مقدمة

يعد جهاز الكمبيوتر أهم الابتكارات التي توصل إليها العقل البشري، ذلك أن ما يميز هذه الأجهزة الالكترونية هو قدرتها الفائقة على معالجة البيانات وتخزينها واسترجاعها بسرعة وجهاز الحاسب لا يقوم بمهامه إلا بعد تغذيته ببرامج رقمية وتجهيزه إذا تطلب الأمر بالوسائط الضرورية التي تجعله أكثر فعالية وملائمة لمتطلبات العصر بما في ذلك مجال الاتصالات الرقمية كل ذلك يشكل نظاما متكاملا يسمى بالنظام المعلوماتي.

وعليه أضحى استخدام الحاسبات ضرورة لا غنى عنها حيث انه واعتبارا من جوان 2018 كان حولي 55.1% أي ما يقارب 4.21 مليار نسمة كانت قادرة على الولوج و استخدام الانترنت بينما في سنة 1990 كان عدد أجهزة الكمبيوتر الشخصية على مستوى العالم تقدر بـ: 100 مليون جهاز كمبيوتر هذا الانتشار جعل العالم قرية كونية صغيرة تسبح في فضاء إلكتروني تتقلص فيه المسافات.

وفي مقابل هذا التقدم العلمي والتكنولوجي الذي فتح آفاقا ضخمة أمام البشرية لتحقيق مستوى أفضل من الحياة، فإنه يحمل في نفس الوقت مخاطر ضخمة تهدد قيمة حقوق وأمن الأفراد والجماعات وبدت الحاجة الماسة لمواجهة تلك المخاطر، ولعل أول هذه التطلعات كانت نحو القانون الذي يعد من أقدس مهامه وضع الصيغ الملائمة للاستفادة من التقدم العلمي وحماية الحقوق والحريات الأساسية للأفراد، ومن هنا كانت أهمية وجود الضوابط القانونية التي يعمل في إطارها التطور التكنولوجي ودون هذه الضوابط يصبح التقدم العلمي يشكل خطرا على المجتمع وعلى حقوق وأمن المواطنين، وعلى ذلك فقد ظهرت علاقات تربط منظومة الحماية القانونية من الجرائم السيبرانية بالمنظومة القانونية من خلال ما يسمى **بقانون المعلوماتية، هذا الأخير يعمل على حماية النظم المعلوماتية لتداولها ويضع الإطار الصحيح لتداولها كما يعمل على تحقيق هذه الحماية من خلال نصوص خاصة أو من خلال إعمال النصوص التقليدية** وعليه لكي تتضح هذه العلاقة نتعرض أولا لمفهوم النظام المعلوماتي.

تعريف النظام السيبراني

هو كل مكونات الحاسب الآلي(**Hardware**) والمعنوية(**Software**) وشبكات الاتصال الخاصة به(**NetWorks**) و بعبارة أخرى هو: **مجموع العناصر المادية وغير المادية يمكن باجتماعها العمل الفوري مع المعلومة،** فالحاسب الآلي منظور إليه من خلال مكوناته المادية المحسوسة لا يعدو أن يكون كتلة حديدية غير قادرة على القيام بشيء في حد ذاتها ومن تلقاء نفسها فالجهاز لا يبحث ولا يقارن ولا يحسب إلا لأن الإنسان قد أعده وأمده بالمعلومات.

بالنسبة للعناصر المادية: يتمثل أساسا في جهاز الحاسب الآلي ومجموعة من ملحقاته والوسائط التي توصل به لكي يتلقى من خلالها المعطيات والمعلومات أو لكي يخرج من خلالها النتائج بعد المعالجة ويتكون من الوحدات التالية:

- **وحدات الإدخال**
- **وحدات الإخراج**
- **وحدة المعالجة المركزية**

– وحدات التخزين

بالنسبة للعنصر المعنوي: عرفه المنشور الفرنسي الصادر في 22 نوفمبر 1981 بأنها: **(مجموع البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات).**

وكما قلنا سابقا أدى التطور الكبير في نظام الفضاء السيبراني إلى **ظهور مجالات أوسع لاستخدام هذه التقنية مما أدى بدوره إلى ظهور علاقات قانونية تنظم كيفية التعامل والتعاطي مع هذا المستحدث المعلوماتي وحمايته من الاعتداءات والاستعمال غير المشروع،** ووضع قواعد كثيرة بنقل التكنولوجيا المعلومات على الوجه الصحيح وعليه كان لزاما إيجاد منظومة قانونية تتصدى لجميع الموضوعات الناشئة عن هذه العلاقات، **وهذا من خلال تطويع النصوص القانونية التقليدية واستحداث تشريعات جديدة خاصة بنظم المعلوماتية** تشكل بذلك ما يسمى بقانون المعلوماتية.

تعريف قانون المعلوماتية (السيبرانية):

السيبرانية فكرة واسعة ولها قوانينها الضابطة ويمكن تعريف قانون السيبرانية بأنه: **مجموع القواعد والأحكام الواردة في شتى فروع القانون والتي يمكن تطبيقها على مسألة معلوماتية بحسب نوع المشكلة المثارة، والتي قد تخضع لأحكام قانونية متعددة.**

أدى ظهور فكرة المعلوماتية إلى:

- أنها تثير قلقا بالغا إذا استخدمت في انتهاك حقوق الأفراد وحرياتهم العامة خاصة القصر منهم.
- كذلك ساهمت في ابتداع عقود جديدة هي عقود المعلوماتية تعتبر المعلومات محل لها.

نطاق هذا القانون: أي المجالات التي يشملها هذا القانون فهو يشمل القوانين التقليدية كالقانون المدني والجنائي و التجاري ويشمل أيضا قوانين حماية الملكية الفكرية والقوانين الخاصة والاتفاقات الدولية في جانبها المتعلق بموضوع نظام المعلومات فمثلا نجد النظرية العامة للعقد وكذلك مصدرها في القانون المدني وبالتالي فهو يعتبر مصدرا للقانون المعلوماتية فيما يتعلق بالتعاقد الالكتروني حيث يطرح هذا النوع العديد **من التساؤلات عن مدى قانونية ومشروعية هذا النوع من التعاقد وكذلك مدى تطابق هذا التعاقد مع وسائل التعبير عن الإرادة.**

الجريمة المعلوماتية أو السيبرانية في الفكر القانوني

أولا الجريمة **هي فعل غير مشروع صادر عن إرادة جنائية يقرر القانون لهذا الفعل عقوبة أو تدبير امنيا،** وتعرف الجرائم في **صورتها التقليدية** لأنها **كل عمل غير مشروع يقع على الإنسان في نفسه أو ماله أو عرضه أو على المجتمع و مؤسساته ونظمه السياسية والاقتصادية** ومن **زاوية قانونية** تعرف بأنها **كل عمل أو امتناع يعاقب عليه القانون بعقوبة جنائية** فلا جريمة ولا عقوبة إلا بنص.

الجريمة السيبرانية **هي جريمة مستحدثة يعتمد مرتكبها على وسائل تقنية ويكون ذا دراية كافية باستخدام النظم المعلوماتية** والإحاطة بمفهومها الدقيق لا يزال محل خلاف فقهي نختصرها في ما يلي:

هناك التعريف **الضيق للجريمة الإلكترونية:** من خلال تركيز كل فقيه على جانب معين في سبيل وضع هذا التعريف فالبعض ذهب إلى تعريفها انطلاقا من الوسيلة التي يستخدمها المجرم في سبيل القيام بالجريمة في حين ركز جانب آخر على **مستوى معرفة المجرم بالتقنيات الحديثة الحاسوب و تكنولوجيا**

الإعلام والاتصال وجانب ثالث من الفقه ذهب إلى تعريفها **بالتركيز على محلها ألا وهو المال المعلوماتي المعنوي.**

وهناك **التعريف الواسع:** توجه الفقه نحو توسيع المعايير المعتمدة لتعريف الجريمة السيبرانية بأن عرفها البعض **بكل سلوك غير مشروع أو غير اخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها وكل استخدام في صورة فعل أو امتناع من شأنه الاعتداء على أي مصلحة مشروعة سواء كانت ماديه أو معنوية يكون ناتج بطريقه مباشره أو غير مباشرة عن تدخل التقنية المعلوماتية و معاقب عليه قانونا أي كان غرض الجاني.**

التعريف المختلط: تعتبر منظمة التعاون والتنمية الاقتصادية من السباقين لوضع تعريف للغش المعلوماتي والجريمة السيبرانية والذي ذهب إلى القول بأنها **كل سلوك غير مشروع أو يتعارض مع قواعد السلوك الأخلاقي وغير مرخص المعالجة الآلية للمعطيات أو انتقال هذه المعطيات** ومنه الجريمة السيبرانية هي **فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات يهدف إلى الاعتداء على الأموال المادية أو المعنوية** أو هي الجريمة التي يكون النظام المعلوماتي فيها وسيلة لارتكاب جريمة تقليدية إما ضد الأموال كالتحويل الالكتروني غير المشروع للأموال أو ضد الأشخاص جريمة السب والقذف عبر الانترنت

التعريف التشريعي: في سبيل التصدي لهذه الجريمة التي أصبحت تمس بالأمن الوطني تم تعديل الكثير من التشريعات الوطنية والدولية وإدخال هذه الجرائم ضمن النطاق الأفعال المجرمة التي يعاقب عليها القانون وتخصيص عقوبات تحد من انتشارها، ففي الجزائر فقد عالج الأمر 97- 10 المتعلق بحماية حق المؤلف والحقوق المجاورة الملغى بالأمر رقم: 03-05 مسألة التعدي على المصنفات المعلوماتية إذ أدرج هذه الاخيرة بموجب المادة 4 فقرة أ ضمن المصنفات المحمية قانونا، ثم صدر القانون 04-15 المؤرخ في 10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66-156 مؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات، أدرج المشرع فيه قسما كاملا متعلقا بجرائم المساس بأنظمة المعالجة الآلية للمعطيات.

إلا ان تطور هذه الجرائم دفع المشرع الى استحداث قانون متخصص في معالجة الجرائم السيبرانية فصدر سنة 2009 أول نص قانوني هو القانون 09-04 متعلق بالجرائم الالكترونية ومكافحتها والذي وضع من خلاله المشرع الجزائري تعريف للجرائم السيبرانية الإلكترونية والتي اصطلح عليها بمصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وذلك لاستبعاد الغموض والمرونة التي تتميز بها التعاريف الفقهية لهذا النوع من الجرائم، وجاء تعريفها بناء على هذا بالقول:" **الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة اخرى او يسهل ارتكبها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية**".

ومن خلال هذه التعريفات نجد أن التعبير عن الجريمة السيبرانية وتحديد مفهومها تغير وتنوع بحسب الزاوية التي ينطلق منها كل تعريف كما أنه تتزاحم المصطلحات في التعبير عن مدلولها فهناك من يعتمد مصطلح الجريمة السيبرانية وهناك من يصطلح عليها بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال وآخر يسميها بجرائم التقنية العالية وآخر يربطها بجهاز الحاسوب او الكمبيوتر الى جانب جرائم الانترنت ايضا.

اهداف الجرائم المعلوماتية:

تهدف الجرائم المعلوماتية لجملة من الغايات نذكر منها:

1- تحصيل مكسب سياسي أو مادي أو معنوي غير مشروع عبر تقنيات المعلومات كعمليات تزوير بطاقات الائتمان والاختراق وتدمير المواقع على الإنترنت وسرقة الحسابات المالية، فبالنسبة لتجريم تزوير الوثائق الإلكترونية، فقد كان القانون الفرنسي رقم(19) الصادر في يناير 1988 أول التشريعات التي جرمت تزوير المستندات المعلوماتي، فنص في المادة(5/462) على أن كل من ارتكب أفعالا تؤدي الى تزوير المستندات المعلوماتية ايا كان شكلها بأي طريقة تؤدي الى حدوث ضرر للغير فإنه يعاقب بالسجن من سنة إلى خمس سنوات وغرامة لا تقل عن 20 ألف فرنك، ونصت الفقرة السادسة من ذات المادة على معاقبة كل من استخدم بتبصير المستندات المعلوماتية المزورة طبقا للفقرة السابقة بل إنه نص على إمكانية ارتكاب جريمة التزوير خطا لان التغيير والتحريف للمعلومات المخزنة خطأ وإن كان غير متصور في المستندات والوثائق التقليدية إلا انه كثير ما يحدث في المجالات المعلوماتية لان الدخول الى الانظمة المعلوماتية لا يحدث دائما بشكل متعمد فمن الممكن أن يحدث بشكل غير متعمد نتيجة الدخول الخاطئ إليه وهو ما يجب نص عليه في تجريم التزوير في المستندات المعلوماتية.

