد عبارات فيها قذف سواء كانت كتابية أو صوتية أو فيديوية تخدش شرف واعتبار المعتدى عليه وسمعته بين أهل وطنه[3].

2. **البريد الالكتروني Email:** تمكن معرفة اسم البريد الالكتروني أي شخص أن يرسل رسائل إلى صاحب البريد وقد يتضمن هذه الرسائل كلام في قذف أو سب يقع تحت طائلة جرائم الاعتداء على الأشخاص الماسة بسمعة الإنسان واعتباره وشرفه.
3. **غرفة المحادثات والدردشة:** هي عبارة عن غرف المحادثات المفتوحة دون تحديد موضوع معين يشترك فيه المستخدمون وقد تكون الغرفة مغلقة لمتحاورين فقط أو محددة بعدد معين،

---

[1] **محمد أمين الشوابكة**، جرائم الانترنت الجريمة المعلوماتية، الطبعة الاولى، دار الثقافة للتوزيع والنشر، عمان الاردن، 2002 ، ص 31.

[2] **محمد عبد الله المنشاوي**، جرائم الانترنت من المنظور الشرعي والقانوني، بحث مقدم إلى مركز القوانين العربية، مكة المملكة العربية السعودية، 2001، ص05.

[3] **المرجع نفسه**، ص06.

أو مفتوحة للجمهور ولمن شاء الدخول فيها هذا من جهة ومن جهة أخرى قد تكون المادة التي تحتوي على القذف أو السب مادة كتابية أو صوتية أو تصويرية إلا أن الكتابة تشكل الصورة الغالبة لمثل هذا النوع من الجرائم.

4. **وسائل الاتصال الالكترونية الهاتف النقال والبلوتوث "Bleutooth "**: يمكن أن يسيء الهاتف النقال استخدامه في غير الغرض المخصص له بحيث يمكن ارتكاب أفعال الاعتداء ضد الأفراد عن طريق الهاتف المحمول باعتباره صورة من صور تقنيات المعلومات والاتصالات الحديثة، والتي أصبح الولوج من خلالها إلى الشبكة العنكبوتية العالمية أمرا بسيط لارتكاب أفعال مجرمة تحظرها النصوص العقابية التقليدية كجرائم القذف والسب والإساءة أو الإهانة المرتكبة باستخدام جهاز الهاتف المحمول والانترنت وذلك إما برسائل تحتوي على القذف والسب الالكترونية المرسلة من شبكة الانترنت بواسطة خدماتها المتاحة إلى الهاتف النقال، وإما بالرسائل الالكترونية التي تتضمن عباراتها قذفا أو سبا بحيث يتم إرسالها من الهاتف النقال إلى شبكة الانترنت من خلال الخدمات التي يوفرها البريد الالكتروني[1].

ثانيا- الجزاءات المقررة لجريمتي القذف والسب عبر الوسائط الالكترونية :

وضع المشرع الجزائري نماذج لجرائم القذف والسب والتي يمكن إسقاطها على جريمة القذف والسب عبر الوسائط الإلكترونية. لذا سنبين عقوبة كل جريمة على النحو الآتي :

1. **الجزاءات المقررة لجريمة القذف عبر الوسائط الالكترونية :**

ميز المشرع بين العقوبات المقررة للقذف الموجه إلى الأشخاص والهيئات النظامية والمؤسسات العمومية بالرغم من تجريمه في نص **المادة 296** من قانون العقوبات الجزائري والتي تنص على: **<< يعد قذفا كل ادعاء بواقعة من شأنها المساس بشرف واعتبار**

[1] **أروى محمد تقوى**، مدى مسؤولية مشغلي الهاتف النقال عن إساءة استخدامه في الاتصال بالأنترنت- دراسة مقارنة، مجلة الحقوق ، العدد 02، كلية الحقوق، جامعة دمشق، ص 371.

الأشخاص أو الهيئة المدعى عليها به أو إسنادها إليهم أو إلى تلك الهيئة ويعاقب على نشر هذا الادعاء .... موضوع الجريمة >>. بحيث نصت هذه المادة على أن محل جريمة القذف هم الأشخاص أو الهيئات، بينما نصت **المادة 144 مكرر** من قانون العقوبات على جريمة القذف الموجه إلى رئيس الجمهورية [1]. كما نصت **المادة 146** من نفس القانون أيضا على القذف الموجه ضد البرلمان أو إحدى غرفتيه أو ضد الجهات القضائية أو ضد الجيش الوطني الشعبي أو هيئة نظامية عمومية[2]، وطبقا لنص المادة 298 ق.ع فإن المشرع الجزائري عاقب على القذف الموجه للأفراد بالحبس من شهرين (2) إلى ستة أشهر (6) وبغرامة من 25.000 دج إلى 100.000 دج أو بإحدى هاتين العقوبتين. ويضع صفح الضحية حدا للمتابعة الجزائية، ويعاقب على القذف الموجه إلى شخص أو أكثر بسبب انتمائهم إلى مجموعة عرقية أو مذهبية أو إلى دين معين بالحبس من خمسة (5) أيام إلى ستة (6) أشهر وبغرامة من 20.000دج إلى 100.000 دج أو بإحدى هاتين العقوبتين.

2. **الجزاءات المقررة لجريمة السب عبر الوسائط الإلكترونية :**

تخضع المتابعة الجزائية في جريمة السب لنفس الإجراءات والأحكام المقررة للقذف بحيث تختلف العقوبة باختلاف صفة الشخص المستهدف بالسب، حيث ميزها على النحو التالي :

أ. **السب الموجه للأفراد:** يعاقب على السب الموجه للفرد أو عدة أفراد بالحبس من شهر (1) إلى ثلاثة (3) أشهر وبغرامة مالية من 20.000دج إلى 100.000 دج، ويضع صفح الضحية حدا للمتابعة الجزائية. و هذا بموجب نص **المادة 299** من قانون العقوبات الجزائري.

---

[1] **المادة 144 مكرر من الأمر رقم 66-156**: << يعاقب بغرامة من 100.000 دج إلى 500.000 دج، كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأية آلية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى .
تباشر النيابة العامة إجراءات المتابعة الجزائية تلقائيا. وفي حالة العود، تضاعف الغرامة >> .

[2] **راجع المادة 146** من أمر رقم 66-156 ، المرجع نفسه.

ب. **السب الموجه على حسب الدين والعرق:** أما السب الموجه إلى شخص أو عدة أشخاص منتمين إلى مجموعة عرقية أو مذهبية أو إلى دين معين يعاقب عيه من خمسة (5) أيام إلى ستة(6) أشهر وبغرامة مالية من 20.000 دج إلى 100.000دج أو بإحدى هاتين العقوبتين. وهذا طبقا لنص المادة 298مكرر من قانون العقوبات الجزائري[1].

وما يحسب للمشرع الجزائري أنه قد وسع من دائرة تجريم فعل السب عندما يرتكب بأية وسيلة من الوسائل الالكترونية أو الإعلامية أو أية وسيلة أخرى حتى لا يفلت الجناة من العقاب كون جريمة السب كثيرة الوقوع بواسطة الحواسيب والانترنت والهواتف الموصولة بشبكة الانترنت[2].

المطلب الثاني

جريمة التحرش الجنسي عبر الوسائط الالكترونية

لا شك أن جريمة التحرش الجنسي كانت ولا زالت من أخطر وأقدم الظواهر الاجتماعية ومع التقدم الهائل الذي شهده العالم في مجال التكنولوجيا والمعلوماتية تطورت أشكال التحرش الجنسي لتنتقل من المجتمع الواقعي إلى العالم الافتراضي، إذ أصبحت وسائل التواصل الالكترونية تشكل أرضا خصبة لفئة من المنحرفين ينشطون بشكل عصابات أو أفراد لاصطياد ضحاياهم وبالتالي تسخير الفضاء الرقمي لخدمة منافعهم الجنسية. وتفاقمت في الآونة الأخيرة شكاوي التحرش الجنسي عبر الوسائط الالكترونية بحيث أضحت شبكة الانترنت البيئة المغرية والمحفزة لانتشار هذا النوع من الجرائم فلم يعد التحرش الجنسي مرتبط بالمقابلة المباشرة بين المتحرش والضحية ، بل أصبح بإمكان المتحرش الدخول إلى بيتك و ممارسة التحرش بكل وقاحة و دون خوف عبر وسائل الاتصال الحديثة كالأنترنت أو الهواتف المحمولة أو البريد الالكتروني.

---

[1] **راجع المادة 298 مكرر**، من أمر رقم 66-156، المرجع السابق.

[2] **تومي يحي**، المرجع السابق، ص 102.

ويمكن أن يحدث التحرش الجنسي الإلكتروني عبر مجموعة متنوعة من التطبيقات أهمها غرف الدردشة، منتديات الانترنت، مواقع التواصل الاجتماعي، الرسائل الفورية، البريد الإلكتروني، الصور الرمزية، الإعلانات، الروابط التلقائية .

ولتوضيح جريمة التحرش الجنسي عبر الوسائط الإلكترونية لا بد من التطرق إلى تعريف و أنماط التحرش الجنسي عبر الوسائط الإلكترونية (**الفرع الأول**)، ومن ثم التطرق إلى صور التحرش الجنسي عبر الوسائط الإلكترونية والجزاءات المقررة لها(**الفرع الثاني**).

الفرع الأول: تعريف و أنماط جريمة التحرش الجنسي عبر الوسائط الإلكترونية

إن التحرش الجنسي شكل من أشكال العنف الجنسي أو المادي أو الأخلاقي أو النفسي يحدث ضررا في كرامة الشخص و شرفه وحريته ويمكن أن يظهر على أرض الواقع في أشكال مختلفة[1]، وهذا راجع لعدة دوافع؛ منها ما هو شخصي كسهولة إخفاء الهوية (القناع الرقمي) والرغبة في الانتقام مع عدم القدرة على المواجهة ومنها ما هو اجتماعي وثقافي كانهيار منظومة القيم الاجتماعية و التفكك الاجتماعي، الغزو الثقافي في ظل العولمة و شبكة الانترنت الدولية و انتشار ثقافة العنف، الانفتاح الاجتماعي[2].

ولقد عرضنا التحرش الجنسي بصفة عامة، وسوف نعرض جريمة التحرش الجنسي عبر الوسائط الالكترونية بصفة خاصة(**أولا**)، ومن ثم التطرق إلى أنماط جريمة التحرش الجنسي عبر الوسائط الإلكترونية(**ثانيا**).

[1] **حاج كولة غانية**، التحرش الإلكتروني الممارس ضد المرأة عبر مواقع التواصل الاجتماعي "الفايسبوك نموذجا"- دراسة حالة معينة من النساء ضحايا التحرش الالكتروني، مجلة العلوم الإنسانية، المجلد 20، العدد 02، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2020، ص 45 .

[2] **أحمد محمد طلعت عبد الحميد ضرغام**، التحرش الجنسي الالكتروني بالسيدات (ماهيته وسبل مواجهته)، ورقة بحثية في إطار دراسة مادة علم الإجرام والعقاب، كلية الحقوق، جامعة الإسكندرية، 2017، ص 10-12.

أولا – تعريف جريمة التحرش الجنسي عبر الوسائط الإلكترونية :

يقصد به التحرش أو المضايقة التي تلحق ضررا وعارا بالمرأة والفتاة أو الطفل وتتضمن نشر الإباحية، الإهانة على أساس النوع والتهديد بالاغتصاب والقتل والكشف عن المعلومات الشخصية وتزويرها عبر الوسائل الإلكترونية، وأشارت أحد الدراسات التي قام بها مركز الملاحظة لحقوق الانترنت أن ظاهرة التحرش الجنسي عبر الوسائط الالكترونية لها طابع متكرر بقوة ويرتبط بنوايا المؤلف أو المستخدم والتسبب في إحداث ضرر وإلحاق أذى بالآخرين[1].

أ. **التعريف الإجرائي للتحرش الجنسي الالكتروني** :هو قيام المتحرش الافتراضي بمضايقة مستخدمي الفايسبوك باختراق حسابهم وابتزازهم أو التشهير بسمعتهم بإرسال التعليقات ورسائل وصور وفيديوهات غبر لائقة عبر مواقع التواصل الاجتماعي ويسبب هذا التحرش الافتراضي إيذاءا نفسيا وأخلاقيا وجنسيا ومن الممكن أن يقوم بالتحرش فرد أو جماعة، وغالبية ضحايا التحرش تكون إناث (متزوجة، عزباء، طالبة، عاملة، ماكثة بالبيت) .

ب. **تعريف المتحرش الافتراضي:** هو شخص افتراضي ينتحل شخصية مجهولة على المنصة الالكترونية يستخدم حسابه بطريقة غير مشروعة ويسبب مضايقات ويسيء للصفحة المسروقة، ويخشى مواجهة الناس في الواقع فيختار المنصة الالكترونية فضاء للمضايقة والتحرش جنسيا بالشخص مهما كانت مكانته الاجتماعية[2].

ثانيا–أنماط التحرش الجنسي عبر الوسائط الإلكترونية :

يشمل التحرش الجنسي الالكتروني عدة أنماط من بينها :

1. **التحرش الجنسي اللفظي** :ويشمل إرسال كلمات خادشة للحياء أو كلمات صوتية تلفظ بكلمات ذات طبيعة جنسية أو وضع تعليقات ذات إيحاء جنسي، ويظهر في شكل هجوم

[1] **حاج كولة غانية**، المرجع السابق، ص 46.

[2] **المرجع نفسه**، ص 46.

جنسي رسائل بدأها المتحرش حول الضحية وعادة ما يمارس هذا النوع من التحرش في غرف الدردشة والمنتديات وكذلك في الاتصالات الالكترونية الخاصة[1].

2. **التحرش الجنسي بين الجنسين:** يشير المتعمد إلى إرسال محتويات مثيرة إباحية أو مقاطع فيديو من خلال التواصل عبر الانترنت مثل البريد الالكتروني ونشرها وتكون هذه المحتويات أكثر أو أقل هجوما اعتمادا على حساسية الفرد الضحية[2].
3. **التحرش البصري:** يتمثل في إرسال الصور والمقاطع الجنسية والطلب من الضحية الكشف عن أجزاء من جسدها أو قيام المتحرش بإرسال صور أو فيديو له وهو في أوضاع مخلة بالآداب .
4. **التحرش بالاكراه:** يحدث التحرش الجنسي من خلال اختراق جهاز الاتصال الخاص بالشخص المتحرش به والحصول على صور خاصة ومعلومات شخصية وإجباره على الموافقة على اللقاء بالمتحرش على أرض الواقع وذلك من خلال الملاحظة أو الابتزاز بنشر الصور أو التشهير عبر وسائل الكترونية مختلفة، أو انتحال الحسابات على مواقع التواصل الاجتماعي[3].

الفرع الثاني : صور التحرش الجنسي عبر الوسائط الإلكترونية والجزاءات المقررة له

شهدت الثورة المعلوماتية تطورا لم يسبق مشاهدته من قبل كونه يمتاز بوتيرة متسارعة أدت إلى ظهور العديد من الجرائم على المنصة الرقمية وكون التحرش الجنسي أصبح بشكل كبير على الفضاء الرقمي متمثل في العديد من الصور أدى هذا إلى وضع نصوص عقابية للحد من هذه الظاهرة .

---

[1] **طوالبية وئام، ماجن أسماء،** التحرش الجنسي عبر الانترنت ، مذكرة ماستر في العلوم الاجتماعية ، كلية العلوم الانسانية والاجتماعية، جامعة الجيلالي بونعامة ، خميس مليانة ، 2015، ص 51.

[2] **المرجع نفسه،** ص 52 .

[3] **مسعود مواكيز، عبابو فاطمة** ، التحرش الجنسي عبر مواقع التواصل الاجتماعي ، مجلة آفاق لعلم الاجتماع ، العدد 16 ، جامعة البويرة ، الجزائر ، 2018، ص 198.

ومن خلال ما ذكرناه سابقا سنوضح صور التحرش الجنسي الالكتروني(**أولا**)، ومن ثم التطرق إلى الجزاءات المقررة لهذه الجريمة.

أولا- صور التحرش الجنسي عبر الوسائط الإلكترونية:

التطور التكنولوجي الذي يشهده اليوم يسبق بكثير التشريعات التي من االمفترض أن تواكبه ويستدعي ذلك اتخاذ مجموعة من الخطوات والإجراءات الإستراتيجية على كافة الأصعدة بالأخص خطوات وإجراءات تدخل ضمن النطاق التنظيمي لا سيما أن التطور التكنولوجي يمتاز بوتيرة متسارعة يجعل الكثير من النصوص والأحكام التنظيمية القائمة غير منطبقة، ومن صور التحرش الجنسي عبر الوسائط الإلكترونية نجد :

1) التحرش الجنسي عبر البريد الإلكتروني: بدأت ظاهرة التحرش باستخدام البريد الإلكتروني ومع انتشار الانترنت أكثر شمل التحرش غرف الدردشة و المنتديات و مواقع التواصل الاجتماعي مثل الفايسبوك والتويتر والواتساب، كما تحول التحرش عن طريق الانترنت من مجرد التركيز على المواضيع الجنسية إلى تصفية حسابات و تشمل أشكال هذا التحرش ملاحقة الآخرين أو التشهير بهم، وقد زادت إمكانية تعرض مستخدمي شبكة الانترنت إلى هذا التحرش بسبب انتشار ثقافة الاستعراض من خلال نشر الصور والمعلومات الشخصية من جهة والفراغ النفسي والعاطفي الذي يدفع بعض الأشخاص لقضاء ساعات طويلة على شبكة الانترنت[1].

ولا يقتصر التحرش فقط على الفتيات إذ يشكو العديد من الرجال من تلقيهم لرسائل غير مناسبة تتضمن صور وعبارات غير لائقة.

[1] **آية عامر**، دراسة الانترنت يسهل التحرش عبر مواقع التواصل الاجتماعي، بحث منشور على الرابط .www. shorouk . Com .بتاريخ 15 مارس 2022، على الساعة العاشرة صباحا.

2) **المضايقات الإلكترونية:** مع تنامي الإعلام الالكتروني فقد تزايد عدد الشكاوي من المضايقات الالكترونية أو ما يسمى بالتخويف الالكتروني إضافة إلى مضايقات التحرش الجنسي وأنواع أخرى من حوادث الإيقاع بالضحايا.

لا يرغب مستخدمي الانترنت في الغالب بوضع معلوماتهم الشخصية على الشبكة الالكترونية وتزداد فرص تعرض الفتيان والفتيات للمضايقات أو التحرش الجنسي الالكتروني وتكون عندما يأخذون في التفاعل مع الآخرين إلكترونيا مثل تبادل الرسائل الفورية أو الدخول في حوار في غرف الدردشة الالكترونية، و ليس من الواضح السبب الذي يقود في هذا السلوك إلا أنه يبدو ممن المحتمل أن تكون غرف الدردشة هذه التي تجري فيها الأحداث مباشرة وبعيدا عن أعين الكبار[1].

3) **الرسائل الفورية:** تسهل التقنيات الحالية في الانترنت تبادل الرسائل المكتوبة لأي شخص يستخدم الكمبيوتر والأجهزة الإلكترونية الأخرى وهذه الوسيلة التي تزداد شعبيتها لدى الصغار والشباب تشكل خطرا عليهم يتمثل في التحرش الالكتروني [2].

4) **غرف الدردشة:** هذه المنتديات الالكترونية المخصصة للحوار تتيح للناس تبادل الرسائل المكتوبة فيما بينهم والمحادثات كما تتيح بعض المواقع للمشاركة وتبادل الصور والأحاديث في نفس الوقت إلا أن غرف الدردشة تشكل خطرا أكبر من ناحية التحرش الجنسي الالكتروني.

5) **المدونات الإلكترونية:** هذه المدونات التي يسجل فيها الكاتب خواطره وآراءه ومعلوماته الشخصية ويمكن لقارئ هذه المدونات إرسال تعليقات أيضا التي قد تقود إلى حوار

[1] **محمود عبد الحليم سليمان،** إيذاء النساء بأثولوجيا التحرش الجنسي الإلكتروني بالمرأة ، مجلة جيل العلوم الانسانية والاجتماعية ، العدد 42 ، مصر ، 2018 ، ص 131 .

