جامعة محمد لمين دباغين – سطيف(02)

كلية الحقوق والعلوم السياسية

قسم الحقوق

محاضرات مقدمة في مقياس:

الجريمة الإلكترونية

لطلبة الحقوق السنة الثانية ماستر

د/ بوراس نادية

السنة الجامعية: 2023/2022

بسم الله الرحمن الرحيم

مقـــدمـــــة:

تعتبر الجريمة إحدى الظواهر الاجتماعية الأكثر تعقيدا وأشدها فتكا بالمجتمع، وقد شكلت هذه الظاهرة عبر السنين ومازالت هاجسا يؤرق المجتمعات البشرية نتيجة مساسها بالمصالح العامة، بل أصبحت تشكل تهديدا لكيان الدول خاصة في عصرنا الحالي، حيث انفجرت ثورة المعلومات التي كشفت النقاب على تكنولوجية متطورة لم تعرفها البشرية من قبل، اذ شهد العالم من خلالها تطورا كبيرا في مجال الإعلام والاتصال بحيث أصبحت وسيلة العالم نحو الرقي الحضاري والاقتصادي وشكل الوصول إليها رهانا رئيسيا للإنسانية لارتباطها بمختلف جوانب الحياة.

وقد احتلت المعلومة المرتبة الأولى في جميع الدول المتقدمة واكتسبت أهمية في مختلف المجالات واعتبرت معيارا لمدى تحضر وتقدم الأمم، وقد صاحب هذا الاهتمام تطورا ملحوظا في نظم المعلومات الآلية أبرزته تكنولوجيا فائقة السرعة القائمة على الحاسب الآلي كوسيلة رئيسية لتشغيل ومعالجة وحفظ البيانات والمعلومات داخل معظم المؤسسات وبين الأفراد في حياتهم اليومية، وقد كان من الطبيعي أن يصحب هذا التطور التكنولوجي تصاعد السلوك الإجرامي واتخاذه أبعادا جديدة لم يعرفها الفقه والقانون من قبل وبات عليه مواكبة هذه الأنماط الإجرامية بالمنع والقمع.

وقد أخذت الآثار السلبية التي خلفتها التقنية العالية للمعلومات حيزا كبيرا من الدراسات من أجل تحديد مفهومها مما نتج عنه وضع عدة مصطلحات للدلالة عليها من بينها؛ الجريمة الإلكترونية، جرائم الحاسوب، الجريمة المستحدثة، جرائم التقنية العالية، جرائم المعلوماتية، جرائم الأنترنيت، أما المشرع الجزائري فقد اعتمد مصطلح جريمة المساس بأنظمة المعالجة الآلية للمعطيات للدلالة على هذه الجريمة بموجب القانون رقم 15/04، اذ ينصرف هذا المصطلح الى المعلومات والنظم الذي يحتوي عليها وهذا ما تم الاشارة إليه في

المادة الثانية(02) من قانون العقوبات رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

هذه الجريمة التي تعتبر من أخطر الجرائم التي انتشرت في الآونة الأخيرة والتي تعاني منها كل دول العالم، لتأثيراتها السلبية على اقتصادها وسياساتها وحتى على الجانب الأخلاقي والثقافي للمجتمع، لذا تم عقد العديد من المؤتمرات والاتفاقيات الدولية لمواجهتها من بينها اتفاقية بودابست لسنة2001 م، والاتفاقية العربية لسنة2010م، والجزائر على غرار دول العالم، ومن خلال حزمة من النصوص القانونية الردعية تحاول جاهدة التضييق من اتساع هذا النوع المستحدث من الإجرام، اذ جاء المشرع الجزائري بأحكام جريمة المساس بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات لسنة 2004، لأهميتها ومساسها المباشر بالمجتمع وتأثيرها السلبي عليه.

أولا: ماهية الجريمة الالكترونية

ازاء التصدي للجريمة للجريمة الإلكترونية لابد من تأصيل هذه الجريمة من خلال التطرق الى؛ تعريفها وبيان خصائصها والجهود الدولية والوطنية لمكافحتها، بناء على ذلك سيتم التطرق الى:

1-تعريف الجريمة الإلكترونية

إن الجريمة الإلكترونية لا تمثل جريمة ذات طابع خاص يقتضي اخضاعها لقواعد خاصة فهي جريمة من جرائم القانون العام، ولا تجعل منها وسيلة أو محل ارتكابها جريمة ذات نوع خاص ، ورغم ما تحدثه هذه الجريمة من أضرار فإن ذلك لا يبرر النظر إليها على أنها نوع خاص من الجرائم، ذلك أن المبدأ العام أن القانون لا يقيم وزنا من حيث التجريم للوسائل أو الطرق التي يمكن أن تتحقق بها الجريمة.