2- تحصيل معلومات ووثائق سرية للمؤسسات والجهات الحكومية والمصرفية والشخصية و ابتزازهم من خلالها.

3- الوصول لمعلومات غير مخول للعامة الاطلاع عليها بشكل غير مشروع وسرقتها او حذفها او تعطيلها او التعديل عليها لتحقيق مصالح مرتكب الجريمة.

خصائص الجرائم السيبرانية:

ان طبيعة الجرائم السيبرانية وتمييزها عن الجرائم التقليدية يرجع الى الوسط الذي ترتكب فيه الجريمة وهي الاداة او الوسيلة التي استخدمها الجاني في ارتكاب فعله غير المشروع، وتتطلب توفر معرفة او حد أدنى من الثقافة التقنية لدى الجاني وهي لا تخرج عن كونها سلوك اجرامي ينشأ بارتكاب فعل جرمه القانون أو الامتناع عن فعل أمر به القانون و تتجه اليه ارادة الجاني رغم وجود نص قانوني يجرم السلوك

ويمكن إجمال هذه الخصائص في عدة نقاط هي:

- جرائم تتم باستخدام الحاسب الآلي كأداة لارتكاب الجريمة.
- جرائم لا يتم في غير أغلب الأحيان التبليغ عنها خاصة إذا تعلق الأمر بالمؤسسات والشركات التجارية تجنبا للإساءة أو اهتزاز ثقة العملاء، حيث تشير الدراسات انما يتم اكتشافه من جرائم المعلومات يصل إلى نسبة 1% والذي يتم الإبلاغ عنه من هذه النسبة لا يكاد يصل الى 5%فقط.
- جرائم صعبة الاكتشاف لعدم تركها الآثار مادية يمكن من خلالها حل القضية ويطلق على هذه الآثار بالآثار المعلوماتية الرقمية، تكمن صعوبة إثبات مثل هذه الجرائم انها لا تترك في الغالب أثرا ماديا ظاهرا يمكن ضبطه فضلا عن التباعد الجغرافي الذي يثير الإشكال بداية.
- جرائم غامضة لصعوبة إثباتها وذلك بسبب غياب الدليل المرئي و لان اغلب البيانات عبارة عن رموز لا يمكن قراءتها، فالوسيلة المستخدمة لارتكاب الجريمة هي نبضة الكترونية ينتهي دورها خلال أقل من

ثانية واحدة، وكأن الجاني يقوم بتدمير الدليل بمجرد استعماله ويقوم بذلك بكل هدوء و دون احداث اية ضجة وذلك على خلاف الكثير من الجرائم التي نعرف.

- جرائم عابرة للحدود الوطنية تلحق اضرار جسيمة تمس عدة أقاليم، أعطى انتشار شبكة الانترنت امكانية لربط أعداد هائلة من أجهزة الحاسوب المرتبطة بالشبكة العنكبوتية من غير أن تخضع لحدود الزمان والمكان لذلك فإن من السهولة بمكان أن يكون المجرم في بلد ما والمجني عليه في بلد آخر، وهنا تظهر الحاجة لوجود تنظيم قانوني دولي وداخلي متلائم معه لمكافحة مثل هذا النوع من الجرائم وضبط فاعليها، وحيث أن التشريعات الداخلية متفاوتة فيما بينها بين كل دولة من دول العالم تظهر العديد من المشاكل حول صاحب الاختصاص القضائي لهذه الجريمة و اشكالات اخرى متعلقة بإجراءات الملاحقة القضائية.
- جرائم تستدعي الإلمام مرتكبها بالمعرفة التقنية والخبرة الفائقة في مجال الحاسب الآلي وقد تم تصنيف مجرمي الجرائم الإلكترونية إلى المخترقين والمحترفين والحاقدين:

✓ **المخترقون** و يعد شخصا بارعا في استخدام الحاسب الآلي ولديه فضول في استخدام حسابات الآخرين بطرق غير مشروعة، الأمر الذي يدل على انهم اشخاص متطفلين وغير مرحب بهم لدى الغير، واغلبهم ما يكون جانبهم تحدي الشباب للدخول إلى المواقع الرسمية وبعض الاحيان الدخول الى مواقع الحسابات من اجل اثبات الذات وغالبا ما تكون أعمارهم في سن المراهقة.

✓ **المحترفون** وهم الأكثر خطورة بين مجرمي الإنترنت، حيث يهدف البعض منهم الى الاعتداء لتحقيق الكسب غير المشروع المتمثل في الناحية المادية وذلك عبر الدخول في حسابات البنوك، ويدخل البعض من اجل تحقيق اغراض سياسية والتعبير عن وجهة نظره أو فكرة، وغالبا تكون أعمار هؤلاء بين 25 و 40 سنة.

✓ **الحاقدون** وهم الذين ليس لديهم أي أهداف للجريمة ولا يسعون لمكاسب سياسية او مادية ولكن يتحركون لرغبة في الانتقام والتأثر بالأمور الطائفية.

- جرائم لا تمتاز بالعنف، لا يستخدم مرتكبها القوة الجسدية والعضلية للقيام بالجريمة.

خصائص المجرم معلوماتي:

1- **المجرم المعلوماتي مجرم متخصص:** تبين في عديد من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر اي انهم يتخصصون في هذا النوع من الجرائم دون أن يكون لهم اي صلة بأي نوع من الجرائم التقليدية الأخرى، مما يبين أن المجرم الذي يرتكب الجريمة المعلوماتية هو مجرم في الغالب متخصص في هذا النوع من الإجرام.

2- **المجرم المعلوماتي مجرم عائد إلى الإجرام:** يعود كثير من مجرمي المعلومات الى ارتكاب جرائم أخرى في مجال الكمبيوتر انطلاقا من الرغبة في سد الثغرات التي أدت الى التعرف عليهم وتقديمهم إلى المحاكمة في المرة السابقة ويؤدي ذلك إلى العودة إلى الإجرام، وقد ينتهي بهم الأمر كذلك في المرة التالية إلى تقديمهم للمحاكمة.

3- **المجرم المعلوماتي مجرم محترف:** يتمتع المجرم المعلومات باحترافية كبيرة في تنفيذ جرائمه حيث انه يرتكب هذه الجرائم عن طريق الكمبيوتر، الأمر الذي يقتضي الكثير من الدقة و التخصص والاحترافية في هذا المجال للتوصل إلى التغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما في حالة البنوك والمؤسسات العسكرية.

4- **المجرم المعلوماتي مجرم غير عنيف:** المجرم المعلوماتي من المجرمين الذين لا يلجؤون الى العنف بتاتا في تنفيذ جرائمهم وذلك لأنه ينتمى الى **الاجرام حيلة** فهو لا يلجأ إلى العنف في ارتكاب جرائمه وهذا النوع من الجرائم لا يستلزم أي قدر من العنف للقيام به والى جانب ما تقدم فالمجرم المعلوماتي ذكي فضلا على أنه متكيف اجتماعيا.

5- **المجرم المعلوماتي على قدر كبير من المعرفة التقنية:** تميز المعرفة مجرمي المعلوماتية حيث يستطيع المجرم المعلوماتي أن يكون تصورا كاملا لجريمته ويرجع ذلك إلى أن المسرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة وذلك قبل تنفيذ الجريمة.

6- **المجرم المعلوماتي لديه الباعث:** الباعث هو الرغبة في تحقيق الربح المادي بطريقة غير مشروعة ويظل هو الباعث الأول وراء ارتكاب الجريمة المعلوماتية ويمكن أن يكون الباعث هو الانتقام من رب العمل، وكمثال عن ذلك في انجلترا أدانت المحكمة المدعو (whitaker) بارتكابه الجريمة المنصوص عليها في المادة الثالثة من قانون إساءة استخدام الحاسوب، وتتلخص وقائع هذه الدعوى بقيام (whitaker) بتطوير برنامج لأحد زبائنه مقابل مبلغ من المال وقد تم إبرام عقد بينهما لهذه الغاية، إلى أنه نتيجة للخلاف حول دفع قيمة البرنامج قام المشتكى عليه بزرع فيروس في البرنامج الأمر الذي أدى إلى عدم إمكانية استخدامه ولقد أثار المشتكى عليه دفعا مفاده بأنه يملك الحق في فعل ذلك بدعوى أنه لا يزال يملك حقوق التأليف الخاصة بالبرنامج، ولم تقبل المحكمة هذا الدفع بدعوى أن هذا الأمر لم يرد النص عليه في العقد المبرم بينهما، أو مجرد الرغبة في قهر نظام الحاسب واختراق حاجزه الأمني، فالمجرم المعلوماتي قد يكون شخص مزدر من القانون أو لديه شعور بأنه فوق القانون.

7- **يتمتع المجرم المعلومات بقدر من المهارة:** يتطلب تنفيذ الجريمة المعلوماتية قدر من المهارة يتمتع بها الفاعل وهذه ليست قاعدة ثابتة ذلك انه هناك الكثير من انجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب هذا النوع من الجرائم.

8- **المجرم المعلوماتي يمتلك خيال النشط وحب انتحال الشخصيات، و حب المخاطرة والتلاعب.**

أسباب ارتكاب الجريمة المعلوماتية:

إن أسباب انتشار الإجرام المعلوماتي تتأثر بلا شك بالثورة المعلوماتية وإذا كانت الأنماط المختلفة للمجرمين المعلوماتيين(مخترق ومحترف وحاقد) تكشف لنا عن اشتراك هؤلاء عند ارتكابهم الجريمة المعلوماتية في غرض واحد هو مجرد الهواية واللهو في بداية الأمر وذلك نتيجة انبهارهم بالثورة المعلوماتية والحاسبات الآلية، ومن ناحية أخرى قد يكون رغبة هؤلاء المجرمين في تحقيق الثراء السريع يمثل أيضا أحد أسباب انتشار

الإجرام السيبراني وأخيرا قد تكون الأسباب الشخصية للمجرمين هي أحد أسباب ذلك، وعليه يمكن تلخيص أسباب انتشار الجريمة المعلوماتية فيما يلي:

- **الولع بجمع المعلومات:** هناك من يقوم بارتكاب جرائم الكمبيوتر بغية الحصول على الجديد من المعلومات، فيرى قراصنة الكمبيوتر ان الحصول على المعلومة يجب ان لا يكون عليه أي قيد، فالقرصان يكرس كل جهده في تعلم كيفية اختراق المواقع المحمية وغالبا ما يكون القراصنة مجموعات الهدف منها التعاون وتبادل المعلومات وتقاسم البرامج والأخبار
- **تحقيق مكاسب مالية:** قد تدفع حاجة البعض الى تحقيق الثراء السريع عن طريق إتاحة الاطلاع على معلومات معينة أساسية ذات أهمية خاصة لمن يطلبها.
- **الدوافع الشخصية:** يتأثر الإنسان في بعض الأحيان ببعض المؤثرات الخارجية التي تحيط به في بيئة المعالجة الآلية للمعلومات مع توافر هذه المؤثرات فإن الأمر يؤول في النهاية إلى ارتكابه لجريمة معلوماتية هذا وتتعدد المؤثرات التي تدفع الإنسان الى اقتراف مثل هذا السلوك سواء كان ذلك بدافع اللهو أو الانتقام .

تصنيف الجرائم المعلوماتية

اذا كانت الجريمة المعلوماتية تعرف بأنها كل فعل او امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية، وعليه يمكن تصور الجريمة المعلوماتية من جانبين كونها وسيلة لارتكاب الاعتداءات وان المعلوماتية محل الارتكاب هذه الاعتداءات.

1- المعلوماتية كوسيلة لارتكاب الاعتداءات

يتعلق الأمر في هذا الإطار باستخدام المعلوماتية كوسيلة لارتكاب الفعل الجرمي وتقسم غالبا إلى جرائم الأشخاص وجرائم الأموال.

أولا: جرائم المعلوماتية ضد الأشخاص

الجرائم ضد النفس او الاشخاص هي الجرائم التي تنال بالاعتداء او تهدد بالخطر الحقوق ذات الطابع الشخصي البحت أي الحقوق اللصيقة بالشخص المجني عليه، والتي تعتبر من بين المقومات الشخصية لأهميتها الاجتماعية.

والمقصود من التطرق لموضوع جرائم الاعتداء على الحياة الخاصة للأشخاص التعرض تلك الجرائم التي يتعذر علينا مواجهتها بالنصوص التقليدية، فالاعتداء عليها يتم بواسطة هذه التقنية، وحيث إن عناصر الحق في الحياة الخاصة يتكون من عناصر ليست محل اتفاق بين الفقهاء فيمكن القول بأنها تشمل حرمة جسم الإنسان والمسكن والصورة والمحادثات والمراسلات والحياة المهنيه.