[2] **جميل عبد الباقي الصغير،** أدلة الإثبات الجنائي و التكنولوجيا الحديثة – أجهزة الرادارات و الحسابات الآلية و البصمة الوراثية ، الطبعة الأولى ، دار النهضة العربية ، 2001 ، ص 100 .

إلكتروني بين القارئ و الآخرين. حيث يكشف كتاب المدونات عن خفايا ذاتهم الشخصية على الانترنت ومن بينها بياناتهم الشخصية[1].

ثانيا- الجزاءات المقررة لجريمة التحرش الجنسي عبر الوسائط الإلكترونية :

تعتبر جريمة التحرش الجنسي الالكتروني من الجرائم الحديثة و الداخلة على قانون العقوبات الجزائري، فهي جنحة تعاقب عليها المادة 341 مكرر من قانون العقوبات الجزائري كما يلي :

أ. الحبس من سنة إلى ثلاث (3) سنوات و غرامة من 100.000 دج إلى 300.000 دج كل شخص يستغل سلطة وظيفته أو مهنته عن طريق إصدار الأوامر للغير أو بالتهديد أو الإكراه أو ممارسة صغوط عليه قصد إجباره على الاستجابة لرغباته الجنسية وهذا ما تنص عليه **المادة 341 مكرر** في فقرتها الأولى من قانون العقوبات الجزائري.

ويعاقب بنفس العقوبة كل من تحرش بالغير بكل فعل أو لفظ أو تصرف يحمل طابعا أو إيحاء جنسي؛ وهذا وفقا **للمادة 341 مكرر** في فقرتها الثانية من نفس القانون[2].

ب. الحبس من سنتين إلى خمس (5) سنوات و غرامة من 200.000دج إلى 500.000 دج إذا كان الجاني من المحارم أو كانت الضحية قاصرا لم تكمل 16 سنة أو إذا سهل ارتكاب الفعل ضعف الضحية أو مرضها أو إعاقتها أو عجزها البدني أو الذهني أو بسبب حالة الحمل سواء كانت هذه الظروف ظاهرة أو كان الجاني على علم بها، وهذا طبقا للفقرة الثالثة من نفس المادة السالفة الذكر.

ج. و تنص الفقرة 4 من نفس المادة المذكورة أعلاه على أنه تضاعف العقوبة في حالة العود[3].

---

[1] **محمد أمين الشوابكة** ، المرجع السابق، ص 117.

[2] راجع **المادة 341 مكرر** من الأمر 66-156، المرجع السابق.

[3] **راجع المادة 341 مكرر**، من الأمر 66-156، المرجع نفسه.

خلاصة الفصل

من خلال ما تطرقنا إليه في هذا الفصل فإن جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية نوع من أنواع الجرائم الإلكترونية التي تعتمد على التقنيات الحديثة لارتكابها في الاعتداء على الغير، وهذا نتيجة للتطورات المتسارعة في تكنولوجيا المعلومات جعلت الوسائل الإجرامية متنوعة كالحاسوب والهواتف الذكية النقالة والبريد الإلكتروني...الخ، حيث يتم الاعتداء على ما تقدمه من خدمات لارتكاب الجرائم؛ كجرائم الاعتداء على الأشخاص التي لها صور متعددة كقذف وسب الأشخاص عبر الوسائط الإلكترونية وكذلك الجرائم التي تمس أضعف فئة اجتماعية (المرأة، الطفل) وقد تستغل هذه الأخيرة في أعمال جنسية أو تمارس عليها وكلها جرائم ارتكبت بحق الأشخاص وكانت الوسائط الإلكترونية والتقنيات سببا في تحقيق الهدف الإجرامي.

الفصل الثاني

الإطار التنظيمي لجرائم الإعتداء على الأشخاص عبر الوسائط الإلكترونية

الفصل الثاني:

الإطار التنظيمي لجرائم الإعتداء على الأشخاص عبر الوسائط الإلكترونية

اهتمت المجتمعات بظاهرة جريمة الاعتداء على الأشخاص عبر الوسائط الإلكترونية كونها ظاهرة دولية، فنظمت المجتمعات الدولية عدة قواعد إجرائية لإثبات مثل هذه الجرائم مما ألقى على عاتق القائمين على مكافحة الجريمة في الدولة عبئا شديدا يفوق القدرات المتاحة لهم وفق أسس وقواعد إجراءات البحث الجنائي والإثبات الجنائي التقليدية، فضلا عن إنشاء أجهزة فنية متخصصة يناط بها عملية الإثبات العلمي لهذه الجرائم .

تبنت العديد من الاتفاقيات والمواثيق الدولية التي تجرم هذه الجريمة بالإضافة إلى التعاون الدولي، وانعقدت عدة مؤتمرات عالمية وإقليمية لمناقشة مخاطر التكنولوجيا والمعلوماتية على الحياة الخاصة للأفراد لإيجاد سبل لمكافحة الجريمة الإلكترونية. كما أن المشرع الجزائري نظم قواعد إجرائية لتكريس الوقاية من هذه الجرائم من خلال إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته إضافة إلى استحداثه قطب جزائي وطني مختص في المتابعة والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .

ويتم تناول هذا الفصل من خلال تقسيمه إلى مبحثين؛ إذ نستهل دراستنا بالقواعد الإجرائية لجرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية(**المبحث الأول**)، ومن ثم التطرق إلى صعوبات و آليات مكافحة الجريمة الإلكترونية(**المبحث الثاني**).

المبحث الأول

القواعد الإجرائية لجرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية

سهلت تقنية المعلومات ارتكاب بعض الجرائم التقليدية فازدادت تفاقما في ظل البيئة الافتراضية التي تمثلها شبكة الانترنت والتي تطور معها الفكر الإجرامي، فظهر نوع جديد من الجرائم هو ما يعرف بالجرائم الإلكترونية، نظرا لعدم ملائمة هذه النظم التقليدية في إثبات تلك الجرائم .

فضلا عن ذلك نجد أن التحقيق من أهم الإجراءات لما له من أهمية في التثبت من حقيقة وقوع الجريمة لينتقل بعد ذلك إلى مرحلة المحاكمة كون الجريمة الإلكترونية لا يمكنها أن تبقى رهينة التحقيق فلا بد أن تصل إلى أروقة المحاكم، حيث تجدر الإشارة إلى الحاجة لتفعيل الجهاز القضائي بقطب متخصص في جرائم تكنولوجيات الإعلام والاتصال بخصوص المتابعة والتحقيق بغرض الكشف عن هذه الجرائم ومعاقبة مجرميها. وهذا ما استحدثه المشرع الجزائري وفقا للأمر رقم 21-11 المتمم لقانون الإجراءات الجزائية[1]. وتأسيسا على ذلك يظهر القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال كوسيلة لضمان فعالية الممارسة القضائية بخصوص هذا النوع من الجرائم، ويمكن اعتباره خطوة لإرساء التخصص القضائي، إذ يختص هذا القطب بالمتابعة والتحقيق، كما يختص بالحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

ومن هذا المنطلق سنوضح القواعد الإجرائية لجرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية من خلال التطرق إلى إجراءات التحقيق في الجريمة الإلكترونية (المطلب الأول)، ومن ثم التطرق إلى إجراءات المحاكمة (المطلب الثاني) .

[1] **أمر رقم 21-11**، المرجع السابق.

المطلب الأول

إجراءات التحقيق في الجريمة الإلكترونية

التحقيق الجنائي في الجرائم الإلكترونية هو نشاط قانوني يتعلق بإجراءات ضبط الجرائم، والبحث عن مرتكبيها وجمع الاستدلالات التي يتطلبها التحقيق والدعوى الجنائية. فهو الضبط القضائي للجاني والدليل على إدانته أو براءته ودور المحقق الأمن (الشرطة) يتلخص في تلقي البلاغ وجمع الاستدلالات ضد مرتكب الجريمة لتقديمه للادعاء والقضاء بأدلة الإدانة[1].

من الواضح أن المشرع الجزائري قد سارع إلى تدارك النقص وسد الفراغ القائم بخصوص مجالات التحقيق الابتدائي إثر التطور الذي عرفته الجريمة بأشكالها الحديثة، حيث نجد أن المشرع حدد اختصاص ضباط الشرطة القضائية إلى كافة الإقليم الوطني، فيما يخص الجرائم الستة المحددة بشكل حصري في قانون الإجراءات الجزائية، من بينها الجريمة الإلكترونية. فاعتمد لهذه الأخيرة مجموعة من الأساليب الحديثة التي تساعد في متابعة الجرائم الإلكترونية[2]، حيث أرسى المشرع قواعد إجرائية جديدة ذات طبيعة خاصة كان من اللازم أن ترد مع التطور الحاصل في حقل الجريمة المعلوماتية كظاهرة حديثة.

وبهذا الصدد جاء القانون **رقم 09-04** المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[3]. كما استحدث لها مؤخرا قطب جزائي وطني مختص بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وذلك بمقتضى الأمر **رقم 21-11** السالف الذكر. والذي يؤول له اختصاص المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها، وهذا وفقا لما جاء في الفقرة الأولى من

---

[1] **محمد موسى مصطفى** ، المرجع السابق ، ص 165 .

[2] **رابح وهيبة**، الجريمة المعلوماتية في التشريع الإجرائي الجزائري، مجلة الباحث للدراسات الأكاديمية، العدد 04، ديسمبر 2014، ص 325 .

[3] قانون **رقم 09-04**، المرجع السابق.

نص **المادة 211مكرر22** من الأمر نفسه[1]. ويتمتع هذا الأخير بسلطات متكاملة وانفرادية دون غيره على مستوى المحاكم الجزائية العادية فيكون التحقيق على جهتين؛ أمام وكيل الجمهورية وأمام قاضي التحقيق. حيث يعد وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المختص الأصيل في نوع هذه الجرائم، حيث يمكن له أن يطالب بملف الإجراءات إذا اعتبر أن الجريمة تدخل ضمن اختصاصه وذلك بعد أحذ رأي النائب العام لدى مجلس قضاء الجزائر، وكل هذه الصلاحيات تؤول إلى وكيل الجمهورية في إطار اختصاصه المشترك الذي نصت عليه **المادة 211 مكرر 27** من قانون الإجراءات الجزائية[2]. أما بالنسبة للتحقيق أمام قاضي التحقيق فنجد هذا الأخير أنه يخضع لسلطة رئيس مجلس قضاء الجزائر، وعلى ذلك فإنه في حالة فتح تحقيق قضائي تحال التماسات وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المتضمنة المطالبة بملف الإجراءات من قبل وكيل الجمهورية، وعليه يصدر قاضي التحقيق أمرا بالتخلي لصالح قاضي التحقيق لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .

وحسب **نص المادة 211 مكرر 13** من ق. إ. ج تبقى كل أوامر بالقبض وأوامر الوضع رهن الحبس المؤقت الصادرة منتجة لآثارها إلى غاية صدور أمر مخالف عن قاضي التحقيق بالقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وطبعا حرصا من المشرع على دقة وإرساء الضمانات الكافية للتحريات من جهة؛ والمتهمين من جهة أخرى[3].

---

[1] راجع **المادة 211 مكرر 22**. أمر رقم 66-155 المؤرخ 18 صفر 1386 الموافق ل 08 يونيو 1966المتضمن قانون الإجراءات الجزائية، ج ر عدد 47، صادر بتاريخ 19 جوان 1966، المعدل والمتمم.

[2] راجع **المادة 211 مكرر 27** من الأمر 21-11 ، المرجع نفسه.

[3] **بن عميور أمينة ، بوحليس إلهام**، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، مجلة البحوث في العقود وقانون الأعمال، المجلد 7، العدد 01، جانفي 2022، ص 77 .

وعلى ذلك يتضح أن إجراءات التحقيق تمر بعدة مراحل، سنتطرق إليها من خلال تبيان الإجراءات الخاصة(**الفرع الأول**)، و من ثم التطرق إلى الإجراءات العامة (**الفرع الثاني**).

الفرع الأول : الإجراءات الخاصة

إن التحقيق هو مجموعة الإجراءات التي يقوم بها المحقق تؤدي إلى اكتشاف الجريمة ومعرفة مرتكبيها تمهيدا لتقديمه إلى المحاكمة لينال عقابه، ولهذا استحدثت التشريعات الحديثة منها التشريع الجزائري إجراءات خاصة من أجل ضبط وتسهيل اكتشاف الجريمة. و تنقسم هذه الإجراءات إلى قسمين منها، الشهادة في مجال الجريمة الإلكترونية كونها لا تختلف من حيث ماهيتها في الجريمة التقليدية وأمر سماع الشهود متروك للمحقق ومرتبط بظروف التحقيق، كذلك استحدث التسرب في مجال المساس بأنشطة الحاسب الآلي لعدة إجراءات ويرجع ذلك لعجز الأساليب التقليدية، ومن خلال هذا المنطلق سنوضح هذه الإجراءات من خلال التالي:

أولا- التسرب واعتراض المراسلات :

يعتبر التسرب واعتراض المراسلات من بين الإجراءات الخاصة التي تساعد على اكتشاف الجريمة وكشف المجرمين، سنوضخ هذه الإجراءات من خلال التالي.

1. التسرب :

وهو الإجراء المستحدث الذي نصت عليه المواد من **65 مكرر 11 إلى مكرر 18** من ق. ا. ج[1]. ويعرف التسرب على أنه تقنية يسمح بموجبها الدخول إلى وسط مغلق مثل جماعة إجرامية وشبكة تتاجر في الممنوعات كالأسلحة أو المخدرات، وتتم هذه العملية بعد اختيار ضابط الشرطة القضائية لأحد العناصر التابعة له الذين تتوفر فيهم بعض الصفات الخاصة كالتأقلم والتكيف مع الوسط المستهدف .

[1] - أمر رقم 66-155، المرجع السابق.

1/أ. شروط التسرب:

- الحصول على إذن مكتوب ومسبق من طرف وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية .
- يتضمن الإذن الجريمة التي تبرر اللجوء إلى التسرب وهوية ضابط الشرطة المنسق للعملية وتجديد المادة، إذ لا تتجاوز أربعة أشهر قابلة للتجديد حسب مقتضيات الجريمة ضمن الجرائم المذكورة وعلى سبيل الحصر في **المادة 65 مكرر 05** من قانون الإجراءات الجزائية؛ ومن ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.
- يراقب التسرب وكيل الجمهورية المتخصص أو قاضي التحقيق وفقا لنص **المادة 65 مكرر 11** من نفس القانون، ويمكن لهما الأمر بوقف التسرب في أي مرحلة[1].

1/ب. التسرب في مجال الإجرام المعلوماتي:

تكون عملية التسرب في الجرائم الإلكترونية بدخول ضابط أو عون شرطة إلى العالم الافتراضي، وذلك عن طريق اشتراكه في المحادثات كغرف الدردشة أو اختراق مواقع معينة مستخدما في ذلك أسماء أو صفات وهيئات مستعارة وهمية سعيا منه للاستفادة منه في كيفية اقتحام الهاكر للموقع أو القيام بحلقات اتصال مع المشتبه فيهم عن طريق البريد الالكتروني.

يدخل في هذا المعنى التسرب الالكتروني الذي يعني قيام ضباط الشرطة القضائية مختص بالاختراق والتوغل في منظومة معلوماتية أو نظام اتصالات إلكترونية أو منصة رقمية من أجل مراقبة المشتبه في تورطهم بارتكاب الجريمة، وذلك لأجل جمع أدلة تكشف مخططهم قبل ارتكاب الجريمة أو القبض عليهم بعد ارتكابها[2].

---

[1] **عبير بعقيقي، فيصل نسيغة**، الإثبات في الجرائم المعلوماتية على ضوء القانون 04/09، مجلة العلوم القانونية والسياسية، المجلد 09، العدد 02 ، 2018، ص 43 .

[2] **فاطمة العرفي**، تطبيق إجراء التسرب الإلكتروني في القانون الجزائري – إشكالية الموازنة بين حماية حق الخصوصية الرقمية ومكافحة جريمة اختطاف الأشخاص، مجلة دراسات وأبحاث في العلوم الانسانية والاجتماعية. المجلد 13 ، العدد 04، 2021، ص 216.

2. اعتراض المراسلات :

يتعلق الأمر بمسألة بالغة الأهمية كونها تشكل انتهاكا لحرمة المراسلات التي كفلها الدستور الجزائري غير أن المشرع الجزائري قد سمح بموجب **المادة 65 مكرر 05** من ق.ا.ج باعتبار المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، وذلك إذا اقتضت ضرورة التحري في الجريمة المتلبس بها في جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات... الخ، ويلاحظ من نص هذه المادة أن المشرع الجزائري قد يسمح بهذا الإجراء في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات حتى تتمكن جهات التحقيق من استخلاص أدلة الإثبات والوصول إلى الحقيقة[1].

كما أشار إليه المشرع الجزائري من خلال نص **المادة 03** من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال مكافحتها على ما يلي: "مع مرّاعاة القوانين التي تراعي سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحري أو التحقيقات القضائية حماية النظام العام وفق القوّاعد المنصوص عليها في الإجراءات الجزائية في هذا القانون وّوضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتوّاها في حينها والقيام بإجراءات التفتيش وّالحجز داخل المنظومة". ولقد كانت وسائل الاتصال في السابق تتمثل في الهاتف أما في الوقت الحاضر فانتقلت إلى البريد الإلكتروني وغرف الدردشة عبر الإّنترنت، ونجد أن المشرع الجزائري قد عرف المراسلات في **المادة 09** من القانون 2000-03[2] بأنها: "اتصال مجسد بشكل كتابي عبر مختلف الوسائل المادية التي يتم توصيلها إلى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه".

وعرف وسائل الاتصال الإلكتروني بأنها الوسائل " ترسل أو إرسال أو استقبال أو إشعارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية، ولهذا فإن مراقبة

[1] **عبير بعقيقي، فيصل نسيغة،** المرجع السابق، ص 43 .

[2] قانون **رقم 2000-03** المؤرخ في 05 أوت، يحدد القواعد العامة المطبقة على البريد و المواصلات السلكية و اللاسلكية، ج.ر، عدد48، الصادر في 06 أوت 2000، المعدل و المتمم.

الاتصال على الإّنترنت أو محتوى البريد الإلكتروني يعتبر جريمة يعاقب عليها القانون لاتصالها بحرمة الحياة الخاصة وهذا ما أشار إليه في **المادة 137** من قانون العقوّبات الجزائري إلا في الحالات التي أجازها القانون كما سبق الذكر في **المادة 03** من قانون 04/09، ولهذا فإن المشرع الجزائري فرّض الحماية القانونية على جميع الاتصالاّت الإلكترونية باعتبارها حق في الخصوصية وأجاز ذلك في الحالات التي يسمح بها القانون من أجل مقتضيات التحري والتحقيق وّالوصول إلى أدلة الإثبات ووفقا لما تتطلبه العدالة الجنائية.

ثانيا- شهادة الشاهد الإلكتروني:

تعتبر الشهادة من الأدلة المهمة في الإثبات التي نصت عليها الشرائع السماوية والتشريعات القانونية القديمة منها والحديثة، وبهذا يحتل الدليل المستخلص من الشهادة مكانة مهمة بين الأدلة الأخرى مما يجعله يحظى باهتمام القاضي الجزائي الذي غالبا ما يحتاج أثناء موازنة الأدلة المقدمة أمامه إلى من رأى الواقعة أو سمع عنها أو أدركها بإحدى حواسه فهي وسيلة إثبات تنطوي على وقائع مادية كما أنها على الرغم من ذلك فهي دليل معنوي أو نفسي[1].