فالجريمة الإلكترونية هي جريمة ملحقة بالقسم الخاص من قانون العقوبات، ولئن كان لها ذاتيتها الخاصة كسائر جرائم القسم الخاص، واذا كان تعريف الجريمة العادية هي كل فعل او امتناع يقرر له القانون جزاء في صورة عقوبة او تدبير أمن مما ينص عليه قانون العقوبات.

وقد اختلفت التعريفات الفقهية التي تناولت هذه الجريمة فمنها من قلص من تعريفها وعرفها على نحو ضيق ومنها من عرفها على نحو واسع، وبالتالي يمكن تقسيم هذه التعريفات الى طائفتين:

أ- الاتجاه الضيق في تعريف الجريمة الإلكترونية

اعتبر أنصار هذا الاتجاه أن الجريمة الإلكترونية لا تكون جريمة كاملة الأركان إلا إذا استخدم جهاز الحاسوب لتجسيد الركن المادي لها، إذ عرفها البعض على أنها :" الجرائم التي تقع على الحاسب الآلي" وكما عرفت أيضا على أنها:" كل نشاط غير مشروع يستهدف جهاز الحاسوب" وهذا الاتجاه يضيق من تعريف الجريمة الإلكترونية بحصره لها فقط في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية والفنية لأجهزة الحاسب الآلي.

ب- الاتجاه الموسع في تعريف الجريمة الإلكترونية

يرى أنصار هذا الاتجاه أن الجريمة الإلكترونية هي التي تتم في محيط أجهزة الكومبيوتر فأي جريمة يمكن ارتكابها بواسطة جهاز الكمبيوتر أو نظام حاسوبي أو شبكة الحاسوب أو داخل نظامه، فهذه الجريمة هي:" كل فعل غير مشروع مرتكب بواسطة الكومبيوتر والأنترانت أو أي وسية إلكترونية أخرى".

وقد وجهت لهذه النظرية عدة انتقادات أهمها الاتساع والعمومية وأن جريمة المساس بأنظمة المعالجة الآلية للمعطيات تستدعي الرجوع الى العمل الأساسي المكون لها وليس فحسب للوسيلة المستخدمة فيها.

والملاحظ أن قوانين العقوبات نادرا ما تضع تعريف في نصوصها التشريعية هذا ما انتهجه المشرع الجزائري اذ لم يتقيد بتعريف محدد لهذه الجريمة ولا لنظام المعالجة الآلية للمعطيات، وإنما جعل ذلك مرتبطا بالتطورات الواسعة والمستمرة التي تعرفها البيئة الافتراضية، التي قد تقضي بوجود وسائل تقنية جديدة تترتب عنها وجود أشكال أخرى من الجرائم الالكترونية، واكتفى بإعطاء الإطار العام الذي تدخل تحت نطاقه مختلف الجرائم المعلوماتية والتي تستجد مع كل تطور.

وعليه وبالنظر إلى الانتقادات الموجهة للاتجاهين السابقين وأخذ من إيجابيات الرأيين ومقارنتهما مع التعريف العام للجريمة العادية يمكن تحديد تعريف شامل للجريمة الإلكترونية بأنها:" هي كل فعل أو امتناع غير مشروع يهدد بخطر أو ينذر بضرر، باستخدام التقنيات الحديثة كجهاز الحاسوب والهاتف الذكي، وتقع بقصد الاعتداء على حق أو مصلحة أو بيانات يحميها القانون، وهي أيضا الإضرار بالأجهزة والأنظمة والشبكات".

2- خصائص الجريمة الإلكترونية

تنفرد جرائم الحاسب الآلي بسمات تميزها عن الجرائم العادية(التقليدية) سواء تعلق هذا الاختلاف بالجريمة في حد ذاتها أو بالمجرم الالكتروني، وسيتم توضيح ذلك وفق ما يلي:

أ- الخصائص المتعلقة بالجريمة

إن الجريمة الإلكترونية أو جريمة المساس بأنظمة المعالجة الآلية للمعطيات تمس بتقنية المعلومات سواء باعتبارها وسيلة في تنفيذ الجريمة أو محل للجريمة هذا الأمر الذي أضفى عليها مجموعة من السمات التي تميزها عن الجرائم العادية؛ وتتمثل في:

- **جريمة عابرة للحدود الجغرافية**

إن المجتمع الإلكتروني لا يعترف بالحدود الجغرافية فهو مجتمع متفتح عبر شبكات لا تتقيد لا بالزمان ولا بالمكان ولا يخضع لقوانين حراس الحدود، فهذه الجريمة تتسم بالطابع

الدولي، خاصة اذا كان جهاز الحاسوب متصل بشبكة الأنترنت وما ترتبه هذه الأخيرة من جعل معظم دول العالم في اتصال دائم عبر الخط " online" وبالتالي يسهل ارتكاب جريمة المساس بأنظمة المعالجة الآلية للمعطيات من دولة الى أخرى، فهذه الجريمة هي شكلا جديدا من أشكال الجرائم العابرة للحدود الاقليمية بين دول العالم، التي يتم ارتكابها عن بعد وذلك لعدم التواجد المادي في مكان الجريمة ومن ثم تتباعد المسافات بين الفعل الاجرامي وبين النتيجة التي يسعى الفاعل لتحقيقها.

- **جريمة أقل جهدا وعنفا من الجريمة العادية**

إذا كانت الجريمة بصورتها التقليدية تحتاج لجهد عضلي كالقتل والسرقة، الضرب والجرح.....فإن الجريمة الإلكترونية على العكس لا تحتاج لأدنى مجهود عضلي بل تعتمد على الدراية الذهنية والتفكير المدروس القائم على معرفة كبيرة لتقنية الحاسب الالي لذلك سميت بالجرائم اللطيفة، ولذلك كان الشرط الاساسي للمجرم الالكتروني توفر العلم الكافي لكيفية عمل الحاسب الالي وكيفية تشغيله بالإضافة الى الاحاطة ببعض البرامج التشغيلية لهذا الجهاز.

- **جريمة سريعة التنفيذ**

تتم الجريمة الالكترونية في بيئة المعالجة الآلية أو البيئة الإلكترونية، إذ يمكن تنفيذها خلال نصف دقيقة وبضغطة زر فحسب ومحو آثارها في الجزء الآخر من الدقيقة، مما ينتج عنه صعوبة اكتشافها واثباتها وتحديد مكان وقوعها وبالتالي يصعب تحديد القانون الواجب التطبيق، اذ يسهل اخفائها وطمس معالمها وآثارها ودلائلها.

ب- الخصائص المتعلقة بالمجرم الإلكتروني

لا يمكن أن نكون بصدد مجرم عادي في الجرائم الإلكترونية بل لابد أن نكون أمام مجرم له احترافية مميزة في استخدام أجهزة إلكترونية متصلة بشبكة الأنترنت، ولا يشترط المؤهل العلمي العالي المكتسب من الدراسة في المجال الالكتروني فيمكن أن ترتكب هذه

الجريمة بمجرد التفاعل الاجتماعي ودون أي دراسة، هذا ما يجعل هذا المجرم يتصف بمميزات تختلف في جوهرها عن خصائص المجرم العادي؛ ويمكن ذكر أهم هذه الخصائص على النحو الآتي:

- **شخص ذكي**

يتصف المجرم الالكتروني بذكاء عالي وقدر كبير من سرعة الفهم وسرعة الاطلاع والنشاط الذهني المتقدم الذي يسعى إلى خداع مختلف الأجهزة الرقمية حيث يستغل مهارته التقنية في اختراق الشبكات وكسر كلمات المرور أو الشفرات ...، حيث يستطيع أن يكون تصور كامل لجريمته قبل تنفيذها، وما يمكن ملاحظته في العديد من القضايا المطروحة على مختلف المحاكم أن المجرم الإلكتروني متخصص فقط في الجريمة الإلكترونية دون الجرائم العادية ولا تكون له أي علاقة بهذه الأخيرة، لأنه ينتمي إلى إجرام الحيلة.

- **مجرم محترف**

يتمتع هذا النوع من المجرمين باحترافية كبيرة في تنفيذ الجرائم بالكمبيوتر الأمر الذي يقتضي الخبرة والمهارة التقنية، وعلى ذلك لا يمكن لأي شخص أن يرتكب هذا النوع من الجرائم دون المعرفة التامة بكيفية التعامل مع جهاز الحاسوب والأنترنت وكذا الهواتف الذكية المتصلة بشبكة الأنترنت ومختلف البيانات والمعلومات بشكل منهجي دقيق، الأمر الذي يقتضي الكثير من الدقة والتخصص والاحترافية في هذا المجال للتغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر.