اما علاقة الحياة الخاصة بالتقنية الالكترونية فقد ظهرت أهميتها بانتشار بنوك المعلومات في الاونة الاخيرة لخدمة أغراض متعددة وتحقيق أهداف المستخدمين في المجالات العلمية والثقافية والعسكرية، ففي فرنسا أصدر المشرع القانون رقم (17) لسنة 1978 الخاص بالمعالجة الآلية للبيانات والحريات، وتضمن الباب الأول من ذلك القانون مجموعة من المبادئ القانونية التي اشارت الى ان المعالجة الإلكترونية للبيانات يجب أن تكون لخدمة المواطن فقط ولا يجوز أن تتضمن اعتداءات على شخصيته أو حياته الخاصة وحرياته، وفي الباب

الثاني انشأ ذلك القانون ما أطلق عليه اللجنة القومية الخاصة بمراقبة تنفيذ أحكام هذا القانون ووجوب استشارة اللجنة قبل معالجة البيانات، وورد في القانون استثناءان يتعلق الأول بحالة جمع البيانات الضرورية في إثبات الجرائم و بشرط ان يكون هذا التخزين لدى جهات قضائية او لدى السلطات العامة، والثاني يتعلق بحرية الصحافة بنشر البيانات الشخصية المعالجة في موضوع معين في اطار حرية التعبير.

اما في امريكا فهناك أكثر من قانون لحماية البيانات أو الحياة الخاصة، وكان أول قانون صدر بهذا الخصوص سنة 1970 لحماية البيانات وحق الوصول إليها لتصحيح البيانات غير الصحيحة وجاء في المادة 552 /أ على أنه لا يجوز لأية جهة أن تنشئ أي معلومات يتضمنها نظام المعلومات بأي وسيلة من وسائل الاتصال لأي شخص او لأي جهة اخرى ما لم يكن ذلك بناء على طلب كتابي و بموافقة صاحب الشأن الذي تتعلق به المعلومات، وتم إيراد استثناءات على هذا النص في حالة ما إذا كان ذلك تحقيقا للمصلحة العامة أو إجابة لأمر المحكمة، كذلك صدر في الولايات المتحدة الأمريكية قانون خصوصية الاتصالات الإلكترونية سنه 1986.

بينما الحال في بريطانيا مختلف عن فرنسا وأمريكا حيث أنها ترفض أن تعترف باستقلالية الحق في الحياة الخاصة، ففي قضية كوريللي ضد وول الشهيرة حيث قام المدعى عليهم بنشر وبيع صور المدعية دون إذنها الأمر الذي دفعها للقضاء وطلب التعويض وإيقاف النشر والبيع رفضت المحكمة الحكم لها على اساس ان ادعائها لا يرتكز إلى أي أساس من القانون، فليس هناك نص يجرم هذا وان نشر الصورة لا ينطوي على التشهير بالمدعية، وعلى هذا المنوال سار القضاء الإنجليزي في العديد من الأحكام مستندا في ذلك إلا أن فكرة الخصوصية في حد ذاتها هلامية غير محددة المضمون وتمس مسائل حساسة دستورية وسياسية ولا أساس قانوني لإمكانية الاضرار به ومن الصعوبة بمكان وضع حدود فاصلة بين ما يعد من العموم وما يعد من الخصوص، بالإضافة إلى انه لا توجد سوابق قضائية في هذا الخصوص.

غير ان هذا الاتجاه لا يمكن ان نأخذ به على اطلاقه في انجلترا حيث توجد العديد من النصوص التي تحمي الحياة الخاصة متناثرة بين القانون المدني والجنائي كنصوص التشهير والقذف الواردة في قانون العقوبات الانجليزي، ونصوص التعدي على ملكية الغير، والمضايقات والإخلال بالثقة، وقانون التلغراف السلكي عام 1949، وقانون البريد العام عام 1967.

جرائم الشرف والاعتبار: في هذا الإطار غالبا ما يقوم المجرم بنشر معلومات في الانترنت قد تكون سرية أو مضللة عن ضحيته والذي قد يكون فردا أو مؤسسة وتتعدد الوسائل المستخدمة في هذا النوع من الاعتداءات ولعل أهمها الدخول إلى الملفات المخزنة واخذ المعلومات الخاصة والسرية للأفراد، مما يفسح المجال لإيقاع الإضرار بهم عن طريق نشر هذه المعلومات أو استخدامها في غير الغاية المحددة لها.

الجرائم الجنسية:

إن الاستخدام اللاقانوني واللأخلاقي لشبكة الانترنت غالبا ما يؤثر على آلاف المستخدمين خاصة من فئة الأحداث، حيث يقع البعض منهم عرضة للاستغلال الجنسي بعد إيهامهم بالرغبة في تكوين علاقات صداقة، هذه العلاقات التي يسعى المجرمون إلى تطويرها لغايات إجرامية في نفوسهم من هذه الجرائم تحريض القاصرين على أنشطة جنسية كالتحرش الجنسي وترويج الدعارة، وعلى صعيد آخر فإن فئة الأطفال هم أكثر ضحايا

جرائم المعلومات، والإحصائيات العالمية تشير إلى أن 21 %من الأطفال الذين يستخدمون البريد الالكتروني يستقبلون رسائل بريد الكتروني دعائية كل يوم وبخاصة خلال فترات العطلة، حيث يقضي الكثير منهم الوقت في تصفح الانترنت، وغالبا ما يتم استدراج الأطفال عن طريق غرف الدردشة، وطلب صورهم للعبث بها ونشرها خصوصا بالنسبة لفئة الفتيات.

ثانيا: جرائم المعلوماتية ضد الأموال

تشمل جرائم السطو على أرقام البطاقات الائتمانية، لعب القمار، التزوير، الجريمة المنظمة والمخدرات وغسيل الأموال، ولعل جرائم هذا القسم اوضح كونها مجرمة حيث لا تختلف في نتيجتها عن جرائم التقليدية إلا أنه توجد اختلافات في تصنيف هذه الجرائم.

1- السطو على أرقام البطاقات الإئتمانية: بدأ مفهوم التجارة الإلكترونية ينتشر منذ السبعينيات وذلك لسهولة الاتصال بين الطرفين ولإمكانية اختزال العمليات الورقية والبشرية، فضلا عن السرعة في إرسال البيانات وتخفيض تكلفة التشغيل والاهم هو إيجاد أسواق أكثر اتساعا، والتاريخ حافل بأسماء الذين قاموا بسرقات كثيرة من أشهرها قضية الأمريكي "كيفين ميتنيك" الذي قام بسرقة الأرقام الخاصة بـ 20 ألف بطاقة ائتمان وقد تم القبض عليه والحكم عليه بالسجن لمدة عام ولكنه لم يخرج من السجن على اعتبار أنه لا توجد شبكة لا يستطيع اختراقها وقد تعالت الأصوات المطالبة بالإفراج عنه، كما ظهرت جماعات تقوم بعمليات قرصنة باسمه.

2- القمار عبر الانترنت: ويمكن تقسيم الطرق التي تتم ممارسة القمار على الانترنت من خلالها إلى ثلاث فئات: اليانصيب المراهنات وألعاب الكازينو، حيث يمكن لأي مستخدم أن يبدأ لعب القمار بعد قيامه بالخطوات التالية تحميل البرنامج المجاني من موقع القمار، ومشروعية الجريمة قد تختلف داخل البلد الواحد، فنجد أن داخل الولايات المتحدة الأمريكية ألعاب القمار عبر الانترنت مسموح بها في ولاية لاس فيغاس، بينما هي محرمة قانونا في ولاية نيويورك.

3- تزوير البيانات: تعد من أكثر الجرائم انتشارا فلا تكاد تخرج جريمة من جرائم نظم المعلومات من شكل من أشكال تزوير البيانات وتتم عملية التزوير بالدخول الى قاعدة البيانات وتعديل البيانات الموجودة بها او اضافة معلومات مغلوطة بهدف الاستفادة غير المشروعة من ذلك.

و من التطبيقات القضائية في هذا الشأن قضية الولايات المتحدة ضد Zezev حيث تتلخص وقائع هذه الدعوى:" بقيام شخص يعمل في شركة مقرها كازاخستان باختراق النظام المعلوماتي العائد لشركة تعمل في ولاية نيويورك الأمريكية تقوم بتزويد الأخبار والمعلومات المالية إلى كافة أرجاء العالم، حيث تمكن المشتكى عليه من الدخول إلى البريد الالكتروني الخاص بمدير الشركة ومدير الأمن فيها، الأمر الذي مكنه من الحصول على معلومات بالغة السرية ليقوم بعدها بإرسال عدد من الرسائل الالكترونية إلى مدير الشركة لإخباره بأن النظام المعلوماتي الخاص بالشركة قد تم اختراقه، وطالب بمبلغ قدره 200 ألف دولار مقابل عدم قيامه بنشر واقعة الاختراق وهو ما يضر بسمعة الشركة ويلحق بها خسائر مالية كبيرة، تم اعتقال المشتكى عليه في مدينة لندن أثناء حضوره لاستلام المبلغ المتفق عليه بعد أن اخبر مدير الشركة الشرطة بذلك، وطالبت الولايات المتحدة الأمريكية ترحيله إليها لمحاكمته بعد أن تم توجيه ست تهم إليه من بينها التآمر لإتلاف البيانات المخزنة

وهي الجريمة التي يعاقب عليها بمقتضى المادة الثالثة من القانون، وقد قضت محكمة الاستئناف بتأييد قرار محكمة الدرجة الأولى بالموافقة على تسليم المشتكى عليه إلى الولايات المتحدة باعتبار أن فعل الشخص المطلوب تسليمه ارتكب جريمة يعاقب عليها بموجب المادة الثالثة من قانون إساءة استخدام الحاسوب لعام 1990 .

4- الجرائم المنظمة: يتبادر الى الذهن عند التحدث عن هذه الجريمة عصابات المافيا لأنها من أشهر المؤسسات الإجرامية المنظمة والتي تبادر بالأخذ بالوسائل التقنية الحديثة سواء في تنظيم او تنفيذ اعمالها ومن ذلك إنشاء مواقع خاصة بها على شبكه الانترنت لمساعدتها في إدارة العمليات وتلقي المراسلات واصطياد الضحايا و توسيع أعمالها وغسيل الأموال.

5- تجاره المخدرات عبر الانترنت: في عصر الانترنت اضيف الى اولياء الامور مخاوف جديدة لا تقتصر على رفقاء السوء فقط، بل يضاف إليها مواقع السوء التي لا تتعلق بترويج المخدرات وتشويق النَشْئ لاستخدامها فقط بل تتعداه إلى تعليمهم كيفية زراعة وصناعة المخدرات بكافة أصنافها و بأبسط الوسائل المتاحة، كما أن مشروعية الجريمة أمر نسبي من دولة الى أخرى فمثلا تجارة المخدرات محرم نهائيا في بعض البلدان مثل الجزائر والأردن بينما في الدول الاسكندينافية مصرح بها في حدود الاستعمال الشخصي فقط.

6- غسيل الأموال: يعرف غسل الأموال بأنه أي عملية من شأنها إخفاء المصدر غير المشروع الذي اكتسب منه الأموال، وتلعب التجارة الالكترونية دورا مهما في عقد الصفقات عبر الانترنت كصفقات السيارات والعقارات أو المعادن الثمينة، كما يمكن للأنظمة الحاسوبية التي تعمل في البنوك في مساعدة المجرمين على ايداع اموالهم ذات المصدر المشبوه ومن ثم اعادة سحبها في الخارج بعمولات صعبة كالدولار .

7- الإرهاب السيبراني: لا يوجد اتفاق عالمي على ماهية الأفعال الجرمية التي يمكن أن يطلق عليها إرهابا، إلا أنه يشترط ان يكون للفعل الاجرامي اهداف و اغراض سياسيه حتى يمكن اعتباره إرهابا ومجال الإرهاب بواسطة الحاسوب والانترنت واسع وكبير خاصة مع تنامي انتشار الحواسيب حول العالم وزيادة الحرص على ربطها بالانترنت.

2- المعلوماتية محل لارتكاب الاعتداءات

بالنظر إلى الطبيعة الخاصة للأنظمة المعلوماتية الموصولة بشبكة الانترنت فان الأفعال الجرمية المرتكبة تعد مستحدثة لارتباطها في اغلب الاحيان اما بأمن الأنظمة المعلوماتية وسلامتها أو بسرية البيانات والمعلومات التي تحتويها تلك الأنظمة.