وتظهر قوة الشهادة دليلا في جرائم الاعتداء ضد الأشخاص المرتكبة باستخدام تكنولوجيا النظام المعلوماتي المتوفرة في الحاسوب والهاتف النقال وشبكة الانترنت طالما أن هذه الأخيرة من الجرائم المستحدثة التي يصعب على المحقق أن يتوصل إلى دليل تقليدي فيها، وذلك بسبب الصعوبات المتعددة والمتمثلة في قلة الخبرة لدى المحققين بالإضافة إلى سهولة محو الأدلة، وكون الشهادة دليلا في جرائم القذف والسب المرتكبة بإساءة استخدام الحاسوب والهاتف النقال يصعب محوها[2]، وعليه قد تكون الشهادة دليلا لا يمكن إبعاده كونها الدليل الوحيد القائم في الدعوى مما يؤدي إلى تعاظم دورها في إثبات الجرائم في إطار جرائم الإعتداء ضد الأفراد باستعمال تقنية المعلومات ونظم الاتصالات (الحاسوب، الهاتف النقال، الشبكة المعلوماتية

[1] **أمل فاضل عبد حسان، أحمد حمد الله**، الإثبات الجنائي في جرائم إساءة الهاتف النقال، مجلة كلية القانون للعلوم القانونية و السياسية، عدد 07، ص 322.

[2] **المرجع نفسه**، ص 322.

العالمية)، وبالتالي سنتناول الشهادة في نطاق جرائم الاعتداء على الأشخاص المرتكبة بواسطة تكنولوجيات الإعلام والاتصال كالحاسب الألي وأجهزة الهاتف النقال الذكية المتطورة الموصولة بشبكة الانترنت على النحو الآتي.

1. تعريف الشهادة :

هي في الأصل اخبار الشخص بما يكون قد راه أو سمعه بنفسه أو أدركه على وجه العموم بحواسه، ومن ثم فإن الشهادة هي دليل مباشر في الدعوى باعتبارها تنصب على الواقعة مباشرة، فالشهادة يمكن أن تكون مباشرة والتي يقصد بها أن المعلومات التي يدلي بها الشخص وصلت إلى حواسه بصورة مباشرة ودون وساطة شخص أخر. فهذا الشاهد هو من رأى أو سمع[1]، والدليل على ذلك كشهادة أحد الأشخاص بأنه شاهد المتهم يقوم بسب أو قذف شخص بعبارات مخدشة للشرف والاعتبار وذلك عن طريق إجراء مكالمة هاتفية بواسطة هاتفه أو من خلال رسالة الكترونية sms ، إذ أن هذه الشهادة يمكن الأخذ بها قانونا بعد استخلاص ما يثبت ذلك من الشريحة عن طريق استخدام نظام استعادة محتويات شرائح الهاتف. أما بالنسبة للشهادة غير المباشرة (الشهادة السمعية)، فالشاهد هنا لم ير الجاني يرتكب الجريمة أو يسمعه يتوعد أو يهدد المجني عليه، ولكنه سمع من شخص أخر أن الجاني قام بفعل ذلك[2]، كشهادة شخص بأنه سمع أن فلانا قام بتهديد وابتزاز المجني عليها بنشر صور لها مخلة تمس بشرفها وسمعتها على شبكة الانترنت أو عبر مواقع التواصل الاجتماعي.

إن الشاهد في جريمة القذف والسب والتهديد المعلوماتية هو الشاهد الفني صاحب الخبرة والتخصص في تقنية المعلومات(الحاسوب والهاتف النقال....الخ) والذي لديه دراية ومعلومات واسعة للولوج في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تستدعي البحث

[1] **خالد ممدوح إبراهيم**، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية ،2010 ، ص 259.

[2] **عبد الفتاح بيومي حجازي**، أصول التحقيق الجنائي و التأديبي، دار الفكر الجامعي، الإسكندرية، 2005 ، ص 106.

والتنقيب عن أدلة الجريمة داخل الحاسوب أو الهاتف النقال بحيث يطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي[1].

2. تقدير الشهادة عبر الوسائط الإلكترونية :

تتنوع قوانين الأدلة الجنائية في الإثبات الجنائي للجرائم الإلكترونية، بين من يأخذ بقانون الأدلة في ذات الجريمة الإثبات ومن يأخذ قانون الإثبات القائم على حرية المحقق الجنائي في الاقتناع بما يقدم له.

وفي نظام الأدلة الإقناعية للجريمة الإلكترونية مثل: الشهادة والإقرار فإن القاضي لا يقيده المنظم بأدلة إثبات معينة، وإنما يترك له حرية الإثبات وفقا لسلطته التقديرية في تقدير الأدلة و يترتب على ذلك أن للقاضي الجنائي قبول أي دليل يمكن أن يتولد منه اقتناعه و أنه هو الذي يقدر قدرته في الإثبات على قدر اقتناعه[2].

ثالثا- المراقبة الإلكترونية :

طبقا لنص **المادة 04** من **القانون رقم 09-04** المتعلق بالقواعد الخاصة بالرقابة من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي جاء بعنوان مراقبة الاتصال الالكترونية – الحالات التي تسمح باللجوء إلى الرقابة الالكترونية.

1. تعريف المراقبة الإلكترونية :

نجد أن المشرع الجزائري لم يعرف هذا الإجراء من خلال **القانون رقم 09-04** ولهذا سنتطرق للتعريف الفقهي الذي وضع له العديد من التعريفات نذكر منها: "المراقبة الإلكترونية تعتمد على الاتصالات والتسجيل محلها المحادثات الخاصة سواء كانت مباشرة أو غير مباشرة، أي سواء كانت مما يتبادله الناس في مواجهة بعضهم البعض أو عن طريق وسائل الاتصال السلكية واللاسلكية".

---

[1] **علي عدنان الفيلا**، إجراءات التحقيق الابتدائي في الجريمة المعلوماتية، مجلة الحقوق، مجلد 08 ، العدد 12 ، العراق ، 2013 ، ص 476.

[2] **تميم بن عبد الله بن سيف التميمي**، المرجع السابق، ص 204 .

ورأي آخر يرى أن المراقبة هي: "نوع خاص من استراق السمع مسلط على الأحاديث الشخصية والمحادثات"[1] .

2. شروط و آليات المراقبة الإلكترونية :

يمكن أن نستنتج شروط وآليات المراقبة الإلكترونية في التشريع الجزائري[2]، من خلال نص **المادة 65 مكرر 05** من قانون الإجراءات الجزائية على أنها :

– اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

– وضع ترتيبات تقنية دون موافقة المعنيين من أجل بث وتسجيل الكلام المتفوه به بصفة خاصة.

– في حالة توفير المعلومات عن احتمال الاعتداء على المنظومة المعلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

– لمقتضيات التحري والتحقيق القضائي، عندما كان يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

– في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

أما بالنسبة لإجراءات تنفيذ المراقبة الإلكترونية وفقا لما جاء في **القانون رقم 09-04** فنصت عليه **المادة 04** منه[3] وهي:

– الإذن المكتوب، ويتضمن (التعريف والمراقبة، طبيعية الجريمة، تسليم الإذن، كتابة وتحديد المدة التي لا تتجاوز 4 أشهر قابلة للتجديد) .

– طرق التنفيذ، وتشمل:(سرية الإجراءات، التسيير، المحاضر).

---

[1] **أحمد مسعود مريم**، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون 04/09، مذكرة ماجستير، كلية الحقوق و العلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2013، ص 79 .

[2] **عبير بعقيقي، فيصل نسيغة**، المرجع السابق، ص 41-42.

[3] راجع **المادة 04** من قانون رقم 09-04، المرجع السابق.

الفرع الثاني : الإجراءات العامة

تنقسم هذه الإجراءات إلى مجموعتين، وتسمى المجموعة الأولى بإجراءات الأدلة؛ أما الثانية فتعرف بالإجراءات الاحتياطية ضد المتهم. وسنوضح هذا من خلال التطرق إلى المعاينة والتفتيش إلى جانب الاستجواب والخبرة .

أولا- المعاينة :

1.تعريف المعاينة:

عرفها العديد من الفقهاء منه:

الدكتور محمد زكي أبو عامر عرفها بأنها: "الرؤية بالعين لمكان أو شخص أو شيء لإثبات حالة، وضبط كل ما يلزم لكشف الحقيقة".

كما عرفها الدكتور أحمد فتحي سرور بأنها: "إثبات مباشر ومادي لحالة الأشخاص والأمكنة ذات الصلة بالحادث عن طريق رؤيتها أو فحصها فحصا حسيا مباشرا "[1].

من هذه التعريفات يتبين أن المعاينة هي ملاحظة وفحص مباشر لمكان معين أو شخص أو شيء معين، يفيد في كشف الحقيقة وان كانت إجراء يجوز الأخذ به في جميع الجرائم إلا أنها قد تكون غير مجدية في بعضها لأنها إجراء هادف بغرض كشف وصيانة العناصر المادية التي تتعلق بالجريمة .

2.تعريف المعاينة عبر الوسائط الإلكترونية :

يقصد به معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية أو الانترنت وتشمل الرسائل المرسلة منه أو التي يستقبلها وجميع الاتصالات التي تمت من خلال الكمبيوتر والشبكة المعلوماتية[2].

[1] **محمد علي سكيكر**، الجريمة المعلوماتية وكيفية التصدي لها، د.ط، دار الجمهورية للصحافة، مصر، 2010 ، ص 68

[2] **تميم عبد الله بن سيف التميمي**، المرجع السابق، ص 206.

3.إجراءات معاينة الأدلة المعلوماتية في مسرح الجريمة :

الجريمة الإلكترونية مثلها مثل باقي الجرائم الأخرى تحتاج إلى بعض الإجراءات أثناء معاينة الجريمة وأثناء جمع الأدلة المتعلقة بالجريمة بالإضافة إلى بعض الإجراءات الخاصة بالجريمة الإلكترونية، ومن ذلك :

- تصوير الحاسب والأجهزة الطرفية المتصلة به، وكل ما له صلة بالجريمة في مسرح الجريمة ويتم تسجيل وقت وتاريخ ومكان التقاط الصور.
- ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام، حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر على المحكمة .
- التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة ونحوها، والأقراص الممغنطة وترفع البصمات الموجودة عليها .
- التحقيق مع الشهود والأشخاص الذين لهم علاقة بالجريمة. والتحفظ على البيانات والمستندات الموجودة على الجهاز .

وبعد ذلك يأتي دور الخبراء والفنيين في جمع الأدلة الإلكترونية من مسرح الجريمة، أو من تتبع الآثار الإلكترونية التي يمكن من خلالها التوصل إلى المعتدي[1].

ثانيا– التفتيش :

يقتضي الحديث عن تفتيش المعلومات الواقع على التقنيات الحديثة المتمثلة في نظم الكمبيوتر والانترنت، وللإحاطة بكل عناصر التفتيش يجب الاعتماد على التعريف التقليدي للتفتيش وذلك لمعرفة خصوصية التفتيش عن المعلومات التي تختلف عن الإجراءات التحقيقية الأخرى ومن خلال هذا المنطلق سنوضح مفهوم التفتيش من خلال التالي :

1. تعريف التفتيش :

يعرف التفتيش بصفة عامة أنه: << البحث في مستودع سر المتهم أو الإطلاع على محل منحه القانون حماية خاصة، يتمثل هذا المستودع وهذا المحل في جهاز للمعلومات كالكمبيوتر

[1] **تميم عبد الله بن سيف التميمي**، المرجع السابق، ص 213-214.

أو أنظمة الانترنت، وذلك للبحث عن أشياء مادية أو معنوية تفيد في كشف الحقيقة نسبتها إلى المتهم[1] >>.

2. ضوابط التفتيش عبر الوسائط الالكترونية :

نجد ضوابط معينه يجب إتباعها عند التعرض للحريات الشخصية بإجراء من الإجراءات التي تمس حريتهم كالتفتيش، وهدف ذلك هو تحقيق الموازنة بين مصلحه المجتمع كعقاب المجرم وبين حقوق الأفراد وحرياتهم. وتنقسم الضوابط العامة إلى نوعين: ضوابط موضوعية، وضوابط شكلية.

أ. **الضوابط الموضوعية:** يقصد بها الشروط اللازمة لإجراء التفتيش الصحيح ويمكن حصرها في ثلاث ضوابط(السبب، المحل، السلطة المختصة للقيام به).

أ/1. وجود سبب للتفتيش في البيئة الإلكترونية :

سبب التفتيش في الجرائم عموما هو السعي نحو الحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث، ويتمثل في وقوع جريمة ما جناية أو جنحة، اتهام شخص أو أشخاص معنيين بارتكابها أو المشاركة فيها، وتوافر قرائن أو أمارات قوية على وجود أشياء تفيد في كشف الحقيقة لدى المشتبه فيه أو المتهم أو في مسكنه أو بشخص غيره أو مسكنه، وهو ما ينطبق على الجريمة الإلكترونية[2] .

أ/2. محل التفتيش :

يقصد بمحل التفتيش ذلك المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره في الجريمة التقليدية فإن التفتيش ينصب على شخص المتهم أو غير المتهم، وكذلك على مسكن المتهم وما في حكمه وملحقاته[3]، أو على مسكن غير المتهم وما في حكمه وملحقاته

---

[1] **محمودي سماح**، مشكلات التفتيش الجنائي عن المعلومات في الكمبيوتر والانترنت، مجلة الحقوق والعلوم السياسية،العدد 08 ، الجزء الأول، جوان 2017، ص 328.

[2] **لينذا بن طالب**، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، العدد 16، جوان 2017، ص 492.

[3] **قدري عبد الفتاح الشهاوي**، ضوابط التفتيش في التشريع المصري والمقارن، منشأة المعارف، الإسكندرية، 2005، ص 111.

لكن في الجريمة المعلوماتية فإن محل التفتيش هي كل مكونات الحاسوب سواء كانت مادية أو معنوية، وكذلك شبكات الاتصال الخاصة به، كما سبق شرحه وبيانه.

ولكي يتم التفتيش على هذه الحال ينبغي الإشارة إلى أن هذه الأخيرة لا تكون قائمة بذاتها، بل تكون إما موضوعة في مكان ما كالمسكن أو المكتب، أو تكون صحبة مالكها أو حائزها كما هو الشأن في الحاسوب المحمول أو الهاتف النقال الذكي. سبق وأن أشرنا إلى مدى قابلية المكونات المادية والمعنوية للحاسوب وشبكات الاتصال الخاصة به للتفتيش[1].

أ/3. السلطة المختصة بالتفتيش :

إن لتفتيش إجراء من إجراءات التحقيق التي تمس بالحرية الشخصية للأفراد، حرصت التشريعات الجنائية على إسنادها لجهة قضائية تكمل تلك الحريات والحقوق وتضمنها، إلا أن هذه التشريعات لم تسر على نسق واحد فيما يخص تحديد الجهة التي يعهد لها بالتحقيق الابتدائي لتكون صاحبة الاختصاص الأصيل بإجراء التفتيش، فقد ذهبت بعض القوانين كالتشريع المصري إلى منح هذه السلطة للنيابة العامة، حيث لما صدر قانون الإجراءات الجنائية بموجب قانون رقم150 لسنة 1950 عاد مرة أخرى على نظام الجمع بين سلطتي التحقيق والاتهام بيد النيابة العامة باستثناء جرائم معينة. رأى أن يختص بها قاضي التحقيق[2]، بخلاف الحال عند كل من الجزائر وفرنسا حيث أخذا بنظام الفصل بين سلطتي الاتهام والتحقيق، حيث عهدت هذه الأخيرة لقاضي التحقيق أما الأولى فعهدت للنيابة العامة.

أ/4. الإذن بالتفتيش :

غالبا ما يصدر الإذن بتفتيش مسكن المتهم وينصرف هذا الإذن إلى كل ما يتواجد في المسكن، ومن ثم هل يجوز بمقتضى هذا الإذن لضباط الشرطة القضائية الولوج إلى البيئة

[1] **قدري عبد الفتاح الشهاوي**، المرجع السابق، ص 111.

[2] **عائشة بن قارة مصطفى**، حجية الدليل الالكتروني في مجال الإثبات الجنائي– دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2009، ص 63-64.

الرقمية والتغلغل في المنظومة المعلوماتية للبحث عن أدلة إثبات التي يمكن أن تكون محل الضبط؟

في هذه الحالة يرى أغلب الفقهاء أنه يجب أن يحدد إذن التفتيش المكان المراد تفتيشه والشخص أو الأشياء المراد تفتيشها وضبطها(أجهزة الحاسوب، صور جنسية إلكترونية خاصة بالأطفال، مصنفات إلكترونية مقلدة...)، والهدف من هذا التحديد في إذن التفتيش هو تجنب التفتيش الاستكشافي، بحيث لا يترك للمأذون بالتفتيش أي سلطة تقديرية في ذلك، إلا أن هناك صعوبة في احترام هذا الشرط أثناء الممارسة العملية في تفتيش أجهزة الكمبيوتر[1]، ويرجع ذلك إلى الطبيعة الخاصة لهذه الأخيرة. أما المشرع الجزائري في القواعد الخاصة بإجراء التفتيش المعلوماتي الواردة في **قانون رقم 09-04** لا نجده يتحدث عن هذا الشرط، كل ما في الأمر أنه تحدث عن إعلام جهات التحقيق السلطة القضائية المختصة في حالة تمديد التفتيش إلى منظومة معلوماتية أخرى.

ب. الضوابط الشكلية :

إن هذه الضوابط أو الشروط الشكلية لا تهدف إلى تحقيق مصلحة العدالة في ضمان صحة الإجراءات التي تتخذ لجمع الأدلة فحسب، بل تقيم بالإضافة إلى مقتضيات الإجراء سياجا يحمي حقوق والحريات الفردية. وتتمثل هذه الضوابط الشكلية في:

ب/1. إجراء التفتيش بالحضور الضروري لبعض الأشخاص المعنيين بالقانون :

يعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون في الجرائم التقليدية، وذلك لضمان الإطمئنان على سلامة الإجراء الغني عن البيان أن التفتيش فيه اطلاع على أسرار الغير. فبالنسبة لتفتيش الأشخاص لم تشترط التشريعات الإجرائية لصحته حضور شهود عند تفتيشهم، أما فيما يتعلق بتفتيش المساكن؛ ينص القانون الجزائري على وجوب حصول إجراء التفتيش المتعلق بالمساكن أو ملحقاتها بحضور المشتبه فيه أو المتهم عندما يتم تفتيش مسكنه –سواء من طرف قاضي التحقيق أو ضابط الشرطة القضائية – وإذا تعذر ذلك بامتناعه عن

[1] **عائشة بن قارة مصطفى**، المرجع السابق، ص 63.

حضور التفتيش أو كان هاربا، يتم هذا الإجراء بحضور شاهدين من غير الموظفين الخاضعين لسلطة القائم بالتفتيش[1].

ويلاحظ أن التعديل الذي أدخله المشرع الجزائري على قانون الإجراءات الجزائية بموجب **القانون رقم 06-22** في **المادة 45** منه[2]، حيث استغنى على ضمانة حضور الأشخاص المحددين في الفقرة الأولى في جرائم معينة منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، والحكمة من ذلك ترجع إلى ضرورة إضفاء نوع من السرية أثناء جمع الدليل الإلكتروني، خاصة وأن هذا الدليل ذو طبيعة خاصة من حيث سرعة تعديله والتلاعب فيه حتى عن بعد. كما أن هذه الضمانة بدأت تتضاءل أهميتها في الدول التي تأخذ بنظام التفتيش عن بعد، أو ما يطلق عليه الفقه الفرنسي " التفتيش على المباشر".

ب/2 الميعاد الزمني لإجراء التفتيش في الجرائم المعلوماتية :

يقصد بشرط الميعاد الزمني في التفتيش، أن يجريه القائم به خلال فترة زمنية عادة ما يحددها المشرع، وذلك حرصا على تضييق نطاق الاعتداء على الحرية الفردية وحرمة المسكن . إنّ القانون الجزائري يحظر تفتيش المنازل وما في حكمهما في وقت معين[3]، وهو محدد في القانون الإجراءات الجزائية من خلال **المادة 47** من الساعة الخامسة صباحا على الساعة الثامنة مساءا، وهناك حالات استثنائية يجوز فيها الخروج عن هذه المواعيد ويصح إجراء التفتيش في أي ساعة من ساعات الليل والنهار[4].

وأن المشرع الجزائري قد أورد في قانون الإجراءات الجنائية **المادة 3/64** أنه: << عندما يتعلق الأمر بتحقيق جار في إحدى الجرائم المذكورة في **المادة 3/47** ، وكذا أحكام **المادة 47مكرر** حيث أجاز التفتيش في كل محل سكني أو غير سكني في كل ساعة من ساعات

---

[1] راجع **المادة 45** من أمر رقم 66-155 ، المرجع السابق .