- **مجرم غير عنيف**

المجرم الالكتروني لا يلجأ الى العنف الجسدي وإنما قد ينتج عن فعله الإجرامي عنف معنوي كجريمة السب والقذف عبر مواقع التواصل الاجتماعي، أيضا الجرائم الإرهابية الإلكترونية التي تهدف إلى بث الخوف والرعب وسط المواطنين، واذ نتج عن فعله قتل فلا يكون قد لجأ فيه إلى عنف جسدي بل مجرد حيل تقنية كالألعاب الإلكترونية التي خلفت

الكثير من الضحايا ودفعت بالضحايا إلى قتل أنفسهم أو ذويهم دون لجوء المجرم فيها إلى عنف جسدي.

- **مجرم عائد للإجرام**

يعود الكثير من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الكمبيوتر انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وتقديمهم للجهات القضائية المختصة ومحاكمتهم من قبل، هنا تتوفر شروط الحكم عليهم بالعود الى ارتكاب الجريمة.

3- الجهود الدولية و الوطنية لمواجهة الجريمة الإلكترونية

عملت المجتمعات والدول عبر فترات متلاحقة في مواجهة الجريمة الإلكترونية من خلال المنظمات والاتفاقيات الدولية، والجزائر كغيرها من دول العالم اتخذت عدة اجراءات على مستوى المنظومة التشريعية والتنظيمية رغبة من المشرع في التصدي لهذه الجريمة وما يصاحبها من أضرار على الأفراد وعلى مختلف المؤسسات في الدولة.

أ- الجهود الدولية في مكافحة الجريمة الإلكترونية

- **المنظمات الدولية**

الجريمة الالكترونية شكلا جديدا من اشكال الجرائم العابرة للحدود الدولية بين كافة دول العالم ،هذامايجعل ضرورة للتعاون الدولي في هذا المجال .

- جهود الامم المتحدة

عملت الامم المتحدة منذ نشأتهاعلى رسم سياسة ناجحة في مواجهة الجريمة بكل انواعها وذلك من خلال اقرار العديد من التوصيات وانشاءلجان متخصصة وقد توصلت فيمؤتمرها الثامن المنعقد بهفانا سنة 1990 الى اصدار قانون خاص بكل الجرائم الالكترونية ومن اهم هذه توصيات هذا المؤتمر:

- تعزيز التعاون الدولي من اجل منع استخدام شبكة الانترنات في ارتكاب الجرائم المتصلة بالمخذات.
- انشاءاتفاقية عالمية للامن السبيراني.
- نشر دليل يخص منع الجرائم المتصلة باجهزة الكمبيوتر ومكافحتها.
- مجموعة من القواعد الموضوعية والاجرائية في مجال الجرائم الإلكترونية.

- **اتفاقية بودابست2001**

تعتبرهذه الاتفاقية اول اداة لمكافحة الجريمة الالكترونية وهي تابعة لمجلس اوربا ، وقد وقعت على هذه الاتفاقية ازيد من 50 دولة، حددت اهم الاجراءات القضائية والمتعلقة بطلبات المساعدة المتبادلة بين الدول في غياب اتفاقيات دولية.

- **الاتفاقية العربية2010**

تم عقد هذه الاتفاقية بالقاهرة سنة 2010 وقد شارك فيها اغلب وزراء العدل والداخلية العرب، وتهدفالى تعزيز التعاون بين الدول العربية في مواجهة الجرائم الالكترونية.

ب- **الجهود الوطنية في مكافحة الجريمة الإلكترونية**

عمد المشرع الجزائري إلى تعديل العديد من القوانين لجعلها تتماشى والتطورات الإجرامية في مجال تكنولوجيا الاعلام والاتصال كما استحداث قوانين جديدة عامة وخاصة لضمان الحماية الجنائية للمعاملات الإلكترونية، اضافة الى استحداث العديد من الهيئات ، ويمكن بيان ذلك وفق ما يلي:

- **الجريمة الإلكترونية في القوانين العامة**

حاول المشرع الجزائري إصدار العديد من القوانين العامة للتصدي للجريمة الإلكترونية فقام بجهود لمحاربة قراصنة الأنترانت وكيفية القبض عليهم واحالتهم على الجهات القضائية

المختصة متأثرا بذلك بمختلف التشريعات سواء الغربية أو العربية والتي وضعت قوانين تفصيلية لهذه الجريمة، ومن المسائل التي أولها المشرع الجزائري اهتمام في هذا النوع من الاجرام تلك التي تستهدف الأشخاص والأموال وأمن الدولة.