أولا: التدمير المتعمد للأنظمة المعلوماتية

نعني بالأنظمة المعلوماتية في شبكة الانترنت المعدات، الآلات والمعلوماتية، الكمبيوتر والبرامج وقواعد وبنوك المعلومات ومواقع الويب ومنتديات المناقشة والمجموعات الإخبارية وكل وسيلة معلوماتية أخرى مخصصة لصناعة أو معالجة أو لتخزين أو الاسترجاع أو لعرض أو لنقل أو لتبادل المعلومات، وتطبيقا لذلك أدانت محكمة ولاية نيوجيرسي في الولايات المتحدة ديفيد سميث حيث اسند إليه تهمة إنتاج "فيروس ميليسا" الذي اجتاح الولايات المتحدة عام 1999 وتسبب في عطل أكثر من مليون جهاز حاسب آلي وخسارة مالية قدرت بحوالي 80 مليون دولار وتم الحكم عليه وفقا للفقرة (A1030) البند الخامس من المرسوم رقم (18) الذي

يعاقب على إتلاف البرامج والتسبب في الإضرار اجهزة الحاسب الالي المحمية والتي عرفها ذلك القانون بأنها اجهزة الحاسب الالي العاملة لدى الحكومة أو لدى المؤسسات المالية والتجارية.

ثانيا: انتهاك سرية البيانات

رغم أن وسائل المعلوماتية قد تسهل على الفرد تجميع البيانات وتخزينها ومعالجتها في أوقات قياسية إلا أنها قد تمثل تهديدا مباشرا وتحديا الحياة الخاصة والحريات الفردية أن كل اتصال بالانترنت يمكن ان يترك اثرا ما حتى وإن لم يدرك مستخدم الشبكة ذلك، في فرنسا فان القانون العقوبات الفرنسي الصادر عام 1993 نظم هذه المسألة أيضا فنص في المادة 3/323 كل من يدخل بطريقة مخادعة لمعطيات داخل نظام المعالجة الآلية أو من يحذف أو يعدل بطريقة مخادعة معطيات موجودة في النظام فإنه يعاقب بالسجن لمدة ثلاث سنوات وغرامة قيمتها 300 ألف فرنك فرنسي.

ثالثا: قرصنة البرامج

أصل مصطلح قرصنة يرجع إلى عملية السلب والنهب وكل ما يؤخذ بطريق السرقة والنصب في البحر استخدم لاحقا للدلالة على قيام البعض بالسطو على مؤلفات الآخرين واستخدامها بغير وجه حق.

مفهوم المعطيات الشخصية ومعالجتها الآلية

أفاد قانون حماية الأشخاص الطبيعيين في مجال في معالجة المعطيات الشخصية بان هذه الأخيرة هي:" كل معلومة بغض النظر عن دعامتها، متعلقة بشخص معرف أو قابل للتعرف عليه المشار آلية في هذا القانون بمصطلح الشخص المعني بصفه مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم قد التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الاجتماعية".

والمعطيات الشخصية تطورت مع تطور الإنترنت، فلم يعد المتاح منها الاسم، اللقب والعنوان البريدي بل زادت وتنوعت لتشمل صورة الشخص وصوته، علاوة على طائفة أخرى من البيانات التي تتعلق بقدرته المالية وسلوكياته وعادته وميوله وأذواقه، والأشد من ذلك كله، البيانات التي تتعلق بجسم الإنسان "البيانات البيومترية" فالمعطيات الشخصية قد تحتوي على بيانات حساسة متعلقة بالحياة الخاصة للأفراد وهذا الحق هو عصب الحرية الشخصية وركيزة أساسية لحقوق الإنسان والحريات العامة، مما يتطلب الاحترام من قبل السلطات والأفراد، كما يقتضي في الوقت ذاته أن تكفل له حماية ضد الانتهاك غير المشروع لهذا الحق.

وعلى ذلك استرسل المشرع في ضبط المفاهيم المتعلقة بالمعطيات الشخصية الى تعرضه لمفهوم المعطيات الحساسة وهذا بنصه الصريح على أن:" **المعطيات الحساسة هي معطيات ذات طابع شخصي تبين الأصل العرقي أو الإثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني، أو تكون متعلقة بصحته بما فيها معطياته الجينية**".

كما بين ذات القانون في المادة 3 منه، أن المقصود بمعالجة المعطيات الطابع ذات الشخصي هو كل عملية أو مجموعة من العمليات بطرق تنجز بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملائمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال، عن طريق الإرسال أو النشر أي شكل آخر من أشكال الإتاحة أو التقريب أو الربط

البيني وكذا الإغلاق أو التشفير أو المسح أو الإتلاف، وبين أن المعالجة الآلية للمعطيات الشخصية هي مجموع العمليات المنجزة كليا أو جزئيا بواسطة طرق آلية، مثل تسجيل المعطيات و تطبيق عمليات منطقيه و/أو حسابية على هذه المعطيات أو تغييرها أو مسحها أو استخراجها أو نشرها.

وفي هذا الصدد نشير إلى أن ملف المعطيات الشخصية ذات طابع الشخصي هو كل مجموعة مهيكلة من المعطيات ذات الطابع الشخصي، يمكن الولوج إليها وفق معايير معينة، سواء كانت هذه المجموعة ممركزة أو غير مركزة أو موزعة بطريقة وظيفية أو جغرافية مثل المحفوظات وبنوك المعطيات والملفات الإحصاء.

المبادئ الأساسية لحماية المعطيات الشخصية

حدد القانون رقم 18-07 في الباب الثاني منه أن المبادئ الأساسية التي ترتكز عليها عملية حماية المعطيات الشخصية، ومن ثم فإن احترامها و تكريسها يشكل ضمان قانوني هام لحماية هذا الحق وباستقراء أحكام هذا الباب نجد أن هذه المبادئ تتمثل في:

1. **مبدأ الموافقة المسبقة والصريحة للشخص المعني:**

أفاد قانون حماية المعطيات الشخصية بأنه لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلا بالموافقة الصريحة للشخص المعني، والذي له أن يتراجع عنها في أي وقت كما حدد الحالات التي تكون معالجتها ضرورية ومن ثم فإن موافقة الشخص المعني لا تكون واجبة.

مع العلم انه لا يمكن اطلاع الغير على المعطيات ذات الطابع الشخصي الخاضعة للمعالجة إلا من اجل انجاز الغايات المرتبطة مباشرة بمهام المسؤول عن المعالجة والمرسل إليه، وبعد الموافقة المسبقة للشخص المعنى، وعليه تعتبر غير معالجة غير مشروعة كل معالجة في غياب هذا الرضا المسبق، فهذا الأخير يحل كل خلاف يمكن أن ينشأ بين المسؤول عن المعالجة والشخص المعني، إذ أم ممارسة كل منهما لحقوقه وواجباته تتوقف على جواب الشخص المعني.

2. **مبدأ المشروعية:**

أوجب المشرع الجزائري أن تتم معالجة المعطيات الشخصية وبخاصة في البيئة الرقمية بطريقة مشروعة ونزيهة، وذلك باحترام المقتضيات القانونية اللازمة والتقيد بالإجراءات المقررة لذلك، كما يجب أن تكون المعطيات الشخصية مجمعة لغايات محددة وواضحة ومشروعة، وان تكون كل معالجة لاحقة متناسبة مع هذه الغايات.

3. **مبدأ التناسبية:**

يستوجب هذا المبدأ أن تكون المعطيات ذات الطابع الشخصي ملائمة ومناسبة وغير مفرطة بالنظر للغايات التي تم على أساسها تجميعها في البداية ومعالجتها فيما بعد، حيث يلزم في كل معالجة أن تتبن على معطيات تجمعها علاقة مباشرة بالغايات التي حددت ابتداء للمعالجة. فهذه المعطيات لا يلزم أن تكون مجدية فقط ولكن ضرورية كذلك بالنظر إلى الغايات المعالجة من اجلها المعطيات، ويلزم بالإضافة إلى ذلك أن تكون غير مبالغ فيها بالمقارنة مع الغايات المذكورة.

4. **مبدأ الصحة والدقة:**

يجب أن تكون المعطيات صحيحة ومحينة قدر الإمكان إلى جانب اتخاذ التدابير الكفيلة بمحو المعلومات الخاطئة أو الغير المكتملة. الأمر الذي يفعل كل من مبدأ الشفافية في معالجة المعطيات ذات الطبيعة الشخصية، ومبدأ السرية ومبدأ تأمين المعالجة الآلية لهذه المعطيات .

5. **مبدأ محدودية مدة حفظ المعطيات:**

يلزم وفق هذا المبدأ أن تكون المعطيات ذات الطابع الشخصي محفوظة بشكل يؤدي الى التعرف على الأشخاص المعنيين، خلال مدة لا تتجاوز المدة الضرورية لإنجاز الغايات التي من اجلها تم جمعها ومعالجتها. ويقتضي هذا أن لا يتم حفظ المعطيات على وجه نهائي ودائم بملفات آلية ، حيث يتوجب أن تتحدد مدة الحفظ بشكل مؤقت على ضوء الغايات المرتبطة بكل ملف يتم تكوينه لغايات معينة، إلا إذا تم الحصول على إذن بحفظ هذه المعطيات بعد المدة المحددة، بناء على طلب من المسؤول عن المعالجة لمصلحة مشروعة، وهذا لأغراض تاريخية أو إحصائية أو علمية.

6. **مبدأ التقيد بالإجراءات المسبقة عن المعالجة:**

مفاد هذا المبدأ أن المشرع الجزائري اوجب للقيام بمعالجة المعطيات ذات الطابع الشخصي، ضرورة مراعاة إجراءات شكلية تسبق عملية المعالجة، وذلك من اجل ضمان حماية حقوق وحريات الشخص المعني، وتأمين مراقبة فعالة على مختلف المعالجات التي يقوم بها المسؤول عن المعالجة، ومن ثمة فإن هذا الأخير لا يمكنه القيام بأي معالجة إلا بعد الحصول على تصريح مسبق لدى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي. أو لترخيصها إذا ما تبين لها عند دراسة التصريح المقدم لها أن المعالجة المعتزم القيام بها تتضمن أخطارًا ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص.

استحداث السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

إدراكا من المشرع الجزائري بأهمية المعطيات الشخصية وضرورة حمايتها لا سيما في البيئة الرقمية، تم استحداث سلطة وطنية لحماية المعطيات ذات الطابع الشخصي بموجب القانون 18-07 كآلية تتصدي للمخاطر التي تهددها، وتكفل تنفيذ أحكامه من جهة أخرى، لذا وجب التعرض لهذا الضمان الهام على النحو التالي:

1- **تنظيم السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:**

حسب المادة 22 من القانون 18-07 تنشأ لدى رئيس الجمهورية سلطة إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي يحدد مقرها في الجزائر العاصمة وتتمتع بالشخصية المعنوية والاستقلال الإداري والمالي حيث تتشكل السلطة الوطنية من تشكيلة بشرية مميزة، فهي تضم ممثلين على العديد من القطاعات والمجالات ذات الصلة بالموضوع، إذ يتم اختيار أعضاء السلطة الوطنية حسب اختصاصهم القانوني و/أو التقني في مجال معالجة المعطيات ذات الطابع الشخصي، ويتم تعينهم بموجب مرسوم رئاسي لعهدة مدتها 5 سنوات قابلة للتجديد. كما يمكنها الاستعانة بأي شخص مؤهل من شانه مساعدتها في أشغالها. ونظرا لطبيعة المهام المسندة لهذه الهيئة واختصاصاتها الحساسة في مجال معالجة المعطيات الشخصية وحمايتها، ألزم القانون وقبل تنصيب أعضائها في وظائفهم بأداء اليمين القانوني أمام مجلس قضاء الجزائر بالصيغة المحددة في المادة 24 من القانون أعلاه.

هذا وقد اوجب القانون على رئيس وأعضاء السلطة الوطنية المحافظة على الطابع السري للمعطيات ذات الطابع الشخصي والمعلومات التي اطلعوا عليها بهذه الصفة ولو بعد انتهاء مهامهم، ما لم يوجد نص قانوني يقضي بخلاف ذلك. وبالمقابل يستفيد من حماية الدولة ضد التهديدات والإهانات أو الاعتداءات من أية طبيعة كانت التي قد يتعرضون لها بسبب أو خلال تأديتهم لمهامهم أو بمناسبتها.

2- مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

تكلف السلطة الوطنية أساسا بالسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام القانون رقم 18-07، وضمان عدم انطواء استعمال تكنولوجيات الإعلام والاتصال على أي إخطار اتجاه حقوق الأشخاص والحريات العامة والحياة الخاصة.