[2] **قانون رقم 06-22** مؤرخ في 2006/12/20 يعدل ويتمم الأمر رقم 66-155 ، يتضمن قانون الإجراءات الجزائية، ج.ر، عدد 84، صادر بتاريخ2006/12/24

[3] **عائشة بن قارة مصطفى**، المرجع السابق، ص493.

[4] راجع **المادة 47** من أمر رقم 66-155، المرجع السابق.

النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص >> من قانون الإجراءات الجزائية[1]، حيث استثنى تطبيق هذه الضمانات على طائفة من الجرائم المذكورة في هذه المادة من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

والملاحظ أن المشرع غلب في هذه الحالة مصلحة المجتمع في تحقيق العدالة على مصلحة الأفراد في حقهم على الحفاظ على حرمتهم الخاصة لاسيما حرمة المسكن باعتباره مستودع أسرارهم، إلا أن ما يبرره ويقل من خطورته الطبيعة الخاصة لهذه الجرائم خاصة الجريمة الإلكترونية وطبيعة الدليل لإثباتها فهو قابل للمحو والتعديل في أقل من ثانية لأن مرتكبها ذو دراية بالأمور التقنية، وما يزيد من الصعوبة إذا كان هذا الدليل الإلكتروني هو الوحيد في الدعوة الجنائية. أما بالنسبة للأماكن العامة، فإذا وجد الشخص في هذه الأماكن وهو يحمل معه مكونات الحاسوب سالفة الذكر أو كان مسيطرا عليها أو حائزا لها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال[2].

ب/3 محضر التفتيش في الجرائم المعلوماتية :

باعتبار أن التفتيش من أعمال التحقيق، لا بد من تحرير محضر يثبت فيه ما أسفر التفتيش عنه من أدلة والقانون لم يتطلب شكلا خاصا، وبالتالي لصحة محضر تفتيش نظم الحاسوب لا يشترط سوى ما تستوجبه القواعد العامة في المحاضر عموما، بأن يكونا مكتوبا باللغة الرسمية وأن يكون مؤرخا وموقعا عليه، كما يجب أن يتضمن كافة الإجراءات المتبعة من طرف الشخص المتخصص في الحاسوب والإنترنت الذي تم الاستعانة به في مجال الخبرة الفنية الضرورية[3].

---

[1] راجع **المادة 64** من أمر رقم 66-155، المرجع نفسه.

[2] **عائشة بن قارة مصطفى**، المرجع السابق، ص493-494.

[3] **المرجع نفسه**، ص 494 .

ثالثا– الاستجواب :

إن الاستجواب، يعتبر مرحلة مهمة في إجراءات التحقيق، حيث يتم الحصول على اعترافات أو معلومات تمكن القائمين على الاستجواب من التأكد من ارتكاب الجريمة من الشخص المستوجب أو عدم وجود أي علاقة بينه وبين الجريمة المرتكبة. إذ يتم مناقشة الشخص المستوجب حول وقائع الجريمة وتفاصيلها، ومطالبته له بإبداء رأيه في الأدلة القائمة ضده إما تفنيدا وإما تسليما، وذلك قصد الكشف عن الحقيقة واستظهارها بالطرق القانونية[1].

إن الإجراءات المقررة للاستجواب في الجريمة المعلوماتية تحكمها نفس الضوابط المقررة لاستجواب المتهم في جريمة تقليدية، لكن الفرق يكمن في ضرورة تأهيل السلطة المختصة التي تتولى إجراءات الاستجواب، ذلك أن جهات التحقيق لابد أن تكون مؤهلة للتحقيق في جرائم المعلوماتية حتى يمكن استيعاب واقعة التحقيق والتعامل مع مفردات الجريمة، سيما وأن المجرم الذي ارتكب الجريمة والذي يحقق معه ليس بمجرم عادي.

رابعا– الخبرة :

تعتبر الخبرة من بين أهم الإجراءات التي ينبغي الاهتمام بها في إطار التحقيق في الجريمة المعلوماتية، وذلك راجع إلى صعوبة التعامل مع هذا النوع من الجرائم وعدم الدراية بمجالاتها التقنية والمعرفية والفنية.

إذ تقتضي عمليات البحث الجنائي والتحقيق في جرائم الانترنت الاستعانة بخبرات عديدة ومتنوعة، ويتم اعتماد الخبراء بالارتكاز على نوعية الأساليب المستخدمة في الارتكاب (التلاعب بالبيانات، التلاعب في البرامج الأساسية أو برامج التطبيقات، الغش أثناء نقل وبث البيانات، تزوير المستندات المدخلة في أنظمة الحاسبات الآلية أو الناتجة بعد المعالجة)[2].

[1] **محمد حدة**، ضمانات المتهم أثناء التحقيق، الجزء الثالث، الطبعة الأولى، دار الهدى، 1992، ص 306 .

[2] **صغير يوسف**، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق و العلوم السياسية، جامعة مولود معمري-تيزي وزو، 2013، ص 90.

ويتعين على الخبير في الجرائم المرتكبة عبر الانترنت التنسيق مع المحقق الجنائي في هذه الجريمة، بما في ذلك حصر الأدلة المتوفرة وترتيبها وفقا لأهمية كل دليل أو بيئة أو قرينة، كما يجب على المحقق الجنائي أن يشرح للخبراء الجوانب القانونية لطبيعة عملهم مع التأكيد على ربط الأدلة والخبرة العلمية بعناصر وأركان الجريمة المقام عنها الدعوى الجنائية ضد المتهم[1].

المطلب الثاني

مرحلة المحاكمة

من المؤكد أن الجريمة الإلكترونية لا يمكنها أن تبقى حبيسة أو رهينة التحقيق أو التحريات إذ لا بد أن تدخل في مرحلة جديدة، لتصل إلى أروقة المحاكم التي تختص بمحاكمة أو متابعة مرتكبي الجريمة المعلوماتية، وبالتالي وجود جهاز قضائي من أجل محاكمة هؤلاء المجرمين لذلك وجد جهاز قضائي جديد يختص بالفصل في الجرائم الإلكترونية، وذلك نظرا لخطورتها وهو ما يعرف بالقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .

وسنوضح مرحلة المحاكمة من خلال التطرق إلى تشكيلة واختصاص المحكمة في الجريمة الإلكترونية (**الفرع الأول**)، ومن ثم التطرق إلى القواعد العامة للمحاكمة(**الفرع الثاني**) .

الفرع الأول : تشكيلة واختصاص المحكمة في الجريمة الإلكترونية

أولا- تشكيلة المحكمة :

تختلف تشكيلة المحكمة الجزائية بحسب نوع قسم الجنح خاصة الجريمة الإلكترونية على مستوى المحكمة. وينشأ على مستوى محكمة مقر مجلس قضاء الجزائر العاصمة قطب جزائي وطني متخصص في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها[2]،

[1] **عبد الفتاح بيومي حجازي**، الدليل الجنائي و التزوير في جرائم الكمبيوتر والانترنت – دراسة معمقة في جرائم الحاسب الآلي، بهجات للطباعة و النشر، مصر، 2009، ص 99 .

[2] **بن عميور أمينة ، بوحليس إلهام** ، المرجع السابق ، ص 73 .

أي كل جريمة ترتكب أو يسهل ارتكابها باستعمال منظومة معلوماتية أو نظام الاتصالات الالكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال .

وبالرجوع إلى **المادة 211 مكرر 24** نجد أن القطب الجزائي الوطني يتشكل من وكيل الجمهورية وقاضي التحقيق ورئيس ذات القطب، توكل لهم مهمة حصرية تكمن في المتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكذا الجرائم المرتبطة بها[1]

ثانيا- اختصاص المحكمة في الجريمة الإلكترونية :

سبق للمشرع بموجب القانون **رقم 04-14**[2] أنه نص على جواز تمديد الاختصاص المحلي لبعض المحاكم المذكورة على سبيل الحصر إلى دائرة اختصاص محاكم أخرى حيث خصها بنوع محدد من الجرائم الخطيرة والمعقدة.

والقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال واحدٌ من هذه الأقطاب الجزائية، حيث أخضعه المشرع لقواعد اختصاص مختلفة نحتاج لتحديدها إلى كل من الاختصاص المحلي والنوعي[3].

1. الاختصاص المحلي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال:

يتمثل الاختصاص المحلي في الأصل حسب ما جاء في نص **المادة 329 فقرة 01** من قانون الإجراءات الجزائية، والتي جاء فيها ما يلي: "تختص محليا بالنظر في الجنحة محكمة محلّ الجريمة أو محكمة محل إقامة أحد المتهمين أو شركاؤهم أو محل القبض عليهم، ولو كان هذا القبض لسبب آخر."

---

[1] راجع المادة **211 مكرر 22 و المادة 211 مكرر 24** من أمر رقم 11/21، المرجع السابق.

[2] قانون **رقم 04-14** المؤرخ في 10 نوفمبر 2004، المعدل للأمر رقم 66-155 المؤرخ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية، ج.ر، عدد71، الصادر في 2006.

[3] **بن عميور أمينة، بوحليس إلهام**، المرجع السابق، ص 74 .

ومع هذا وضع المشرع استثناء نصت عليه **الفقرة 05** من المادة نفسها والتي جاء فيها ما يلي: "يجوز تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف."

وبخصوص الاختصاص بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب اختصاص محلي موسع يبرر الخروج عن معايير الاختصاص الأصلية[1]، وهذا ما أكده المشرع في نص **المادة 211 مكرر 23** من القانون رقم 21-11 السابق الذكر، والتي جاء فيها ما يلي: "يمارس وكيل الجهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب صلاحيتهم في كامل التراب الوطني."

ويقصد أن المشرع منح للقطب الجزائي المذكور اختصاصا إقليميا وطنيا، كما أنه وبموجب نص **المادة 211 مكرر 26** من نفس القانون خول المشرع القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال اختصاصا حصريا فيما يخص الجرائم التي حددتها **المادتين 211 مكرر 24 و 211 مكرر 25** في كافة أنحاء التراب الوطني دون سواه، و ذلك بالنظر إلى خصوصية تلك الجرائم التي وجد من أجلها وبموجب تشكيلة قضاة متخصصة في هذا النوع من الجرائم التي تتسم بالخطورة والتعقيد والتي تمتد إلى خارج حدود الدولة الجزائرية[2]، وبالإضافة إلى الاختصاص الحصري للقطب الجزائي الوطني، يقوم اختصاص هذا الأخير حسب **نص المادة211 مكرر 27** والتي يمتد الاختصاص المحلي بها لوكيل الجمهورية إلى دائرة اختصاص مجاكم أخرى، كذلك الشأن بالنسبة لقاضي التحقيق[3] .

---

[1] **بن عمير أمينة، بوحليس إلهام**، المرجع السابق، ص 74 .

[2] **المرجع نفسه**، ص 74-75 .

[3] راجع المادة **211 مكرر27** من أمر رقم 21-11 ، المرجع السابق .

2. الاختصاص النوعي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال :

يقصد به أن تكون الجهة الجزائية مختصة بنوع واحد من الجرائم التي يحددها القانون وذلك من حيث طبيعتها أو جسامتها[1] وعليه قام المشرع الجزائري بإنشاء القطب الجزائي الوطني المتخصص، ومنح له صلاحية الفصل بشكل حصري في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكذا الجرائم المرتبطة بها، وذلك من خلال نص **المادة 211 مكرر 24**، وكذا الجرائم الأكثر تعقيدا .

بالإضافة إلى هذا مدّ المشرع اختصاص القطب الجزائي الحصري إلى النظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا أو المرتبطة بها أيضا وذلك على أساس تعدد الفاعلين أو الشركاء، أو المتضررين بسبب اتساع ارتكابها، أو لطابعها المنظم الذي قد يكون عابر للحدود الوطنية أو لمساسها بالنظام والأمن العموميين والتي تستوجب المساعدة والتعاون القضائي الدولي لما تتطلبه من وسائل تحري خاصة وفنية[2]، حيث أنه سب وأن وسع الاختصاص في مجال المساعدة والتعاون القضائي الدولي في النظر للجرائم المتصلة بتكنولوجيات الإعلام والاتصال للجهة القضائية المختصة بها والمرتكبة خارج الحدود الوطنية متى كان مرتكبها أجنبيا وتستهدف مؤسسات الدولة والدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

الفرع الثاني : قواعد وإجراءات سير المحاكمة في الجريمة الإلكترونية

أولا- القواعد العامة للمحاكمة في الجريمة الإلكترونية :

لا تختلف إجراءات سير المحاكمة في الجرائم الإلكترونية عن الإجراءات المتبعة في غيرها من الجرائم غير أن ارتباط الجريمة الالكترونية بتقنيات ومصطلحات فنية وعلمية قد

[1] **بوعزة نضيرة**، المحاكم ذات الاختصاص المحلي الموسع كآلية لمكافحة الإجرام الخطير، مجلة ميلاف للبحوث و الدراسات، المجلد 07، العدد 01، جوان 2021، ص 184 .

[2] راجع المادة **211 مكرر 25** من أمر رقم 21-11 ، المرجع السابق .

تشكل صعوبة في وجه القضاة أثناء نظرهم في الدعوى المتعلقة بهذا النوع من الجرائم، وهذا ما أدى إلى ضرورة أن تسبق مرحلة المحاكمة مرحلة تحضيرية يتم من خلالها توضيح ما قد يكشف هذه الجرائم من غموض .

تنفذ المحاكمة بمجموعة من المبادئ تنطبق على المحكمة الجزائية لقسم الجنح على مستوى المحكمة أو الغرفة الجزائية، سنوضح هذه المبادئ من خلال التالي:

1. علانية الجلسات :

جل التشريعات تقر بمبدأ علانية الجلسة، وذلك أن العلانية تسمح للجمهور بمراقبة عمل المحكمة ومنه الإطمئنان والشعور بالعدالة وهذا على التحقيق الأولي الذي تقوم به ضباط الشرطة القضائية وكذا التحقيق الإبتدائي الذي تقوم به الجهات التحقيق، فكلاهم يتم في سرية، إلا أن العلانية ليست في جميع الجلسات بل القاضي سلطة تقديرية في إخراج القصر من الجلسة، كما يمكن أن تكون الجلسة سرية إذا كان في علانيتها خطر على النظام العام والآداب العامة، إلا أن هذا الحكم يجب أن يصدر في جلسة علنية[1]، ويحكم هذا المبدأ نص **المادة 285**من قانون الإجراءات الجزائية الجزائري.

2. **شفوية المرافعات:**

لأطراف الخصومة الحق في مناقشة كل دليل يعرض بالجلسة حتى يتمكن الجميع من الدفاع عن نفسه ولا يتم الإكتفاء بالتحقيقات الأولية والإبتدائية التي سبقت المحاكمة.

3. حضور أطراف الخصومة :

لا يجوز إجراء المحاكمة دون أطراف الخصومة لذلك أوجب المشرع حضور كل من الضحية والمتهم أما بالنسبة للنيابة فهي جزء من التشكيلة.

[1] **بعرة سعيدة**، الجريمة الإلكترونية في التشريع الجزائري-دراسة مقارنة، مذكرة لنيل شهادة الماستر، جامعة محمد خيضر بسكرة،2015-2016، ص 96 .

4. تدوين التحقيق النهائي :

لا يمكن للمحكمة أن تنعقد في حالة غياب أمين الضبط لأن دوره يتجسد في تدوين كل ما يدور بالجلسة وفي الأخير نستنتج أن الجريمة الإلكترونية لم يخص لها إجراءات المتابعة خاصة بها وإنما تخضع نفس إجراء الجريمة التقليدية[1].

ثانيا- إجراءات سير المحاكمة في الجريمة الإلكترونية :

تستهل المحكمة جلستها بالإعلان أولا عن افتتاحها بالقول باسم الشعب الجزائري الجلسة مفتوحة، ثم المناداة على أطراف الخصومة بداية بالمتهم والضحية والشهود والمسؤول المدني والتأكد من حضورهم أو غيابهم، ثم يتم التحقيق من هوية المتهم وتبليغه بالتهمة المنسوبة إليه والمادة القانونية المتابع بها، وإذا كانت الدعوى غير مهيأة للحكم أمرت المحكمة بتأجيلها إلى أقرب جلسة، وفي هذه الحالة وطبقا لأحكام **المادة 339 مكرر6** المستحدثة بموجب **الأمر رقم 15-02** المؤرخ في المؤرخ في 23 جويلية 2015 من قانون الإجراءات الجزائية[2]، تتخذ المحكمة إحدى الإجراءات التالية:

(ترك المتهم حرا، إخضاع المتهم لتدابير أكثر من تدابير الرقابة القضائية المنصوص عليها في **المادة 125 مكرر1** من قانون الإجراءات الجزائية الجزائري، وضع المتهم في الحبس المؤقت).

ومع الإشارة إلى أن هذه التدابير لا تقبل الاستئناف، فإذا كان المتهم قد سبق حبسه من طرف قاضي التحقيق عن طريق الحبس المؤقت أو بموجب إجراءات المثول الفردي؛فإنه يساق بواسطة القوة العمومية لحضور الجلسة ويخطره رئيس الجلسة بأن له الحق في اختيار محام الدفاع عنه فإن طلب ذلك أمهله القاضي مهلة لا تقل عن ثلاثة أيام ليحضر دفاعه ثم يواجه القاضي المتهم بكل الأدلة القائمة ضده، ويتم مناقشتها بالتفصيل من طرف القاضي وبعدها يقوم القاضي بسماع الشهود، وبعد الانتهاء من التحقيق تعطى الكلمة للطرف المدني فقط دون

[1] **بعرة سعيدة**، المرجع السابق، ص 96.

[2] راجع **المادة 339 مكرر6** من أمر رقم 66-155، المرجع السابق .

المطالبة بالعقوبات الجزائية، لتقوم بعد ذلك النيابة العامة بالمرافعة وتقديم التماساته في الشق الجزائي فقط.

وفي الأخير يقوم دفاع المتهم بتقديم مرافعته وتقديم إلتماساته، ويكون بعدها لنيابة العامة والمدعى حق الرد على موافقة محامي المتهم، وتعطى الكلمة الأخيرة بعدها للمتهم ومحاميه ثم يعلن رئيس الجلسة إقفال باب المرافعات ويصدر حكمه في نفس الجلسة أو يحدد تاريخ لاحق ليتم النطق بالحكم[1].

[1] **محمد بوعمرة، سيدعلي بنينال،** جهاز التحقيق القضائي في الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، جامعة آكلي محند اولحاج –البويرة، 2019-2020، ص 50.

المبحث الثاني

صعوبات وآليات مكافحة الجريمة الإلكترونية

إن مكافحة الجريمة الإلكترونية ليست بالأمر الهين نظرا لخصوصية مرتكب الجريمة الإلكترونية في جد ذاتها، وكون المجرم المعلوماتي يتميز بذكاء خارق فإن هذا يصعب من الكشف عليه باستعمال وسائل التفتيش التقليدية، كما أن إثبات الجريمة الإلكترونية من الأمور الصعبة، نظرا لصبغتها اللامادية وهو ما يتطلب اعتماد أشخاص مدربين ومختصين في تعقب الدليل الرقمي. فالكثير من المشاكل التي تؤثر على عملية التحقيق تؤدي بها إلى الخروج بنتائج تنعكس على نفسية المحقق بفقدان الثقة في نفسه وفي أدائه وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون الغير القادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها، وانعكاسها أيضا على المجرم نفسه فإن الجهات الأمنية غير قادرة على اكتشاف أمره.

ثم إن الجهود الدولية والعربية جاءت كآلية لمكافحة الجرائم الإلكترونية فهي داعمة للجهود التي تبذلها مختلف الدول في تشريعاتها الداخلية، فهي بمثابة قوانين استرشادية تأخذ بها الدول لمواجهة الجرائم المستحدثة بما فيها تلك المرتكبة عبر الوسائط الإلكترونية. فهناك العديد من الدول التي اتخذت سبيل تطوير قانون العقوبات، كما هناك دول ارتأت إفرادها بقوانين خاصة.

ومن هذا المنطلق سنتناول صعوبات مكافحة الجريمة الإلكترونية(**المطلب الأول**)، إضافة إلى توضيح آليات مكافحة الجريمة الإلكترونية (**المطلب الثاني**).