- **الدستور**

لقد كفل الدستور الجزائري لسنة 1996م وكذا مختلف التعديلات الطارئة عليه خاصة دستور 2020م، حماية الحقوق الأساسية والحريات الفردية وعلى أن تضمن الدولة عدم انتهاك حرمة الحياة الخاصة، وقد تم تكريس هذه المبادئ الدستورية بموجب ما تضمنته نصوص قانون العقوبات وما يكمله من قوانين على غرار قانون الاجراءات الجزائية، والتي تهدف بالأساس الى منع المساس بهذه الحقوق.

ومن أهم هذه المبادئ الدستورية ما جاء في المادة 35 :" تضمن الدولة الحقوق الأساسية والحريات" و المادة 39 التي جاء فيها :" تضمن الدولة عدم انتهاك حرمة الإنسان" والمادة 44:" لا يتابع أحد ولا يوقف أو يحتجز إلا ضمن الشروط المحددة بالقانون وطبقا للأشكال التي نص عليها....." فلا يجوز انتهاك حرمة الحياة الخاصة للأفراد وحرمة شرفهم من خلال حماية سرية المراسلات والاتصالات الخاصة بكل أشكالها إذ تنص المادة 47 فقرة 02:".....لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت.....".

- **القانون المدني**

ترتيبا على الأهمية الدستورية لحرمة الحياة الخاصة فقد بين المشرع الجزائري أن كل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصه أن يطلب وفق هذا الاعتداء التعويض عما يكون قد لحقه من ضرر وذلك وفقا لمقتضيات المادة 124 من القانون المدني:" كل عمل أي كان يرتكبه المرء يسبب ضررا للغير يلزم من كان سبب في

حدوثه بالتعويض" فقد جاء هذا النص عاما شاملا لأي اعتداء يقع على أي حق من الحقوق الملازمة للشخص بما فيها الحق في الحياة الخاصة، وقد تطرق هذا النص لمبدأ هام هو حق من وقع اعتداء على حياته الخاصة في التعويض عما لحقه من ضرر .

وعليه 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 الحياة الخاصة على شبكة الأنترنت ، والضرر عنصر متحول وصعب التحديد في الجرائم التي تمس الخصوصية على المواقع الإلكترونية لما تشكله من صعوبة في الإثبات وتحديد لهوية المعتدي.

- **أحكام قانون العقوبات**

تطرق المشرع الجزائري في أحكام قانون العقوبات إلى تجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة للإجرام، مما دفع بهذا المشرع إلى تعديل قانون العقوبات سنة 2001 م بموجب القانون رقم 09/01 المؤرخ في 2001/06/26م المعدل والمتمم للقانون رقم 155/66 المتضمن قانون العقوبات في القسم الأول تحت عنوان :" الإهانة والتعدي على الموظفين ومؤسسات الدولة" فنص في المواد 144 مكرر، 144مكرر2 والمادة 146 على جرائم الإهانة والقذف على رئيس الجمهورية باستعمال مختلف الوسائل الإلكترونية، وقد كان هدف المشرع منع استخدام هذا الفضاء الافتراضي للمساس بأجهزة الدولة.

سنة 2004م قام المشرع الجزائري بتعديل آخر لقانون العقوبات بموجب القانون رقم 15/04 المؤرخ في 2004/11/10م وقصد من ذلك مكافحة الجرائم الإلكترونية الناشئة عن إساءة استعمال هذه التقنية بإضافة قسم سابع مكرر تحت عنوان" المساس بأنظمة المعالجة الآلية للمعطيات" فتضمن هذا القسم تسع مواد من 394 مكرر الى 394 مكرر7، وأدرج ضمن هذه المواد جملة من الجرائم الإلكترونية التي تجعل من جهاز الحاسوب وسيلة

لارتكاب الجرائم كالجرائم الإرهابية الإلكترونية أو جرائم أمن الدولة المرتكبة إلكترونيا، أو التي تجعل جهاز الحاسب الآلي هدافا لارتكاب الجريمة كجريمة الدخول والبقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات.

ومن ضمن ما اعتمد المشرع الجزائري عليه للتصدي للجريمة الماسة بأنظمة المعالجة الآلية للمعطيات في سنة 2009م سن قواعد خاصة في قانون العقوبات تهدف هذه القواعد إلى الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وذلك بموجب القانون رقم 04/09 الذي اعتبر المعلوماتية مال يمكن سرقته وفق المادة 350مكرر01، وقد وضع المشرع من خلال هذا القانون ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراء التفتيش والحجز داخل المنظومة المعلوماتية سعيا منه للحفاظ على النظام العام ومستلزمات والتحقيقات القضائية.

أما سنة 2016 وبموجب القانون رقم 02/16 المؤرخ في 19 جوان 2016 أضاف المشرع مادة قانونية تحمل رقم 394 مكرر8 وقد بين من خلالها العقوبات التي تطبق على مقدم خدمة الأنترانت حال ثبوت مسؤوليته الجنائية ذلك أن دور هذه الفئة يعتبر أساسيا في تشغيل الانترنت.

- **أحكام قانون الاجراءات الجزائية**

أدرك المشرع الجزائري أن المواجهة الفعالة لجريمة المساس بأنظمة المعالجة الآلية للمعطيات لا تكون فقط بإرساء قواعد موضوعية ذات طبيعة ردعية وإنما لابد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية تحفظية والتي من شأنها تفادي وقوع الجريمة الإلكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخطرها.

من أهم ما جاء به في مكافحة هذا النوع من الإجرام تعديل قانون الاجراءات الجزائيةسنة 2006 بموجب القانون رقم 06/22 الذي جاء بإجراءات مستحدثة تطبق على هذه الجريمة لعل من أهمها ما يلي:

تمديد الاختصاص

اذ تم تمديد الاختصاص لوكيل الجمهورية ولضباط الشرطة القضائية إلى كل ربوع الوطن في هذا النوع من الجرائم.

التفتيش

يتم التفتيش في الجريمة العادية من قبل رجال الشرطة القضائية و بموجب اذن كتابي صادر عن وكيل الجمهورية أو قاضي التحقيق ولابد من استظهار هذا الاذن عند التفتيش الذي يمس الأماكن أو الأشخاص كما يجب حضور المتهم أو من ينوبه أو شهود ولا يمكن التفتيش الا في ساعات محددة قانونا من الساعة 05:00 صباحا الى 20:00 مساءا.

أما التفتيش في الجريمة المعلوماتية فيقوم به ضباط الشرطة القضائية الى جانب الجهات القضائية التي يؤول اليها الاختصاص للتحقيق في هذه الجريمة ، كما يمكن اللجوء الى اشخاص مؤهلين كالخبراء والتقنيين في الاعلام الالي لإجراء هذه العمليات – التفتيش– على المنظومة المعلوماتية وتزويد الجهات القضائية بالمعطيات التي تحتاجها، هذا ويجدر الاشارة الى أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في الجريمة العادية وذلك من حيث الشروط الشكلية والموضوعية وفق لما جاء في المادة 07/45 من ذات القانون.

وإن كانت المعطيات المبحوث عنها مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن التفتيش هنا لا يتم إلا بطلب المساعدة من السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

التوقيف للنظر

وتختلف اجراءات التوقيف للنظر بالنسبة للجريمة الماسة بأنظمة المعالجة الآلية للمعطيات عن الجريمة العادية، اذ يمدد هذا التوقيف مرة واحدة فقط وهذا ما جاء في المادة 06/51 من قانون الاجراءات الجزائية.

اعتراض المراسلات

يقصد باعتراض المراسلات تسجيل أو نسخ مختلف المراسلات التي تكون في شكل بيانات قابلة للإنتاج، التوزيع، التخزين، الاستبدال، والاستقبال التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية في اطار البحث والتحري عن الجريمة وأدلتها.

المشرع الجزائري كغيره من التشريعات يسمح لسلطات البحث والتحري اذا استدعت ضرورة التحقيق في جرائم الماسة بأنظمة المعالجة الالية للمعطيات اللجوء الى اجراء اعتراض وتسجيل المحادثات والاصوات والتقاط الصور والاستعانة بكل الترتيبات التقنية اللازمة من أجل الوصول للكشف على ملابسات الجريمة ذاتها دون التقيد بقواعد التفتيش والضبط في الجريمة التقليدية.

حجز المعطيات المعلوماتية : يتم اللجوء لهذا الاجراء عندما يتم اكتشاف معطيات من قبل السلطة التي تباشر التفتيش في منظومة معلوماتية هذه المعطيات تكون مخزنة كما تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة وأن يتم نسخ المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

- **مكافحة الجريمة الإلكترونية وفق القوانين الخاصة**

نظرا لخطورة النتائج المترتبة على هذه الجريمة وتأثيراتها السلبية التي قد تمس مختلف شرائح المجتمع، سعى المشرع الجزائري لوضع قوانين أكثر دقة وتخصص لمواجهة هذا النوع من الإجرام من خلال سن قوانين خاصة لعل أهمها ما يلي:

- **قانون البريد والمواصلات السلكية واللاسلكية**

واكب القانون رقم 03/2000 المؤرخ في 2000/08/05 الذي حدد القواعد العامة المتعلقة بالبريد والمواصلات التطور الذي شهدته مختلف التشريعات العالمية مسايرة للتطور التكنولوجي لذلك بات من السهل إجراء التحولات المالية بطريقة إلكترونية حسب نص المادة

87 منه، وقد تم تعديل هذا القانون بموجب قانون البريد والاتصالات الإلكترونية رقم 04/18 والمؤرخ 2018/05/10 فالأشخاص المرخص لهم تقديم خدمة المواصلات السلكية واللاسلكية والموظفين متعاملو الشبكات العمومية الذين ينتهكون سرية المراسلات أو المساعدة على ذلك يعاقبون وفق المادة 137 من قانون العقوبات التي قرر لمشرع الجزائري من خلالها تسليط عقوبة تتراوح من 03 أشهر الى 05 سنوات وغرامة مالية تقدر ب30000دج الى 500000 دج.

- **قانون تكنولوجيا الاعلام والاتصال**

عرف القانون 04/09 المعدل والمتمم لقانون العقوبات نظام المعلوماتية بأنه نظام منفصل أو هو مجموعة من الأنظمة المتعلقة ببعضها البعض حيث يقوم كل واحد بمعالجة للمعطيات تنفيذا لبرامج أخرى، حيث وضع المشرع من خلال هذا القانون مجموعة من الأحكام الاجرائية الخاصة بالجريمة المعلوماتية في مجال الإعلام والاتصال وقد ركز فيه على إجراء التفتيش وحجز المعطيات.

- **قانون حقوق التأمينات الاجتماعية**

شدد قانون التأمينات الاجتماعية على كل مساس غير مشروع بالبطاقات الإلكترونية للمؤمن له اجتماعيا، وقرر عقوبات ردعية على كل من يستلم بهدف الاستعمال الغير مشروع للبطاقة الإلكترونية للمؤمن له اجتماعيا المفتاح الإلكتروني لهيكل العلاج لمهني الصحة وذلك وفق للمادة 93 مكرر02 من هذا القانون، كما تضاعف هذه العقوبة على كل من يقوم عن طريق الغش بتعديل أو حذف كلي أو جزئي لمعطيات التقنية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا إضافة إلى تشديد العقوبة من سنتين إلى 05 سنوات وغرامة من 500000دج إلى 5000000دج على كل من يحوز أو يصنع أو يوزع بطاقة إلكترونية للمؤمن له اجتماعيا.

- **قانون التوقيع والتصديق الإلكتروني**

نص المشرع الجزائري بموجب القانون رقم 04/15 على القواعد العامة المتعلقة بالتصديق والتوقيع الالكتروني من خلال استحداث مركز شخصنة الشريحة للإمضاء الالكتروني وانشاء سلطة التصديق الالكتروني، وتمكين كافة المتدخلين في نشاط القطاع من امهار الوثائق الادارية والمحررات القضائية بتوقيع الكتروني موثق بهدف اتاحة الخدمات القضائية عن بعد.

وقد أدرج المشرع من خلال هذا القانون نظام الاثبات بالكتابة في الشكل الإلكتروني ضمن قواعد الإثبات والاعتراف بحجية التوقيع والتصديق الإلكتروني في الاثبات، كما نص في المادة 71 من القانون رقم 03/15 على معاقبة كل من يستعمل بطريق غير قانوني العناصر الشخصية بإنشاء توقيع إلكتروني شخص آخر في حين تضمنت المادة 73 عقوبة لكل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية اطلع عليها اثناء قيامه بالتدقيق.

- **الهيئات**

- **الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الاعلام والاتصال**

سنة 2009 تم انشاءهيئة للوقاية من الجرائم المتصلة بتكنولوجيا لاعلام والاتصال ومكافحتها هذه الهيئة التي تعتبر ذات كفاءة وخبرة عالية في مجال الاعلام والاتصال، وتكلف هذه الهيئة ب:

- تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والإتصال ومكافحتها.
- مساعدة مختلف الجهات القضائية والشبه قضائية في التحقيق والتحري.
- جمع واستغلال كل المعلومات التي تسمح بالكشف عن الجرائم الالكترونية ومكافحتها.

- **المعهد الوطني للادلة الجنائية**

تم انشاءهذا المعهد بموجي مرسوم رئاسي رقم 184/04 ، واهم مهامه:

- انجاز الخبرات والتحليل بناءا على طلب من الجهات القضائية سواء في الجريمة التقليدية او الإلكترونية.
- تقديم دعم تقني للجهات القضائية في الجرائم المعقدة والصعبة الاثبات.

ثانيا: أركان الجريمة الإلكترونية

ان الجريمة ظاهرة مركبة الأركان ، ولها جانبين جانب مادي وهو الفعل الصادر عن الجاني وجانب نفسي يتمثل في الحالة النفسية المرافقة للفعل من حيث ما توفر من علم وارادة لدى الفاعل ، فكيان الجريمة هو عدم امكان قيامها على ركن واحد فقط ويرجع هذا التعدد في اركانها ان للانسان كيان مادي هو اعضاء جسده وكيان نفسي، والجريمة سواء العادية او الالكترونية تدور فيهما معا هذا دون اهمال ما نص عليه المشرع من تجريم للفعل وجزاء له :

1- الركن المادي

أ- الركن المادي التام

من المقرر لا جريمة دون ركن مادي يجسد المظهر الخارجي لها ومن خلاله يتقرر الاعتداء على المصلحة المحمية قانونا ولا يتميز الركن المادي في الجريمة الالكترونية عن الجريمة التقليدية الا ما استثني بنص خاص، وعليه فهذا الركن يتكون من:

- السلوك الاجرامي:

هذا السلوك الذي يكون بالفعل او بالامتناع:

الفعل الايجابي: مثل ما جاء في مقتضيات المادة 394مكرر من ق.ع حول الدخول او البقاء عن طريق الغش في منظومة معلوماتية، جرائم النشر، التشهير....

الامتناع: ترتكب هذه الجريمة باتخاذ موقف سلبي وتسمى الجريمة الالكترونية بالامتناع

- النتيجة:

المشرع الجزائري عاقب على تحقق النتيجة في الجريمة الالكترونية كما عاقب على بعض الافعال المشكلة لخطورة محتملة ودون انتضار وقوع اضرار فعلية، مثال : تشديد العقوبة اذا نتج عن الولوج الغير مشروع الى نظام المعلومات والغاء البيانات او البرامج او نسخها او المساس بعمل النظام المعلوماتي وتعطيل كل الشبكة المعلوماتية او الحاسب الآلي.

- العلاقة السببية:

تعني السببية في اطار الركن الماديللجريمة الالكترونية اسناد النتيجة المعاقب عليها لسلوك الفاعل عن طريق الربط بينهما ولا يختلف المفهوم العادي لصلة السببية عما هو عليه الحال في الجريمة الالكترونية.

ب- الركن المادي الناقص

يقصد بالركن المادي الناقص الحالة التي يتوقف فيها السلوك الاجرامي او تخيب اثاره فلا تتحقق النتيجة المطلوبة لتمام الجريمة لسبب خارج عن ارادة الفاعل، اما فيالجريمة الالكترونية فالمشرع الجزائري عمل باحكام المادة 39مكرر7.

ثانيا: الركن المعنوي للجريمة الالكترونية

يتجه الركن المعنوي الى :

- القصد الجنائي
- الخطأ الجزائي

المحور الثالث: أنواع الجرائم الإلكترونية

يمكن التميز بين نوعين من الجرائم المستحدثة:

1- **الجرائم الماسة بانظمة المعالجة الالية للمعطيات وهي كل الجرائم الموجهة ضد جهاز الحاسب الآلي** مثل:

- جريمة الدخول او البقاء غيرمشروع في نظام المعالجة الالية للمعطيات (المادة 394مكرر)
- جريمة التلاعب بمعطيات الحاسب الآلي (394 مكرر 01)

2- الجرائم التي يكون فيها الحاسب الالي وسيلة لارتكاب الجرائم

ترتكب هذه الجرائم :

- **ضد الاشخاص** : كجرايمة القذف ، السب، الجرائم الجنسية ضد الاطفال....
- **ضد الاموال** : جريمة السرقة الالكترونية.....
- **المساس بامن الدولة:** الجرائم الارهابية، الخيانة ، التجسس....