وعلى ذلك تتولى السلطة مهام عديدة تتمثل في ما يلي:

- منح التراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي.
- إعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم.
- تقديم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة.
- تلقي الاحتجاجات والطعون والشكاوى بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي وإعلام أصحابها بمآلها.
- الترخيص بنقل المعطيات ذات لطابع الشخصي نحو الخارج وفقا للشروط المنصوص عليها في هذا القانون.
- الأمر بالتغييرات اللازمة لحماية المعطيات ذات الطابع الشخصي المعالجة.
- الأمر بإغلاق معطيات أو سحبها أو إتلافها.
- تقديم أي اقتراح من شانه تبسيط وتحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي.
- نشر التراخيص الممنوحة والآراء المدلى بها في السجل الوطني المشار إليه في المادة 28 من هذا القانون.
- تطوير علاقات التعاون مع السلطات الأجنبية المماثلة مع مراعاة المعاملة بالمثل.
- إصدار عقوبات إدارية وفقا لأحكام المادة 46 من هذا القانون.
- وضع معايير في مجال حماية المعطيات ذات الطابع الشخصي.
- وضع قواعد السلوك والأخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي

بالإضافة إلى هذه المهام، هناك مهام أخرى حيث تفيد المادة 29 من القانون 18-07 انه يمكن للسلطة الوطنية أن تحدد بموجب أنظمة الشروط والضمانات المرتبطة بحقوق الشخص المعني في المجالات المتعلقة بحرية التعبير والصحة والشغل والبحث التاريخي والإحصائي والعلمي والمراقبة عن بعد واستعمال تكنولوجيات الإعلام والاتصال بالتنسيق مع القطاعات المعنية. كما يمكن للسلطة الوطنية أن تقرر تأمين الإرسال لا سيما

عن طريق تشفيره، في حالة ما إذا كان سير المعطيات ذات الطابع الشخصي في الشبكة، ويمكن أن تحتوي على مخاطر على حقوق الأشخاص المعنيين وحرياتهم والضمانات الممنوحة لهم.

وبناء على ما سبق تعد السلطة الوطنية تقريرا سنويا عن أعمالها وتقدمه إلى رئيس الجمهورية ولا يتلقى أعضاء السلطة الوطنية في ممارسة نشاطاتهم أية تعليمات من أي سلطة من السلطات، فهي سلطة مستقلة حيث يصفها الجزائري بأنها إدارية مستقلة؛ وضمان معالجتها في الإطار القانوني وهي حماية وقائية قبل وقوع الاعتداء على هذه المعطيات كما تضمن عناية أخرى بعدية وتحفظية تتمثل في القواعد الإجرائية الواجب اتخاذها لحماية المعطيات الشخصية وحفظها من كل ما قد يهدد سلامتها قبل بدء المتابعة القضائية

التدابير التي تتخذها السلطة الوطنية في حالة مخالفة القانون 18-07

منح المشرع الجزائري للسلطة الوطنية مجموعة إجراءات إدارية تتخذ في حق المسؤول عن المعالجة في حال خرقه لأحكام هذا القانون أدرجها المشرع تحت عنوان **الإجراءات الإدارية** والتي تتمثل في الإجراءات التالية:

1) **الإنذار:** لا يعد الإنذار في حد ذاته جزاء في يد السلطة الوطنية وإنما عادة ما يأخذ شكل التنبيه لتذكير المسؤول عن المعالجة بإلزامية معالجة الوضع واتخاذ التدابير الكفيلة للجعل من نشاطه مطابقا للأحكام القانونية المنصوص عليها في القانون الخاص بحماية المعطيات الشخصية.

2) **الأعذار:** وهو وسيلة قانونية منحها المشرع للسلطة الوطنية بغرض إخطار وإخبار المسؤول عن المعالجة بالتزامه للأحكام القانونية الخاصة بالقانون رقم 18-07 خلال مدة محددة قبل اللجوء للقضاء.

3) **السحب المؤقت لمدة لا تتجاوز سنة أو السحب النهائي لوصل التصريح أو الترخيص:** عملا بقاعدة توازي الأشكال فإن السلطة الوطنية تقوم بتجريد المسؤول عن المعالجة الذي لم يجعل من نشاطه مطابقا لأحكام القانون من وصل التصريح أو الترخيص وذلك بسحبها بقرار إداري والذي يعد من اخطر الجزاءات الإدارية وقد يكون هذا السحب مؤقت لمدة لا تتجاوز السنة، وقد يكون نهائي وذلك على حسب جسامة وخطورة المخالفة المرتكبة.

ومن تطبيقات هذا الجزاء ما نصت عليه المادة 48 من القانون 18-07 بقولها :".... يمكن للسلطة الوطنية حسب الحالة ودون أجل سحب وصل التصريح أو الرخيص إذا تبين بعد إجراء المعالجة موضوع التصريح أو الترخيص، أنها تمس بالأمن الوطني، أو أنها منافية للأخلاق أو الآداب العامة".

تحديد حقوق الشخص المعني بالمعالجة والتزامات المسؤول عنها

عرف القانون 18-07 الشخص المعني بالمعالجة بأنه كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع المعالجة، كما أفاد بان المسؤول عن المعالجة هو كل شخص طبيعي أو معنوي عمومي أو خاص، أو أي كيان آخر يقوم بمفرده أو بالاشتراك مع الغير بتحديد الغايات من معالجة المعطيات ووسائلها. وهذا باعتبارهما محورا نظام معالجة المعطيات الشخصية.

حيث خص ذات القانون الشخص المعني بالمعالجة بجملة من الحقوق المتكاملة فيما بينها، وجب كفالتها له والسماح له بممارستها في كل وقت وكل مساس بها يشكل انتهاكا للقانون يوجب المساءلة الجنائية وبالمقابل ألزم المسؤول عن المعالجة باتخاذ التدابير الواجبة لضمان سلامة المعالجة وحمايتها من العبث ومن ثم فإن

كفالة هذه الحقوق، والحرص على القيام بهذه الالتزامات يعد من ضمانات حماية المعطيات الشخصية في البيئة الرقمية، وجب التعرض لها بالدراسة كالتالي:

1- حقوق الشخص المعني بالمعالجة:

نظرا لمخاطر الوسائل التقنية المعلوماتية الحديثة التي يعرفها مجال المعطيات في البيئة الرقمية قرر القانون للشخص المعنوي حقوقا وجب ضمانها واحترامها وتتمثل في الحقوق التالية:

- **الحق في الاعلام:**

إن الأصل في الحق في الإعلام يقتضي أنه يجب على المسؤول عن المعالجة أو من يمثله مسبقا وبصفة صريحة دون لبس، إعلام كل شخص يتم الاتصال به قصد تجميع معطياته ذات الطابع الشخصي بهوية المسؤول عن المعالجة وعند الاقتضاء هوية ممثله وأغراض المعالجة ما لم يكن على علم مسبق بها، وكذا كل معلومة إضافية مفيدة لا سيما المرسل إليه ومدى إلزامية الرد والآثار المترتبة عن ذلك وحقوقه ونقل المعطيات إلى بلد أجنبي.

وإذا لم يتم جمع المعطيات ذات الطابع الشخصي لدى الشخص المعنوي يجب على المسؤول عن المعالجة أو من يمثله قبل تسجيل المعطيات أو إرسالها للغير أن يزوده بالمعلومات المشار إليها أعلاه ما لم يكن قد علم بها مسبقا. وفي حالة جمع المعلومات في شبكات مفتوحة ، يجب إعلام الشخص المعني ما لم يكن على علم مسبق بأن المعطيات ذات الطابع الشخصي المتعلقة به يمكن أن تتداول في الشبكات دون ضمانات السلامة وأنها قد تتعرض للقراءة أو الاستعمال غير المرخص من طرف الغير.

- **الحق في الولوج:**

إن الحق في الولوج والاستفسار عن المعطيات المعالجة وخصائصها ومصدرها والجهات التي أرسلت إليها هذه المعطيات هو حق تكفله المادة 34 من القانون رقم 18-07، والتي نصت على أنه من حق الشخص المعني أن يحصل من المسؤول عن المعالجة التأكيد على أن المعطيات الشخصية المتعلقة به كانت محل معالجة أم لم تعالج، فهذا الحق لا يقتصر على تأكيد المعطيات فقط، بل يشمل على المعلومات المنصبة على غايات المعالجة وفئات المعطيات التي تنصب عليها والمرسل إليهم، هذا من جهة، ومن جهة أخرى يتمتع الشخص المعني كذلك بالحق في الإحاطة بطريقة مفهومة بالمعطيات الخاضعة للمعالجة، وبكل معلومة متاحة حول مصدر المعطيات.

وبالتالي يلزم المسؤول عن المعالجة عند استيفاء جميع الشروط المنصوص عليها قانونا أن يمكن الشخص المعني من ممارسة حقه في الولوج وفق ما سبق ذكره، غير انه إذا كان الطلب المقدم من طرف الشخص المعني يفتقد الى الدقة بسبب تخلف احد العناصر اللازمة لتمكينه من ممارسة العمليات المرتبطة بالحق في الولوج، فإنه يمكن للمسؤول عن المعالجة أن يدعو الشخص المعني بالطلب تزويده بالعناصر المختلفة، وذلك قبل انتهاء الأجل الذي تحدده اللجنة الوطنية بناءا عل طلب المسؤول عن المعالجة، بقصد الإجابة على طلبات الولوج المشروعة، كما يمكنه الاعتراض على الطلبات التعسفية من حيث عددهم وطابعها المتكرر، وفي هذه الحالة يلزمه اثبات الطابع التعسفي لها .

- **الحق في التصحيح:**

الأصل يقصد بالحق في التصحيح حسب نص المادة 35 من القانون 18-07 حق الشخص المعني في الحصول بصفة مجانية من المسؤول عن المعالجة على تحيين أو تصحيح مسح أو إغلاق المعطيات الشخصية التي تكون معالجتها غير مطابقة لهذا القانون بسبب الطابع غير المكتمل أو غير الصحيح لتلك المعطيات على الخصوص، أو لكون معالجتها ممنوعة قانونا. ويلزم المسؤول عن المعالجة بالقيام بالتصحيحات اللازمة مجانا لفائدة الطالب في أجل 10 أيام من إخطاره.

بالإضافة لذلك له حق تبليغ الغير الذي أوصلت إليه المعطيات بكل تحيين أو تصحيح أو مسح أو إغلاق للمعطيات ذات الطابع الشخصي، يتم تطبيقها للحق السابق، ما لم يكن ذلك مستحيلا مع إمكانية استعمال الحق المنصوص عليه في هذه المادة من قبل ورثة الشخص المعني.

- **الحق في الاعتراض:**

يحق للشخص المعني أن يعترض لأسباب مشروعة على معالجة المعطيات ذات الطابع الشخصي وله الحق في الاعتراض على استعمال المعطيات المتعلقة به لأغراض دعائية ولاسيما التجارية منها من طرف المسؤول الحالي عن المعالجة أو مسؤول عن معالجة لاحقة.

ولا تطبق هذه الأحكام إذا كانت المعالجة تستجيب لالتزام قانوني أو إذا كان تطبيق هذه الأحكام قد استبعد بموجب إجراء صريح في المحور الذي يرخص بالمعالجة.

- **منع الاستكشاف المباشر:**

يمنع الاستكشاف المباشر بواسطة آلية اتصال أو جهاز الاستنساخ البعدي أو بريد إلكتروني أو أي وسيلة تستخدم تكنولوجيا ذات طبيعة مماثلة، باستعمال بيانات شخص طبيعي، وفي أي شكل من الأشكال لم يعبر عن موافقته المسبقة عن ذلك.

غير أنه يرخص بالاستكشاف المباشر عن طريق البريد الإلكتروني، إذا ما طلبت البيانات مباشرة من المرسل إليه، وفق لأحكام هذا القانون، بمناسبة بيع أو تقديم خدمات إذا كان الاستكشاف المباشر يخص منتجات أو خدمات مشابهة يقدمها نفس الشخص الطبيعي أو المعنوي وتبين للمرسل إليه بشكل صريح لا يشوبه لبس إمكانية الاعتراض دون مصاريف باستثناء التكلفة المرتبطة بإرسال الرفض على استعمال بياناته وقت جمع هذه الأخيرة وكلما وجه إليه بريد إلكتروني لأجل الاستكشاف.

وفي جميع الحالات يمنع إرسال رسائل بواسطة آليات الاتصال الهاتفي وجهاز الاستنساخ البعدي والبريد الالكتروني لأجل الاستكشاف المباشر، دون الإشارة إلى بيانات صحيحة لتمكين المرسل إليه من إرسال طلب توقيف هذه الاتصالات دون مصاريف غير تلك المرتبطة بإرسالها، كما يمنع إخفاء هوية الشخص الذي أوصلت لفائدته الرسائل وكذلك ذكر موضوع لا صلة له بالخدمات المقترحة.