المطلب الأول

صعوبات مكافحة الجريمة الإلكترونية

هناك العديد من الجهود المبذولة للحد من الجريمة المعلوماتية، إما من قبل المشرعين أو من قبل سلطات التحقيق والضبطية القضائية دولية كانت أو داخلية، إلا أن هذه الجهود تصطدم بالعديد من العراقيل والصعوبات من بينها صعوبات اكتشاف وإثبات الجريمة الالكترونية وذلك يرجع إلى طبيعتها اللامادية أساسا والصعوبات المتعلقة بالجانب القضائي والمتعلقة بالقانون الواجب التطبيق[1] .

تثير الجريمة الالكترونية عدة صعوبات تحول دون مكافحتها بشكل ناجع، سنوضح هذه الصعوبات من خلال التطرق إلى صعوبات الاكتشاف (**الفرع الأول**)، ومن ثم التطرق إلى صعوبات الإثبات (**الفرع الثاني**).

الفرع الأول: صعوبات الاكتشاف

إن اكتشاف الجرائم المعلوماتية أمر في غاية الصعوبة، مما يحتم على المشرع أو المحقق القضائي تدارك هاته المعوقات من أجل درء هذه الجريمة وكذا حماية الأفراد منها، ومن هاته الصعوبات نجد :

أولا- فقدان الآثار التقليدية للجريمة الإلكترونية :

وهو من بين ما يميزها عن باقي الجرائم، وارتكابها يتم دون أن يشعر بها القائمون على تشغيل الأجهزة المعلوماتية، مما يبقي هاته الجريمة مجهولة ما لم يبلغ عنها للجهات المعنية بالتحقيق الجنائي. كما أن البيانات والمعلومات التي تشتمل عليها لا تتضمن آثار أو بصمات يمكن التعرف من خلالها على مرتكب هذه الجريمة .

[1] **فريجة محمد هشام**، النظام القانوني للجريمة المعلوماتية – صعوبات تحقيق الأمن الإلكتروني، حوليات جامعة قالمة للعلوم الاجتماعية والإنسانية، العدد 24 ، جوان 2018 ، ص 150 .

ثانيا– تعمد الجناة إلى تدابير أمنية من أجل إخفاء جرائمهم :

وهذا عن طريق التلاعب بالقواعد والبيانات والبرامج في الكمبيوتر، خاصة وأن التخزين الإلكتروني غير مرئي ومكتوب بلغة الأرقام، أو فرض تدابير احترازية من أجل عدم تسهيل إجراءات التفتيش التي يتوقع الجناة حدوثها كاستخدام كلمات السر، أو إعطاء تعليمات خفية بين هذه البيانات أو تشفيرها حتى يستحيل على جهات التحري والبحث الوصول إلى كشف هاته الأفعال غير المشروعة؛ مما يشكل عقبة أمام إقامة الدليل على الجريمة الإلكترونية وإثباتها[1].

ثالثا– التكتم على الجريمة المعلوماتية من قبل الجهات المجني عليها :

تحرص هاته الجهات والتي غالبا ما تكون مصرفا أو مؤسسة مالية أو شركة على التكتم وعدم الإبلاغ على مثل هذه الجرائم التي راحت ضحيتها، خوفا من الخسائر التي يمكن أن تتكبدها جراء هذا الإبلاغ، أو حتى قد يتوخى بعض المجني عليهم من وراء العزوف عن الإبلاغ عدم إتاحة الفرصة للأجهزة الأمنية من الاطلاع على معلومات لم يجر الابلاغ عنها[2].

ومنه عدم تبليغ السلطات المختصة في مكافحة هذه الجريمة يبقيها مستترة ما لم يتم الإبلاغ عنها، و من ثم فالصعوبات التي نواجه أجهزة الأمن و المحققين هو أن هذه الجرائم لا تصل إلى علم السلطات المعنية بالصورة التي تحكم الجريمة التقليدية .

رابعا– نقص الخبرة لدى جهات التحقيق والتحري :

بالنظر إلى التكوين والخبرات المكتسبة لرجال الضبط القضائي، وسلطات التحقيق والتحري مقارنة بحداثة الجرائم وتقنياتها العالية، نجدها تتطلب من القائمين على البحث والتحري إلمام

[1] **فريد منعم صبور**، حماية المستهلك عبر الانترنت ومكافحة الجرائم الإلكترونية- دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2010 ، ص 32 .

[2] **موسى مسعود أرحومة**، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2009، ص 05 .

كافي بها وخبرة فنية في مجال الجريمة المعلوماتية والنظم الإلكترونية والبيانات ولا يكفي أن تكون لهم الخافية القانونية فقط، بل هذا الأخير يمكن أن يكون بدوره العنصر المحفز والمساعد لمرتكبي الجرائم المعلوماتية[1] .

كما أنه من بين التحديات والمشاكل التي تواجه أجهزة الأمن وأجهزة العدالة الجنائية في جرائم الانترنت، وأن الجناة في هذه الجرائم لهم مفردات ومصطلحات خاصة بهم لدرجة أنهم يطلقون على أنفسهم اسم النخبة بدعوى أنهم الأكثر دراية ومعرفة بعالم الانترنت وأسرار الكمبيوتر ولغاته.

الفرع الثاني : صعوبات الإثبات

إن الجريمة المعلوماتية في صفتها تتميز بالخفاء وعدم تركها لآثار مادية يمكن متابعتها، كما تتسم بالخطورة وصعوبة الاكتشاف، ثم إن ما يميز الجريمة المعلوماتية هو صعوبة تحديد مكان وقوعها أو مكان التعامل معها بسبب اتساع نطاقها المكاني وتعدد مرتكبيها ووسائل استعمالها وضخامة بياناتها.

وترجع صعوبة إثبات الجريمة المعلوماتية إلى عدة أمور منها ما يلي :

أولا- غياب الدليل المادي للجريمة:

إن الطبيعة غير المرئية للجريمة الإلكترونية أو الأدلة المتحصل عليها من خلال هاته الجريمة تعتبر أحد أبرز المشكلات التي تلقي بظلالها على جهات الأمن والملاحقة والمحققين، خاصة إن قلنا بأن أغلب المعلومات والبيانات التي يتم تداولها عبر الكمبيوتر والتي من خلالها تتم العمليات الإلكترونية تكون في صورة رموز وأرقام مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال جهاز الكمبيوتر. ومنه فالجرائم التي ترتكب

[1] **عبد الفتاح بيومي حجازي** ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص 122.

على العمليات الإلكترونية، والتي تعتمد في موضوعها على التشفير والأرقام السرية والتخزين الإلكتروني، يصعب أن تخلف وراءها آثار مرئية تكشف عنها أو يستدل من خلالها على المجرمين المعلوماتيين[1] .

ثانيا- سهولة إخفاء الدليل وإعاقة الوصول إليه :

حيث أنه يمكن للمجرم المعلوماتي أن يجعل من الصعب الاحتفاظ بدليل الجريمة الإلكترونية كما يمكنه في أقل من ثانية أن يمسح أو يغير البيانات والمعلومات الموجودة في الكمبيوتر، على خلاف الجرائم التقليدية المادية التي لا يمكن محو آثارها هذا من جهة. ومن جهة فإن الجريمة المعلوماتية تحتاج إلى خبرة فنية، ويصعب على المحقق التقليدي التوصل إليها، إذ تتطلب إلمام خاص بتقنيات الكمبيوتر ونظم المعلومات سواء لارتكابها أو التحقيق فيها أو حتى من أجل ضمان ملاحقة قضائية فعالة[2] .

ثالثا- صعوبات إثبات الجريمة الإلكترونية في قلة الإبلاغ عن وقوعها :

غالبا لا يتم الإبلاغ عن الجرائم المعلوماتية إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير، بل ويصعب حتى كشفها وحصرها ومتابعة مرتكبيها.

كما أن الصعوبة تتمثل في الاعتماد على الخداع في ارتكابها ثم إن الخاصية التي تميزها هو الذكاء في ارتكابها، ذلك أن الإجرام الالكتروني هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، كما أن المجرم الإلكتروني ذو مهارات تقنية عالية وإلمام بتكنولوجيا النظم المعلوماتية وهو ما يزيد من صعوبة الأمر[3].

---

[1] **غازي عبد الرحمن، هيان الرشيد**، الحماية القانونية من جرائم المعلوماتية (الحاسب و الانترنت)، أطروحة لنيل شهادة الدكتوراه في القانون، كلية الحقوق، الجامعة الاسلامية في لبنان، 2004، ص 539 .

[2] **فريجة محمد هشام**، المرجع السابق ، ص 153 .

[3] **أحمد خليفة الملط**، الجرائم المعلوماتية، دار الفكر الجامعي، د.ب.ن، سنة 2005، ص 28 .

المطلب الثاني

آليات مكافحة الجريمة الإلكترونية

رغم الايجابيات التي أتى بها التطور في العلوم وانتشار تقنيات تكنولوجيا المعلومات أدى من جهة أخرى إلى ظهور نوع جديد من الجرائم والتي تعرف بالجرائم الإلكترونية وتعتبر كنتيجة حتمية للانفتاح العالمي ولكل تقدم مستحدث، ونظرا لسرعة تنفيذ وسهولة الإخفاء للجريمة وتعدد صورها وأشكالها أصبحت تتم وتنظم إلكترونيا مما أضفى عليها صعوبة الملاحقة.

حيث يتخطى هذا النوع المستجد من الجرائم في أغلب الأحيان حدود الدول، فبات من الضروري أمر مكافحة الجريمة الإلكترونية باعتبارها تهدد كيان المجتمعات مما جعل العديد من الدول تسارع لتطوير بنيتها التشريعية، ونظرا للتزايد المستمر لهذا النوع المستحدث في الإجرام ولعجز القوانين العقابية التقليدية على احتواء هذه الظاهرة المستحدثة.

ومن خلال هذا المنطلق سنوضح في هذا المطلب آليات مكافحة الجريمة الإلكترونية من خلال التطرق إلى المكافحة التشريعية للجريمة الإلكترونية(**الفرع الأول**)، ومن ثم التطرق إلى المكافحة الدولية (**الفرع الثاني**)، إضافة إلى التعاون الدولي لمكافحة الجريمة الإلكترونية (**الفرع الثالث**).

الفرع الأول : المكافحة التشريعية للجريمة الإلكترونية

رغبة من المشرع الجزائري في التصدي لظاهرة الإجرام الإلكتروني ما يصاحبها من أضرار معتبرة على الأفراد وعلى مؤسسات الدولة من جهة، ومحاولة منه لتدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى، عمد منذ الألفية الثانية إلى تعديل العديد من

القوانين الوطنية بما فيها التشريعات العقابية على رأسها قانون العقوبا ، وقام باستحداث قوانين أخرى خاصة لضمان الحماية الجنائية للأشخاص[1].

نتناول في هذا الفرع مظاهر مكافحة المشرع الجزائري للجريمة الإلكترونية من خلال التطرق إلى دور القوانين العامة في مكافحة الجريمة الإلكترونية (**أولا**)، وصولا إلى دراسة الهياكل الخاصة لمكافحة الجريمة الإلكترونية (**ثانيا**).

أولا- مكافحة الجريمة الإلكترونية بموجب القوانين العامة :

حاول المشرع الجزائري، إصدار قوانين عامة وخاصة وهياكل وأجهزة للتصدي للجرائم الإلكترونية، فهناك جهود معتبرة قام بها المشرع الجزائري في محاربة قراصنة الانترنت وإحالتهم قانونا على المحاكم، متأثرا بجل الدول العربية التي وضعت قوانين لمكافحة الجريمة الإلكترونية، ومن أهم الأمور التي أولها المشرع الجزائري أهمية قصوى أمن الدولة والحفاظ على النظام العام.

1. مكافحة الجريمة الإلكترونية بموجب الدستور الجزائري والقانون المدني :

أ. مكافحة الجريمة الإلكترونية بموجب الدستور الجزائري :

لقد كفل دستور الجزائر لسنة 1996 وكذا التعديل الطارئ عليه بموجب القانون المعدل لسنة2020 حماية حقوق الأساسية والحريات الفردية، وعلى أن تضمن الدولة عدم انتهاك حرمة الإنسان، وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجنائية وقوانين خاصة أخرى والتي تحظر كل مساس بهذه الحقوق، ومن أهم المبادئ الدستورية العامة:

المادة 38: الحريات الأساسية وحقوق الإنسان والمواطن مضمونة.

[1] **بوضياف اسمهان**، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، سبتمبر 2018، ص 360 .

المادة 44: حرية الابتكار الفكري والفني والعلمي مضمونة للمواطن، حقوق المؤلف يحميها القانون.

لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي، الحريات الأكاديمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون[1] .

كما تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة للتنمية المستدامة للأمة. إذ لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، كما أن القانون يحمي سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة .أن القانون يحمي حقوق المؤلف ولا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا أمر قضائي[2].

ب.مكافحة الجريمة الإلكترونية بموجب القانون المدني الجزائري:

ترتيبا على الأهمية الدستورية لحرمة الحياة الخاصة فقد سارع المشرع ونص على أن لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر، في **المادة 124** من التقنين المدني الجزائري "**كل عمل أيا كان يرتكبه المرء يسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض**" وقد جاء هذا النص عاما وشاملا لأي اعتداء يقع على أي حق من الحقوق الملازمة للشخصية بما فيها الحق في الحياة الخاصة، وقد أورد هذا النص مبدأ مهما هو حق من وقع اعتداء على حياته الخاصة في التعويض عما لحقه من ضرر. فالمسؤولية المدنية ترتب الحق في الحكم بالتعويض << **فالفعل الضار هو أساس المسؤولية >>** وهو الركن الأساسي الذي يؤسس عليه الحق في رفع الدعوى القضائية عن الاعتداءات الإلكترونية التي تمس بالحياة الخاصة على شبكة الانترنت، وهو عنصر متحول وصعب التحديد في الجرائم التي تمس الخصوصية على المواقع الإلكترونية لما تشكله من صعوبات في الإثبات وفي

[1] **فضيلة عاقلي**، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر <<الجرائم الإلكترونية>>، طرابلس، بتاريخ 24-25 مارس 2017، ص 127

[2] **المرجع نفسه**، ص 127.

تحديد هوية المعتدي، وفي هذه المسألة المشرع الجزائري حذا حذو المشرع الفرنسي الذي أقام المسؤولية عن الفعل الإلكتروني الشخصي على أساس الخطأ الواجب الإثبات فلا يكفي أن يحدث الضرر الذي يمس عناصر الحياة الخاصة بل يجب أن يكون ذلك الفعل الإلكتروني قد وصل إلى درجة الخطأ الذي يشكل اعتداء قابل للإثبات وان وقع على الشبكة[1].

2. مكافحة الجريمة الإلكترونية بموجب قانون العقوبات الجزائري وقانون الإجراءات الجزائية الجزائري :

أ- مكافحة الجريمة الإلكترونية بموجب قانون العقوبات الجزائري :

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون **رقم 04- 15**المؤرخ في 10 نوفمبر 2004 المتمم لأمر رقم 22-15 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، ويتضمن هذا القسم ثمانية مواد من **المادة 394 مكرر** إلى **المادة 394 مكرر07.**

وبغرض تدارك الفراغ القانوني، فقد قام المشرع الجزائري بموجب القانون **رقم 04-15** باستحداث جملة من النصوص والتي جرم من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات وحدد لكل فعل منها ما يقابله من الجزاء، إذ قام المشرع الجزائري بسن جملة من القواعد القانونية الموضوعية والتي حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات وما يقابلها من جزاء أو عقوبة[2]، وإلى جانب ذلك فقد قام المشرع الجزائري بسن

[1] **حسين نوارة**، آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا، الملتقى الوطني" اليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، الجزائر، 29 مارس 2017 ، ص121-122 .

[2] **قانون رقم 04-15** مؤرخ في 2004/11/10 يعدل ويتمم الأمر رقم 66-156، يتضمن قانون العقوبات، جريدة رسمية عدد 71، صادر بتاريخ 2004/11/10 ، معدل ومتمم .

قواعد إجرائية جديدة تتعلق بالتحقيق تتماش مع الطبيعة المميزة للجرائم الإلكترونية وذلك من خلال تعديل قانون الإجراءات الجزائية بموجب قانون رقم 06-22[1].

إذ نصت المادة 394 مكرر منها يلي: << **يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000إلى 300.000 دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك،** وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة **تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.0000دج إلى 10.000.000دج** >>. وذلك مهما كانت قاعة المعلوماتية أو طبيعتها لذلك يمكن أن تندرج ضمن هذه الاعتداءات تلك التي تمس ببعض صور الحياة الخاصة. ونصت **المادة 394 مكرر 2** على أنه « **:يعاقب... كل من يقوم عمدا وعن طريق الغش بما يأتي:**

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

2-**حيازة أو إفشاء أو نشر أو استعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم >>** .

وتضيف **المادة 394 مكرر 6** أنه بالإضافة إلى العقوبات الأصلية أي الحبس والغرامة وبالاحتفاظ بحقوق الغير الحسن النية يحكم بالعقوبات التكميلية التالية: << **يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو المكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها>>.**

[1] **قانون رقم 06-22 ، المرجع السابق.**

ب-مكافحة الجريمة الإلكترونية بموجب قانون الإجراءات الجزائية الجزائرية:

بالنسبة لمتابعة الجريمة الإلكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية، كالتفتيش والمعاينة واستجواب المتهم والضبط والتسرب والشهادة والخبرة[1].

نجد أن المشرع نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في **المادة 37** قانون الإجراءات الجزائية، ونص على التفتيش في **المادة 45 الفقرة07**[2] من نفس القانون المعدلة، حيث اعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه، في القواعد الإجرائية العامة من حيث الشروط الشكلية والموضوعية، فالتفتيش وإن كان إجراء من الإجراءات التحقيق قد أحاطه المشرع بقواعد صارمة، وبالتالي لا تطبق الأحكام الواردة في **المادة 44** من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الإلكترونية، ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة في **المادة 51 الفقرة6**[3] وكذا على <<إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور>> من **المادة 65 مكرر05.**

ولقد أدرك المشرع الجزائري جيدا بأن المواجهة الفعالة للإجرام الإلكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية، والتي من شأنها أن تفادى وقوع الجريمة الإلكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها، وهو ما استدركه المشرع بتضمين القانون **رقم 06-22** المعدل لقانون الإجراءات الجزائية تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الإلكترونية تتمثل في مراقبة الاتصالات الإلكترونية تسجيلها والتسرب.

ولقد أشار المشرع الجزائري إلى ظروف وكيفية اللجوء هذا الإجراء في **المادة 65 مكرر5** من قانون الإجراءات الجزائية على النحو: << **إذا اقتضت ضرورات التحري في الجريمة**

---

[1] **فضيلة عاقلي**، المرجع السابق ، ص 130 .

[2] **مولود ديدان**، قانون الإجراءات الجزائية الأمر 11-02 ، دار بلقيس، الجزائر، ص 33 .

[3] راجع **المادة 51 فقرة 06** من أمر رقم 66-155، المرجع السابق.

المتلبس بها، أو التحقيق الإبتدائي في... الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ...يجوز لوكيل الجمهورية المختص أن يأذن:

-باعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكي واللاسلكي.

-وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط تثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص>>.

فبموجب هذه المادة أن المشرع الجزائري يسمح لسلطات التحقيق والاستدلال إذا استدعت ضرورة التحري في الجريمة المتلبس بها، أو التحقيق في الجريمة الإلكترونية، اللجوء إلى إجراء اعتراض المراسلات السلكية اللاسلكية وتسجيل المحادثات الأصوات التقاط الصور، والاستعانة بكل الترتيبات التقنية اللازمة لذلك من أجل الوصول إلى الكشف عن ملابسات الجريمة وإثباتها دون أن يتقيدوا بقواعد التفتيش الضبط المألوفة.

ومع هذا فان المشرع الجزائري لم يطلق حق اللجوء إلى هذا الإجراء، بل أحاطه بمجموعة من الضمانات القانونية التي تحد من تعسف سلطات الاستدلال والتحري وتصون الحقوق والحريات العامة والحياة الخاصة للأفراد[1].

ثانيا- مكافحة الجريمة الإلكترونية بموجب الهياكل الخاصة :

1. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال :

نصت على إنشاء هذه الهيئة **المادة 13** من القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ؛ << تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال

[1] **براهيمي جمال**، مكافحة الجريمة الالكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، العدد2 ، الصادر في 2016/11/15، ص124-125.

ومكافحته .تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم >>، أما مهامها فقد أوردتها المادة 14 من نفس القانون[1].

أ. **تنظيم الهيئة :**

بالرغم من الأهمية المرجوة من هذه الهيئة إلاّ أنّه لم يتم إلى حد الساعة إنشاءها، ولم يصدر تنظيم تشكيلتها ستحوي مجموعة من فإنّ خاص بها يحدد تشكيلتها وتنظيمها وسيرها. وبإستقراء نصوص **القانون رقم09-04** فإن تشكيلتها ستحوي مجموعة من ضباط الشرطة القضائية، والتي ستسمح لهم هذه الصفة بتنفيذ المهام التي أوكلها المشرع نشأت الوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيات الإعلام والاتصال وهي هيئة تابعة للمديرية العامة للشرطة الوطنية الفرنسية وخاضعة للمديرية المركزية للشرطة القضائية، نشأت سنة 2000.

ت.**مهام الهيئة :**

من خلال اسمها فإنَّ للهيئة دوران أساسيان يمكن أن تلعبهما في حالة تأسيسها :

ب/1. الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال : إنَّ إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيات الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، ومن أهم هذه الجرائم: التجسس على الاتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء أو ببطاقات ائتمانهم، اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية..إلخ[2].

ب/2. مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

بحسب نص **المادة 14** من القانون 04/09 فهناك نوعان من المكافحة تقوم بهما هذه الهيئة:

[1] راجع **المادة 14** من قانون09-04 ، المرجع السابق .

[2] **بوضياف اسمهان** ، المرجع السابق ، ص 368 .

-مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية(**المادة 14 فقرة ب** من القانون رقم 09-04)[1]، وبالنسبة للوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيات الإعلام والاتصال بفرنسا، فإن لها مهام أدرجها المرسوم رقم 2000-405 المؤرخ في 15 ماي 2000 المتضمن إنشاء هذه الهيئة تتمثل في :

- تنشيط وتنسيق على المستوى الوطني عمليات المكافحة ضد الفاعلين والمشتركين في إرتكاب الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- القيام بإذن من السلطات القضائية بجميع إجراءات التحري والأعمال التقنية الخاصة بالتحقيقات كمساعدة لمصالح الشرطة القضائية المختصة بتحقيقات لجرائم خاصة ارتكبت أو سهل إرتكابها استعمال تكنولوجيات الإعلام والاتصال، ولكن دون المساس باختصاص باقي الهيئات الوطنية المختصة بمكافحة جرائم معينة نص عليها القانون.
- تقديم المساعدة لمصالح الأمن والدرك الوطنيين، ولجميع إدارات ومصالح الدولة المركزية (المديريات العامة المختلفة) فيما يخص الجرائم التي تدخل في اختصاص هذه الهيئة، إذا طلبت منها هذه المصالح ذلك، ودون أن يؤدي ذلك إلى رفع يد هذه المصالح.
- التدخل من تلقاء نفسها بعد موافقة السلطات القضائية المسبقة (المادة 4 فقرة 2 من القانون قم 09-04[2]) في كل مرة تفرضها الظروف من أجل البحث الميداني في وقائع مرتبطة بتحقيق تقوم به .
- يجب على مصالح الأمن والدرك الوطنيين، إدارات ومصالح الدولة (المديريات العامة) في أقرب الآجال إخطار الهيئة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال فيما تسمح به

[1] قانون **رقم 09-04** المرجع السابق .

[2] راجع **المادة 04** من قانون **رقم 09-04** ، المرجع نفسه.

القوانين وخاصة منها ما يتعلق بالسر المهني –بما كشفته أو وصل إلى علمها من جرائم متصلة بتكنولوجيات الإعلام والإتصال[1].

ب/3. تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وتحديد مكان تواجدهم: في هذا الشأن تقوم الهيئة على المستوى الوطني بتنشيط وتنسيق الأعمال التحضيرية الضرورية ومن ثم تشاركها مع المنظمات (الهيئات) المماثلة لها على مستوى الدول، بدون المساس بتطبيق الاتفاقيات الدولية ومبدأ المعاملة بالمثل، كما أنها تدرس الروابط العملياتية مع الهيئات والمصالح المختصة مع الدول الأخرى من أجل البحث عن جميع المعلومات المتعلقة بالجرائم المعلوماتية وكذلك التعرف على الفاعلين وأماكن تواجدهم[2].

وتتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقات الدولية الثنائية و مبدأ المعاملة بالمثل[3] .

3. **المعهد الوطني للأدلة الجنائية على الإجرام:** يتكون من إحدى عشرة دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية، ودائرة الإعلام الآلي والإلكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد للعدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات[4].

4. **الهيئات القضائية الجزائية المتخصصة:** إنَّ السلطة القضائية ستتعامل تأكيدا في قضايا الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ولاسيما بعد اللّجوء الواسع والمتزايد إلى الشبكات الرقمية في حياة المواطنين، بينما يتطلب الأمر مظاهر تقنية وقانونية لمعالجة هذه

---

[1] **بوضياف اسمهان**، المرجع السابق، ص 369 .

[2] **عبد الفتاح بيومي حجازي**، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر،2007، ص232-233.

[3] راجع **المادة 17** من قانون **رقم 09-04**، المرجع السابق .

[4] **فضيلة عاقلي**، المرجع السابق، ص 133 .

القضايا، وعلى هذا فإن حتمية المعرفة ولو في حدها الأدنى لمعالجة فعالة في هذه المواد التي تجتاح المجال العقابي.

ويتجه النظام القضائي الجزائي إلى إرساء فكرة القضاء المتخصص، وما يؤكد ذلك ما نص عليه القانون **رقم 14-04** المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية(ق.إ.ج)، على أنَّه يجوز تمديد دائرة الاختصاص للمحكمة وكذا لوكيل الجمهورية وقاضي التحقيق عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وهذه الأخيرة أنشأ لها مؤخرا قطب جزائي وطني مختص لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وفقا للأمر **رقم 21-11** السالف الذكر. كما نصت المادة 40 مكرر من ق. إ.ج على أنَّه << تُطبق قواعد هذا القانون المتعلقة بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي يتم توسيع اختصاصها المحلي طبقا للمواد40 ، 37 ، 329 من هذا القانون مع مراعاة أحكام المواد من 40 مكرر 1 إلى 40 مكرر 5 أدناه .

كما تجدر الإشارة بهذا الخصوص إلى أن الأقطاب الجزائية عموما هي عبارة عن: "جهات قضائية متخصصة للنظر في بعض الجرائم التي حددها القانون وليست بجهات قضائية خاصة تنشط بإجراءات قانونية مستقلة تخرج عن نطاق النظام القضائي الساري المفعول". وتأسيسا على ذلك؛ يظهر القطب الجزائي كوسيلة لضمان فعالية الممارسة القضائية بخصوص الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ويمكن اعتباره خطوة لإرساء نظام التخصص القضائي في الجزائر[1]. و القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال واحدٌ من هذه الأقطاب الجزائية، حيث أخضعه المشرع لقواعد اختصاص مختلفة

[1] **بن عميور أمينة ، بوحليس إلهام** ، المرجع السابق ، ص 72 .

ومن ذلك قام المشرع بتوسيع الاختصاص المحلي لدى القطب ومنحه قواعد إجرائية خاصة من شأنها تفعيل التصدي للجرائم المتصلة بتكنولوجيات الإعلام والاتصال .

وإذا كان للقضاء المتخصص جانبين هما تخصص القضاة والأجهزة القضائية المتخصصة فإن هذه الأخيرة تتطلب رصد إمكانيات مادية وبشرية ضخمة، وهو الأمر الذي نعتقد أنَّه جعل المشرع الجزائري لتلافي هذه العقبات التي تواجه القضاء المتخصص يختار أسلوب الأقطاب القضائية[1]، فيتجنب إنشاء هيئات قضائية جديدة لكنّه يوسع من دائرة الاختصاص الإقليمي للمحاكم لتشكل أقطاب قضائية ويمنحها اختصاص نوعي معين في مواد معينة دون أن يمنعها ذلك من الفصل في المواد التي تدخل ضمن اختصاصها العادي، وهذا ما يجعلنا نعتقد من جانب آخر أنَّ التخصص الذي سيسود التنظيم القضائي الجزائري سيرتكز أكثر على الجانب البشري أي تخصص القضاة، ليشكل ذلك حجر الزاوية لفكرة الأقطاب القضائية .

الفرع الثاني: المكافحة الدولية للجريمة الإلكترونية

أمام الصعوبات الكبيرة التي واجهتها الدول في مكافحة الجريمة الإلكترونية عبر قوانينها الداخلية، وفي مواجهة أصعب خاصية لها كونها جريمة متعدية الحدود وجدت الدول نفسها مضطرة لنجاح المكافحة لتكثيف جهودها مع لعضها البعض بالتعاون على مواجهة هذا الإجرام الجديد، وذلك بعقد اتفاقيات دولية لمواجهة هذه الظاهرة والاستفادة من تجارب بعضها البعض .

ومن خلال هذا المنطلق سنتناول هذه الاتفاقيات على النحو التالي :

أولا- الاتفاقيات العربية:

تبدو جهود الدول العربية في مكافحة الجرائم الإلكترونية، من خلال اجتماع ممثلي الدول العربية في المؤتمر العربي للتحضير لمؤتمر القمة العالمية لمجتمع المعلومات في الفترة الممتدّة من 16 إلى 18 يونيو 2003. وقد حضر المؤتمر ممثّلو 19 دولة عربية إضافة إلى مندوبي 9 دول إفريقية كمراقبين وعدة شخصيات مرموقة عالميا في مجال الاتصالات

[1] **عمار بوضياف**، النظام القضائي الجزائري، دار ريحانة، الجزائر، 2003 ، ص229 ،230 .

والمعلوماتية[1]. وأوصى المشاركون في المؤتمر بإنشاء فريق عمل تحت مظلة جامعة الدول العربية لتأمين شبكة المعلومات العربية وحماية المستهلك العربي من جرائم الانترنت، وقد سعى مجلس التعاون لدول الخليج العربي كذلك إلى مكافحة الجريمة الإلكترونية. حيث أوصى منذ سنة 2007 بأن ينخرط أعضاءه في المنظومة العالمية لمكافحة الجريمة الإلكترونية وفق المعايير الدولية[2] .

تعد الاتفاقيات العربية لمكافحة جرائم الكمبيوتر خطوة فعالة في مجال مكافحة الجريمة الإلكترونية ومسلك منطقي وضروري لا بد من اتخاذه لأن المجتمعات العربية ليست بمنأى عن هذه الجرائم الجديدة. وفي نطاق الدول العربية برزت تحديات قانونية كثيرة لتقنية المعلومات على النظم القانونية، ابتدأت منذ مطلع السبعينات، مرت عبر مسيرة متسارعة الأحداث خلفت ورائها مسائل قانونية أوجبت ظهور سلسة من موجات التشريع في حقول قانونية مختلفة[3] :

- **الخصوصية وحماية البيانات الشخصية وبنوك المعلومات** (حقوق إنسان- تنظيم إداري، **جرائم الكمبيوتر والشبكات** (قانون جنائي موضوعي).
- **الملكية الفكرية للمصنفات الرقمية**(قانون مدني بالنسبة للحق المعنوي وقانون الملكية الفكرية كفرع خاص).
- **القواعد الإجرائية الجزائية لمواجهة جرائم التقنية العالية**(أصول إجرائية جنائية)،
- **تشريعات الأمن والمعايير والمقاييس التقني.**(تشريعات تنظيمية وإدارية وتتصل بحماية المستهلك وتتصل أيضا بتشريعات الاتصالات والمعلومات.
- **تشريعات الإثبات بالوسائل الالكترونية وحجية مستخرجات الحاسوب**(قانون البيانات).
- **تشريعات المحتوى الضار وغير المشروع لمواقع المعلوماتية** -(النشر الإلكتروني والمطبوعات والصحافة وقواعد السلوك والإعلان وتتصل بعضها بحماية المستهلك).

---

[1] **أنيس العذار**، مكافحة الجريمة الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 17، العدد 01، 2018، ص 740.

[2] **المرجع نفسه**، ص 740.

[3] **سعيداني سلامي**، تطور التشريعات والاتفاقيات الدولية في مجال الجرائم المعلوملتية (وقائع و مقاربات)، مجلة الأستاذ الباحث للدراسات القانونية و السياسية، المجلد الأول، العدد العاشر، 2018، ص 202 .

– **تشريعات الوسائل المؤتمتة في الحقل المالي والبنوك الالكترونية**(مال وأسواق مالية ومصارف).

– **تشريعات حماية المستهلك في عصر المعلومات ، وتشريعات التجارة الإلكترونية والتواقيع الرقمية**(تجاري وتعاقد واثبات وضرائب و إداري – أي إدارة حكومية بالنسبة للخدمات والمشتريات الحكومية ضمن مفهوم الحكومة الإلكترونية)[1].

وقد أوجبت هذه الحقول اتخاذ تدابير تشريعية أما بوضع تشريعات خاصة في هذه الحقول كل على حدة، أو ضم أكثر من حقل في تشريع مستقل واحد أو من خلال إجراء تعديلات امتدت للعديد من التشريعات المدنية والتجارية والجزائية والإدارية في العديد من دول العالم الصناعية، ومن هنا مثلا نجد هذه الدول تتبنى استراتيجية الحد الأدنى من التنظيم القانوني للتجارة الإلكترونية التي تعتمد على التنظيم القانوني للمسائل المتقدمة، وهو أمر طبيعي بالنسبة لها – وليس لنا، لأن هذه الدول تلاءمت مع هذه المسائل ووضعت تشريعات عديدة في هذه الحقول.

أما في البيئة العربية فان مجتمعاتنا لم تتقاطع مع هذه الموجات التشريعية إلا في حدود بعض المسائل الرئيسة في حقل الملكية الفكرية للمصنفات الرقمية كبرامج الحاسوب وقواعد البيانات والدوائر المتكاملة بسبب التزامات دولنا للدخول في عضوية منظمة التجارة الدولية؛ وبسبب متطلبات اتفاقية تربس الخاصة بالملكية الفكرية إضافة إلى بعض المسائل المتعلقة بالمقاييس والمواصفات وتشجيع الاستثمار والجمارك والاتصالات في المسائل المرتبطة بالتقنية وجهد تام، فلم يتحقق شيء يذكر رغم أن الدول العربية تبنت منذ نهاية العام المنصرم مبادرات متقدمة في حقل تقنية المعلومات كما بالنسبة لمشروعات مدينة دبي للأنترنت وسوق دبي الالكتروني في دولة الإمارات العربية، ومبادرات القرى الذكية في مصر، ومبادرة تقنية

[1] **سعيداني سلامي، المرجع السابق**، ص 202 .

المعلومات في الأردن وما تبعها من تبنى مفهوم وشعار الحكومات الالكترونية في كل من دبي والأردن ومصر وقطر والبحرين وغيرها[1].

ويمكننا في ضوء قراءة التجربة العربية في التعامل مع العصر الرقمي واحتياجاته التشريعية أن نلحظ تخبطا في التعامل مع المتطلبات التشريعية لتقنية المعلومات، وهو أشبه بحالة التخبط التي شهدتها النظم المقارنة في مطلع السبعينات وخلال الثمانينات. ولا تزال تشهد بعضا من ملامحه في عدد من مسائل تقنية المعلومات في الوقت الخاص، ففي هذا السياق يلمس المتابع عدم وضوح الرؤية، ويلمس اتجاه المؤسسات التشريعية في الدول النامية ومنها العربية – إلى حلول تدرك التحديات التقنية ذاتها وتدرك حالة التغير والتطور في الاحتياجات القانونية لمواجهة العصر الرقمي[2]. وتدرك أكثر أن الحلول المقتبسة دون إعادة تلاءم واعي ومدروس على الأقل حلول معطلة وليست فاعلة لاعتبارات اجتماعية وسياسية واقتصادية وقانونية، حتى أننا لا نكون مبالغين إن قلنا أن هذه الحلول الجزئية المقتبسة تزيد التحديات ولا توفر حلولا لها كما أنها في بعض الأحيان تقيم مزيدا من العوائق نحو الأهداف النبيلة في خطط توظيف التقنية بدلا من أن تذلل هذه العوائق.

إن شيوع الكمبيوتر وفيما بعد الاتجاه نحو التشبيك عبر مختلف أنواع شبكات المعلومات وفي مقدمتها الانترنت وبناء شبكات وقواعد المعلومات، افرز حاجة ملحة للتدخل من اجل حماية امن المعلومات وحماية الخصوصية والتنظيم الصحيح لحماية الملكية الفكرية ومراعاة آثارها على المجتمع، ومن أجل حماية المستهلك والاعتراف بالحجية وملائمة الوسائل الإلكترونية للتصرفات القانونية بنفس القدر من الملائمة المقبولة والمعترف بها للوسائل غير الإلكترونية، إلى جانب أهمية تنظيم معايير ومقاييس التقنية وحماية المستخدم في نطاقها

[1] **يونس عرب**، تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، ورقة عمل " الاتجاهات التشريعية للجرائم الالكترونية، هيئة تنظيم الاتصالات / مسقط – سلطنة عمان 4 –2 ابريل 2006 ، ص29–30 .

[2] **المرجع نفسه**، ص 30 .

وتنظيم البنى التحتية ضمن تدابير تكفل نماء توظيف التقنية بشكل صحيح وملائم لحاجات المجتمع[1] .

ثانيا- الاتفاقية الأوروبية:

تناولت هذه الاتفاقية كل ما يتعلق بجرائم الحاسوب والانترنت سواء ما يقع ضد الشبكات والمعلومات أو الجرائم التقليدية التي تستخدم في ارتكابها الشبكات المعلوماتية .

من بين هذه الاتفاقيات نجد :

1. اتفاقية بودابست :

جاءت اتفاقية بودابست تتويجا للجهود التي بذلها الاتحاد الأوروبي والمجلس الأوروبي من أجل إيجاد صيغة قانونية لمكافحة الجريمة الإلكترونية، وهي تعد حاليا الإطار المرجعي لمكافحة الجرائم المعلوماتية ووضعت هذه الاتفاقية من قبل مجلس أوروبا بالتعاون مع كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية، وقد دخلت حيز التنفيذ في سنة 2004[2] ويمكن لأي دولة الانضمام إليها .

أبرزت هذه الاتفاقية في صلب تواطئها مدى اقتناع الدول المصادقة عليها بخطورة الجريمة المعلوماتية وبضرورة تظافر الجهود الدولية لمواجهتها، بحيث تعرضت إلى بعض المفاهيم؛ مثل مفهوم النفاذ غير الشرعي ومفهوم الجريمة المعلوماتية وغيرها من المفاهيم التي تستدعي اعتماد مفهوم موحد لتسهيل تطبيق الاتفاقية. كما تضمنت قواعد متعلقة بالتعاون في ميدان مواجهة الجريمة الإلكترونية؛ كالقواعد الخاصة بالاختصاص الترابي للمحاكم وتسليم المجرمين واعتماد شبكة مفتوحة كامل الأسبوع مخصصة لبقية الدول الأعضاء لتوفير المساعدة في الأبحاث المرتبطة بالجرائم المعلوماتية[3] .

[1] **يونس عرب**، المرجع السابق، ص 31 .

[2] **صغير يوسف** ، المرجع السابق ، ص 94 .

[3] **أنيس العذار**، المرجع السابق، ص 740 .

2. اتفاقية الأمم المتحدة :

اهتمت الأمم المتحدة بموضوع الجريمة الالكترونية, ووضعته من بين أولويات نشاطها نظرا لما تسببه هذه الأخيرة من أضرار وخسائر فادحة، وتؤكد على أن منع هذه الجرائم يتطلب استجابة دولية مشتركة بين أعضاء هذه المنظمة بغية التعاون للحد من انتشارها وتعاظم نتائجها من خلال إشرافها على العديد من المؤتمرات الدولية الخاصة لردع الجريمة ومعاقبة المجرمين وإبرامها للاتفاقيات الدولية .