2- التزامات المسؤول عن المعالجة:

يلتزم المسؤول عن المعالجة بوجوب التقيد بالتراتيب المقررة قانونا لعملية المعالجة والمتمثلة أساسا في ما يلي:

- **اتخاذ تدابير لضمان سلامة المعالجة:**

يلتزم المسؤول عن المعالجة وفق القانون أعلاه باتخاذ كل التدابير التقنية والاحترازية اللازمة من اجل حماية وتامين المعطيات ذات الطابع الشخصي من القرصنة والتلف، وكل استخدام غير مشروع خاصة إذا كانت مرسلة عبر شبكة معينة، وتزيد هذه التدابير كلما زادت قيمة وأهمية هذه المعطيات.

وإذا كان المسؤول عن المعالجة يستخدم مسؤولا آخر(مسؤول من الباطن) يعمل لحسابه، وجب على هذا الأخير تقديم الضمانات الكافية من اجل سلامة وتأمين المعطيات ذات الطابع الشخصي، ويجب أن يكون هذا التفويض بعقد أو سند قانوني مكتوب أو يمكن حفظه لأغراض جمع الأدلة.كما ينص القانون بوجه الخصوص على أن لا يتصرف المعالج من الباطن إلا وفقا لتوجيهات وتعليمات من المسؤول الأول عن المعالجة. وهذا من اجل تحديد المسؤوليات القانونية ولكي لا تضيع حقوق الأشخاص بين المسؤول عن المعالجة والمسؤول عن المعالجة من الباطن.

- **ضرورة ضمان سرية المعالجة:**

يجب على المسؤول عن المعالجة أن يلتزم بضمان سرية البيانات الشخصية وكذلك المعالج من الباطن وكافة الأشخاص الذين اطلعوا أثناء ممارستهم لمهامهم على المعطيات ذات الطابع الشخصي ويستمر ذلك حتى بعد انتهاء مهامهم تحت طائلة العقوبات المنصوص عليها حسب المادة 40 من القانون 18-07.

تجريم الانتهاكات الواقعة على نظام المعطيات الشخصية في البيئة الرقمية

نظرا للمخاطر التي تهدد المعطيات الشخصية في البيئة الرقمية استلزمت حماية الحق في الحياة الخاصة للأفراد، ضرورة وضع قواعد عقابية لحمايتها من مختلف التجاوزات والانتهاكات الواقعة عليها حيث أفرد القانون رقم 18-07 جملة نصوص قانونية تجرم وتعاقب الانتهاكات الماسة بالمعطيات الشخصية وكذا معالجتها، وهي بذلك تعد ضمانات قضائية هامة في مواجهة أي مساس بهذا الحق الهام وهذه الجرائم هي:

1- **الجرائم الماسة بالقواعد الموضوعية لمعالجة المعطيات الشخصية:**

جرم القانون رقم 18-07 مجموعة من الأفعال التي تشكل خرقا للقواعد التي يلزم مراعاتها عند القيام بكل معالجة للمعطيات الشخصية وتتمثل هذه الجرائم في:

أ **الجرائم المتعلقة بتسيير المعطيات الشخصية:** وتشمل

-**جريمة المعالجة غير المشروعة:** مجرمة بموجب المواد 54 و59 و2/62 وتتحقق هذه الجريمة بالقيام بأحد الأفعال التالية:

- ✓ معالجة المعطيات الشخصية دون احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة.
- ✓ جمع معطيات ذات طابع شخصي بطرق تدليسية أو غير نزيهة أو غير مشروعة، معاقب عليها بموجب المادة 59 من القانون أعلاه بعقوبة الحبس من سنة إلى ثلاث سنوات وبغرامة مالية من 100.000دج إلى 300.000 دج.
- ✓ الاحتفاظ بالمعطيات الشخصية بعد المدة المحددة قانونا.

-**جريمة الاستعمال غير المشروع للمعطيات:** وترتكب هذه الجريمة من قبل أشخاص معينين قد يكون المسؤول عن المعالجة والمسؤول عن المعالجة من الباطن، ولها عدة صور أهمها:

- ✓ جريمة افشاء معلومات محمية بموجب القانون رقم 18-07 نصت عليها المادة 62 منه.
- ✓ جريمة السماح لأشخاص غير مؤهلين بالولوج لمعطيات ذات طابع شخصي.
- ✓ جريمة نقل معطيات ذات طابع شخصي نحو دولة أجنبية دون احترام شرطي عملية النقل والمنصوص عليها في المادة 44 من ذات القانون ويتمثل الشرطين في ضرورة ترخيص السلطة الوطنية نقل المعطيات الشخصية، و توفير الدولة الأجنبية المزمع نقل المعطيات إليها بالحماية الكافية للحياة الخاصة والحريات الأساسية للأشخاص.
- ✓ جريمة الولوج إلى السجل الوطني لحماية المعطيات ذات الطابع الشخصي دون أن يكون الشخص مؤهلا لذلك، وهذا السجل يمسك من طرف السلطة الوطنية وتقيد فيه مجموعة من البيانات كالملفات التي تكون السلطة العمومية أو الخواص مسؤولان عنها، أيضا التصريحات المقدمة للسلطة الوطنية والتراخيص التي تسلمها، وأي شخص غير مؤهل للولوج في هذا السجل يعاقب بالعقوبات المنصوص عليها في المادة 63 من القانون رقم 18-07.

ب الجرائم المتعلقة بحقوق الشخص المعني:

خول المشرع للأشخاص المعنيين بمعالجة المعطيات ذات الطابع الشخصي مجموعة من الحقوق في مواجهة المسؤول عن المعالجة وذلك بغية تمكينهم من حماية حياتهم الخاصة من كل اعتداء، وعليه فكل اعتداء على هذه الحقوق يشكل فعلا مجرما كإجراء المعالجة رغم اعتراض الشخص المعني، رفض حقوق الإعلام أو الولوج أو التصريح .

ومن الجرائم المتعلقة بحقوق المعني أيضا كل معالجة يجريها المسؤول عن المعالجة دون اخذ الموافقة الصريحة منه حسب ما نصت عليه المادة 55 من القانون 18-07.

2- الجرائم الماسة بالقواعد الإجرائية لمعالجة المعطيات الشخصية:

لحماية المعطيات ذات الطابع الشخصي نص المشرع الجزائري على مجموعة من القواعد الإجرائية يلزم المسؤول عن المعالجة قبل إجرائها ضرورة القيام ببعض الشكليات المسبقة وبالتالي فإن مخالفة هذه الشكليات يعد جريمة معاقب عليها وهذه الجرائم هي:

أ الجرائم المتعلقة بالإجراءات المسبقة عن المعالجة:

وتسمى كذلك جريمة عدم استيفاء الشروط المسبقة للمعالجة حيث ألزم المشرع على المسؤول عن المعالجة القيام بالتصريح بذلك أو الحصول على ترخيص من قبل السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، وانعدام التصريح أو الترخيص يعتبر جريمة يعاقب عليها وفق نص المادة 56 من القانون المذكور أعلاه.

ب الجرائم المتعلقة بإجراءات الحماية والتعاون مع السلطة الوطنية:

ألزم المشرع كل مسؤول عن معالجة المعطيات ذات الطابع الشخصي ضرورة اتخاذ مجموعة من الإجراءات والتدابير بهدف حماية المعطيات الشخصية محل المعالجة وعليه فكل تقصير في اتخاذ هذه الإجراءات يشكل جريمة معاقب عليها.

كما وألزم ذات القانون ضرورة التعاون مع السلطة الوطنية وكل إخلال بذلك يعد جريمة يعاقب على ارتكابها وهي جريمة الامتناع عن التعاون مع السلطة الوطنية، وتتحقق وفقا لنص المادة 61 من ذات القانون بعرقلة عمل السلطة الوطنية إما بالاعتراض على إجراء عملية التحقق في عين المكان، أو عن طريق رفض تزويد أعضائها أو الأعوان الذين وضعوا تحت تصرفها بالمعلومات أو الوثائق الضرورية لتنفيذ المهمة الموكلة لهم من طرف السلطة الوطنية أو الإخفاء أو إزالة الوثائق أو المعلومات المذكورة أو عن طريق إرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب أو عدم تقديمها بشكل مباشر وواضح. وتتحقق أيضا عند امتناع مقدم الخدمات بإعلام السلطة الوطنية والشخص المعني عن كل انتهاك للمعطيات الشخصية وفقا للمادة 66 من القانون 18-07.

النظام القانوني للجريمة المعلوماتية

حاول المشرع الجزائري أن يساير الركب المعلوماتي على غرار التشريعات الاخرى وذلك سواء من خلال إخضاع أفعال الاعتداء على المعلوماتية لنصوص الملكية الفكرية باعتبار المعلوماتية نتاج فكر وإبداع وكذا حماية المال المعلوماتي من خلال نصوص قانون العقوبات كما حاول تدارك الفراغ التشريعي في مجال مكافحة الجريمة المعلوماتية من خلال قانون القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لعام 2009.

الحماية الجنائية للمعلوماتية من خلال نصوص الملكية الفكرية:

تبنى المشرع الجزائري نظام الحماية وفقا لحقوق المؤلف والحقوق المجاورة وهو ما سارت عليه غالبية التشريعات والاتفاقيات الدولية، وتتمثل الحماية بالنصوص المعدلة لحقوق المؤلف في الاعتراف صراحة بوصف المصنف المحمي لمصنفات الاعلام الالي وتجريم عملية تقليده.

1- تجريم عملية التقليد

نص المشرع الجزائري في الأمر 03-05 على جريمة التقليد و الجرائم المشابهة لها حيث تنص المادة 151 منه في الحالات التالية:

- ✓ الكشف غير المشروع عن مصنف او اداء فني.
- ✓ المساس بسلامة مصنف أو أداء فني.
- ✓ استنساخ مصنف او اداء فني بأي اسلوب من الاساليب في شكل نسخ مقلدة أو مزورة
- ✓ استيراد نسخ مقلدة أو تصديرها.
- ✓ بيع نسخ مزورة من مصنف أو اداء فني.
- ✓ تأجير مصنف أو اداء فني او عرضه للتداول.

2- الجزاءات المقررة لجرائم التقليد

لقد ربط المشرع الجزائري الحماية بتاريخ الانتهاء من الابتكار أو تاريخ النشر أو التوزيع لأول مرة حيث اصبحت الدعوى الجزائية او المدنية مقبولة حتى ولو لم يتم الإيداع، وتجدر الإشارة إلى أنه بالإضافة إلى الطرق التقليدية لتحريك الدعوى العمومية فإن المادة 160 من الأمر 03-05 تنص على حق مالك الحقوق

المحمية ومن يمثله بتقديم شكوى للجهة القضائية في حالة ما إذا كان ضحية الأفعال المنصوص والمعاقب عليها في الأمر 03-05.

نشير الى ان المشرع الجزائري قد خول لصاحب المصنف المعتدى عليه إجراء تحفظيا يتمثل في عملية حجز التقليد وهو إجراء يسهل إثبات عملية التقليد، هذا الإجراء تحفظي يمكن بواسطته حجز الوثائق والنسخ الناتجة عن الاستنساخ غير المشروع او التقليد وذلك حتى في غياب ترخيص قضائي مسبق.

للقاضي سلطة اتخاذ احدى التدابير الآتية المادة 147 من الأمر 03-05:

- ايقاف كل عملية صنع جارية ترمي الى الاستنساخ غير المشروع للمصنف أو للاداء المحمي او تسويق دعائم مصنوعة بما يخالف حقوق المؤلفين والحقوق المجاورة.
- القيام ولو خارج الأوقات القانونية بحجز الدعائم المقلدة والإرادات المتولدة من الاستغلال غير المشروع للمصنفات والأداءات.
- حجز كل عتاد استخدم أساسا لصنع الدعائم المقلدة.

كما نصت المادة 165 من الأمر 97-10 المعدل و المتمم بالأمر -05 المتعلق بحقوق المؤلف على العقوبات على النحو التالي:

للقاضي أن يطبق عقوبة أصلية: الحبس من ستة اشهر الى ثلاث سنوات والغرامة من 500 الف الى الى مليون دينار وذلك سواء تمت عملية النشر داخل الجزائر أو خارجها.

للقاضي سلطة تقرير عقوبات تكميلية: تتمثل في مصادرة المبالغ المساوية لمبلغ الإيرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو أداء محمي ومصادرة وإتلاف كل عتاد انشأ خصيصا لمباشرة نشاط غير مشروع وكل النسخ المقلدة والمصادرة هنا وجوبية.