نجد من بين أهم المؤتمرات المبرمة في مجال مكافحة الجريمة الإلكترونية، المؤتمر الثامن المنعقد سنة 1990 الذي توصل إلى عدة توصيات بعد دراسته للتقرير الذي أعدته لجنة الخبراء العشرين، بتكليف من المؤتمر السابع المنعقد بميلانو سنة 1985 حول موضوع حماية نظم المعالجة الآلية الاعتداءات التي تمس الحاسوب الآلي[1].

الفرع الثالث: التعاون الدولي لمكافحة الجريمة الإلكترونية

لما كان التعاون الدولي هو السبيل الفعال لمكافحة الجرائم الإلكترونية فإن ذلك يتطلب التخفيف من الفوارق بين نظم العقاب الداخلية بين تلك الدول حتى يلجأ المجرم المعلوماتي إلى الأنظمة القانونية الأكثر تسامحا، وقد ظهرت آثار التقارب في قبول حالات تفويض الاختصاص في اتخاذ إجراءات جمع الأدلة والتحقيق وتسليم المجرمين والاعتراف بالأحكام الجنائية الأجنبية وهذا التعاون يساعد على تقليل الجرائم عبر الحدود[2].

ونظرا لأهمية التعاون الدولي أدى الانتشار الواسع والمتسارع للتقنية المتمثلة في الحسابات الآلية وشبكات الاتصال الخاصة بها والتطور الهائل في عالم البرمجيات فاستغل البعض هذه المعرفة لارتكاب الجرائم سواء تلك الواقعة على تكنولوجيا المعلومات، أو تلك التي ترتكب

[1] **بوشعرة أمينة، موساوي سهام**، الإطار القانوني للجريمة الإلكترونية –دراسة مقارنة، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة –بجاية، ص50 .

[2] **محمد علي سكيكر**، المرجع السابق، ص 109 .

بالوسائط الإلكترونية لذلك أصبح من الضروري أن يكون هناك تعاون دولي واسع المدى في مكافحة هذه الجرائم[1] .

ويقتضي التعاون بين التشريعات المختلفة من أجل مكافحة الجرائم المعلوماتية قيام كل دولة بتطبيق قوانينها على ما يرتكب فوق أرضها وتحت سمائها وذلك بالنسبة لما يتفق عليه العالم من تشريعات وصور التعاون الدولي، المساعدة القضائية، وتسليم المجرمين .

أولا- المساعدة القضائية :

ظهر التعاون بين الدول في وجود نصوص في معظم الاتفاقيات الخاصة بالجرائم التقليدية للجوء إلى المساعدة المتبادلة لتحقيق السرعة والفعالية في إجراء وملاحقة عقاب مرتكبي هذه الجرائم[2] .

وتتم غالبا بمقتضى اتفاقيات ومعاهدات دولية تنطوي على تبادل السلطات القضائية المختصة المعلومات لمعاقبة وإلقاء القبض على مرتكبي الجريمة المعلوماتية ألا وهو المجرم المعلوماتي وذلك نظرا لكون الجريمة المعلوماتية عابرة الحدود. فالمساعدة القضائية الدولية المتبادلة هي تبادل السلطات المختصة المعلومات واتخاذ إجراءات تحفظية لجمع الأدلة الإلكترونية الخاصة في الحالة العادية، وفي الحالة الغير العادية يتم استعمال وسائل الاتصال السريعة كالفاكس وغيرها من الوسائل من شروط أمن كافية للتأكد من صحتها.

ولكي تكون طلبات المساعدة القضائية الدولية المتبادلة صحيحة لا بد من التقيد والالتزام بقيود قانونية تتمثل في[3] :

- أن يكون في تنفيذ طلبات المساعدة المساس بالسيادة الوطنية أو النظام العام .
- ضرورة المحافظة على سرية المعلومات المبلغة .
- عدم استعمال هذه المعلومات في غير الموضع .

---

[1] **ناصر بن محمد البقمي** ، مكافحة الجرائم المعلوماتية و تطبيقاتها في دور مجلس التعاون لدول الخليج العربية ، الطبعة الأولى ، مركز الامارات للدراسات والبحوث الاستراتيجية ، دولة الامارات العربية المتحدة –أبو ظبي ، 2008 ، ص 29 .

[2] **محمد علي سكيكر** ، المرجع السابق ، ص 112 .

[3] **أمير فرج يوسف** ،المرجع السابق ، ص 455 .

1. صور المساعدة القضائية :

من صورها[1] :

- تبادل المعلومات، ويشمل تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد ارتكاب إحدى الجرائم .
- أن يكون الفعل الإجرامي المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوبة إليه .
- أن تكون الإجراءات المطلوب اتخاذها عن الجريمة المرتكبة مقررة في قانون الدولة المطلوب إليه على الجريمة ذاتها .
- أمن يؤدي الإجراء المطلوب للوصول إلى الحقيقة .
- تبادل الانابة القضائية الدولية، وذلك باتخاذ إجراء قضائي من إجراءات الدعوى الجنائية.

2. المحكمة المختصة بنظر الجرائم الإلكترونية :

إعمالا للفقرة الأولى من المادة 22 من القانون النموذجي بشأن مكافحة جرائم الانترنت فإن المحاكم الوطنية المختصة بالنظر في الدعوى المترتبة عن الجرائم المعلوماتية التي يطبق عليها قانون الدولة الوطني، وعلى ذلك فإن الجرائم المعلوماتية أيا كان نوعها سواء وقعت عن طريق شبكة الانترنت أو شبكة معلوماتية داخلية سواء كان ذلك داخل الدولة أو خارجها شريطة أن يكون القانون الوطني صالحا للتطبيق عليها فإن المحاكم الوطنية تكون هي المختصة بنظر هذه الجرائم دون غيرها من المحاكم. ويتحدد الاختصاص المكاني لرفع الدعوى وفقا للضوابط الثلاثة (مكان وقوع الجريمة، مكان إقامة المتهم، ومكان ضبط المتهم)[2] .

ثانيا- تسليم المجرمين :

وهي العملية التي يكون في الغالب منصوص عليها في الاتفاقيات والمعاهدات الدولية، وقد نص المشرع الجزائري في **القانون رقم 09-04** على اختصاص السلطات القضائية

---

[1] **محمد علي سكيكر** ، المرجع السابق ، ص 111- ص113 .

[2] **المرجع نفسه** ، ص 114 .

الجزائية الجزائرية إذا كان مرتكب الجريمة الماسة بالمعطيات أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني، لكنه أغفل على تسليم المجرمين في حالة فرار المجرم المعلوماتي. غير انه وطبقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات اشترطت على ضرورة وجود اتفاقية من أجل تسليم المجرمين في هذا النوع من الجرائم، واستبعدت وجود اتفاقيات تسليم بين الدول الأطراف، إلا أن هذا التسليم تحكمه مجموعة من الإجراءات الواجب اتباعها من قبل كل دولة طرف طلبت التسليم[1] .

3. شروط التسليم :

- التجريم المزدوج ويقصد به أن يكون الفعل المطلوب التسليم من أجله مجرما في تشريع الدولة المطلوب إليها التسليم أيا كانت صورة العقاب[2] .
- اختصاص الدولة طالبة التسليم مختصة بملاحقة الشخص المطلوب تسليمه من جهة، ومن جهة أخرى يجب أن يكون الفعل المعاقب عليه طبقا للقانون الجزائري .
- عدم جواز تسليم الرعايا ممنوحي اللجوء السياسي .
- وأيضا ما يتعلق بالشخص المراد تسليمه وما يتعلق بالجريمة محل التسليم والجرائم السياسية التي لا يجوز التسليم فيها، ويرفض التسليم فيها فانشأ عقبة تحول دون التعاون الدولي في هذا المجال .
- كما يشترط أن يكون الفعل على درجة معينة من الجسامة، بمعنى أن يكون مخالف؛ إذ أن يكون جناية أو جنحة وأن يكون العقاب على الجناية أو الجنحة بعقوبة سالبة للحرية، ويشترط أن تكون الدولة طالبة التسليم مختصة بمحاكمته[3] .

4. إجراءات التسليم :

تتمثل هذه الإجراءات في مايلي[4] :

---

[1] **أمير فرج يوسف**، المرجع السابق، ص 455 .

[2] **هشام عبد العزيز مبارك**، تسليم المجرمين بين الواقع والتطبيق، الطبعة الأولى، دار النهضة العربية، القاهرة، ص 281.

[3] **محمد علي سكيكر**، المرجع السابق، ص 115 .

[4] **سليمان عبد المنعم**، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين، دار الجامعة الجديدة، 2007، ص 220-221 .

- تقديم طلب التسليم وتكون كتابة إلا في حالة الاستعجال .
- ارفاق طلب التسليم بمجموعة من المستندات الدالة على ارتكاب الشخص المجرم محل التسليم .
- دراسة الطلب، ثم الرد عليه في النهاية .
- كما توجد أساليب لمجابهة الجريمة المعلوماتية ومكافحتها سواء على المستوى الدولي المتمثل في الاتفاقيات الدولية خاصة اتفاقية بودابست 2001، وكذا الاتفاقية المتعلقة بحماية الملكية الفكرية .
- بالإضافة إلى جهود تبذل على المستوى العربي ممثلة في القانون العربي النموذجي، أما بالنسبة للمشرع الجزائري فقد واكب ولو بقدر قليل الحركية التشريعية التي فرضت نفسها عالميا في مجال مكافحة الجريمة المعلوماتية، لينتهي بنا الأمر إلى التعاون الدولي في مجال مكافحة الجريمة متمثلة في المساعدة الدولية المتبادلة وكذا تسليم المجرمين .

خلاصة الفصل

جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية من أحد أهم القضايا التي لا تزال صوب الدراسة خاصة من الجانب القانوني، بحيث أخذت هذه الأخيرة منحنيات صارمة، ولهذا لجأت الدول إلى سن وتفعيل إجراءات عامة وخاصة لهذه الاعتداءات. فقد خضعت للعديد من السبل والآليات القانونية التي من شأنها أن تحيط و تلم بها رغم صعوبة التحكم لتحصر هذا النوع من الجرائم وهذا لشساعة الوسائط الإلكترونية وتعددها، ولهذا أخذت المجتمعات الدولية وجوب توحيد التعاون الدولي وتبني العديد من الاتفاقيات في مجال مكافحة جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية.

خاتمة

من خلال دراستنا لجرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية توصلنا إلى أنها أكثر الجرائم التي شهدها العالم بأسره وهذا نتيجة الثورة الرقمية نظرا لكون التكنولوجيا عابرة للحدود، فأمام هذا التطور ارتبطت به ظهور ما يعرف بالإجرام المعلوماتي و ذلك نتيجة للاستخدام السيئ للمعلوماتية أو الحاسوب الذي نتج عن هذا الأخير عدة أضرار لا يمكن حصرها، وذلك لأنها تهدد أمن المعطيات من جهة وتمس بحرية الأفراد من جهة أخرى.

حيث تختلف هذه الجرائم عن الجرائم المعروفة في العالم التقليدي كون الجريمة الإلكترونية تتسم بخصائص مميزة عن الجريمة التقليدية، فقد حصرنا موضوع دراستنا فقط على جريمة القذف والسب وكذا جريمة التحرش الجنسي عبر الوسائط الإلكترونية من خلال تعرفنا على طبيعة هذه الجرائم المنتشرة بالأخص على الشبكة العنكبوتية والتي انتشرت بصورة مذهلة دون مراعاة أخلاقيات الدول.

كما توصلنا إلى أن المشرع الجزائري قد حاول مواكبة التطور التكنولوجي في مثل هذه الجرائم، والتي تعتبر من الجرائم الخطيرة التي بدأ المشرع الجزائري في التعامل معها بنوع من الدقة و الذي سبق أن تطرق إليها في العديد من المواد في قانون العقوبات، وأبرز لها اهتماما أكثر من خلال وضعه للقانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها؛ والذي سعى من خلالها إلى وضع نصوص قانونية جديدة رادعة لمثل هذه الجرائم كونها تتزايد بسرعة فائقة مع التطورات التي تشهدها البيئة الإلكترونية.

وبالنظر إلى الطبيعة الخاصة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال جعلت منها ظاهرة بالغة الخطورة على المجتمع والأمن الوطني، مما أدى للتوجه الجديد للمشرع الجزائري و ذلك بإنشاء قطب جزائي وطني مختص بمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والذي جاء نتيجة تعديل المشرع الجزائري لقانون الإجراءات الجزائية.

كما تبين أن هذا الموضوع يثير اهتمام التشريعات الوطنية والاتفاقيات الدولية إلى توفير الحماية للأشخاص وذلك عن طريق إصدار ومعاقبة مرتكبيها، وقد وضع المشرع الجزائري ترسانة قانونية تضمن حماية الأشخاص وحقوقهم المادية والمعنوية عبر الوسائط الإلكترونية لمختلف الجرائم التي تقع في هذا الإطار .

من خلال ما تطرقنا إليه ، توصلنا إلى العديد من النتائج و الاقتراحات التالية :

النتائج :

*- وجود قصور تشريعي في مكافحة جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية .

*- انتشار العديد من الممارسات اللاأخلاقية التي تمس بشرف واعتبار الشخص بواسطة التقنيات الحديثة في عصر المعلوماتية .

*- مسايرة المشرع الجزائري للتطور التكنولوجي الحاصل وذلك بوضع ترسانة قانونية كفرض عقوبات على الجرائم الناتجة عن مثل هذه الجرائم .

*- عدم إيجاد تقنيات دقيقة تكشف عن أدلة إثبات تخص هذا النوع من الجرائم المستحدثة وهذا نظرا لصعوبة الكشف عن الدليل كونه يتطلب عمليات فنية وعلمية نظرا لطبيعته، بالإضافة إلى سهولة استخدام التقنية العلمية في إخفائه وإتلافه.

*- مسايرة القوانين الإجرائية لمثل هذه الجرائم إذا واكبت التطورات الحاصلة على مستوى إجراءات التحقيق وهذا ما جاء في قانون 04/09 السالف الذكر كالتفتيش والضبط في المنظومة المعلوماتية وحتى ذلك المتصلة عن بعد.

*- أن أجهزة العدالة الجنائية لم تعد قادرة لوحدها على إثبات هذا النوع من الجرائم، إنما أصبح من الضروري أن تساند هذه الأخيرة جهات خاصة تكون عونا لها كأجهزة الشرطة متخصصة للبحث والتحري في الجرائم المعلوماتية، وكذا فريق للتحقيق في هذا النوع من الجرائم .

*- إحالة المشرع الجزائري القضايا المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال إلى القطب الجزائي الوطني المختص و النظر في مثل هذه الجرائم .

*- سعي المشرع الجزائري و الجهود الدولية لمواجهة هذه الجرائم إلا أن نصوصه لا تزال ناقصة في الإحاطة بهذه الجرائم و الحد منها .

الاقتراحات :

بالاعتماد على النتائج السابقة سنركز على بعض من اقتراحاتنا و توصياتنا :

*-ضرورة خلق ثقافة اجتماعية جديدة تندد بجرائم الانترنت مع تفعيل أسلوب التوعية والتهذيب لدى مستخدمي شبكة الاتصالات العالمية وحثهم على الاستخدام الأمثل لهذه التقنيات.

*- ضرورة نشر الوعي الرقمي بين المستخدمين وكيفية تفادي التعدي على بياناتهم الشخصية وتعريفهم بحجم الخطورة التي ترصدهم في حالة عدم اتخاذ الاحتياطات الوقائية اللازمة.

*- تشجيع الجامعات والمراكز البحثية على تنظيم العديد من الندوات والمؤتمرات التي تعالج تطور الإجرام المعلوماتي وكيفية مكافحة مثل هذه الجرائم والحد من أثارها.

*- العمل على تكريس قواعد قانونية جديدة تتناسب مع طبيعة الجرائم المعلوماتية وإنشاء وحدات مختصة للبحث والتحري والتحقيق في الجريمة المعلوماتية.

*- أن يقوم المشرع الجزائري بتعديل مواد قانون العقوبات بإضفاء الوسائط الإلكترونية وأي نوع من أنواع شبكات الاتصال عن بعد خصوصا في ظل تطور وسائل الاتصال السلكية واللاسلكية وهذا لما تقوم به من تسهيل عملية ارتكاب مثل هذه الجرائم. وعلى المضرور في حالة الاعتداء على اعتباره وشرفه الإسراع في التقدم بشكوى للشرطة القضائية وعدم التماطل في رفع دعوى قضائية.

*- تكثيف التعاون الدولي والانضمام إلى الاتفاقيات الدولية المتعلقة بمثل هذه الجرائم لمكافحة جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية.

*- ضرورة تشديد العقوبة على مرتكب جرائم الاعتداء على الأشخاص عبر الوسائط الإلكترونية نظرا لخطورتها.

قائمة المصادر والمراجع

قائمة المراجع:

- **الكتب:**

1- أحسن بوسقيعة، قانون العقوبات في ضوء الممارسات القضائية، د.ط، منشورات بيرتي، الجزائر، 2007.

2- أحمد خليفة الملط، الجرائم المعلوماتية، د.ط، دار الفكر الجامعي، د.ب.ن، سنة 2005.

3- أسامة أحمد المناعسة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الالكترونية- دراسة مقارنة، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، .2014

4- تميم بن عبد الله سيف التميمي، الجرائم المعلوماتية في الاعتداء على الأشخاص (قذف- سب- تشهير) وفقا للشريعة الإسلامية والنظام السعودي والقانون القطري، الطبعة الاولى، مكتبة القانون والاقتصاد، الرياض، 2016.

5- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة – أجهزة الرادارات والحسابات الآلية والبصمة الوراثية، الطبعة الأولى، دار النهضة العربية، 2001 .

6- حسن حسين زيتون، تصميم التدريس رؤية منظومية، الطبعة الثانية، عالم الكتب، 2001.

7- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الإسكندرية ، 2010 .

8- رحيمة الطيب عيساني، الوسائط التقنية الحديثة وأثرها على الإعلام المرئي والمسموع، د.ط، الرياض، 2010.

9- الزيدي وليد، القرصنة على الانترنت والحاسوب، الطبعة الأولى، دار أسامة للنشر، عمان.

10-سليمان عبد المنعم، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين، د.ط، دار الجامعة الجديدة، 2007.

11- طارق عفيفي، صادق أحمد، الجرائم الإلكترونية-جرائم الهاتف المحمول، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2015.

12- عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، الطبعة الاولى، دار الثقافة للنشر والتوزيع، عمان، 2010.

13- العاقل غريب أحمد، جرائم الإهانة والقذف والسب معلقا عليها بأحكام النقض والمحكمة الإدارية العليا، د، ط، مركز معلومات النيابة الإدارية ، مصر، 1954.

14- عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي- دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، 2009.

15- عباس مصطفى صادق، الإعلام الجديد المفاهيم والوسائل والتطبيقات، الطبعة الأولى، دار الشروق للنشر والتوزيع، رام الله، فلسطين، 2008.

16- عباس ناجي حسن، الوسائط المتعددة في الإعلام الالكتروني دراسة مقارنة، الطبعة الأولى، دار صفاء للطباعة والنشر والتوزيع، المملكة الأردنية الهاشمية، عمان، 2016.

17- عبد الحميد الشواربي، جريمة القذف والسب في ضوء القضاء والفقه، د.ط، دار المطبوعات الجامعية، الاسكندرية مصر، 1985.

18- عبد الحميد بسيوني، الوسائط المتعددة، الطبعة الأولى، دار النشر للجامعات، القاهرة، 2002.

19- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006.

20- عبد الفتاح بيومي حجازي، أصول التحقيق الجنائي والتأديبي، د.ط، دار الفكر الجامعي، الإسكندرية، .2005

21- عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الانترنت، د.ط، دار الكتب القانونية، مصر، 2007.

22- عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2007،

23- عدلي خليل، القذف والسب وتحريك الدعوى الجنائية عنهما، د.ط، دار الكتب القانونية، القاهرة، 1996.

24- عمار بوضياف، النظام القضائي الجزائري، د.ط، دار ريحانة، الجزائر، 2003.

25- عمار عباس الحسيني، جرائم الحاسوب والانترنت الجرائم المعلوماتية، الطبعة الأولى، كلية القانون، زين الحقوقية والأدبية، بيروت- لبنان، 2017، ص380.

27- فريد منعم صبور، حماية المستهلك عبر الانترنت ومكافحة الجرائم الإلكترونية- دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2010.

28- فؤاد حسين العزيزي، الجرائم المعلوماتية-دراسة مقارنة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2014، .

29- قدري عبد الفتاح الشهاوي، ضوابط التفتيش في التشريع المصري والمقارن، منشأة المعارف، الإسكندرية، 2005.

30- لؤي الزغبي، الوسائط المتعددة، د.ط، منشورات الجامعة الافتراضية السورية، 2020.

31- محمد الألفي، جرائم النشر الإلكتروني، د.ط، مركز تطويق الإدارة والتنمية، مصر، 2008.

32- محمد أمين الرومي، جرائم الكمبيوتر والانترنت، د.ط، دار المطبوعات الجامعية، الإسكندرية، 2004.

33- محمد أمين الشوابكة، جرائم الانترنت الجريمة المعلوماتية، الطبعة الاولى، دار الثقافة للتوزيع والنشر، عمان الاردن، 2002.

34- محمد جاسم فلحي، النشر الالكتروني الطباعة والصحافة الالكترونية والوسائط المتعددة، د.ط، دار المناهج للنشر والتوزيع، عمان، 2005.

35- محمد جاسم فلحي، النشر الالكتروني في الطباعة والصحافة الالكترونية والوسائط المتعددة، دار المناهج للنشر والتوزيع، عمان، 2006.

36- محمد حدة، ضمانات المتهم أثناء التحقيق، الجزء الثالث، الطبعة الأولى، دار الهدى، 1992.

37- محمد صبحي نجم، شرح قانون العقوبات الجزائري، القسم الخاص، الطبعة الثانية، ديوان المطبوعات الجامعية، الجزائر، 1990.

39- محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، د.ط، دار الجمهورية للصحافة، مصر، 2010.

40- محي الدين تيتاوي، النشر الالكتروني والآخراج الصحفي، د.ط، شركة مطابع السودان للعملة، الخرطوم، 2004.

41- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، الطبعة الاولى، مطابع الشرطة، مصر، .2008

42- منير محمد الجنبهي، ممدوح الجنبهي، التبادل الالكتروني المعلوماتي، د.ط، دار الفكر الجامعي، مصر، .2004

43- مولود ديدان، قانون الإجراءات الجزائية الأمر 11-02 ، د.ط، دار بلقيس، الجزائر الجديدة، .2007

44- ناصر بن محمد البقمي، مكافحة الجرائم المعلوماتية وتطبيقاتها في دور مجلس التعاون لدول الخليج العربية، الطبعة الأولى، مركز الامارات للدراسات والبحوث الاستراتيجية، دولة الامارات العربية المتحدة –أبو ظبي، 2008.

45- نبيل صقر، الوسيط في شرح 50 جريمة من جرائم الأشخاص، شركة دار الهدى للنشر والتوزيع، الجزائر، .2009

46- نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان-الأردن، 2008.

47- هشام عبد العزيز مبارك، تسليم المجرمين بين الواقع والتطبيق، الطبعة الأولى، دار النهضة العربية، القاهرة.

- **الأطروحات ورسائل الماجستير:**

✓ **أطروحات دكتوراه:**

1- تومي يحي، جرائم الاعتداء ضد الأفراد باستخدام تكنولوجيات الإعلام والاتصال، أطروحة دكتوراه، كلية الحقوق، جامعة الجزائر1، 2017-2018.

2- غازي عبد الرحمن، هيان الرشيد، الحماية القانونية من جرائم المعلوماتية (الحاسب والانترنت)، أطروحة لنيل شهادة الدكتوراه في القانون، كلية الحقوق، الجامعة الاسلامية في لبنان، 2004.

3- هروال هبة نبيلة، جرائم الانترنت دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد-تلمسان، 2013-2014، ص75.

✓ **رسائل ماجستير:**

- **أحمد مسعود مريم**، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون 04/09، مذكرة ماجستير، كلية الحقوق و العلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2013.

- **رصاع فتيحة**، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد، تلمسان، 2011-2012.

- **صغير يوسف**، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري-تيزي وزو، 2013.

- **طيبي محمد**، ثقافة الانترنت – دراسة ميدانية لاستعمالات الشبكة بمدينة تيهرت، رسالة ماجستير مقدمة لقسم علم المكتبات والعلوم الوثائقية، كلية العلوم الإنسانية والحضارة الإسلامية، جامعة وهران، 2009-2010

- **محمد بركات الحجار**، أثر الإعلان التجاري على السلوك الشرائي لمستخدمين خدمات الهواتف الذكية المحمولة في مدينة عمان، مذكرة مقدمة لنيل درجة الماجستير، كلية الأعمال، جامعة الشرق الأوسط، 2011

- **مريم ماضوي**، تأثيرات الهاتف النقال على أنماط الاتصال الاجتماعي لدى الطالب الجامعي، مذكرة لنيل شهادة الماجستير، كلية العلوم الإنسانية والاجتماعية والعلوم الإسلامية، جامعة الحاج لخضر، باتنة، 2012-2013، ص105..

- **هناء إسحاق، عبد الرحيم الشيباني**، المسؤولية الجزائية عن جريمتي السب والقذف بالوسائل الالكترونية، أطروحة ماجستير، جامعة الإمارات العربية المتحدة، كلية القانون العام، 2018

✓ **مذكرات ماستر:**

- **بعرة سعيدة**، الجريمة الإلكترونية في التشريع الجزائري–دراسة مقارنة، مذكرة لنيل شهادة الماستر، جامعة محمد خيضر بسكرة، 2015–2016.

- **بوشعرة أمينة، موساوي سهام**، الإطار القانوني للجريمة الإلكترونية –دراسة مقارنة، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة –بجاية.

- **شلاخ لطيفة، قريشي الحاج العربي إبراهيم**، انتشار الجريمة الإلكترونية الماسة بالأشخاص في البيئة الجزائيةٌ دراسة ميدانية لبعض مستخدمي مقاهي النت في مدينة مسيلة، مذكرة لنيل شهادة ماستر في علوم الإعلام والاتصال، كلية العلوم الإنسانية والاجتماعية، قسم العلوم والاتصال، جامعة محمد بوضياف– المسيلة، 2017.

- **طوالبية وئام، ماجن أسماء**، التحرش الجنسي عبر الانترنت، مذكرة ماستر في العلوم الاجتماعية، كلية العلوم الانسانية والاجتماعية، جامعة الجيلالي بونعامة، خميس مليانة، 2015.

- **محمد بوعمرة، سيدعلي بنينال**، جهاز التحقيق القضائي في الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، جامعة آكلي محند اولحاج –البويرة، 2019–2020.

- **مراد يتار**، الجرائم المرتكبة عبر الوسائط الإلكترونية، رسالة لنيل شهادة الماستر في القانون الخاص، تخصص العلوم الجنائية والأمنية، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة القاضي عياض مراكش، 2017–2018.

- **المقالات:**

- **أمل فاضل عبد حسان، أحمد حمد الله**، الإثبات الجنائي في جرائم إساءة الهاتف النقال، مجلة كلية القانون للعلوم القانونية والسياسية، عدد72.

- **أروى محمد تقوى**، مدى مسؤولية مشغلي الهاتف النقال عن إساءة استخدامه في الاتصال بالانترنت- دراسة مقارنة، مجلة الحقوق ، العدد 02، كلية الحقوق، جامعة دمشق.

- **أنيس العذار**، مكافحة الجريمة الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 17، العدد 01، 2018.

- **براهيمي جمال**، مكافحة الجريمة الالكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، العدد2 ، الصادرة في 2016/11/15.

- **بن عميور أمينة ، بوحليس إلهام**، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، مجلة البحوث في العقود وقانون الأعمال، المجلد 7، العدد 01، جانفي 2022.

- **بوضياف اسمهان**، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، سبتمبر 2018.

- **بوعزة نضيرة**، المحاكم ذات الاختصاص المحلي الموسع كآلية لمكافحة الإجرام الخطير، مجلة ميلاف للبحوث والدراسات، المجلد 07، العدد 01، جوان 2021.

- **حاج كولة غانية**، التحرش الإلكتروني الممارس ضد المرأة عبر مواقع التواصل الاجتماعي "الفايسبوك نموذجا"- دراسة حالة معينة من النساء ضحايا التحرش الالكتروني، مجلة العلوم الإنسانية، المجلد 20، العدد 02، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2020.

- **حصة راشد محمد السليطي**، جرائم القذف والسب العلني عبر الانترنت- دراسة مقارنة، المجلة القانونية والقضائية، العدد 01، قطر، 2015.

- **رابح وهيبة**، الجريمة المعلوماتية في التشريع الإجرائي الجزائري، مجلة الباحث للدراسات الأكاديمية، العدد 04، ديسمبر 2014.

- **سعيداني سلامي**، تطور التشريعات والاتفاقيات الدولية في مجال الجرائم المعلوملتية (وقائع ومقاربات)، مجلة الأستاذ الباحث للدراسات القانونية و السياسية، المجلد الأول، العدد العاشر، 2018.

- **عبير بعقيقي، فيصل نسيغة**، الإثبات في الجرائم المعلوماتية على ضوء القانون 04/09، مجلة العلوم القانونية والسياسية، المجلد 09، العدد 02 ، 2018.

- **علي عدنان الفيلا**، إجراءات التحقيق الابتدائي في الجريمة المعلوماتية، مجلة الحقوق، مجلد 08، العدد 12، العراق، 2013.

- **فاطمة العرفي**، تطبيق إجراء التسرب الإلكتروني في القانون الجزائري – إشكالية الموازنة بين حماية حق الخصوصية الرقمية ومكافحة جريمة اختطاف الأشخاص، مجلة دراسات وأبحاث في العلوم الانسانية والاجتماعية. المجلد 13، العدد 04، 2021.

- **فريجة محمد هشام**، النظام القانوني للجريمة المعلوماتية – صعوبات تحقيق الأمن الإلكتروني، حوليات جامعة قالمة للعلوم الاجتماعية والإنسانية، العدد 24 ، جوان 2018

- **ليندا بن طالب**، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، العدد 16، جوان 2017.

- **محمود عبد الحليم سليمان**، إيذاء النساء بأثيولوجيا التحرش الجنسي الإلكتروني بالمرأة، مجلة جيل العلوم الانسانية والاجتماعية، العدد 42، مصر، 2018.

- **محمودي سماح**، مشكلات التفتيش الجنائي عن المعلومات في الكمبيوتر والانترنت، مجلة الحقوق والعلوم السياسية، العدد 08 ، الجزء الأول، جوان 2017.

- **مسعود مواكيز، عبابو فاطمة**، التحرش الجنسي عبر مواقع التواصل الاجتماعي، مجلة آفاق لعلم الاجتماع، العدد 16، جامعة البويرة ، الجزائر، 2018.

- **النصوص القانونية:**

✓ **الأوامر:**

- **أمر رقم 155/66** المؤرخ 18 صفر 1386 الموافق ل 08 يونيو 1966، المتضمن قانون الإجراءات الجزائية، ج ر عدد 47 صادر بتاريخ 09 جوان 1966، المعدل والمتمم.

- **أمر رقم 156/66** المؤرخ في 08 جوان 1966 يتضمن قانون العقوبات، ج.ر، عدد 71، صادر بتاريخ 11 جوان 1966، المعدل والمتمم.

- **أمر رقم 21-11** المؤرخ في 16 محرم 1443 الموافق ل 25 غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق ل 08 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج.ر، عدد65، الصادر بتاريخ 26 أوت، 2021.

✓ **القوانين:**

- **قانون رقم 2000-03** المؤرخ في 05 أوت، يحدد القواعد العامة المطبقة على البريد والمواصلات السلكية واللاسلكية، ج.ر، عدد48، الصادر في 06 أوت 2000، المعدل والمتمم.

- **قانون رقم 14/04** المؤرخ في 10 نوفمبر 2004، المعدل للأمر رقم 66-155 المؤرخ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية، ج.ر، عدد71، الصادر في 2006.

- **قانون رقم 04-15** مؤرخ في 2004/11/10 يعدل ويتمم الأمر رقم 66-156، يتضمن قانون العقوبات، جريدة رسمية عدد 71 ، صادر بتاريخ 2004/11/10 ، المعدل والمتمم.

- **قانون رقم 06-22** مؤرخ في 2006/12/20 يعدل ويتمم الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، ج.ر، عدد 84، صادر بتاريخ2006/12/24.

- **قانون رقم 09-04** لمؤرخ في 14 شعبان 1430، الموافق ل 05 غشت 2009، يتضمن القواعد الخاصة من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر، العدد 47، الصادر بتاريخ 16 غشت 2009.

- **المداخلات :**

- **فضيلة عاقلي**، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر <<الجرائم الإلكترونية>>، طرابلس، بتاريخ 24-25 مارس 2017

- **موسى مسعود أرحومة**، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، 2009.

- **حسين نوارة**، آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة إلكترونيا، الملتقى الوطني" آليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، الجزائر.

- **البحوث الجامعية:**

- **أحمد محمد طلعت عبد الحميد ضرغام**، التحرش الجنسي الالكتروني بالسيدات (ماهيته وسبل مواجهته)، ورقة بحثية في إطار دراسة مادة علم الإجرام والعقاب، كلية الحقوق، جامعة الإسكندرية، 2017.

- **محمد عبد الله المنشاوي**، جرائم الانترنت من المنظور الشرعي والقانوني، بحث مقدم إلى مركز القوانين العربية، مكة المملكة العربية السعودية، 2001.

- **يونس عرب**، تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، ورقة عمل " الاتجاهات التشريعية للجرائم الالكترونية، هيئة تنظيم الاتصالات / مسقط – سلطنة عمان- 24ابريل2006 .

- **المواقع الإلكترونية:**

- **آية عامر**، دراسة الانترنت يسهل التحرش عبر مواقع التواصل الاجتماعي، بحث منشور على الرابط www. shorouk. Com .بتاريخ 15 مارس 2022 على الساعة العاشرة صباحا.

فهرس الموضوعات

فهرس الموضوعات

الموضوع	الصفحة
تشكر	/
إهداء	/
مقدمة	01
الفصل الأول: الإطار المفاهيمي لجرائم الإعتداء على الأشخاص عبر الوسائط الإلكترونية	
المبحث الأول: ماهية جرائم الإعتداء على الأشخاص عبر الوسائط الإلكترونية	10
المطلب الأول: مفهوم الوسائط الإلكترونية	11
الفرع الأول: تعريف الوسائط الإلكترونية	12
الفرع الثاني: خصائص الوسائط الإلكترونية	14
أولا: التفاعلية	15
ثانيا: التنوعية	15
ثالثا: التكاملية	16
رابعا: التزامنية	17
خامسا: الرقمنة الإلكترونية	17
سادسا: المرونة	18
المطلب الثاني: وسائل ارتكاب جرائم الإعتداء على الأشخاص عبر الوسائط الإلكترونية	18
الفرع الأول: الوسائل المادية	18
أولا: جهاز الحاسوب	18
ثانيا: الهاتف الذكي	21
الفرع الثاني: الوسائل التقنية	24

أولا: الانترنت	24
ثانيا: استخدامات الانترنت	25
المبحث الثاني: صور جرائم الإعتداء على الأشخاص عبر الوسائط الإلكترونية	29
المطلب الأول: جريمتي القذف والسب عبر الوسائط الإلكترونية	30
الفرع الأول: تعريف جريمتي القذف والسب عبر الوسائط الإلكترونية	31
أولا: تعريف جريمة القذف عبر الوسائط الإلكترونية	31
ثانيا: تعريف جريمة السب عبر الوسائط الإلكترونية	32
الفرع الثاني: أركان جريمتي القذف والسب عبر الوسائط الإلكترونية	34
أولا: أركان جريمة القذف عبر الوسائط الإلكترونية	33
ثانيا: أركان جريمة السب عبر الوسائط الإلكترونية	38
الفرع الثالث: أساليب جريمتي القذف والسب عبر الوسائط الإلكترونية والجزاءات المقررة لها	41
أولا: أساليب جريمتي القذف والسب عبر الوسائط الإلكترونية	41
ثانيا: الجزاءات المقررة لجريمتي القذف والسب عبر الوسائط الإلكترونية	43
المطلب الثاني: جريمة التحرش الجنسي عبر الوسائط الإلكترونية	45
الفرع الأول: تعريف وأنماط جريمة التحرش الجنسي عبر الوسائط الإلكترونية	46
أولا: تعريف جريمة التحرش الجنسي عبر الوسائط الإلكترونية	47
ثانيا: أنماط التحرش الجنسي عبر الوسائط الإلكترونية	47
الفرع الثاني: صور التحرش الجنسي عبر الوسائط الإلكترونية والجزاءات المقررة لها	48
أولا- صور التحرش الجنسي عبر الوسائط الإلكترونية	49
ثانيا- الجزاءات المقررة لجريمة التحرش الجنسي عبر الوسائط الإلكترونية	51
خلاصة الفصل	52

الفصل الثاني: الإطار التنظيمي لجرائم الإعتداء على الأشخاص عبر الوسائط الإلكترونية	
المبحث الأول: القواعد الإجرائية لجرائم الإعتداء على الأشخاص عبر الوسائط الإلكترونية	55
المطلب الأول: إجراءات التحقيق في الجريمة الإلكترونية	56
الفرع الأول: الإجراءات الخاصة	58
أولا: التسرب واعتراض المراسلات	58
ثانيا: شهادة الشاهد الإلكتروني	61
ثالثا: المراقبة الإلكترونية	63
الفرع الثاني: الإجراءات العامة	65
أولا: المعاينة	66
ثانيا: التفتيش	69
ثالثا: الاستجواب	72
رابعا: الخبرة	72
المطلب الثاني: مرحلة المحاكمة	73
الفرع الأول: تشكيلة واختصاص المحكمة في الجريمة الإلكترونية	73
أولا: تشكيلة المحكمة	73
ثانيا: اختصاص المحكمة في الجريمة الإلكترونية	74
الفرع الثاني: قواعد وإجراءات سير المحاكمة في الجريمة الإلكترونية	76
أولا: القواعد العامة للمحاكمة في الجريمة الإلكترونية	76
ثانيا: إجراءات سير المحاكمة في الجريمة الإلكترونية	78
المبحث الثاني: صعوبات وآليات مكافحة الجريمة الإلكترونية	80
المطلب الأول: صعوبات مكافحة الجريمة الإلكترونية	81

الفرع الأول: صعوبات الاكتشاف	81
أولا: فقدان الآثار التقليدية للجريمة الإلكترونية	82
ثانيا: تعمد الجناة إلى تدابير أمنية من أجل إخفاء جرائمهم	82
ثالثا: التكتم على الجريمة المعلوماتية من قبل الجهات المجني عليها	82
رابعا: نقص الخبرة لدى جهات التحقيق والتحري	82
الفرع الثاني: صعوبات الإثبات	83
أولا: غياب الدليل المادي	83
ثانيا: سهولة إخفاء الدليل وإعاقة الوصول إليه	84
ثالثا: قلة الإبلاغ عن وقوعها	84
المطلب الثاني: آليات مكافحة الجريمة الإلكترونية	85
الفرع الأول: المكافحة التشريعية للجريمة الإلكترونية	85
أولا: مكافحة الجريمة الإلكترونية بموجب القوانين العامة	86
ثانيا: مكافحة الجريمة الإلكترونية بموجب الهياكل الخاصة	91
الفرع الثاني: المكافحة الدولية للجريمة الإلكترونية	96
أولا: الاتفاقيات العربية	96
ثانيا: الاتفاقية الأوروبية	100
الفرع الثالث: التعاون الدولي لمكافحة الجريمة الإلكترونية	101
أولا: المساعدة القضائية	102
ثانيا: تسليم المجرمين	103
خلاصة الفصل	106
خاتمة	108
قائمة المراجع	111

فهرس الموضوعات	122