- كما تأمر الجهة القضائية بتسليم العتاد او النسخ المقلدة أو قيمة ذلك وكذلك الايرادات موضوع المصادرة للمؤلف أو أي مالك حقوق أخر يكون عند الحاجة بمثابة تعويض.
- يمكن للقاضي بناء على طلب الطرف المدني الأمر بنشر أحكام الإدانة على نفقة المحكوم عليه على أن لا تتعدى المصاريف قيمة الغرامة المحكوم بها.
- للقاضي أن يضاعف العقوبات المقررة وذلك في حالة العود مع امكانية غلق المؤسسة التي يستغلها المقلد أو شريكه مدة لا تتعدى ستة أشهر.

الحماية الجنائية المعلوماتية من خلال نصوص قانون العقوبات:

تدارك المشرع الفراغ القانوني في مجال الجريمة المعلوماتية وذلك استحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون رقم 04-15 المتضمن قانون العقوبات مركزا على الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات.

1- ضرورة خضوع نظام المعالجة الآلية للمعطيات للحماية فنية

يسعى المتخصصون بأمن المعلومات للحفاظ على خصوصية البيانات المتناقلة عبر الشبكات وبالأخص حاليا شبكة الانترنت لتأمين سرية الرسائل الإلكترونية وسرية البيانات المتناقلة وخاصة منها المتعلقة بالأعمال التجارية الرقمية، ويمثل التشفير أفضل وسيلة للحفاظ على سرية البيانات المتناقلة وعليه فإن الخبراء

يؤكدون على ضرورة استخدام أسلوب التشفير لمنع الآخرين من الاطلاع على الرسائل الإلكترونية، وكذلك بدأت الكثير من الشركات في المعاملات التجارية الهامة على شبكة الإنترنت للتأكد من هوية المتعامل معها اشتراط أن يوقع المتعامل معها الكترونيا على العقل التغلب على جريمة انتحال شخصية الغير وإبرام صفقات تجارية باسمه .

2- الأركان الأساسية لجريمة الاعتداء على نظم المعالجة الآلية للمعطيات

الركن المادي: يتمثل في أشكال الاعتداء على نظم المعالجة الآلية للمعطيات والتي هي:

- ✓ الدخول والبقاء غير المشروع في نظام المعالج الآلية للمعطيات.
- ✓ الاعتداءات العمدية على المعطيات حيث نص المشرع الجزائري في المادة 394 مكرر 2 من قانون العقوبات عليها وتتمثل في :

1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات المخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم.

الركن المعنوي: يشترط لتوافر الركن المعنوي أن تتجه إرادة الجاني الى فعل الدخول او الى فعل البقاء أو أن يعلم الجاني أنه ليس له الحق في الدخول إلى النظام والبقاء فيه، وعليه لا يتوافر الركن المعنوي إذا كان الدخول الجاني او بقائه داخل النظام مسموح به اي مشروع او اذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول او في البقاء أو في نطاق هذا الحق كأن يجهل بوجود حظر الدخول او البقاء أو كان يعتقد خطأ أنه مسموح له بالدخول فإذا توافر القصد الجنائي بعنصريه العلم والإرادة فإنه لا يتأثر بالباعث على الدخول أو البقاء فيضل القصد قائما حتى ولو كان الباعث هو الفضول او إثبات القدرة على المهارة والانتصار على النظام.

كما جرم المشرع الجزائري المساس بحرمة الحياة الخاصة بموجب المواد من 303 مكرر إلى 303 مكرر3 من هذا القانون.

عقوبات جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات:

نص المشرع على مجموعة من العقوبات في هذه الجرائم الماسة بالنظام والمتمثلة في:

أولا: العقوبة الاصلية

1- عقوبة الدخول أو البقاء داخل النظام:

- **الصورة البسيطة لجريمة:** حدد المشرع عقوبة هذه الجريمة بالحبس من ثلاثة اشهر الى السنه والغرامة من 50000 إلى 100000(المادة 394 مكرر)
- **الصورة المشددة لجريمة:** نص المشرع في الماده 394 مكرر فقرة 3/2 على مضاعفة العقوبة اذا ترتب على هذا الدخول او البقاء حذف او تغيير المعطيات النظام اما اذا انجر على هذا الدخول او البقاء تخريب النظام عمل المنظومة فان العقوبة تكون الحبس من ستة اشهر الى سنتين والغرامة من 50000 الى 150000.

2- **عقوبة الاعتداء العمدي على المعطيات**

حدد المشرع عقوبة الاعتداء العمدي علي المعطيات الموجودة داخل النظام في المادة 394 مكرر1 بالحبس من ستة اشهر الي ثلاث سنوات وبغرامة من 500000 الى 2000000 كما عاقبه على استخدام هذه المعطيات في ارتكاب الجرائم الماسة الانظمة المعلوماتية و كذا حيازة او انشاء او نشر أو استعمال المعطيات المتحصل عليها من احدى الجرائم الماسة بالأنظمة المعلوماتية في نص المادة 394 مكرر 2 بالحبس من شهرين الى ثلاث سنوات وبغرامة من 1000000 الى 5000000 .

ثانيا:العقوبات المقررة للشخص المعنوي

اقر المشرع مبدأ المسالة للشخص المعنوي في القانون 04-15 المؤرخ في 10-11- 2004 وذلك بموجب نص المادة 51 مكرر منه، كما حدد ثلاثة شروط لإمكان مساءلة الشخص المعنوي جنائيا وهي كالتالي:

1- أن ترتكب إحدى الجرائم المنصوص عليها قانونا.
2- أن تكون بواسطة احد اعضاء اول ممثلي الشخص المعنوي.
3- أن ترتكب الجريمة لحساب الشخص المعنوي.

كما حدد في المادة 18 مكرر من نفس القانون العقوبات المطبقة على الاشخاص المعنوية حيث جاء فيها ما يلي: "العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح هي:

- الغرامه التي تساوي من مرة الى خمس مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.
- **واحدة او اكثر من العقوبات الاتية:**
  - ✓ حل الشخص المعنوي.
  - ✓غلق المؤسسة او فرع من فروعها لمده لا تتجاوز خمس سنوات.
  - ✓ الاقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات.
  - ✓ المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر، نهائيا لمدة لا تتجاوز خمس سنوات.
  - ✓ مصادرة الشيء الذي استعمل في ارتكاب الجريمة او نتج عنها.
  - ✓نشر وتعليق حكم الادانة.
  - ✓ الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس سنوات وتنصب الحراسة على ممارسة النشاط الذي ادى الى الجريمة او الذي ارتكبت الجريمة بمناسبته.

ثالثا: عقوبة الاشتراك الشروع في الجريمة

1- **عقوبة الاشتراك:** يعاقب المشرع على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الاشد.

شروط المعاقبة على الاتفاق الجنائي يمكن استخلاصها من نفس المادة 394 مقرر 5 من قانون العقوبات وهي كالتالي:

- ✓ مجموعة أو اتفاق.

- ✓ بهدف تحضير جريمة من الجرائم الماسة بالأنظمة المعلوماتية.
- ✓ تجسيد هذا التحضير بفعل مادي.
- ✓ فعل المشاركة في هذا الاتفاق.
- ✓ القصد الجنائي .

تعتبر الاعمال التحضيرية التي تسبق عملية البدء في تنفيذ الجريمة غير معاقب عليها كقاعدة عامة إلا اذا توافر نص قانوني خاص يجرمها، ومن هذا المنطلق وبالعودة الى المادة 394 مكرر 5 من قانون العقوبات المستحدثة بموجب القانون 04-15 نجد أن المشرع الجزائري ينص على أن: " **كل من شارك في مجموعة أو اتفاق تألف بغرض الاعداد لجريمة او اكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بنفس العقوبات المقررة للجريمة ذاتها**".

وقد تبنى المشرع هذا التوجه خلافا للقواعد العامة المقررة في اطار قانون العقوبات والتي تنص على ان العقاب لا يتقرر إلا في الجرائم الواقعة فعلا والتامة المكتملة الأركان أو الجرائم التي تقف عند مرحله الشروع أو المحاولة، ويعود هذا الاستثناء في التجريم إلى خطورة الجرائم السيبرانية التي تقتضي التصدي لها بكافه الوسائل الردعية والعقابية الممكنة، وتقرير نوع من الحماية المتقدمة والوقاية لنظم المعالجة الالية للمعلومات والمعطيات ضد المخاطر التي تنشا على النشاط غير المشروع.

2- **عقوبة الشروع:** نصت المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي على عقوبة الشروع وتبناها المشرع في المادة 394 مكرر 7 من قانون العقوبات فالجرائم الماسة بالأنظمة المعلوماتية لها وصف جنحي ولا عقاب على الشروع في الجنح إلا بنص، حيث تنص هذه المادة: "**يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها**".

يبدو من خلال هذا النص رغبة المشرع في توسيع نطاق العقوبة بحيث تشمل اكبر قدر من الافعال الماسة بالأنظمة المعلوماتية إذ جعل الشروع في احداها معاقب عليه في نفس عقوبة الجريمة التامة.

ويعرف الشروع في القانون:" **كل محاولات ارتكاب جناية تبتدئ بالشروع في التنفيذ او بأفعال لا لبس فيها تؤدي مباشرة الى ارتكابها تعتبر كالجناية نفسها اذا لم توقف اولم يخب اثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى ولو لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها**".

رابعا: العقوبة التكميلية

- ✓ **المصادرة:** هي العقوبة تكميلية تشمل الاجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية مع مراعاة حسن النية.
- ✓ **إغلاق المواقع:** الأمر يتعلق بالمواقع التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.
- ✓ **اغلاق المحل أو مكان الاستغلال:** إذا كانت الجريمة قد ارتكبت بعلم مالكها، ومثال ذلك إغلاق مقهى انترنت الذي ترتكب فيه مثل هذه الجرائم بشرط توفر العنصر العلم لدى مالكها.

آليات مكافحة الجرائم السيبرانية على المستوى الدولي والوطني

أولا:الجهود الدولية في مجال مكافحة الجرائم السيبرانية

الواقع أن خاصية العالمية التي تميز جرائم المعلوماتية قد دفعت رجال القانون والفقهاء إلى الدعوة لمواجهتها من خلال وضع قواعد اتفاقية تعبر عن تصور دولي موحد من شأنه تدارك النقائص والثغرات التي تعتري منظومة القوانين الداخلية للدول وذلك بهدف التقليل من حدة آثار هذه الجريمة .

وفي هذا الإطار تضافرت الجهود من أجل وضع إطار قانوني اتفاقي يسمح بمتابعة مرتكبي جرائم المعلوماتية ومعاقبتهم، وهو الأمر الذي تجسد في اتفاقيات ثنائية ومتعددة الأطراف متعلقة بالمسألة، سواء على المستويين الدولي أو الإقليمي، ومن أجل بيان تلك الجهود من الأهمية بمكان الإشارة إلى بعضها بإيجاز فيما يأتي:

1-المؤتمر الدولي لحقوق الإنسان الخاص لسنة 1968:

يعتبر هذا المؤتمر من أول المؤتمرات التي تعكس الجهود الدولية في مكافحة جرائم الانترنيت، حيث عقد بالعاصمة الإيرانية في نهاية ستينيات القرن الماضي، وقد أكدت الفقرة 18 من هذا الإعلان صراحة إلى أن التقدم العلمي والتقني يمكن أن يعرض حقوق وحريات الفرد للخطر، وهو الأمر الذي لقي صدى واسعا من طرف الغالبية العظمى من الدول المتقدمة، وذلك من خلال التجسيد الفعلي لمضمون هذه التوصية في تشريعاتها الداخلية.

2-قانون الأونسيترال النموذجي للتجارة الإلكترونية لسنة1996

يعد هذا القانون من أهم الجهود الدولية في مجال مكافحة الجرائم المتعلقة بالمعلوماتية على المستوى الدولي، ويعد لبنة للعمل الكبير الذي قامت به" الأنسترال " في سبيل وضع نصوص نموذجية لتزويد المشرعين الوطنيين بمجموعة قواعد مقبولة دوليا ترمي إلى تذليل العقبات القانونية وتعزيز القدرة على التنبّؤ بالتطورات القانونية في مجال التجارة الإلكترونية لمواجهة جرائم المعلوماتية في مجال التجارة الإلكترونية، وقد لقي هذا القانون قبولا من طرف مشرعي الدول والمتعاملين، لاسيما بعد أن اعتمدته لجنة الأمم المتحدة سنة1996.

3-القانون النموذجي المتعلق بالتوقيع الإلكتروني لسنة 2001

يعتبر هذا القانون تكملة للجهود التي بذلتها لجنة" الأونسترال "في سبيل مكافحة الجرائم المعلوماتية المتعلقة بالتجارة الدولية، حيث تكفل بوضع قواعد موحدة من شأنها حماية التوقيع الإلكتروني، وهو ما كرسته الكثير من الدول في تشريعاتها الداخلية، علاوة عن الجهود الدولية لمواجهة الجرائم المعلوماتية عكفت الكثير من الدول إلى معالجة هذه الجرائم على المستوى الإقليمي، وهذا ما يتضح من خلال النموذجين التاليين:

أ -**الاتفاقية الأوروبية لجرائم الانترنيت لسنة 2001:** دخلت هذه الاتفاقية حيز التنفيذ سنة 2004، ويطلق عليها البعض تسمية" اتفاقية بودابست"، وقد جاءت تتويجا للجهود التي بذلها المجلس الأوروبي في سبيل التوصل إلى وضع إطار اتفاقي فعال لمكافحة الجرائم المعلوماتية، ومن أهم الدول التي وقعت عليها خارج دول الاتحاد الأوروبي نذكر جنوب إفريقيا واليابان والولايات المتحدة الأمريكية .

وتأتي أهمية هذه الاتفاقية في كونها اتفاقية تهدف إلى توفير إطار دولي مشترك للتعامل مع الجرائم الالكترونية حيث تلتزم الدول الموقعة عليها بتعديل تشريعاتها لمواجهة التحديات التي تفرضها تكنولوجيا

المعلومات، إذ تولت تحديد الجرائم المعلوماتية، واعتماد أدوات إجرائية لمكافحة الجريمة المعلوماتية وضبط مرتكبيها .

ب –قانون عربي استرشادي لمكافحة الجريمة المعلوماتية: تم اعتماد مشروع هذا القانون في الدورة التاسعة عشر لمجلس وزراء العدل العرب سنة2003، قبل أن يعتمده وزراء الداخلية العرب سنة2004.

والملاحظ أن هذا القانون أشار لأنواع الجرائم التي تقع عن طريق الكمبيوتر والانترنت بصفة عامة، وأحال إلى التشريعات الداخلية كلما يتعلق الأمر بأركان هذه الجرائم وكذلك العقوبات التي تطبق عليها، وفي هذا السياق تضمن الباب السابع من هذا القانون فصلا خاصا يتعلق بالجرائم المعلوماتية الواقعة على حقوق الأشخاص، حيث أدرجت فيه أربعة مواد(من المادة 461 إلى
المادة 464 منه)، وأشارت إلى حماية خصوصية الأشخاص من خطر الجرائم المعلوماتية وكيفية تتبع المجرمين والعقوبات المقررة لهذه الجرائم. ورغم ذلك يبقى هذا القانون فضفاض ولم يعط الجريمة المعلوماتية ما تستحقه من الاهتمام الأمر الذي جعل أحكامه عاجزة عن مواجهة خطر الجرائم المعلوماتية.

الجدير بالإشارة أن الاهتمام على المستوى المحلي بمكافحة الجريمة المعلوماتية قد زاد مع استشعار دول الجوار خطر الإرهاب الدولي وفي هذا السياق اجتمع في ماي 2002 وزراء دول الثمانية بمدينة ترومبلن بكندا لإصدار وثيقة تتضمن مجموعة من التوصيات حول تعقب آثار الاتصالات الهاتفية عبر الحدود من أجل مكافحة الأعمال الإرهابية، وفي ماي 2004 أصدرت دول الثمانية بيانا مشترك صدر بعنوان" مواصلة تعزيز القوانين المحلية"، وأوصى جميع الدول أن
تواصل تحسين القوانين التي تجرم إساءة استخدام الشبكات الالكترونية، والتي تسمح بسرعة التعاون بشأن التحقيقات المتصلة بالإنترنت.

ولعل أفضل وأنسب أنواع التعاون هو التعاون الثنائي الذي ساعد ومن المنتظر أن يضل محافظا على تلك الصفة في مكافحة الجريمة الالكترونية.

ثانيا:آليات مكافحة الجرائم السيبرانية في ضوء القانون 09- 04

كخطوة جديدة قام المشرع الجزائري بسن القانون 09- 04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ووضع مجموعة من التدابير الوقائية والإجرائية للوقاية من هذه الجرائم ومكافحتها وأهمها:

1- التدابير الوقائية

أ: المراقبة الالكترونية

حيث سمح باللجوء لهذا الإجراء في حالات محددة حصرا المادة 4 من القانون 09-04 وتكون بموجب إذن مكتوب من السلطات القضائية المختصة:

- ✓ للوقاية من الأفعال الإرهابية أو التخريبية أو الجرائم الماسة بأمن الدولة أو في حاله توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

- ✓ كذلك لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى هذا الإجراء.
- ✓ ويمكن الاستعانة بالمراقبة الالكترونية في إطار تنفيذ المساعدة القضائية الدولية المتبادلة.

ب: الاستعانة بمزودي الخدمات للوقاية من الجرائم السيبرانية

❖ **التزامات مقدمي الخدمات:** يراد بقدمي الخدمات أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها، حيث ترد عليهم بعض الالتزامات الواجب القيام بها من أجل مساعدة سلطات المختصة بالتفتيش للوصول إلى المجرم المعلوماتي، ويقع على عاتق مقدمي الخدمات القيام بالالتزامات التالية:

أ- مساعدة السلطات: يتعين على مقدمي الخدمات الالتزام بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 من قانون 09-04 تحت تصرف السلطات المختصة.

كما يتعين عليهم كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

ب- حفظ المعطيات المتعلقة بحركة السير: يتعين على مقدمي الخدمات في هذه الحالة الالتزام بحفظ ما يلي:

- ✓ المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
- ✓ المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.
- ✓ الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.
- ✓ المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.
- ✓ المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال
- ✓ وكذا عناوين المواقع المطلع عليها.

أما بالنسبة لنشاطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة" أ "من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

هذا وتحدد مدة حفظ المعطيات المذكورة سابقا بسنة واحدة ابتداء من تاريخ التسجيل، وأن أي إخلال بالالتزامات السابقة من شأنه إقامة المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية وإمكانية الخضوع لعقوبة قد تصل إلى الحبس من 6 إلى غاية 5 سنوات وبغرامة من 50000 إلى 500000 دج أما الشخص المعنوي فيخضع لعقوبة الغرامة المقررة وفقا للقانون العقوبات الجزائري.

❖ **الالتزامات الخاصة بمقدمي خدمة" الانترنت:**

زيادة على الالتزامات السابقة يتعين على مقدمي خدمات الانترنت ما يلي:

- التدخل الفوري لسحب المعطيات التي يتيحون الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكنا.
- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.

إن ما سبق ذكره يعتبر في غاية الأهمية، ذلك أن المصلحة العامة تقتضي من مزودي الخدمات في الجرائم المعلوماتية خاصة ما تعلق منها بالجرائم الماسة بأمن الدولة والأنشطة غير القانونية الممارسة ضدها القيام بإبلاغ السلطات المختصة بعناوين هؤلاء الأشخاص وكذا بريدهم الالكتروني والصفحة الشخصية الأمر الذي يتعين معه في البداية أن يسعى مزودي الخدمات إلى

الحصول على المعلومات الخاصة بالأشخاص المستخدمين قبل مباشرة عملية الاستفادة من الخدمة، لكن هذا الأمر لا يعني السماح للمزود الخدمة بالتلاعب بالبيانات المتحصل عليها حيث يقع هو آخر عليه التزام يقضي بعدم استخدام تلك البيانات الشخصية التي في حوزته بما يخالف القانون، بمعنى أن التزامات مزودي الخدمة أكبر من رواد أو المستفدين من الخدمة حيث يقع عليهم التزام حماية بيانات مستخدميهم وتخزينها، وضرورة التبليغ عن الأنشطة غير المباشرة التي يقومون بها.

2- التدابير الإجرائية

أ: تفتيش وحجز المنظومة المعلوماتية

لمقتضيات حماية النظام العام أو المستلزمات التحريات أو التحقيقات القضائية الجارية تم وضع مجموعه من الترتيبات التقنية لمراقبه الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية، كما إن إجراء الحجز يمكن أن تصادفه عده إشكالات تتعلق بأسباب تقنيه على السلطات التي تقوم بالتفتيش استعمال تقنيات مناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها الموضوع تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

ويمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية.

ب: تمديد الاختصاص بنظر هذه الجرائم

يؤول الاختصاص للمحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة خارج الإقليم الوطني في حالة ارتكاب الجريمة من أجنبي وكانت جريمة تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

ج: تبادل المساعدة القضائية الدولية

سمح المشرع الجزائري بإمكانية تبادل المساعدة القضائية الدولية لجمع الأدلة المتعلقة بالجريمة في شكلها الالكتروني ومن الممكن الاستجابة لطلبات المساعدة الرامية إلى تبادل المعلومات أو اتخاذ إي إجراءات تحفظيه وفقا للاتفاقيات الدولية أو وفقا لمبدأ المعاملة بالمثل.

د: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

استحدثت هذه الهيئة بموجب القانون 09-04 وبقيت تشكيلتها وتنظيمها وكيفية سيرها لتحدد عن طريق التنظيم الذي توالت فيه التغييرات ابتداء المرسوم الرئاسي رقم 15-261 ثم المرسوم الرئاسي رقم 20-183 المؤرخ في 13 يوليو 2020 ويتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها حيث إعادة تنظيم الهيئة وعرفها بأنها سلطه إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطه رئيس الجمهورية ويحدد مقرها في الجزائر العاصمة ويمكن نقله إلى أي مكان من التراب الوطني بموجب مرسوم رئاسي، وتتكون الهيئة من مجلس توجيه ومديرية عامة يوضعان تحت السلطة المباشرة لرئيس الجمهورية ويقدمان عرضا عن نشاطاتهما.

ثالثا: القوانين المدعمة للقانون 09-04 للحد من للحد من الإجرام السيبراني

- **القانون18-04 المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية**

وضع هذا القانون مجموعة من آليات للتصدي للجرائم المتعلقة بالعالم الافتراضي من بينها:

- استحداث سلطة ضبط تسهر على احترام متعاملي البريد والاتصالات لالكترونية للأحكام القانونية والتنظيمية المتعلقة بالبريد والاتصالات الالكترونية والأمن السيبراني.
- تجريم انتهاك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الالكترونية أو إفشاء مضمونها أو نشرها أو استعمالها دون ترخيص من المرسل أو المرسل إليه أو الأخبار بوجودها.
- تجريم محاوله فتح أو تخريب أو تحويل البريد أو المساعدة في ارتكاب هذه الجريمة.

خلال السنوات الأخيرة أصبح استعمال تكنولوجيا المعلومات والاتصال لأهداف إجرامية يشكل تحديا حقيقيا لجل الدول، والجزائر في إطار إستراتيجيتها الأمنية المبنية على مواكبة التطورات الحاصلة أنشأت مجموعة من الأجهزة التي من شانها وضع حد والتقليل من هذه الجرائم السيبرانية نذكر:

- **مركز الوقاية من جرائم الآلي والجرائم المعلوماتية للدرك الوطني:** انشأ هذا المركز سنة 2008 ويعتبر الجهاز الوحيد المتخصص لهذا المجال في الجزائر ويهدف أساسا إلى تأمين منظومة المعلومات لخدمة الأمن العمومي.
- **المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:** يعتبر مؤسسة عمومية ذات طابع إداري انشأ بموجب المرسوم الرئاسي رقم 04-183 المؤرخ في 26 جوان 2004 ومن مهامه:

- القيام بالخبرات العلمية أو خبرات اللازمة في توجيه التحقيقات القضائية بطلب من القضاة من اجل كشف الحقيقة بالأدلة العلمية لتحديد هوية مرتكبي الجنايات والجنح.
- العمل على ترقية البحوث التطبيقية وأساليب التحريات التي أثبتت فعاليتها في ميادين علمي الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي.

❖ **المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني .**

كما تبنى المشرع الجزائري إستراتيجية جديدة لمكافحة الجرائم المعلوماتية حيث قام بإنشاء منظومة وطنية لأمن الأنظمة المعلوماتية بموجب المرسوم الرئاسي رقم20–05 مؤرخ في 20 جانفي 2020، وتعتبر هذه المنظومة أداة الدولة في مجال امن الأنظمة المعلوماتية وتشكل الإطار التنظيمي لإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذها.

وتشمل المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني على كل من **مجلس وطني لأمن الأنظمة المعلوماتية** مهمته إعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، والموافقة عليها وتوجيهها، وكذلك على **وكالة لأمن الأنظمة المعلوماتية** تكلف بتنسيق وتنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية. الأنظمة المعلوماتية تكلف بتنسيق وتنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية.