وزارة التعليم العالي والبحث العلمي
Ministry of High Education and Scientific Research
جامعة محمد البشير الإبراهيمي برج بوعريريج
University of Mohamed el Bachir el Ibrahimi-Bba
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي في الحقوق

تخصص: إعلام آلي و انترنت

الآليات العقابية لمكافحة الجريمة الالكترونية في الجزائر

إعداد الطالبتين: إشراف الدكتوراه: رمضاني مريم

- ماضـــي نعيمة

- بن ناصف وردة

لجنة المناقشة

الاسم و اللقب	الرتبة	الصفة
رفاف لخضر	أستاذ محاضر أ	رئيسا
رمضاني مريم	أستاذ مساعد ب	مشرفا و مقررا
بلقمري ناهد	استاذ محاضر ب	ممتحنا

السنـــة الجـامعيـــة

﴿2021-2022﴾

يعيش العالم اليوم أزهى عصوره العلمية والتكنولوجية وذلك بفضل الثورة المعلوماتية وتوسيع استخدام شبكة الانترنت التي حققت طفرة ملحوظة في مستويات التقدم التقني والعلمي، شملت معظم نواحي الحياة خاصة التطور الهائل في مجال الاتصالات والأنظمة المعلوماتية ، تهاوت أمامها الحدود السياسية والحواجز بين الدول والشعوب وضاقت معها الأماكن وتقلصت فيها المسافات واختزلت وطوت الأبعاد ، بما يتميز من عنصري السرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها في أوقات جد قياسية ومن ثم نقلها وتبادلها عن بعد بين الأطراف المختلفة داخل الدولة الواحدة أوبين عدة الدول .

ولا شك أن هذه الثورة المعلوماتية قد انعكست بصورة ايجابية على كثير من جوانب الحياة المعاصرة بسبب ما توفره من الوقت والجهد والتكلفة على الإنسان تجعل حياته اليومية أكثر سهولة ويسر .

وبالرغم من المزايا والفوائد الجمة التي تحققت وتتحقق يوما بعد يوم في كل مناحي الحياة بفضل تقنيات ووسائل تكنولوجيات المعلومات والاتصالات ، إلا أن الاستخدام المتنامي لهذه التقنيات انطوى في الوقت ذاته على بعض الجوانب السلبية ،التي تمثل تهديدا خطيرا للأمن والاستقرار في المجتمع جراء سوء استعمال هذه التقنيات واستغلالها على نحو غير مشروع وبطرق من شانها أن تلحق الضرر بمصالح الأفراد والجماعات، والمساس بأمن الدول واستقرارها ، الشيء الذي استتبعه ظهور نمط جديدا من الجرائم ازدادت مع الوقت وتعددت صورها وأشكالها يطلق عليها تسمية " **الجرائم الالكترونية**" ،وقد عرفت تطورا مذهلا سواء في أشخاص مرتكبيها أوفي أسلوب ارتكابها والتي تتمثل في استخدام آخر ما توصل إليه العلم وتطويعه في خدمة الجريمة .

ولا جدال فيه أن الجريمة الالكترونية من اخطر واعقد الجرائم على الإطلاق، وتأتي في مقدمة الأشكال الجديدة للجريمة المنظمة ، وخطورة هذه الجرائم نابعة من طبيعتها المتميزة والمعقدة من حيث ذاتية أركانها وحداثة أساليب ارتكابها والبيئة التي ترد عليها ، وخصوصية مرتكبيها ووسائل كشفها ، فهي جريمة تقنية سهلة الارتكاب تنشا في الخفاء ببيئة الكترونية افتراضية لا تترك أي آثار محسوسة ،ويقترفها مجرمون أذكياء يمتلكون

أدوات المعرفة الفنية للتعامل في مجال المعالجة الآلية للمعطيات ويتمتعون بمهارات وخبرات تقنية عالية، كما أنها جرائم عبر الحدود، مما أضفى على هذا النمط من الجرائم سمة التعقيد وصعوبة السيطرة والملاحقة القانونية الإجرائية والعقابية في ظل نصوص جنائية ذات طابع تقليدي لا تتوافق مع هذه الأنشطة الإجرامية المستحدثة .

كل هذا دفع المشرع الجزائري إلى تدارك الفراغ التشريعي والقصور الذي يعتري تطبيق النصوص العقابية، لمكافحة هذا النوع المستجد من الإجرام العابر للحدود عن طريق تنقيح القوانين الداخلية وسن قوانين تستجيب والتحولات الراهنة من خلال القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتضمن تعديل قانون العقوبات ،والقانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، وكذا سن نصوص جديدة عملت في مختلف موادها على وضع العديد من الآليات الردعية والعقابية وتعزيزها بهيئات وطنية أهمها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال التي تم إنشاءها بموجب قانون 09-04 المذكور أعلاها وقد صدرت بعده عدة أوامر تبين طبيعتها وطريقة سيرها آخرها المرسوم الرئاسي 21-439 المؤرخ في 2021/11/07 المتضمن إعادة تنظيم الهيئة ، ومن أجل تحقيق المواجهة الفعالة لظاهرة الإجرام الالكتروني قام المشرع الجزائري بتمديد الاختصاص المحلي لضباط الشرطة القضائية إلى كامل الإقليم الوطني بموجب القانون 06-22 المعدل لقانون الاجراءات الجزائية، بالإضافة إلى تدخله سنة 2021 لإنشاء قطب جزائي ذو اختصاص وطني يعنى بمكافحة جرائم تكنولوجيات الإعلام والاتصال ،بموجب الأمر رقم 21-11 المؤرخ في25 غشت2021 يتمم الأمر رقم 66-155 المؤرخ في 8يونيو1966 والمتضمن قانون الإجراءات الجزائية، بباب سادس عنوانه القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

ويعتبر هذا التشريع نقلة نوعية في النصوص الإجرائية الجزائية أنيط بها مكافحة الجريمة الالكترونية والحد من انتشارها ،وكذا تامين الأنظمة المعلوماتية من اعتداءات المجرمين وتوقيع العقاب عليهم.

أهمية الموضوع : تبدو أهمية هذا البحث في انه يقدم أسلوبا علميا وقانونيا يمكن الاستعانة به في وضع إطار قانوني للجريمة المعلوماتية عبر الانترنت، والوسائل والآليات العقابية لمكافحتها، كون أن تطور الأوجه القانونية والتشريعية لا يكون دائما بخطى موازية مع تطور الجريمة المعلوماتية، وهوما ينتج عنه عجز التشريعات القائمة عن مواجهة هذا الخطر الداهم، مما يتطلب إعادة النظر في وسائل المكافحة التقليدية وابتكار أساليب جديدة لمكافحة فعالة وناجعة لمواجهة لهذا النوع من الاجرام .

وكذا إثراء المكتبة الجامعية وخاصة مكتبة الحقوق بموضوع يعالج الآليات العقابية لمكافحة الجرائم الالكترونية في التشريع الجزائري .

أسباب اختيار الموضوع :هناك أسباب ذاتية ،وأخرى موضوعية دعتنا إلى اختيار هذا الموضوع والتي تتمثل في :

الأسباب الذاتية :تتعلق هذه الأسباب بالرغبة الشخصية لدراسة هذا الموضوع والتعمق فيه كونه يعتبر من الجرائم المستجدة الأكثر تعقيدا ،بالنظر إلى المحيط الذي ترتكب فيه .

أيضا قمنا باختيار هذا الموضوع نظرا لاهتمامنا الكبير بمجال المعلوماتية من الناحية التقنية ،مما دفع بنا إلى دراسة الجانب القانوني العقابي في التشريع الجزائري ، خاصة في السنوات الأخيرة وبظهور الوباء العالمي كوفيد 19 ،الذي غير سياسات الدول، وحيث انه أدخل الشعوب في حجر إجباري، أدى إلى توقف الحياة العملية، مما اضطر الأشخاص والمؤسسات والدول إلى التوجه بشكل جد مفرط نحو استخدام التكنولوجيات الحديثة عبر شبكات الاتصال أهمها شبكة الانترنت لتسيير مصالحهم وتلبية احتياجاتهم عبرها، وبالتبعية تنامي الإجرام الالكتروني وتطور صوره خاصة الإرهاب الدولي ، الذي وضع كل تشريعات العالم في تحد مع الزمن لسن منظومة قانونية تتصدى لهذه الظاهرة المستحدثة .

الأسباب الموضوعية: من الأسباب الموضوعية التي دعتنا إلى اختيار بحثنا ما يلي :

– ان هذا البحث يعتبر من المواضيع الجديدة ذات القيمة العلمية في كافة مجالات الحياة العامة والخاصة التي يجب ترصدها باستمرار ومعالجتها ، كونه حديث ،ومختلف عن

أشكال التجريم الكلاسيكية، لم يجرمها المشرع الجزائري إلا سنة 2004 حرصا منه على مواكبة عصر التكنولوجيا وتوفير حماية شاملة للنظام المعلوماتي ،فتنوعت أوجه الحماية من خلال تعديل القوانين العامة ،واستحداث قوانين خاصة لضمان حماية جنائية فعالة بسن نصوص تشريعية عقابية .

أهداف البحث :نسعى من خلال هذه الدراسة إلى جملة من الأهداف تتمثل في :

– الرغبة في تسليط الضوء على ظاهرة إجرامية تزداد بمعدلات قياسية خاصة مع الانتشار الهائل لاستعمال جهاز الكمبيوتر وشبكة الانترنت.

– بيان أشكال الاعتداء على نظام المعلومات المرتكب من طرف المجرم المعلوماتي .

– تحديد الإجراءات والآليات المستجدة من قبل المشرع الجزائري المتعلقة بالتحري والتحقيق في الجرائم الالكترونية ،وبالتالي وضع الخطوط العريضة للتعرف على طرق المكافحة العقابية في هذا النوع من الإجرام .

–**الدراسات السابقة**: خلال البحث اطلعنا على العديد من الدراسات السابقة، لم نصادف اي موضوع سابق يتناول التعديلات الحديثة للمشرع الجزائري بخصوص هذه الجرائم الا في بعض جزئيات من موضوعنا نذكر منها :

1– الدراسة الأولى :" التحقيق الجنائي في الجرائم الالكترونية " أطروحة لنيل شهادة الدكتوراه في العلوم تخصص قانون، الطالب : براهيمي جمال ،جامعة مولود معمري تيزي وزو 2018.

كان الهدف من هذه الدراسة التعرف على طرق وآليات التحقيق في مثل هذه الجرائم ، ثم اقتراح الحلول القانونية المناسبة والممكنة لتجاوز العقبات وللاستفادة منها في المواجهة الفعالة للجرائم الالكترونية ،هذا المقصد الأول .

أما المقصد الثاني ، فهو تطبيقي ينبع من كون هذه الدراسة تأتي في وقت تهم فيه عدة دول بما فيها الجزائر إلى إعادة النظر في قوانينها الإجرائية ، مما قد يتيح لهذا البحث

توجيه أنظار المشرع في هذه الدول إلى ضرورة مسايرة تشريعاتها للتطور التكنولوجي واستدراك الفراغ التشريعي الملحوظ في هذا المجال .

انحصرت إشكالية الدراسة فيما يلي: إبراز إلى أي مدى يمكن الاعتماد على إجراءات التحقيق التقليدية لإثبات جرائم الكترونية ارتكبت في عالم افتراضي غير ملموس

ويتفرع عن سؤال الدراسة الرئيسي ، الأسئلة الفرعية التالية :

– هل تطبيق هذه الإجراءات كافيا وفعالا لاحتواء متغيرات هذا النمط المتجدد والمتطور من الجرائم ، او سيؤدي الى عدم الوفاء بمتطلبات مبدأ الشرعية الإجرائية .

جوانب الاستفادة والاختلاف: محاولة التعرف على طرق التحقيق واثبات الجريمة الالكترونية خاصة فيما تعلق بالفصل الثاني من دراستنا .

أما نقاط الاختلاف فكانت أن موضوع دراستنا كان حول كل الآليات العقابية التي انتهجها المشرع الجزائري لمكافحة الجريمة الالكترونية ، اذ تناولنا التعديلات الحديثة الطارئة مؤخرا على التشريع الجزائري حول الإجرام الالكتروني .

2– الدراسة الثانية:" آليات مكافحة الجريمة المعلوماتية في التشريع الجزائري " مذكرة لنيل شهادة الماستر في القانون تخصص قانون جنائي وعلوم جنائية ، الطالبة : غربي جميلة ، جامعة أكلي محند اولحاج البويرة 2021/2020. تهدف دراسة هذا الموضوع إلى تسليط الضوء على ظاهرة إجرامية يزداد انتشارها بمعدلات قياسية مع الانتشار الهائل لاستعمال جهاز الكمبيوتر وشبكة الانترنت ومحاولة الكشف عن الأساليب الحديثة والمبتكرة في ارتكاب الجريمة الالكترونية ومعرفة موقف المشرع الجزائري في تصديه لهذه الظاهرة

انحصرت إشكالية الدراسة فيما يلي : مدى فعالية الآليات القانونية الموضوعية والإجرائية التي خصها المشرع الجزائري لمكافحة الجريمة المعلوماتية والحد منها .

جوانب الاستفادة والاختلاف :كانت الاستفادة من خلال تطرق الباحث الى تقديم رؤية متكاملة حول الجرائم الالكترونية وخصائصها وأنواعها وحداثتها في المجتمع .

أما جوانب الاختلاف بالرغم من تقارب موضوع دراستنا مع هذه الدراسة الا أنها اختلفت عنها في المجال الزماني والمكاني والأهداف التي سعت اليها .

3- الدراسة الثالثة:" جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري " مذكرة لنيل شهادة الماستر في العلوم القانونية تخصص قانون الأعمال ، الطالبين : محمد بوعمرة– سيد علي بنينال، جامعة أكلي محند اولحاج البويرة 2020/2019.
تهدف دراسة هذا الموضوع إلى تحديد جهاز التحقيق في الجريمة الالكترونية وكذا طرق التحقيق في استخلاص أدلة الإثبات الجنائية في الجرائم الالكترونية ،كما تهدف الى تقديم رؤية خاصة بالمسرح الرقمي الافتراضي غير المرئي .

انحصرت إشكالية الدراسة فيما يلي: مدى استطاعة أجهزة التحقيق في الجريمة الالكترونية مواكبتها ومواجهتها في التشريع الجزائري .

ويتفرع عن سؤال الدراسة الرئيسي الاسئلة التالية :

– ما هي الجريمة الالكترونية وما هو المجرم الالكتروني؟ ما المقصود بالضبط والتحري في الجرائم الالكترونية؟ ما هي الإجراءات المتعلقة بالتحقيق في الجريمة الالكترونية؟ كيفية ضبط الدليل الالكتروني وحجيته لدى القاضي الجزائري ؟

جوانب الاستفادة والاختلاف :عند دراسة الباحث لكيفية ضبط الدليل الالكتروني ومدى حجيته لدى القاضي الجزائري، وتقديم دراسة مفصلة حول الجهاز المختص بالتحقيق في الجرائم الالكترونية ساعدنا في أخذ فكرة حول انجاز الفصل الثاني من دراستنا .

أما نقاط الاختلاف فكانت في إشكالية الدراسة وكذا الخطة ومنهج البحث المتبع.

صعوبات البحث: على الرغم من الصعوبات العديدة التي واجهتها منها قلة المراجع ،كون ان دراستنا من المواضيع الحديثة، لم تتوج بأبحاث كثير ومعمقة على المستوى الوطني التي تعالج هذا النوع من الجرائم على ضوء القانون الجزائري وبصفة ادق قانون العقوبات، ورغم ذلك حاولنا انجاز بحثنا بالمراجع والمصادر المتوفرة حاليا .

الإشكالية :ماهي الاستراتيجية القانونية التي انتهجها المشرع الجزائري من أجل التصدي للجريمة المعلوماتية ومكافحتها ؟

ويثير هذا التساؤل عدة إشكاليات لا يمكن تجاوزها ، بغية ضبط المفاهيم نذكر منها :

– ما المقصود بالجرائم الالكترونية ؟ومن هو المجرم المعلوماتي ؟وعلى اي اساس يتم تصنيف صور الاعتداء على النظام المعلوماتي؟

– ما هي الآليات العقابية التي انتهجها المشرع الجزائري لمكافحة الجريمة الالكترونية ؟

منهج الدراسة : وقد اعتمدنا في دراستنا هاته على المنهج الوصفي التحليلي من خلال تعريف الجرائم الالكترونية وخصوصيتها واصنافها ،وكذا دراسة شخصية المجرم الرقمي، و تحليل النصوص القانونية العقابية التي تبناها المشرع الجزائري في مكافحة الجريمة الالكترونية .

هيكل الدراسة: قوام هذه الدراسة النصوص والقوانين العقابية لمكافحة الجرائم المعلوماتية في التشريع الجزائري ، لذا ارتأينا تقسيم هذا البحث إلى فصلين نتناول في أولهما الأحكام العامة للجريمة الالكترونية بتبيان مفهومها وخصوصيتها ،وكذا تحديد أركانها والمجرم المعلوماتي ثم نصل الى تصنيفها.

اما في الفصل الثاني سنضفي عليه جانبا تطبيقيا بالتطرق إلى الاليات العقابية للمكافحة الجريمة الالكترونية في ظل الترسانة القانونية الجزائرية.

لنخلص في الاخير دراستنا بخاتمة تنطوي على اهم النتائج التي توصلنا اليها ومجموعة الاقتراحات التي نوصي المشرع الجزائري باتخاذها من اجل ضمان سياسة عقابية فعالة لمكافحة هذا النوع من الإجرام.

الفصل الأول

ماهية الجريمة الالكترونية

أدى التطور الهائل في تكنولوجيا المعلومات والاتصالات وزيادة الترابط الالكتروني والاعتمادية المتزايدة على التقنية والانترنت إلى ظهور نوع جديد من الجرائم المستحدثة تختلف عن الجرائم التقليدية أطلق على تسمية **بالجرائم الالكترونية او الجرائم المعلوماتية cybercrime** نتيجة الاستخدام السيئ للتقنيات الحديثة ، وتطويع هذه التقنية للقيام بأعمال إجرامية بسرية تامة، جعل من الانترنت بيئة مثالية لتنفيذ العديد من الجرائم المتعددة والمتنوعة يصعب حصرها، وقد عرفت تطورا ملحوظا ومذهلا في عصرنا هذا سواء في شخصية مرتكبيها (المجرم المعلوماتي) أوفي اسلوب ارتكابها نتيجة اعتمادها على الوسائل التي أتاحتها الثورة المعلوماتية خاصة الانترنت والاجهزة الذكية ليصبح إجراما لا حدود له على مستوى العالم الافتراضي، واضحت الجرائم المرتكبة باستخدام التقنية من الموضوعات الحديثة التي فرضت نفسها على المستوى الوطني والدولي.

وعليه سوف نتناول في هذا الفصل تعريف الجريمة الالكترونية والخصائص التي تتميز بها واركانها في المبحث الاول، كما سنتطرق الى دراسة تصنيفاتها الجريمة الالكترونية والمجرم المعلوماتي في المبحث الثاني .

المبحث الأول

مفهوم الجريمة الالكترونية

تعتبر الجريمة الالكترونية ظاهرة إجرامية حديثة النشأة، وذلك لارتباطها بتكنولوجيا المعلومات والاتصالات والكمبيوتر، وقد أحاط تعريف الجريمة المعلوماتية الكثير من الغموض، وتعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لها ، بل ان البعض ذهب الى ترجيح عدم وضع تعريف، بحجة ان هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب الكتروني .

ومما لا شك فيه ان عدم الاتفاق على وضع تعريف شامل للجريمة الالكترونية ، هو خشية حصر نطاقها داخل إطار تجرمي محدد قد يضر بها ، خاصة في ظل التطور المستمر للتقنية المعلوماتية والذي نلمسه كل يوم ، فما يتم تجريمه اليوم قد يصبح غير ذي أهمية بالنسبة لصور مستحدثة أخرى قد ظهرت نتيجة استخدام تقنيات جديدة [1].

وبالرغم من ذلك نجد بعض المهتمين بدراسة هذا النمط الجديد من الاجرام من الفقهاء قد بذلوا جهودا مضنية في محاولة تعريف مناسب يتلاءم وطبيعة الجرائم الالكترونية .

المطلب الأول

تعريف الجريمة الالكترونية

حيث ادت الحداثة التي تتميز الجرائم الالكترونية واختلاف النظم القانونية والثقافية بين الدول الى عدم الاتفاق على مصطلح موحد للدلالة عليها، وعدم الاتفاق هذا انجر عليه عدم وضع تعريف موحد لهذه الظاهرة الإجرامية المستحدثة ، فالبعض من الفقهاء ينظر اليها بالمفهوم الضيق والبعض الأخر ينظر إليها بالمفهوم الموسع، سنتناول فيه تعريف الجريمة الالكترونية من الجانب اللغوي واصطلاحي وكذا تعريف المشرع الجزائري .

[1] رشيدة بوكر ،**جرائم الاعتداء على نظم المعالجة الالية في التشريع الجزائري المقارن**. منشورات الحلبي الحقوقية مستغانم :الجزائر،2012 ، ص 38.

الفرع الاول : التعريف اللغوي والاصطلاحي للجريمة الالكترونية

تتكون الجريمة الالكتـرونية من لفظين : لفـظ الجريمة ولفـظ الكترونية .

اشتقت كلمة –الجريمة– في اللغة من الجرم وهو التعدي ،او الذنب، وجمع الكلمة اجرام وجروم وهو الجريمة ، وقد جرم يجرم واجترم واجرام فهو مجرم وجريم ، وعرفت الشريعة الاسلامية الجريمة بانها "**محظورات شرعية زجر الله عنها بحد او تعزيز** "[1]

-**كلمة الكترونية** مشتقة من كلمة الكتروني وجمعه الكترونيات المنسوب الى الالكتروني

حيث بدأ ينتشر العقل الالكتروني في كل المكاتب أو ما يسمى الة الحاسوب ، تعتمد على مادة الالكترون لإجراء أدق العمليات الحسابية .

وعرف الكمبيوتر أو الحاسب الالي " اي جهاز الكتروني ثابت ،أ ومنقول سلكي ،أولا سلكي يحتوي على نظام معالجة البيانات ،أو تخزينها، أو ارسالها، أو استقبالها ،أو تصفحها يؤدي وظائف محددة بحسب البرامج والاوامر المعطاة له "

وعرفت معاهدة بودابست الدولية سنة 2001 النظام المعلوماتي بانه " كل جهاز بمفرده أو مع غيره من الاجهزة من الآلات المتواصلة بينها ،أو المتصلة والتي يمكن أن يقوم واحد منها أو أكثر تنفيذا البرنامج معين بأداء المعالجة الالية للبيانات "[2]

ثانيا – التعريف الاصطلاحي للجريمة الالكترونية :

عرفت الجريمة بصفة عامة على انها كل فعل غير مشروع صادر عن ارادة اثمة يقرر له القانون عقوبة او تدابير احترازية، اما الجرائم الالكترونية هي الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت تعتمد على المعلومة بشكل رئيسي .

لم يتفق الفقه الجنائي على ايراد تسمية موحدة للجريمة الالكترونية ، فهناك عدة تسميات والمفاهيم المتقاربة والمنشقة من الاجرام الالكتروني وهي كالتالي :

[1] علي حسن الطوالبة ،**الجريمة الالكترونية**، جامعة العلوم التطبيقية مملكة البحرين،2008 ،ص 46.
[2] خالد ممدوح ابراهيم، **الجرائم المعلوماتية** .ط 2 ،دار الفكر الجامعي :الاسكندرية 2019 ،ص ص 20-21.

جرائم التقنية العالمية **high–tick** ،الجرائم المعلوماتية **information crimes**الجرائم الرقمية**digital crime** ،السبيركرايم**cyber crime** ،جريمة اصحاب الياقات البيضاء*white cillar**الجرائم الناعمة**softe crimes** ،الجرائم النظيفة **clean crimes**، جرائم الكمبيوتر والانترنت وجرائم الحاسب الالي **computer crimes** ، والجرائم المرتبطة بالكمبيوتر **computer– relatedcrimes**.

للدلالة على الافعال التي يكون فيها الكمبيوتر هدفا للجريمة ،اما اصطلاح الجرائم المرتبطة بالكمبيوتر فيراد به تلك الجرائم التي يكون الكمبيوتر فيها وسيلة لارتكاب الجريمة [1].

ثالثا : التعاريف الفقهية للجريمة الالكترونية

اختلف الفقهاء حول وضع تعريف موحد للجريمة الالكترونية، ويعود ذلك لاختلاف حول تحديد نطاق هذه الجريمة المستجدة، فالبعض ينظر اليها بالمفهوم الضيق اولا والبعض الاخر ينظر اليها بالمفهوم الموسع .

01/ الاتجاه الضيق للجريمة الالكترونية :

يستند انصار هذا الاتجاه في تعريفهم للجريمة الالكترونية الى وسيلة ارتكاب الجريمة ويشترطون ارتكابها بواسطة الحاسوب وان يكون الجاني ذا معرفة بالتقنية وهذا ما جاء به **الفقيه تايدمان**tiedemanأنها "كل اشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب " والبعض الاخر عرفها أنها "الجرائم التي يكون للحاسب فيها دورا ايجابيا أكثر منه سلبيا"[2]

وعرفها الفقيه **توم فوريستر** أنها "فعل اجرامي والتي تتم باستخدام الحاسوب كأداء رئيسية" وهنا من عرفها أنها " عمل غير قانوني يستخدم فيه الحاسب كأداة او موضوع الجريمة "

[1] رشيدة بوكر المرجع السابق ، ص36 .

* يطلق لفظ ذوبي الياقات البيضاء على الاشخاص الذين يستخدمون التكنولوجيا الحديثة في ارتكاب جرائمهم دون اراقة الدماء او استخدام اسلحة فبمجرد الضغط على زر الكمبيوتر يحققون اعمالهم الاجرامية .

كما عرفها الدكتور **ديفيد تومبسون** "اية جريمة يكون متطلبا لاقترافها ان تتوفر لدى فاعلها معرفة بتقنية الحاسوب " كما عرفت انها الجريمة التي يتم ارتكابها اذ قام شخص ما باستخدام معرفته بالحاسوب بعمل غير قانوني "

هذا ما جاء به **الفقيه ماروي** عرف الجريمة الالكترونية " عمل غير مشروع يرتكب بواسطة الحاسب الالي كأداة رئيسية اوهي مجموعة صور السلوك الاجرامي التي ترتكب بواسطة المعالجة الالية للمعلومات "[1]

ومن التعريفات التي وضعها انصار هذا الاتجاه ايضا ان الجريمة المعلوماتية هي" كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازما لارتكابه من ناحية وملاحقته من ناحية اخرى "

كما عرفها ايضا " هي التي تقع على جهاز الكمبيوتر او داخل نظامه فقط " اوهي نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الكمبيوتر او تلك التي يتم تحويلها عن طريقه "

اما التقرير الصادر عن وزارة العدل الامريكية لعام 1989 في دراسة وضعها معهد ستانفورد الدولي للأبحاث وتبنتها الوزارة – فقد عرف جرائم تقنية المعلومات بانها " اية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها "[2]

وعرفها مكتب تقييم التقنية في الولايات المتحدة الامريكية من خلال تعريف جريمة الحاسب " بانها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا"[3].

وعرفها leslieball بانها " فعل اجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية "

[1] على حسن الطوالبة، **الجرائم الالكترونية** ، جامعة العلوم التطبيقية :مملكة البحرين، 2008 ص 48.
[2] رشيدة بوكر المرجع السابق ص 39.
[3] احمد خليفة الملط ،**الجرائم المعلوماتية**. ط 2 ، دار الفكر الجامعي: الاسكندرية ،2006 ص 84.

وعرفها كل من hard.castele– r .tott بأنها " تلك الجرائم التي يكون قد حدث في مراحل ارتكابها بعض عمليات فعلية داخل الحاسب " اي يكون للحاسب دور ايجابي اكثر من سلبي.[1]

وعليه يعتمد اصحاب هذا الاتجاه على ضرورة المام الفاعل بتقنية المعلومات واستخدام الحاسوب لإمكانية اعتبارها من الجرائم الالكترونية .

لقد تعرضت معظم التعاريف السابقة للنقد بسبب قصورها واتسامها بالعمومية والاتساع اذ ركز الفقهاء على موضوع الجريمة، وركز البعض الاخر على وسيلة ارتكابها، بينما ركز اخرون على فاعل الجريمة ،بينما نرى ان الجريمة المعلوماتية قد تقع على الحاسب الالي بشقيه المادي والمعنوي ممثلا بالكيان المنطقي بالاعتداء على البيانات المخزنة والمتبادلة بين الحاسب الالي وشبكاته .

02/ الاتجاه الموسع للجريمة الالكترونية :

نظرا للانتقادات التي وجهت للتعريف الضيق للجريمة المعلوماتية حاول الفقهاء تعريفها على نحو واسع لتفادي القصور الذي لحق بتعريفات الاتجاه الضيق ،بحيث يعتمد هذا الاتجاه في تعريف الجريمة الالكترونية على اساس موضوع الجريمة و هو المعالجة الالية للبيانات ، فكل تعريف او تعديل او نقل ونسخ غير مشروع لها يعد جريمة الكترونية .

اذ يعتبر الفقيه **rosemblatt** انها " نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسوب او التي تحول عن طريقه "

واخذت بنفس الاتجاه **الدكتورة قشقورش** الجريمة الالكترونية " انها كل سلوك غير مشروع او غير مسموح به فيما يتعلق بالمعالجة الالية للبيانات "[2]

كما يعتبر الفقيه **كاردار ميشال** الجريمة الالكترونية "استخدام الحاسب كأداة لارتكاب الجريمة بالإضافة الى الحالات المتعلقة بالولوج غير المرخص لحاسوب الضحية او

[1] احمد خليفة الملط ، المرجع السابق، ص 85.
[2] غانم مرضى الشمري، **الجرائم المعلوماتية(ماهيتها خصائصها كيفية التصدي لها)** .الدار العملية الدولية ، 2016 ص ص27-28.

بياناته ، كما تتمثل هذه الجريمة في الاعتداءات المادية على جهاز الحاسوب في حذ ذاته او المعدات المتصلة به ، وكذلك الاستخدام الغير المشروع لبطاقات الائتمان بالإضافة الى تزيف المكونات المادية والمعنوية للحاسوب "

وفقا لهذا الاتجاه تعتبر الجرائم المرتكبة عبر الانترنت هي الجريمة الناجمة عن ادخال بيانات مزورة في الانظمة ، واساءة استخدام المخرجات اضافة الى افعال اخرى تشكل جرائم اكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر.

كما جاء في توصيات الامم المتحدة في المؤتمر العاشر بمنع الجريمة ومعاقبة المجرمين المنعقد في فينا 2000 " انها اي جريمة يمكن ارتكابها بواسطة نظام حاسوبي او شبكة حاسوبية او داخل نظام حاسوبي والجريمة تلك التي تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية "[1]

كما ذهب مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية ocpe في عام 1983 الى تعريف الجريمة المعلوماتية بانها " كل فعل او امتناع من شانه الاعتداء على الاموال المادية والمعنوية يكون ناتجا بطريقة مباشرة او غير مباشرة عن تدخل التقنية المعلوماتية"[2].

وفي تقرير الجرائم المتعلقة بالحاسوب اقر المجلس الاوروبي بقيام المخالفة (الجريمة) في كل حالة يتم فيها تغير المعطيات او بيانات او برامج الحاسوب او محوها او كتابتها اواي تدخل اخر في مجال انجاز البيانات أو معالجتها وتبعا لذلك تسبب في ضرر اقتصادي او فقد حيازة ملكية شخص اخر او بقصد الحصول على كسب اقتصادي له او لشخص اخر فلا يمكن اعتبارها جريمة الكترونية بمجرد وقوع افعال يكون الحاسب الالي دورا في هذا النشاط الاجرامي ،او ضمنه فبعض الجرائم مثلا كسرقة الحاسوب لا يمكن اعتبارها جرائم الكترونية بمجرد ان الحاسوب اواحد اجزائه كان محلا للسرقة .

[1] محمد امين الشوابكة ،**جرائم الحاسوب والانترنت (الجريمة المعلوماتية)**، 2009 ص ص09-10.
[2] احمد خليفة الملط ، المرجع السابق ،ص 87.

نرى ان هذه التعاريف جاءت شاملة للاعتداءات على الجانب المادي للحاسب الالي وشبكاته المحلية أو الممتدة كالأنترنت، بالإضافة الى الجانب المعنوي ومرد ذلك ان نظم الحاسب الالي يشمل كل مكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة حيث يمكن من خلالها تحقيق وظيفة او هدف معين.

الفرع الثاني :تعريف المشرع الجزائري للجريمة الالكترونية

لم يتخلف المشرع الجزائري بدوره عن ركب التشريعات التي وضعت تعريفا للجرائم الالكترونية ، نتيجة تأثره بالثورة المعلوماتية التي نتج عنها اشكال جديدة من الجرائم وذلك من خلال التعديلات الذي أدخله على قانون العقوبات بموجب القانون رقم 04-15 المتمم لقانون العقوبات[1]الذي افرد لها قسما خاصا بها في المواد من 394 مكرر الى 394 مكرر 07 .

واستحدث القانون رقم 09-04 المؤرخ2009/08/05 تسمية "**المساس بأنظمة المعالجة الالية للمعطيات** " للدلالة على الجريمة المعلوماتية معتبرا في ذلك ان النظام المعلوماتي في حد ذاته وما يشمله من مكونات غير مادية محلا للجريمة ، حيث جاء في نص المادة 02 الفقرة "أ " على ان الجرائم المتصلة بتكنولوجيا الاعلام والاتصال هي جرائم المساس بأنظمة المعالجة الالية للمعطيات المحددة في قانون العقوبات اواي جريمة اخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية.

وعرفت الفقرة "ب" من نفس المادة المنظومة المعلوماتية بأنها" مجموعة من الانظمة المتصلة ببعضها البعض أو المرتبطة ، يقوم واحد منها أو أكثر لمعالجة الية المعطيات تنفيذ لبرنامج معين [2]"

اعتمد المشرع الجزائري في تحديده لمدلول الجريمة الالكترونية على مصطلح المساس بأنظمة المعالجة الالية للمعطيات وهذا ما أكده قانون العقوبات ، بحيث يمثل نظام

[1]القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 **المتمم لقانون العقوبات** ،الجريدة الرسمية العدد 71 الصادر بتاريخ 10 نوفمبر 2004.

[2]القانون رقم 09-04 المؤرخ في 05 اوت 2009،**المتعلق بالوقاية من المتعلقة بتكنولوجيا الاعلام والاتصال ومكافحتها** ،الجريدة الرسمية، العدد 47 بتاريخ 16 اوت 2009.

المعالجة الالية للمعطيات المسالة الاساسية أو الشرط الاساسي واللازم تحققه حتي يمكن اعتبار هذه الجرائم الكترونية في القانون الجزائري، وعليه فالمشرع الجزائري اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الالكترونية اولهما معيار وسيلة الجريمة وهو نظام الاتصالات الالكتروني ، وثانيهما معيار موضوع الجريمة المساس بأنظمة المعالجة الالية للمعطيات ،وثالثهما معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليه في قانون العقوبات .

التعريف الاجرائي :وبدورنا نرى ان الجرائم المرتكبة عبر الانترنت هي كل اعتداء يقع على نظم الحاسب الالي وشبكاته أو بواسطتها، أو كل سلوك غير مشروع يمس النظام المعلوماتي المادي أو المعنوي، وكل فعلاو امتناع عن فعل يضر بالأشخاص أو الاموال أو أمن الدولة .

المطلب الثاني :خصائص الجريمة الالكترونية

ان طبيعة الجريمة الالكترونية كظاهرة اجرامية مستجدة ترتكب في بيئة افتراضية تجمع بين الذكاء الاصطناعي والذكاء البشري تنفرد بعدة خصائص تميزها عن الجرائم الكلاسيكية اهمها :

1-خطورة جرائم الحاسب الالي : تتميز الجرائم الالكترونية بالخطورة الشديدة على النظام المعلوماتي بالنظر لحجم الاضرار الكبيرة التي تنجر عنها المساس خاصة بالاقتصاد المؤسسات ، كما انها تعتدي بالأمن القومي، والسياسي، والاقتصادي خاصة البنوك التي تعتبر الهدف الرئيسي لمجرمي الجرائم المعلوماتية ، وذلك لاعتمادها كليا على انظمة نقل التمويل الكترونيا، كما تطال الاعتداءات الحق العلمي والثقافي والاقتصادي للمجتمع ويقف عائقا في التنمية ، بالإضافة الى مخاطر متعددة كفقدان الثقة بالتقنية الالكترونية وتهديد الملكية الفكرية وقتل روح ابداع انسان[1].

2-الجريمة الالكترونية تتطلب وجود حاسب الي ومعرفة تقنية استخدامه : الحاسب كوسيلة يعتبر من المتطلبات الرئيسية لارتكاب جرائم الحاسب الالي ، فلا يمكن الحديث

[1] علي حسن الطوالبة ،المرجع السابق ، ص 60 .

عن جريمة معلوماتية دون استخدام جهاز الحاسوب، كما تتطلب هذه الجرائم الماما كافيا لمهارات ومعارف فنية وتقنية بعلوم الحاسوب واستخدامه وتشغيله ، فأكثرية مقترفي هذه الجرائم من المتخصصين في معالجة المعلومات اليا[1] .

3-جريمة ناعمة تنفذ بسرعة : لا تتطلب لارتكابها العنف ولا استعمال الادوات الخطيرة كالأسلحة وغيرها ، فنقل بيانات ممنوعة والتلاعب بأرصدة البنوك مثلا لا تحتاج الا الى لمسات أزرار فهي من الجرائم الناعمة تعتمد بشكل كبير على القدرة الذهنية والتفكير العلمي القائم على المعرفة بتقنيات الحاسوب والانترنت والمام بتكنولوجيا النظم المعلوماتية تنفذ بسرعة[2] فاغلب الجرائم المعلوماتية ترتكب في وقت قصير جدا لا يتجاوز الثانية .

4-الجريمة المعلوماتية جريمة عابرة للحدود : الجريمة المعلوماتية تتسم غالبا بالطابع الدولي ، ذلك ان الطابع العالمي لشبكة الانترنت وما يرتبه ، جعل معظم دول العالم في حالة اتصال دائم على خط on line يسهل ارتكاب الجريمة من دولة الى دولة اخرى فالجريمة المعلوماتية لا تعترف بالحدود بين الدول والقارات ، فهي جريمة عابرة للقارات بين العالم كافة [3]، اذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم بين الدول والانظمة يفصل بينهما الاف من الاميال مثل جرائم التعدي على قواعد البيانات وتزوير واتلاف المستندات الالكترونية والاحتيال المعلوماتي والقرصنة ... الخ .

ذلك ان قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف اصقاع الارض انعكست ايضا على طبيعة الاعمال الاجرامية ، وهذا ما يعني ان مساحة مسرح الجريمة المعلوماتية لم تعد محلية بل اصبحت عالمية [4].

ان هذه الجرائم هي صورة من صور العولمة ، فمن حيث المكان يمكن ارتكاب هذه الجرائم عن بعد ، وقد يتعدد هذا المكان بين اكثر من دولة ومن الناحية الزمنية تختلف المواقيت بين الدول ، الامر الذي يثير في كثير من الاحيان تحديات قانونية وادارية بل وسياسية بشان مواجهتها لا سيما فيما يتعلق بإجراءات الملاحقة الجنائية ،اهمها القانون

[1] غانم مرضى الشمري ،المرجع السابق ، ص 39.
[2] على حسن الطوالبة ،المرجع السابق ،ص 70.
[3] خالد ممدوح ابراهيم ،**الجرائم المعلوماتية** .ط 2 ، دار الفكر الجامعي الاسكندرية ص 77.
[4] نفس المرجع، ص 78 .

الواجب التطبيق والقضاء المختص ،بالإضافة الى اشكالية الملاحقة القضائية فهل هـ وقانون الدولة التي وقع فيها النشاط الاجرامي ؟ ام الدولة التي يقيم فيها الجاني ؟ أو الدولة الي اضر بمصالحها ؟ لذا بات من الضروري ايجاد الوسائل المثالية للتوفيق بين التشريعات الخاصة بهذه الجرائم عن طريق ابرام الاتفاقيات الدولية الخاصة بتسليم المجرمين والوسائل الكفيلة لمكافحة هذا النوع من الجرائم [1].

5-صعوبة اكتشاف الجريمة الالكترونية : تتميز جرائم الحاسب الالي بصعوبة اكتشافها كون انه لا يتم الابلاغ عنها لعدم اكتشافها من قبل الضحية ، واذا اكتشفت الجريمة فلا يكون ذلك الا بمحض الصدفة ، بل بعد وقت طويل من ارتكابها مما يساعد على عدم التعرف على مرتكبي الجرائم الالكترونية وذلك بسبب احجام البنوك والشركات ومؤسسات الاعمال عن الابلاغ عن مرتكبيها خوفا من الاضرار بالمركز المالي للجهة المعتدى عليها وتجنبا للإساءة الى السمعة وهز ثقة العملاء[2].

كذلك اخفاء اسلوب ارتكاب الجريمة خوفا من قيام الاخرين بتقليد هذا الاسلوب ، وهوما يدفع المجني عليه الى الاحجام عن ابلاغ السلطات المختصة عن الجريمة وهوما يزيد فرص للمجرم المعلوماتي في الافلات من العقاب ، حتى في حالة الضبط لا يتعاون مع جهات التحقيق خوفا ممار يترتب على ذلك من دعاية مضادة وضياع الثقة[3].

هذا ما نتج عدم وجود احصائيات مضبوطة ودقيقة تحدد الحجم الحقيقي لهذه الظاهرة الاجرامية .

6-صعوبة اثبات الجريمة الالكترونية: الجرائم الالكترونية تتصف بالخفاء اي عدم وجود اثار مادية يمكن على اساسها متابعتها ،وهي خطيرة وصعبة الاكتشاف سواء في تحديد مكان وقوعها أو مكان التعامل معها بسبب اتساع نطاقها المكاني وضخامة البيانات

وترجع صعوبة اثبات الجريمة المعلوماتية الى عدة امور هي :

[1] خالد ممدوح ابراهيم ،**الجرائم المعلوماتية** .ط 2 ، .دار الفكر الجامعي الاسكندرية 2019 ،ص 95.
[2] احمد خليفة الملط ،المرجع السابق ، ص 95.
[3] نفس المرجع ،ص 95.

أ- لا تترك اثار مادية لها بعد ارتكابها : ان هذه النوعية من الجرائم الالكترونية الرقمية لا تترك اثرا ماديا في مسرح الجريمة الالكتروني ،فليس هناك اموال أو أشياء مفقودة وانما هي ارقام تتغير في السجلات ولا توجد مستندات ورقية ،ولا تترك شهود يمكن استجوابهم ولا ادالة مادية يمكن فحصها كونها جريمة تقع في بيئة الكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الالكترونية غير مرئية[1].

ب -يتم ارتكاب جريمة الحاسب عادة عن بعد : فلا يتواجد الفاعل في مسرح الجريمة وتتباعد المسافات بين الفاعل والنتيجة ، وهذه المسافات لا تقف عند حدود دولة بل تمتد الى النطاق الاقليمي لدول اخرى مما يضاعف صعوبة اثباتها أ وملاحقتها .

ج-سرعة محو الدليل وتوفر وسائل تقنية تعرقل الوصول اليه : يسهل محو الدليل من شاشة الكمبيوتر في زمن قياسي باستعمال البرامج المتخصصة لذلك ، اذ يتم عادة في لمح البصر وبمجرد لمسه خاطفة على لوحة المفاتيح بجهاز الحاسوب على اعتبار ان الجريمة تتم في صورة اوامر تصدر الى الجهاز، وما ان يحس الجاني بان امره سينكشف حتى يبادر بإلغاء هذه الاوامر، الامر الذي يجعل كشف الجريمة وتحديد مرتكبيها امر في غاية الصعوبة 3.

7-صعوبة التحقيق والتحري في نطاق الجريمة الالكترونية : ينطوي التحري والتحقيق في الجرائم الالكترونية على مشكلات وتحديات ادارية وقانونية يصعب على المحقق التقليدي التعامل معها ، كون التحقيق في الجريمة الالكترونية الرقمية ذات البنية الرقمية يحتاج لإمكانيات مادية وقوعد واجراءات تختلف عن التحقيق في الجرائم التقليدية سواء من حيث طبيعة السلوك الاجرامي الالكتروني ، اومن حيث طبيعة الدليل الالكتروني او وسائل واليات كشف الجريمة والوصول الى الدليل الالكتروني.

حيث تتطلب جرائم الكمبيوتر والانترنت المام خاصا بتقنيات الكمبيوتر ونظم المعلوماتية سواء للتحقيق فيها او لملاحقتهم قضائيا، لذا يجد الضبطية القضائية احيانا انفسهم غير

[1]امير فرج يوسف ،**الجرائم المعلوماتية على شبكة الانترنت**. دار المطبوعات الجامعية ، 2009 ،ص 18.
3موسى مسعود ،**ارجومة الاشكاليات الاجرامية التي تثيرها الجريمة المعلوماتية عبر الوطن المؤتمر المغاربي اول** ص 3.

قادرين على التعامل بالوسائل الاستدلالية والاجراءات التقليدية مع هذه النوعية من الجرائم فضلا عن صعوبة اجراء التحريات السرية وتتبع مسار العمليات الالكترونية العابرة للحدود كما ان رجال الشرطة قد لا يتعاملون بمهارة واحترافية مع الدليل الالكتروني المستمد من الجريمة المعلوماتية فقد يتسبب المحقق بدون قصد أو بطريق الخطأ في اتلاف الدليل الالكتروني أو تدميره[1].

اذن تتركز السمات الذاتية لعناصر التحقيق في سرعة الكشف خشية ضياع الدليل الالكتروني ، وخصوصية التفتيش والضبط الملائمة لهذه الجرائم ،يتطلب فريق تحقيق ذا سمات ذاتية في تكوينه ، خاصة فريق ضبط وتحريز الادلة الالكترونية الذي يجب ان يكون من بين اعضائه محقق في مجال الحاسب الالي وخبير في الحاسب الالي ومكوناته المادية والمعنوية ومدرب على التعامل مع الادلة الالكترونية وطرق تقييمها[2].

8-وقوع الجريمة الالكترونية اثناء المعالجة الالية للبيانات: من خصائص الجريمة المعلوماتية انها تقع اثناء عملية المعالجة الالية للبيانات والمعطيات الخاصة بالكمبيوتر * ويمثل هذا النظام الشرط الاساسي الذي ينبغي توافره حتى يمكن البحث في قيام أو عدم قيام اركان الجريمة المعلوماتية خاصة بالتعدي على نظام المعالجة البيانات ، ذلك انه في حالة تخلف هذا الشرط تنتفي الجريمة المعلوماتية .

فالجرية الالكترونية قد تقع اثناء عملية المعالجة الالية للبيانات ،في اي مرحلة من المراحل الاساسية لتشغيل نظام المعالجة الالية للبيانات ،سواء عند مرحلة ادخال البيانات أو اثناء مرحلة المعالجة ، أو أثناء اخراج المعلومات ، ففي مرحلة الادخال تترجم المعلومات الى لغة مفهومة من قبل الالة ، يكون من السهل ادخال بيانات جديدة لا علاقة لها بالمعطيات القائمة ،ومحو البيانات الاساسية المطلوب ادخالها ، وفي مرحلة

[1] خالد ممدوح ابراهيم ،المرجع السابق ،ص ص 88-89

[2] مصطفى محمد موسى ،**التحقيق الجنائي في الجرائم الالكترونية** . ط 2008 ،مطابع الشرطة شارع المرور: القاهرة ص.167

*عملية المعالجة الالية للبيانات أو المعطيات عرفت " انها كل مركب يتكون من وحدة أو مجموعة وحدات معالجة و التى تتكون كل منها من الذاكرة والبرامج والمعطيات واجهزة الادخال والاخراج واجهزة الربط والتي يربط بينهما مجموعة من العلاقات والتي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات على ان يكون هذا المركب خاضعا لنظام الحماية الفنية

المعالجة يمكن ادخال اي تعديلات على البرنامج يمكن التلاعب في برامج النظام المعلوماتي فيتم ادخال بيانات غير مصرح بها أو استبدالها بالبيانات الاساسية أو تشغيل برامج جديدة تلغي جزئيا أو كليا عمل البرامج الاصلية ،اما المرحلة الاخيرة المتعلقة بالمخرجات وفيها تتم التلاعب في النتائج التي يخرجها النظام المعلوماتي بشان بيانات غير صحيحة ادخلت فيها معالجة غير صحيحة [1].

[1] خالد ممدوح، ابراهيم المرجع السابق، ص 84.

المطلب الثاني

اركان الجريمة الالكترونية

تعد اركان الجريمة الاساس والاصل لقيام اي جريمة ، ونكون امام تصرف يعاقب عليه القانون ، فلا يمكن القول بوجود جريمة الكترونية دون توافر الاركان الثلاثة المعروفة في الجريمة الكلاسيكية والتي تختلف نوعا ما عن الجريمة التقليدية .

فالمشرع اشترط لقيام الجريمة الإلكترونية وجود ثلاثة اركان اساسية وهي الركن المادي الذي يمثل كيانها الملموس ويعبر عن ارادة الفاعل بصورة يمكن اثباتها ، اما الركن المعنوي يعبر عن ارادة المجرم المعلوماتي ، اما الركن الشرعي فيعني وجود نص قانوني يحدد الجريمة والجزاء الجنائي المقرر لها هذا ما نستشفه في هذا المطلب.

الفرع الاول :الركـن الشرعــي

تعتبر الجريمة عمل غير مشروع يجرمه القانون ويعاقب عليه، وذلك بالنظر لما يقرره القانون ونواهي تجرم وتعاقب على كل سلوك أو فعل ترى فيه السلطة المختصة بالتشريع انه يرقى لدرجة التجريم بما يشكله من مساس بمصالح الجماعة بتعريضها بوجه عام للخطر [1].

وانطلاقا من مبدا الشرعية وفقا لأحكام المادة الاولى من قانون العقوبات التي تنص " **لا جريمة ولا عقوبة أو تدابير امن بغير قانون** "وما يتماشى مع المادة 160من دستور 2016 التي تنص على ان تخضع العقوبات الجزائية الى مبدا الشرعية والشخصية[2].

جرم القانون رقم 04-15 بعض صور الجريمة المعلوماتية ونص على العقوبات المقررة لمرتكبيها في القسم السابع مكرر تحت عنوان " المساس بأنظمة المعالجة الالية

[1] بوخبزة عائشة ،**الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري**. مذكرة ماجستير في القانون الجنائي كلية الحقوق جامعة :وهران الجزائر 2012-2013 ص 62.

[2] القانون رقم 01/16 مؤرخ في 06 مارس ،**يتضمن التعديل الدستوري** جريدة رسمية العدد 14 الصادرة في 07 مارس 2016.

للمعطيات " من الفصل الثالث وذلك من المواد 394 مكرر الى 394 مكرر 07 من قانون العقوبات المعدل والمتمم .

في حين جاء القانون 09-04 الصادر بتاريخ 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها كجانب وقائي يحدد من وقوع الجرائم ، وهذا تطبيقا لمبدا الشرعية وعدم جواز متابعة شخص بأفعال غير مجرمة قانونا [1].

الفرع الثاني :الركــن المــادي

ان النشاط أو السلوك المادي في الجريمة الالكترونية يتطلب وجود بيئة رقمية وجهاز كمبيوتر واتصال بشبكة الانترنت ويتطلب ايضا معرفة بداية هذا النشاط والشروع فيه ونتيجته والعلاقة السببية بين النشاط الاجرامي والفعل الضار، فأي فعل اجرامي تسبقه اعمال تحضرية من شانها تفعيل الركن المادي ،وعلى سبيل المثال كان يقوم مرتكب الجريمة بتجهيز الكمبيوتر لكي يحقق له حدوث الجريمة ، فيقوم بتحميل الحاسب ببرامج الاختراق، اوان يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج الى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة أو يقوم بإعداد برامج فيروسات تمهيدا لبثها [2]

01- النشاط الاجرامي :

ويشترط ايضا في الركن المادي مباشرة التصرف التقني وان يكون لهذا الفاعل دراية كافية وتحكم في هذه الوسائل وهذا ما اورده المشرع في المادة الثانية من القانون 09-04 " **جرائم المساس بأنظمة المعالجة الالية المحددة في قانون العقوبات واي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية .**

يتمثل الركن المادي في اشكال الاعتداء على نظام المعالجة الالية للمعطيات وهذا ما نصت عليه المادة 394مكرر من قانون العقوبات ت بقولها "**يعاقب بالحبس من ثلاث اشهر الى سنة وبغرامة من 50.000 دج الى 100.00 دج كل من يدخل أويبقى عن**

[1] القانون رقم 09-04 المؤرخ في 05 اوت 2009 ،**المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها**،الجريدة الرسمية العدد 47 بتاريخ 2009/08/16.

[2] خالد ممدوح ابراهيم ،**فن التحقيق الجنائي في الجرائم الالكترونية**، دار الفكر الجامعي: الاسكندرية 2009،ص 52 .

طريق الغش في كل أو جزء من منظومة المعالجة الالية للمعطيات أو يحاول ذلك تضاعف العقوبة اذا ترتيب عن ذلك الحذف أو تغيير لمعطيات المنظومة ، واذا ترتب عن الافعال المذكورة اعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة اشهر الى سنتين والغرامة من 50.000 دج الى 150.00 دج "[1]

من خلال هذه المادة نتعرض للنشاط الاجرامي المرتكب من قبل المجرم المعلوماتي .

الدخول: وهو عملية ولوج غير شرعي الى نظام التشغيل في الحاسب من قبل اشخاص لا يملكون سماحيات الدخول ،بهدف القيام بأعمال غير قانونية مثل التجسس والسرقة[2].

البقاء: نقصد به البقاء بطريقة غير مشروعة، اي التواجد داخل نظام المعالجة الالية لمعطيات ضد ارادة من له الحق في السيطرة على هذا النظام في كل أو جزء من المنظومة المعالجة الالية للمعلومات[3]أو يحاول ذلك، فمجرد محاولة تعتبر جريمة يعاقب عليها القانون، وتشدد العقوبة على هذا الفعل ، كما تضاعف العقوبة في حالة المساس هذه المعطيات سواء بالحذف ،أو التغيير ،أو المحو.

كما تناولت المادة 394 مكرر من قانون العقوبات الاعمال المادية التي يقوم بها المجرم المعلوماتي كالتعديل ، أو الادخال ، سواء كان المساس العمدي بالمعطيات داخل النظام بالدخول والبقاء ولمحو والتعديل والادخال للبيانات والمعلومات، أو المساس العمدي بالمعطيات خارج النظام حسب المادة 394 مكرر 02 بالنشر، التوفير، والتجميع والبحث وكذا تصميم البرامج من اجل الوصول الى نظم المعالجة الالية وتحقق عملية الاختراق والقيام بأعمال غير مشروعة .

02- النتيجة الاجرامية :الاصل ان يتطلب لقيام الجريمة الالكترونية وجود ما يسمى بالنتيجة الاجرامية التي يرتبها أو يحدثها النشاط الاجرامي، هذه النتيجة في الغالب من الاحيان تظهر بصورة اثر مادي ضار أو اعتداء على حق يحميه القانون ، فاغلب

[1] القانون رقم 01/16 مؤرخ في 06 مارس .**يتضمن التعديل الدستوري**، جريدة رسمية العدد 14 الصادرة في 07 مارس 2016.

[2] رشيدة بوكر ،المرجع السابق ، ص178.

[3] نفس المرجع ،ص251.

الجرائم المعلوماتية يلتزم لتوافرها تحقق النتيجة الاجرامية مثلا كالاختراق من شانه الحاق ضرر بالبيانات والمعطيات التي يحتويها النظام تجعله غير صالح لأداء وظائفه .

03- العلاقة السببية :لكي يكتمل البناء القانوني للجريمة في ركنها المادي لا بد ان يرتبط السلوك بالنتيجة التي تحققت اي يجب توفر العلاقة السببية بين السلوك والنتيجة ، بحيث ان امكن رد هذه النتيجة الى عامل اخر غير سلوك المجرم المعلوماتي تنقطع علاقة السببية وتنتفي المسؤولية الجزائية ، فليس من العدل مساءلة شخص على نتيجة تحققت بفعل اخر مثلا كتعطل النظام اواي سبب اخر .

الفرع الثالث: الركــن المعنــوي

يتخذ الركن المعنوي في اغلب الجرائم بصفة عامة صورة القصد الجنائي ، والذي يتحقق بتوافر ارادة لعمل غير شرعي لدى الجاني مع علمه ان القانون يجرمه، ونفس الامر ينطبق على الجريمة الالكترونية بتوافر الارادة الجرمية لدى الفاعل وهي حالة ذهنية ونفسية يكون عليها الجاني ساعة اقدامه على ارتكاب الجريمة ،وهذا ما يظهر من خلال استعمال المشرع الجزائي لعبارة " **الغش** " " **العمد** " في المواد 394 مكرر و394 مكرر 1 و394 مكرر 2 و394 مكرر 5 وهذا ان دل على شيء انما يدل على ان الجريمة الالكترونية جريمة عمدية ولا يفترض فيها عنصر الخطأ .

اضافة الى وجوب توافر العلم لكافة العناصر الداخلية في تشكيل الجريمة ومن قبيل ذلك ضرورة علم الجاني ان فعله ينصب على نظام المعالجة الالية وليس على شيئ اخر، وان يعلم بانه ليس له الحق في الدخول والبقاء الى نظام المعالجة الالية ، فضلا عن ذلك لا بد ان يعلم الجاني بخطورة الفعل به على المصلحة التي يحميها .

المبحث الثاني

أنواع الجرائم الالكترونية ومرتكبيها

لتعدد أنواع جرائم الانترنت لم يوضع لها معايير محددة من أجل تصنيفها ، وذلك تأسيسا على التطور المستمر للشبكة والخدمات التي تقدمها .

كما أن محترفي الجرائم المعلوماتية يتمتعون بقدرة عالية من الذكاء وإلمام جيد بالتقنية العالية، واكتسابهم معارف عملية وعلمية ،وانتمائهم إلى التخصصات المتصلة بالحاسوب من الناحية الوظيفية ،وهذه السمات تتشابه مع سمات الياقات البيضاء .[1]

المطلب الأول

تصنيف الجرائم الالكترونية

صنف الفقهاء والدارسون الجرائم الالكترونية ضمن فئات متعددة ، تختلف حسب الأساس والمعيار الذي يستند إليه التقسيم المعني ، فبعض الفقهاء أسس تقسيمه على تعدد محل الاعتداء وكذا تعدد الحق المعتدى عليه فتوزع الجرائم وفق هذا التقسيم إلى:

– جرائم تقع على الأموال وتلك التي تقع الأشخاص وأخرى تقع على المصلحة العامة .

وقد صنفها معهد العدالة القومي بالولايات المتحدة الأمريكية عام 1985 بحسب علاقتها بالجرائم التقليدية .

– بينما يصنفها البعض حسب النتيجة المترتبة على السلوك الإجرامي فيقسمها إلى:

جرائم ذات نتيجة وأخرى شكلية.

– وهناك من يقسمها إلى جرائم كمبيوتر وجرائم انترنت.

[1] محمود أحمد طه، **المواجهة التشريعية لجرائم الكمبيوتر والأنترنت**، دار الفكر والقانون: المنصورة 2013 ، ص 18.

– وثمة تقسيم يعتمد على دور الكمبيوتر في ارتكاب الجريمة حيث يلعب الكمبيوتر ثلاثة أدوار في ميدان ارتكاب الجرائم :

– **الأول :**قد يكون الكمبيوتر هدفا للجريمة ،وذلك كما في حالة الدخول غير المصرح به إلى النظام ،أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة ، أو تعديلها وكما في حالة الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم ،ويكون الكمبيوتر هدفا للجريمة بان توجه هجمات ضد الكمبيوتر، أو خدماته المساس بالسرية ،أو المساس بالسلامة والمحتوى والتكاملية لتعطيل القدرة والكفاءة .

– **الثاني :**قد يكون الكمبيوتر أداة لارتكاب جرائم تقليدية كما في حالة استغلاله للاستيلاء على الأموال بإجراء تحويلات غير مشروعة ، أو استخدام التقنية في عمليات التزييف والتزوير ،الاستيلاء على أرقام بطاقات الائتمان وإعادة استخدامها ، كما يستخدم في جرائم القتل والدخول إلى قواعد البيانات الصحية والعلاجية وتحويرها ،أو تحوير عمل الأجهزة المخبرية ،وكذا التأثير على عمل برمجيات التحكم في الطائرة ، أو السفينة بشكل يؤدي إلى تدميرها وقتل ركابها .

– **الثالث :**قد يكون الكمبيوتر بيئة الجريمة كما في تخزين برامج القرصنة ، أوفي استخدامه لنشر المواد غير القانونية ، أو استخدامه أداة تخزين ، أو اتصال لصفقات ترويج المخدرات وأنشطة الشبكات الإباحية ونحوها .[1]

– كما اعتمدت الاتفاقية الأوروبية لجرائم الكمبيوتر والانترنت لعام 2001 (اتفاقية بودابست 2001) تقسيما تضمن أربع طوائف رئيسية لجرائم الكمبيوتر والانترنت:

1– الجرائم التي تستهدف العناصر السرية والسلامة وديمومة توفر المعطيات و النظم .

2– الجرائم المرتبطة بالكمبيوتر.

3– الجرائم المرتبطة بالمحتوى (وهي الجرائم المتعلقة بالأفعال الإباحية واللاأخلاقية).

[1] محمود أحمد طه، المرجع السابق، ص 18 .

4- الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة (قرصنة البرمجيات)[1]

ومن خلال ما سبق يمكن تصنيف الجرائم المعلوماتية كما يلي :

الفرع الأول : الجرائم الالكترونية الواقعة بواسطة النظام المعلوماتي

وهنا لا يكون النظام المعلوماتي هو محل الجريمة ، بل يكون الحاسب الآلي هو الوسيلة لتسهيل النتيجة الإجرامية باستخدام النظام المعلوماتي ،ويكون الهدف من ورائها الربح بطريق غير مشروع ، الاعتداء على أموال الغير ، الاعتداء على الأشخاص وسلامتهم وحياتهم الخاصة ، أوفي سمعتهم أو شرفهم والاعتداء على أمن الدولة وأسرارها .

أولا : الجرائم الواقعة على الأشخاص :

رغم الايجابيات والفوائد التي جاءت بها الشبكة المعلوماتية والتسهيلات المقدمة للفرد ،إلا أنها جعلت الأشخاص أكثر عرضة للانتهاك منها :

1- جريمة التهديد :يقصد به زرع الخوف في النفس بالضغط على إرادة الإنسان، وتخويفه من أضرار ما ستلحقه أو تلحق أشخاص له بهم صلة .

ويجب أن يكون التهديد على قدر من الجسامة المتمثلة بالوعيد بإلحاق الأذى ضد نفس المجني عليه أو ماله أو ضد نفس أو مال الغير ،ولا يشترط أن يتم إلحاقا لأذى فعلا أي تنفيذ الوعيد لأنها تشكل جريمة أخرى قائمة بذاتها ، تخرج من إطار التهديد إلى التنفيذ الفعلي ،وقد يكون التهديد مصحوبا بالأمر أو طلب القيام بفعل أو الامتناع عن فعل ، أو مجرد الانتقام .ولقد أصبحت الانترنت الوسيلة المثلى لارتكاب جرائم التهديد ،ومن هذه الوسائل :

- **البريد الالكتروني**: عن طريق مراسلة المجني عليهم بالبريد الالكتروني متضمن تهديد بارتكاب جريمة ضدهم . وهنا يطبق النص التقليدي لجريمة التهديد في أغلب التشريعات.

[1] محمود أحمد طه ،المرجع السابق ، ص 18 .

- **صفحات الويب**: بقيام شخص إنشاء موقع خاص به ينشر عليه تهديد لشخص آخر.[1]

- **انتحال الشخصية** :وهي جريمة الألفية الجديدة، وذلك نظرا لسرعة انتشار ارتكابها خاصة في الأوساط التجارية .وهي استخدام شخصية فرد بطريقة غير شرعية للاستفادة من ماله أ وسمعته أو مكانته أو لإخفاء هوية المجرم .وعليه بدأت الكثير من المعاملات الحساسة على شبكة الانترنت خاصة التجارية منها إلى التوجه نحو اعتماد وسائل التوثيق الالكتروني كالتوقيع الرقمي وتوثيق الهوية للحد من ارتكاب هذه الجريمة .

- **انتحال شخصية أحد المواقع**: ويتم ذلك عن طريق اختراق أحد المواقع للسيطرة عليه ، ليقوم بتركيب برنامج خاص به هناك ،باسم الموقع المشهور.

2- جرائم السب والقذف : للمساس بشرف الغير وسمعتهم ،واعتبارهم ، ويكون القذف والسب كتابيا أوعن طريق المطبوعات أو رسوم ، عبر البريد الالكتروني أو الصوتي ، أو صفحات الويب بعبارات تمس الشرف . وتعتبر من أكثر الجرائم شيوعا في نطاق شبكة الانترنت . وهناك مواقع متخصصة تعمل على إبراز سلبيات الشخص المستهدف وإفشاء أسراره [2] .

3- المواقع الإباحية والدعارة :وفرت شبكة الانترنت أكثر الوسائل فعالية وجاذبية لصناعة ونشر الإباحية بشتى وسائل عرضها ، من صور وفيديو وحوارات في متناول الجميع .

وقد وجد العاملون في مجال الرذيلة والإباحية في شبكة الانترنت وسيلة حديثة ذات كفاءة وكفاية عالية في الدعوة إلى ممارسة البغاء والإعلان عن الفجور عبر مواقع الويب ،وذلك كله في إطار التقنية الفنية التي يستخدمها الجاني في ارتكابه للجريمة وصعوبة اكتشاف هذه الجرائم وتحديد مصدرها وإقامة الدليل عليها [3] .

---

[1] خالد حسن أحمد لطفي ،**جرائم الانترنت بين القرصنة الالكترونية وجرائم الابتزاز الالكتروني دراسة مقارنة** . دار الفكر الجامعي : الإسكندرية 2018 ، ص ص 28-29 .

[2] لينا محمد الأسدي، **مدى فعالية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية دراسة مقارنة**. دار ومكتبة الحامد للنشر والتوزيع :عمان 2008، ص 36.

[3] خالد ممدوح ابراهيم،**الجرائم المعلوماتية**،المرجع السابق ،ص ص 125-126 .

4- التشهير وتشوه السمعة :يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحيته والذي قد يكون فردا أو مؤسسة تجارية أو سياسية. تتعدد الوسائل المستخدمة في هذا النوع من الجرائم ، لكن في مقدمة هذه الوسائل إنشاء موقع على الشبكة يحوي المعلومات المطلوب نشرها أ وإرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين، بالإضافة إلى الجرائم الخاصة بتشويه السمعة الشائعات والأخبار الكاذبة لمحاربة الرموز السياسية والفكرية وحتى الدينية من أجل تشكيك الناس في مصداقية هؤلاء الأفراد وقد يكون الهدف من ذلك هو الابتزاز.[1]

5- جرائم الاعتداء على حرمة الحياة الخاصة :قد يستخدم النظام المعلوماتي في الاعتداء على حرمة الحياة الخاصة ، كما لو قام شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص آخر بدون علمه وبغير إذنه، أو أن يكون تجميع هذه المعلومات بموجب موافقة سابقة من صاحبها ولكن قام الشخص المكلف بحفظها باطلاع الغير عليها دون إذن صاحبها، كما في حالة الأسرار المودعة لدى المحاسبين أ ولدى المحامين أو لدى الأطباء ،وكل هذه الأسرار يحميها القانون ويجرم إفشاءها بطرق غير مشروعة ودون موافقة صاحبها. ويدخل في نطاقها جريمة تسجيل المحادثات الشخصية أو مراقبتها بأي وسيلة حيث نجد بعض المتسللين يستطيعون اختراق شبكة الانترنت بطرق غير مشروعة والتنصت على هذه المكالمات[2].

ثانيا : الجرائم الواقعة على الاموال :

من المعلوم أنه باتت الكثير من المعاملات المالية في وقتنا الحاضر تتم بواسطة الشبكات الالكترونية ، مما زاد في تطور وسائل الدفع الالكتروني ،الأمر الذي أدى إلى تطور الجريمة الالكترونية بغاية الحصول على الأموال بأقل تكلفة ممكنة .[3]

---

[1] خالد حسن أحمد لطفي ،المرجع السابق ، ص 31 .

[2] خالد ممدوح ابراهيم، **الجرائم المعلوماتية** ، المرجع السابق، ص 124 .

[3] رحموني محمد، **خصائص الجريمة الالكترونية ومجالات استخدامها**. جامعة أحمد دراية – أدرار مجلة الحقيقة، العدد 41 ، تاريخ قبول المقال للنشر 2018/01/10 ، ص 446 .

وجرائم الأموال بشكل عام هي الجرائم التي تنال بالاعتداء أو تهدد بالخطر الحقوق ذات القيمة المالية ، ويدخل في نطاقها كل حق ذي قيمة اقتصادية ويدخل في إطار التعامل .وبالتالي يكون أحد عناصر الذمة المالية للشخص .[1]

ومع هذا التطور ابتكرت طرق ووسائل للسطو على هذا التداول المالي بطريق غير مشروع [2]، وتعددت بطبيعة الحال الوسائل التي يتم من خلالها الاعتداء على الأموال عبر الانترنت .

وبالتالي فان قدرة المعلوماتية على نقل البيانات ومعالجتها قد أكسبها قيمة تجارية ذات طابع مالي، وهوما هيأ فرصة لظهور قيم اقتصادية مستحدثة ،وعليه السطو عليها بطريق غير مشروع ومنها :

1- **جرائم الكترونية تطال بطاقات الائتمان والتحويلات المالية :**لقد أضحت بطاقات الائتمان محلا للاعتداء في ظل التطور التقني . وغالبا ما يتم ذلك عن طريق معرفة المعلومات الشخصية الخاصة بالمجني عليه صاحب البطاقة .[3]مما يسهل على المجرم الالكتروني الولوج إلى النظام المعلوماتي ،ويكون ذلك سواء بالتواجد على الشبكة أثناء إتمام عملية ما أو بإدخال بيانات إلى ذاكرة الجهاز ،ويكون ذلك باستخدام الاحتيال ،وكذلك الاحتيال بواسطة بطاقات الدفع الالكتروني.

أ- **الاحتيال :**يتم الاحتيال على الضحية من خلال تضليله بوجود مشروع يحصل من ورائه على أموال مما يدفعه إلى الانسياق وراء تغرير المجرم الالكتروني ،ويكون ذلك سواء باتصال عبر الشبكة بين الجاني الالكتروني والمجني عليه ، أومن خلال استخدام المجرم الالكتروني البيانات الكاذبة التي تساعده على إيهام الكمبيوتر والاحتيال عليه بغاية الحصول على الأموال .

ب- **الاحتيال بواسطة بطاقات الدفع الالكتروني :** يتم الدفع الالكتروني بواسطة بطاقة الدفع الالكتروني بتحويل مالي من المصدر وهو بنك العميل إلى رصيد متعامل آخر، كل

[1] لينا محمد الأسدي ،المرجع السابق، ص48 .
2 خالد حسن أحمد لطفي ، المرجع السابق ، ص 32 .
[3] لينا محمد الأسدي ،المرجع السابق ، ص 49.

ذلك يتم بواسطة شبكة التسوية الالكترونية الدولية (مثلا ماستر كارد) ، حيث يقوم المجرم بكسر كلمة السر للبطاقة الالكترونية أو خداع الصراف الآلي ،وبالتالي يتمكن من الحصول على السلع والخدمات من خلال ملأ نموذج الكتروني ببيانات بطاقة الائتمان الخاصة بالمشتري .

ويمكن الاحتيال باستخدام بطاقات الائتمان من قبل صاحب البطاقة الشرعي وذلك بإساءته استخدام بيانات البطاقة الائتمانية أثناء مدة صلاحيتها أو قيامه باستخدامها بعد مدة صلاحيتها أو إلغائها .

وقد يكون البنك مصدر البطاقة قد ألغاها أثناء مدة صلاحيتها بسبب سوء استخدامها من العميل الذي يتعين عليه إعادتها إلى البنك والذي قد يمتنع عن ذلك ويستمر في استعمالها باستخدام بياناتها في تعاملاته عبر الشبكة وهو ما يشكل جريمة النصب بمجرد ملأ البيانات لإقناع الغير بوجود ائتمان وهمي .[1]

2- سرقة أموال البنوك :وتحقق بواسطة استخدام المجرم الالكتروني الكمبيوتر بغرض الدخول إلى الشبكة والوصول غير المشروع إلى البنوك وغيرها من المؤسسات المالية ،وتحويل الأموال من الحسابات الخاصة بالعملاء إلى حسابات أخرى، وقد يتم ذلك بكميات بسيطة بصفة متكررة بحيث لا يلفت الانتباه ،وقد يتم دفعة واحدة .

3- غسيل الأموال التي تتم عبر الانترنيت: إن جريمة غسيل الأموال هي من الجرائم المعاصرة وهي من صور الجريمة المنظمة .

يقصد بغسيل الأموال توظيف الأموال داخل الدولة أو خارجها في أعمال مشروعة وذلك لطمس الأصل غير المشروع لهذه الأموال .وغالبا ما يتم ذلك عن طريق تسلل الأموال إلى المشروعات الاقتصادية والتأثير فيها . ويعاد استغلالها بعد ذلك على أنها من مصدر ربح مشروع[2] .

[1] خالد حسن أحمد لطفي ، المرجع السابق، ص 36 .

[2] رحموني محمد، المرجع السابق ، ص 447 .

ونتيجة التطور فقد استفاد مجرم وغسيل الأموال من التقنية ومميزاتها لتحقيق أغراضهم الإجرامية، وما دفع بهم إلى استعمال الوسائل المستحدثة هي السرعة وإغفال التوقيع وانعدام الحواجز الحدودية بين الدول ، كما أن البطاقات الذكية والتي تشابه بطاقات البنوك التي تستخدم في مكائن الصرف الآلية ، تساعد على تحويل الأموال بواسطة المودم أو الانترنت مع ضمان التشفير وأمان العملية .[1]وهذا الأمر جعل عمليات غسيل الأموال عبر الوسائل التقنية ،وخاصة عبر شبكة الويب العالمية ، تتم بسرعة ودون أن تترك أي أثر في الغالب .

4- الجرائم الواقعة على حقوق الملكية الفكرية والأدبية : يقصد بحقوق الملكية الفكرية ذلك النوع من الحقوق الذي يرد على الأشياء المعنوية غير المحسوسة من خلق الذهن ونتاج الفكر ، فيثبت لصاحبها أبوة هذا الحق ونسبته إليه وحده ويعطيه احتكار استغلاله ماليا ويكف له الحصول على ثمراته .

ويمكن القول إن حقوق الملكية الفكرية المتعلقة بالمعلومة الالكترونية تتسع لتشمل الحقوق المتعلقة بالمؤلف ،والحقوق المتعلقة ببراءة الاختراع ،وأخيرا الحقوق المتعلقة بالعلامات التجارية .

ويكمن الهدف الرئيسي من إقرار الحماية الجنائية لحقوق الملكية الفكرية لمعلومة الالكترونية ، تشجيع الناس على ابتكار البرامج التي من شانها المساهمة وبشكل كبير في إثراء الدول وتقدمها .[2]

5- قرصنة البرمجيات :هي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية على أسطوانات وبيعها للناس بسعر أقل. و جريمة نسخ المؤلفات العلمية والأدبية بالطرق الالكترونية من الجرائم المستحدثة ،وذلك تأسيسا على أن المعلومة الأدبية والفكرية ذات قيمة أدبية ومادية ،بالإضافة إلى براءات الاختراع التي تخول لمالكها حق معنوي وآخر مالي .

[1]/ لينا محمد الأسدي، المرجع السابق ، ص 51.
[2]محمود أحمد طه ،المرجع السابق، ص 77 .

وعليه يتبين لنا أن الجرائم المرتكبة على الأموال عبر شبكة الانترنت، لا يمكن حصرها لأنها متعددة ومتشعبة ، كما يتبين التكييف القانوني للوقائع حسب كل حالة وذلك نظرا للفراغ القانوني الحاصل في هذا المجال ،وهذا يتطلب ضرورة صدور نصوص قانونية تحصر الأفعال والممارسات اليومية خاصة أمام الإحصائيات المسجلة والمتنامية [1]

ثالثا : الجرائم الواقعة على أمن الدولة :يقوم الإرهابيون باستخدام الانترنيت لاستغلال المؤيدين لأفكارهم وجمع الأموال لتمويل برامجهم الإرهابية والاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على نشر الفيروسات [2] .

و تتمثل هذه الجرائم في جرائم الإرهاب والتجسس والجريمة المنظمة ، وهذا ما نعالجه في النقاط التالية :

1- الإرهاب والجريمة الالكترونية :مما لا شك فيه أن ظاهرة الإرهاب أضحت عالمية ، حيث ظهرت الكثير من التنظيمات التي تتبنى هذا الفكر في مختلف دول العالم وبمختلف التسميات ،وتظهر العلاقة بين الإرهاب والجريمة الالكترونية من خلال تجنيد وتجييش أعضاء جدد في التنظيم ، أو حشد الهمم بواسطة استخدام مختلف وسائل التواصل الالكتروني ،كما يتم تبني العمليات الإرهابية والدعاية لهذه التنظيمات وأعمالها من خلال مختلف الوسائط والمواقع الالكترونية بما يحقق أهدافها.[3]

2- التجسس والجريمة الالكترونية :يقوم المجرمون بالتجسس على الدول والمنظمات والشخصيات والمؤسسات الوطنية أو الدولية ،وتستهدف خاصة : التجسس العسكري ، السياسي ،والاقتصادي ،وذلك باستخدام التقنية المعلوماتية ،وتمارس من قبل دولة على دولة ، أومن شركة على شركة ...وذلك بالاطلاع على المعلومات الخاصة المؤمنة في جهاز آلي ،وغير مسموح بالاطلاع عليها ، كأن تكون من قبيل أسرار الدولة [4].

---

[1] خالد حسن أحمد لطفي ، المرجع السابق، ص 38 .

[2] نفس المرجع ، ص ص 38 -39.

[3] رحموني محمد، المرجع السابق ، ص 448 .

[4] خالد حسن أحمد لطفي، المرجع السابق، ص 39 .

الفرع الثاني :الجرائم الالكترونية الواقعة على النظام المعلوماتي :

إذا كانت أشكال الجريمة الالكترونية متعددة و متنوعة ، على نحو ما تناولناه سابقا ،إلا أن نطاق هذا البحث لا يتسع للتعرض لكافة أنواع الجرائم المعلوماتية ،ولذلك سوف يكون تعرضنا لأهم الجرائم المحتمل وقوعها ومن أهمها:

أولا : الاعتداء على برامج النظام المعلوماتي :وهنا يستوجب الأمر أن يكون الجاني على معرفة ودراية ذات درجة عالية في مجال البرمجة . وغالبا تقع هذه الجرائم على البرامج التطبيقية وبرامج التشغيل .

1- البرامج التطبيقية :يقوم الجاني بتحديد البرنامج ثم التلاعب فيه للاستفادة منه ماديا ،وذلك بتعديل البرنامج ،ويكون الهدف من تعديل البرامج اختلاس النقود ، حتى ولوكان باستقطاع مبالغ قليلة لكن لفترات زمنية طويلة لتحقيق الفائدة ، بدون إثارة الشبهات ، أما التلاعب فيأخذ عدة أشكال ، فقد يكون عن طريق زرع برنامج فرعي في البرنامج الأصلي مثلا، يسمح له الدخول غير المشروع في العناصر الضرورية للنظام المعلوماتي حيث يصعب اكتشاف هذا البرنامج لدقته وصغر حجمه .

2- برامج التشغيل :وهي البرامج المسئولة عن عمل نظام معلوماتي من حيث قيامها بتنظيم وضبط وترتيب التعليمات الخاصة بالنظام .

وتقوم الجريمة هنا عن طريق تزويد البرنامج بمجموعة تعليمات إضافية ليسهل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي وتأخذ شكلين هما :

أ- المصيدة :وهو إعداد برنامج به ممرات وفراغات في البرنامج وتفرعات إضافية، وهنا يمكن للبرنامج استخدام البرنامج في أي وقت ، ويصبح المهيمن على نظام صاحب العمل .

ب- تصميم برنامج :هو قيام برنامج خصيصا يصعب اكتشافه لارتكاب الجريمة ومراقبة تنفيذها .[1]

[1] خالد حسن أحمد لطفي ، المرجع السابق، ص 40 .

ثانيا : الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي :إن الصورة الغالبة لتحقيق غاية المجرم المعلوماتي في نطاق الشبكة تتمثل في فعل الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه دون إذن، ومن ثمة قيام الجاني بارتكاب فعله الذي قد يكون مجرم فيشكل أحد أنواع جرائم الانترنت . ويقوم المجرم المعلوماتي بالتلاعب بالمعلومات الموجودة على النظام المعلوماتي أو بإتلافها .

1- جريمة الدخول غير المصرح به :قد تطرقنا اليه سابقا ومع ذلك سنقدم شرحا أوفى عنه ينصرف معنى " الدخول " access في إطار المعلوماتية بصفة عامة ليشمل كافة الأفعال التي تسمح بالولوج إلى النظام المعلوماتي ،ويقصد بالدخول غير المصرح به إلى النظام UNAUTHORIZED ACCESS أن توجه هجمات إلى معلومات الكمبيوتر أو خدماته بقصد المساس بالسرية CONFIDENTIALITY، أو المساس بالسلامة والمحتوى والتكاملية INTEGRITY، أو تعطيل القدرة الكفاءة للأنظمة للقيام بأعمالها AVAILABILITY.

والاختراق هو عبارة عن عملية دخول غير مصرح به إلى أجهزة الغير وشبكاتهم الالكترونية ،ويتم هذا الاختراق بواسطة برامج متطورة .[1]

- **طرق الدخول غير المصرح به :**إن الولوج غير القانوني أو غير المصرح به ، له مجموعة من الصور أهمها : اختراق النظام كله أو جزء منه ،ويستوي هنا أن يكون الجزء ماديا أو برامج جزئية ، أو بيانات مخزنة في نظام التنصيب Installation أو بيانات تتعلق بالمرور أو المحتوى .

وتتعدد الطرق التي يمكن أن يستخدمها المجرم المعلوماتي للدخول للنظام المعلوماتي ومنها : تشغيل كمبيوتر مقفول ، أو مفتوح ، اوعن طريق استعمال كارت التشغيل ، أو بواسطة استعمال خط تلفوني، أومن خلال الدخول من كمبيوتر الى كمبيوتر آخر ،وكذلك بواسطة الدخول الى نظام متصل بنفس الكمبيوتر بدائرة واحدة .[2]

2- التلاعب في المعلومات الموجودة على النظام المعلوماتي :ويتم ذلك بطريقتين :

[1] خالد ممدوح ابراهيم،الجرائم المعلوماتية ،المرجع السابق، ص242.

[2] نفس المرجع ، ص 252.

– الطريقة المباشرة : يكون التلاعب عن طريق إدخال معلومات بمعرفة المسؤول عن القسم المعلوماتي ، كضم مستخدمين غير موجودين بالعمل بهدف الحصول على مرتباتهم الابقاء على مستخدمين تركوا العمل للحصول على مبالغ شهرية ، أوعن طريق تحويل لمبالغ وهمية لدى العاملين بالبنوك باستخدام النظام المعلوماتي بالبنك وتسجيلها واعادة ترحيلها وارسالها لحساب اخر في بنك آخر، بهدف اختلاس الاموال .

– الطريقة الثانية : أما التلاعب غير المباشر ، فيتم عن طريق التدخل لدى المعلومات المسجلة بالنظام المعلوماتي باستخدام أحد وسائط التخزين أو التلاعب عن بعد بمعرفة أرقام وشفرات الحسابات ،قصد التلاعب في الشرائط الممغنطة، أو باستخدام الجاني كلمة سر أو مفتاح شفرة وامكانية تسلل الجاني الى المعلومات المخزنة والحصول على المنفعة المالية من مسافات بعيدة .

اتلاف المعلومات في مجال المعلوماتية بالاعتداء على الوظائف الطبيعية للحساب الآلي وذلك بالتعدي على البرامج والبيانات المخزنة والمتبادلة بين الحواسيب وشبكاته ،وتدخل ضمن الجرائم الماسة بسلامة المعطيات المخزنة ضمن النظام المعلوماتي ويكون الإتلاف العمدي للبرامج والبيانات وكمحوها أو تدميرها الكترونيا أو تشويهها على نحو يجعلها غير صالحة للاستعمال .[1]

كما قد يتم عن الإتلاف عن طريق :

نشر البرامج الخبيثة والضارة :وأشهرها الفيروسات ،ولعل هذه الوسيلة هي من اكثر ما يتردد الحديث بشأنها لخطورتها واتساع مجالها التخريبي ،وفيروس الكمبيوتر هو مرض يصيب الجهاز. وهو عبارة عن برنامج صغير يمكن تسجيله أو زرعه على الأسطوانات المرنة أو الأقراص الصلبة الخاصة بالحاسب. ويظل هذا الفيروس خاملا خلال فترة محدودة ثم ينشط فجأة في توقيت معين ليدمر البرامج والمعلومات المسجلة في الحاسب الأمر الذي يؤدي الى اتلاف المعلومات أو حذفها أو تدوينها ،ومن المعروف ايضا أن العديد من فيروسات الكمبيوتر منها الخبيث الذي يسبب أضرارا ومنها الحميد الذي لا

[1] خالد حسن أحمد لطفي ، المرجع السابق ،ص ص 43- 44 .

يسبب مشكلات بالنسبة لمستخدمي الانترنت [1]ونذكر منها الدودة الحاسوب ،حصان طروادة وبرمجيات أخرى خبيثة وهجينة تضم اكثر من نوع من الفيروسات .

المطلب الثاني

المجرم المعلوماتي

أضافت نظم المعالجة الآلية الكثير من الجوانب الايجابية الى حياتنا ، الا أنها في المقابل جلبت معها نسلا جديدا من المجرمين ، اصطلح على تسميتهم بمجرمي الاعتداء على نظم المعالجة الآلية ، فهذه الاخيرة ينظر اليها دائما بوصفها أداة محايدة وأن مصدر انتهاكها والاعتداء عليها الإنسان ذاته، والذي غالبا ما يهيئ فرصة التعامل معها عن حسن أو سوء نية ، فجوهر المشكلة هو الانسان وشخصيته ودوافعه ،وكما هو معروف فانه لا يمكن لأي عقوبة أن تحقق هدفها سواء في مجال الردع العام أو الردع الخاص ما لم تضع في الاعتبار شخصية المجرم .[2]

تقتضي دراسة خصوصية مجرم الاعتداء على نظم المعالجة الآلية أن يتم تحديد سمات هذا الشخص أولا ، دوافعه ثانيا ،وأخيرا عرض أهم فئاته .

الفرع الأول : السمات الخاصة بالمجرم المعلوماتي :

اولا :1- تعريف المجرم المعلوماتي :لقد تعددت التسميات التي أطلقت على هذه الطائفة من المجرمين بين "قراصنة المعلوماتية" و"الهاكر" والمجرم الالكتروني والمجرم المعلوماتي و"مجرم الانترنت" و"مجرم التقنية ".

ويقصد بالمجرم الالكتروني هو المجرم الذي له القدرة على تحويل لغته الى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الالكتروني في ملحقاته ووسائل الاتصال الرقمية ،وذلك بأداء فعل الامتناع عنه ، مما يحدث اضطرابات في المجتمع الدولي والمحلي .

[1] محمود أحمد طه ،المرجع السابق، ص 47 .

[2] رشيدة بوكر،المرجع السابق ، ص93 .

أو هـ وكل شخص سواء طفل ، رجل ، أنثى ، يأتي أفعال لا إرادية يشكل سلوكا ايجابيا أو سلبيا باستخدام تقنية المعلوماتية لإحداث نموذج إجرامي بالاعتداء على حق أو مصلحة

أو هو مجرم سلك سبيل التقنية لارتكاب جرائمه وهو: " كل شخص طبيعي أو معنوي يتوفر لديه كشرط أساسي معرفة كافية بآلية عمل وتشغيل الحاسب الآلي ، يقوم بعملية اما بحسن نية أو سوء نية كأعمال اتلاف والغش".[1]

فالمجرم المعلوماتي لا يحتاج الى التنقل الحركي الى مكان وقوع الجريمة ، بل يقوم بالفعل الاجرامي عن بعد من حيث الزمان والمكان باستخدام شبكات وخطوط الاتصال بين الجاني ومكان وقوع الجريمة ،ومثال على ذلك : ما قام به الطالب الأمريكي

LAN MURPHYحين عمد سنة 1981 برفقة أصدقائه الى استعمال خط هاتفي للدخول الى ملفات سرية مخزنة في حاسوب تابع للحكومة الفدرالية الأمريكية .[2]

وتجدر الإشارة إلى أن هناك فرق بين مجرم الانترنت ومجرم الحاسب الآلي بالرغم من أن كليهما يعتبران مجرما تقنيا .

2- تعريف مجرم الانترنت :فمجرم الانترنت المتميز هو **الهاكر** الذي يتخذ الشكل الخبيث له في مصطلح **كراكر** في حين ان مجرم الحاسوب هو القرصان مرتكب جرائم العدوان على حقوق الملكية الأدبية والفكرية عامة مع تخصيص جزئية لها تتعلق بمدى امكانية التقنية في السيطرة على استخدام الحاسوب كما هو الشأن في اختراق كلمات العبور لملفات مشفرة مخزنة في الحاسوب ،كل ذلك دون ان يكون الحاسوب مرتبطا بالأنترنت يختلف هذا من جهة ومن جهة أخرى فان المجرم التقني عبر الحاسوب لكونه

[1] بكوش محمد أمين، هروال نبيلة هبة، **خصوصية المجرم الالكتروني – مجرم الأنترنت نموذجا** .مخبر البحث في تشريعات حماية النظام البيئي- مخبر البحث في تشريعات حماية الوظيفة العامة ،مجلة البحوث في الحقوق والعلوم السياسية،مجلد 07 العدد 01 سنة 2021جامعة تيارت الجزائر ،، تاريخ قبول المقال للنشر 2021/05/25 ، ص 76.

[2] غريبي بشرى،**خصوصية المجرم المعلوماتي ودوافعه** . مجلة نوميروس الاكاديمية ، جامعة أبوبكر بلقايد تلمسان مجلد02 العدد02 سنة 2021، تاريخ قبول المقال 2021/05/09 ،ص ص 103-102 .

مجرم لا يتمتع بمدارك علمية أو تخصصية ذات طابع أكاديمي ،إنما هو أبسط من ذلك بكثير ،اذ انه يقترب الى حد كبير من المجرم بالصفة.[1]

ثانيا : الصفات الشخصية للمجرم المعلوماتي :تتميز شخصية المجرم بخصائص وصفات تختلف عن مرتكب الجرائم التقليدية الأخرى، وهذا مرجعه تميز شخصية مرتكبي الجرائم المعلوماتية بالتقدم في مجال استخدام الحاسب الآلي ،وهذا بعكس المجرم العادي الذي غالبا ما يتميز بالقوة العضلية ونادرا ما يتميز بعضهم بعنصر الذكاء.

ويمكن إدراج أهم السمات المشتركة بين فئات الاجرام المعلوماتي من خلال مايلي:

1- المجرم المعلوماتي شخص ذكي ومتخصص : يعتبر الذكاء من أهم صفات مرتكب الجرائم المعلوماتية ،لان ذلك يتطلب منه المعرفة التقنية لكيفية الدخول الى أنظمة الحاسوب الآلي والقدرة على التعديل والتغيير في البرامج وارتكاب جرائم السرقة والنصب وغيرها من الجرائم التي تتطلب المعرفة الكبيرة لارتكاب تلك الجرائم .

وتتجلى أهمية صفة الذكاء بالنسبة لمرتكب الجريمة المعلوماتية في عدم استخدامه للعنف وأنه يستطيع وهو في منزله تحويل عدة ملايين لحسابه من بنك الى آخر اوفي نفس البنك[2]

2- المجرم المعلوماتي يتمتع بالخبرة والمهارة :يتصف مرتكب الجرائم المعلوماتية أيضا بأنه على درجة عالية من الخبرة والمهارة في استخدام التقنية المعلوماتية وذلك لان مستوى الخبرة والمهارة التي يكون عليها هي التي تحدد الاسلوب الذي يرتكب به تلك الجرائم [3]، فهو يتمتع بالمهارة والمعرفة الكافيتين لاختراق المواقع الالكترونية وكسر حواجز الشفرة، فيجب أن يكون على معرفة فنية علمية بجهاز الحاسوب والانترنت وكيفية التعامل مع البيانات وتخزينها ومعالجتها وحذفها حتى يتمكن من اتمام الجريمة وبناءا على ذلك

[1] بكوش محمد أمين، هروال نبيلة هبة، **المرجع السابق** ،ص 76.
[2] خالد ممدوح ابراهيم،**الجرائم المعلوماتية**، نفس المرجع السابق ، ص ص133-134.
[3] نفس المرجع ، ص135 .

فانه لا يستطيع أي شخص أن يرتكب الجرائم المعلوماتية دون المعرفة التامة بكيفية التعامل مع جهاز الحاسوب والانترنت والبيانات والمعلومات بشكل منهجي ودقيق [1].

3- التنظيم والتخطيط :ترتكب أغلب الجرائم من مجموعة مكونة من عدة أشخاص ، يحدد لكل شخص دور معين ويتم العمل بينهم وفقا لتخطيط وتنظيم سابق على ارتكاب الجريمة ، فمثلا تحتاج جريمة مثل نسخ برامج الحاسب الآلي الى شخص يقوم بنسخ تلك البرامج وتحتاج أيضا الى مجموعة تقوم بعملية البيع .

وايضا جريمة زرع الفيروسات تحتاج الى مجموعة من الأشخاص منهم المبرمج الذي يقوم بكتابة البرنامج ومنهم المستخدم الذي يقوم بعملية زرع الفيروسات داخل الاجهزة الأخرى وينتج عن هذا التنظيم صعوبة عملية كشف الجريمة نتيجة للتخلص داخل تلك الجماعة في كل جزء من أجزاء الجريمة .

4- المجرم المعلوماتي شخص اجتماعي :تعتبر هذه الخاصية امتدادا لسمة التخطيط والتنظيم ، فهو يتميز بأنه شخص اجتماعي ، فلا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به بل على العكس من ذلك نجده إنسان متوافق مع مجتمعه [2]،وحيث أن التكيف الاجتماعي ينشأ بين مجموعة لها صفاة مشتركة .فمثلا جماعة صغار نوابغ المعلوماتية لا شك أنهم يتكيفون في أفكارهم فيما بينهم ،وتنشأ بالتالي بينهم صلات وروابط تساعدهم على ارتكاب جرائمهم . وتعد تلك الروابط والصلات النطاق المحلي الى المجال الدولي بحيث تنشأ بينهم روابط دولية تتفق مع أفكارهم ومنهجهم في استثمار تلك المعرفة والتقدم العلمي . وعلى النقيض من ذلك يكون تكيف هؤلاء الاشخاص مع المجتمع الخارجي محدودا وغالبا ما يكونون منعزلين عن المجتمع .[3]

[1] غريبي بشرى، المرجع السابق ، ص 105.
[2] نفس المرجع ،ص 104.
[3] خالد ممدوح ابراهيم،**الجرائم المعلوماتية**، المرجع السابق ، ص 137.

ولذلك يتبين ان وجود الفرد في جماعة يشكل خطورة عليه لأنه ليس فقط يكتسب المهارة التقنية والفنية ولكن يزيد أيضا لديه الملكة الإجرامية ومحاولة إثبات الذات والتفوق العلمي لديه مما يجعله يطور في أسلوب ارتكابه للجرائم .

5- خوف المجرم المعلوماتي من كشف جريمته :يعرف عن مجرم المعلوماتية خوفه من انكشاف جرائمه وانفضاح أفعالهم ، بالرغم من ان هذا الخوف يصاحب المجرمين على اختلاف أنماطهم، الا أنها تتميز المجرمون المعلوماتيون بصفة خاصة لما يترتب عن كشف أمرهم من فقدان لمراكزهم ،ويساعدهم على الحفاظ على سرية أفعالهم طبيعة الأنظمة المعلوماتية نفسها . فخوف المجرم المعلوماتي من انكشاف أفعاله يعود الى انتمائه في الغالب إلى وسط اجتماعي متميز ، سواء من حيث التعليم أو الثقافة أو المستوى المهني وطبيعة العمل .[1]

الفرع الثاني : تصنيفات المجرم المعلوماتي :

إن دراسات علم الاجرام الحديثة في ميدان الإجرام التقنية تسعى في الوقت الحاضر الى إيجاد تصنيف منضبط لمجرمي التقنية ، لكنها تجد صعوبة في تحقيق ذلك بسبب التغيير السريع الحاصل في نطاق هذه الظاهرة المرتبطة أساسا بالتسارع الرهيب في ميدان الكمبيوتر والانترنت.[2]

وجرائم الحاسب الآلي قد تكون بسيطة أو جرائم إرهابية وذلك تبعا لشخصية المجرم المعلوماتي وبما لديه من خبرة في مجال استخدام جهاز الحاسب الآلي والغرض من ارتكاب الجريمة، وقد تكون الخطورة بالغة بحيث ينتج عنها التدمير الكامل للأجهزة أو للشبكة الموصلة بينها ويعتبر كلا العملين جريمة ولكن مع اختلاف درجة كل منها تبعا لنوعية مرتكب الفعل . ومن خلال ذلك تصنيف مرتكبي الجرائم المعلوماتية الى الانماط التالية :

[1] غريبي بشرى، المرجع السابق ، ص 105.
[2] محمود أحمد طه ،المرجع السابق، ص 14 .

1- صغار نوابغ المعلوماتية :ويطلق عليهم لفظ نوابغ المعلوماتية وهي مجموعات تميل الى التحدي الفكري وغالبا ما يكونون في مرحلة المراهقة على الرغم من صغر سنهم الا أنهم قادرون على اقتحام كافة أنواع الأنظمة البنكية والشركات والمؤسسات المالية .

ويتميز هؤلاء المراهقون عن غيرهم من مرتكبي الجرائم التقليدية في أنهم لا يعتبرون أن ما يقومون به يعد جريمة ،لأنهم يعتقدون أن النظام غير القادر على حماية نفسه ليس من الخطأ اقتحامه ،ولذلك فانهم يعتبرون أنفسهم أبطالا لمساعدة المجتمع في تحديد نقاط الضعف الخاصة بالبرنامج الذي تم اقتحامه .[1]**ومثال على ذلك :** حالة قيام مراهق يبلغ من العمر أربعة عشر عاما باقتحام أنظمة جهاز الحاسب الآلي الخاصة بالقوات الجوية الامريكية وحصل منها على معلومات عسكرية خطيرة مما أحدث ارتباكا داخل تلك القاعدة ، أين ترتب عنها اتخاذ قرارات تكلف تنفيذها الكثير من الوقت والجهد والمال .[2]

2- القراصنة :تغير معنى لفظ القراصنة مع ظهور شبكة الانترنت عما كان عليه في الماضي ،لأنه لم يعد معنى القرصنة عمليات سفك الدماء والقتل والتفجير والتدمير باستخدام الاسلحة ، ولكن أصبح للفظ القرصنة مدلول آخر ارتبط بالتطور التكنولوجي .

وأصبح في امكان شخص لا يزيد وزنه على بضعة كيلوغرامات وتتوارى عضلاته خجلا من ضعفه ان يردع العالم باسره وان يستولي على الملايين من الاموال .

وفي عالم القراصنة في مجال الحاسب الآلي وشبكة الانترنت يوجد مصطلحان مترادفان لها وهما :

أ- الهاكرز :ويطلق على المقتحم التقليدي الذي يقوم بالتلصص على الغير ويتاجر في قطاع المعلومات واذا ما واجهته حماية لا يستطيع تخطيها ،فهو ليس له علاقة بتكنولوجيا المعلومات .

ب- الكراكرز :أو الهاكر الخبيث ،وأغلبهم شباب تجاوزوا 25 عاما ويتميزون بالتخصص العالي في مجال الحساب الآلي والذكاء ،والاعتداء المقترفة من طرف هؤلاء تدل على ان

[1] خالد ممدوح ابراهيم،**الجرائم المعلوماتية** ،المرجع السابق،ص143.

[2] غريبي بشرى، المرجع السابق ، ص 107.

الكراكرز يقوم بكل ما هو شيء وشرير وكل ما يشكل جريمة ، من اتلاف وتخريب وارهاب وابتزاز وعدوان على الاموال بالنصب والسرقة .[1]

فهو ذلك الشخص المقتحم الخبير في مجال المعلومات واستخدام الحاسب الآلي ،ويعتمد عمله على كسر الحماية الموجودة حول الشبكات وأجهزة الحاسب الالي ولذلك فان الكراكرز يستطيع اختراق الشبكات واقتحام البرامج ،ويستعين بالتالي **الهاكرز** ب**الكراكرز** اذا ما صادفه أي نوع من انواع الحماية ، ولكن يلاحظ أنه جرت العادة على اطلاق لفظ الهاكرز على كلا النوعين ، أو استخدام لفظ القراصنة عموما .

3- الهواة والمبتدئون :يعتبر نمط الهواة والمبتدئين من الأنماط التي تتميز بخطورتها في ارتكاب الجرائم على الرغم من سلامة القصد لديهم في عدم ارتكاب أي من هذه الجرائم ، وهذا مرجعه لأن دم الدراية في استخدام الحاسبات الآلية يترتب عليه الوقوع في لكثير من الأخطاء . وتبرز خطورة هذا النمط في أن المخاطر التي تحدث نتيجة تصرفاتهم لا يمكن تداركها .

ويمكن أن يترتب كذلك عن محاولة الهواة والمبتدئين القيام بأي تصرف خاطئ مع أنظمة الحاسب الآلي حدوث جرائم في صورتها التامة والتي تتميز بالخطورة لأن من الجرائم ما يرتكب بمجرد حدوث الفعل بصرف النظر عن القصد الجنائي ،وخير مثال لذلك جريمة الدخول غير المشروع في أنظمة الحاسب الآلي فهي تعتبر جريمة تامة .

4- المخربون :عادة ما يكون أشخاص هذه الفئة من الغاضبين في أغلب الأحوال من هيئة معينة وقد يكونون غاضبين من الحياة بوجه عام . ويمكن تقسيم فئة المخربين الى :

أ- **المستخدمون :**هم الذين لديهم تصريح لاستخدام أنظمة الحاسب الالي ويقوم بإتيان تصرفات غير مصرح بها أو مسموح بها تنتج عنها أفعال تخريبية ومثال ذلك قيام الموظف بتصفح ملفات المرتبات والأجور رغبة في الانتقام من رب العمل بقيامه بمسح

[1] خليلي سهام، **خصوصية المجرم الالكتروني** .جامعة أمحمد لمين دباغين سطيف مجلة المفكر ،مجلد02 العدد15 جوان 2017 ،ص 407.

الملفات أو زرع الفيروسات داخل أنظمة الحاسب الآلي ما يكلف الهيئة أموالا طائلا نتيجة لهذه الأفعال التخريبية .

ب- الغرباء :وهم المستخدمين الذين ليس لهم تصريح بالعمل على النظام وفي أغلب الأحوال يكون التخريب هو هدف هؤلاء الدخلاء أو التسلية ،وينتج عن هذه الأفعال نتائج تخريبية وقد يكون المكسب المادي هو هدف من عملية الدخول .

5- المجرمون المحترفون :هذه الفئة هي من أخطر الفئات التي ترتكب الجرائم. لأن الهدف الذي تقوم عليه هذه الفئة ينحصر في نية ارتكاب الفعل الاجرامي ،وهذا هو مصدر الخطورة . ويكونون على درجة كبيرة من المهارة والاتقان والغرض دائما هو المكسب أو الحصول على فائدة مادية أو معنوية .

واخطر جرائم هذه الفئات جريمة التجسس سواء في المجال الصناعي أو التجاري أوفي المجال السياسي أو العسكري ، لأن المعلومات التي يحصلون يكون لها بالغ الأثر .

حيث يترتب على نقل المعلومات عن عدد القوات العسكرية وحجم المعدات جعل الدولة في مركز أقوى لأنها سوف تستعد بما يتناسب مع تلك القوات والعتاد، وذات الحال عن المجال التنافسي في التجارة والصناعة .[1]

الفرع الثالث : دوافع ارتكاب الجريمة المعلوماتية :

البواعث أو الدوافع التي قد تدفع مجرم الاعتداء على نظم المعالجة الآلية إلى ارتكاب جريمته تتنوع وتتباين تبعا لطبيعته ودرجة خبرته في مجال المعالجة الآلية للمعلومات ، فقد تكون الرغبة في تحقيق الثراء أو الكسب المادي [2].

وتتنوع الدوافع الى ارتكاب الجرائم وفقا لما يلي :

[1] خالد ممدوح ابراهيم،الجرائم المعلوماتية ،المرجع السابق، ص ص148-149 .
[2] رشيدة بوكر،المرجع السابق ، ص95 .

أولا :الدوافع الشخصية :ويقصد بها تلك العوامل اللصيقة بشخصية المجرم المعلوماتي والتي تدفعه لارتكاب الجريمة المعلوماتية [1]،والتي سنجملها فيما يلي :

1- تحقيق الربح المادي :يعد أكثر الدوافع تحريكا للجناة لاقتراف جرائم الكمبيوتر ، ذلك أن خصائص هذه الجرائم وحجم الربح الكبير الممكن تحقيقه من بعضها خاصة غش الكمبيوتر أو الاحتيال المرتبط بالكمبيوتر يتيح تعزيز هذا الدافع ،وتحقيق الثراء السريع اما بسرقة الأموال أو تحويلها لحسابه الشخصي داخل البنك ، يستطيع المتهم بمجرد دخوله على انظمة البنوك معرفة أرقام الحاسب وسرقتها أو تحويلها ،ويتم كذلك عن طريق استخدام **كارت فيزا** أو **ماستر كارد** البيع والشراء عبر شبكة الاتصالات الدولية من خلال سرقة تلك الارقام باستخدام شبكة المعلومات .[2]

بحيث تظهر الحاجة الى تحقيق الكسب السريع نتيجة وقوع البعض تحت ضغوط معينة كالمشاكل المالية أو الديون .

2- الرغبة في قهر النظام المعلوماتي واثبات ذلك :تعد الرغبة في قهر النظام المعلوماتي دافعا أقوى من السعي الى تحقيق الربح ، رغم أن هذا الأخير يظهر دافعا أكثر تحريكا للمجرمين المعلوماتيين ، الا أن الدافع الى قهر النظام أيضا تجسد بنسبة معتبرة من تلك الجرائم الالكترونية خاصة ما يعرف بأنشطة المتطفلين ،وهؤلاء ليسوا على جانب كبير من الخطورة الاجرامية وانما هم غالبا يفضلون تحقيق انتصارات تقنية دون أن يتوفر لديهم أية نوايا سيئة ، كما يشكل اختراق الأنظمة الالكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة متعة كبيرة وتسلية تغطي أوقات الفراغ مما يؤدي ذلك إلى الرغبة في تحقيق الذات وقهر النظام المعلوماتي .[3]

كما قد يكون ارتكاب الجرائم من طرف هؤلاء المجرمين بدافع الغرور والمتعة وكذا دافع الشعور بالنقص .

---

[1] غريبي بشرى ، المرجع السابق ، ص 109.

[2] خالد ممدوح ابراهيم، **الجرائم المعلوماتية**، المرجع السابق، ص139 .

[3] غريبي بشرى، المرجع السابق ، ص110.

ثانيا : الدوافع الخارجية : في بعض المواقف يتأثر الانسان ويستسلم للمؤثرات والدوافع الخارجية بارتكابه بعض الجرائم المعلوماتية ، نتيجة لوجوده في بيئة المعالجة الالية للمعلومات والتي سيتم توضيحها كالآتي :

– **دافع الانتقام والحاق الضرر برب العمل :**يعد دافع الانتقام من أخطر الدوافع التي يمكن أن تدفع الشخص الى ارتكاب جريمة ، لأن دافع الانتقام غالبا ما يصدر من شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها وغالبا ما يكون أحد موظفيها الذي يقوم بارتكاب الجريمة المعلوماتية بدافع الانتقام ، نتيجة اما لفصله من عمله أو تخطيه في الحوافز أو الترقية .

ثالثا : دوافع سياسية وتجارية :وهي تعد عوما محرك أنشطة الارهاب الالكتروني ، فكثيرا هي المنظمات في عصرنا الحالي والتي تتبنى بعض الآراء والأفكار السياسية أو الدينية او الإيديولوجية ، ومن أجل الدفاع عن هذه الآراء تقوم بأفعال اجرامية ضد معارضيها ، فمثلا هناك العديد من عمليات الاختراق تعود لأسباب عقائدية حيث تقوم بعض المجموعات التي تتبنى فكرة الاصلاح بعملية رقابة أخلاقية أو اجتماعية أو دينية ، فتتجسس على المواقع التي تقدم خدمات أو معلومات تتعارض مع قناعاتها ،وتعمل على كشف أسرارها أو حتى تدميرها . فهناك بعض المواقع أخذت على عاتقها مهمة التجسس على مواقع حكومية وكشف الأسرار الدبلوماسية والعسكرية ،وأما عن دوافع الحصول غلى المعلومات التجارية بمختلف الأشكال التي تكون عموما دوافعها المنافسة .

وأخيرا لا يمكن حصر أو ذكر كل الدوافع والبواعث التي قد تدفع بالمجرم المعلوماتي الى ارتكاب هذا الفعل المجرم .[1]

وخاتمة ما سبق تبين لنا أن صعوبة تحديد وتقسيم الجرائم الالكترونية راجع إلى تعدد السلوكات المجسدة للركن المادي في مختلف هذه الجرائم ، بسبب التطور المستمر لتقنية المعلومات التي انعكست على السلوك الإجرامي لمجرم الانترنت الذي يستعين بأهم التطورات التي حققتها وستحققها التكنولوجيا .

[1] غريبي بشرى، المرجع السابق ، ص 111.

وتطرح هذه الجريمة المستحدثة الصعوبة البالغة في اكتشاف مرتكبها ومتابعته مع العلم أن معظم هذه الجرائم ترتكب في عالم افتراضي متمثل في الشبكة العنكبوتية ، كما أن هذا النمط المستحدث من الإجرام يطرح إشكالية متابعة المتهم وخاصة إذا كان قد اقترف فعله الإجرامي في دولة أجنبية .

ضف إلى ذلك فان خصوصية المجرم المعلوماتي ودوافعه والخصائص التي تميزه ومختلف تصنيفاته ، فانه لا يوجد لحد الآن إجماع على تعريف موحد له ما عدا بعض الاجتهادات الفقهية .

فالمجرم المعلوماتي يتسم بمهارات علمية وتقنية متطورة ،وذي علم بالتقنية المستخدمة في نظام الحاسب الآلي وعلى اطلاع بكيفية استخدام نظام المعلومات لذلك يوصف هذا النوع من الجرائم بأنه جرائم الأذكياء، وذلك يعود لاستخدام الجناة فيها وسائل فنية معقدة في كثير من الأحيان .

خلاصة الفصل الاول :

في ختام هذا الفصل توصلنا الى ان الجريمة الالكترونية نوع من الجرائم المستحدثة انتجتها الثورة التكنولوجية ، يرتبط وجودها اساسا بوجود نظام معلوماتي يتميز بطبيعة خاصة، مما اوجد صعوبة في وضع تعريف جامع وموجد لها ، فقد اختلفت المفاهيم حولها باختلاف الزاوية التي ينظر اليها ، كما ان طبيعتها الخاصة تجلت في خصائصه المتميزة والمتمثلة ، اذ انها جريمة عابرة للحدود يصعب اكتشافها ، كما تميزت بسرعة تنفيذها من طرف مجرمين اذكياء يملكون منهجية المعرفة التقنية ودراية كافية بطريقة عمل وتسيير النظام المعلوماتي والولوج فيه بسهولة واستغلاله في القيام بأعمال غير مشروعة بغرض اتلاف النظم المعلوماتية تحقيقا لأغراضهم .

وقد عرفت الجريمة المعلوماتية تطورا متسارعا تماشيا مع التطور الهائل الذي يشهده نظام تكنولوجيا الاعلام والاتصال، يصعب معه تحديد اشكال واصناف الاعتداء ،لم تقتصر على الافراد فقط بل تعدت مؤسسات الدولة المالية والاقتصادية وحتي الدول ومؤسساتها الامنية ،تحقيقا لغايات واهداف خطيرة تؤدي الى تدمير اجهزة امن واختراقها واغراض اخرى .

الفصل الثاني

الفصل الثاني

الآليات التشريعية لمكافحة الجريمة الالكترونية في القانون الجزائري

ان التطور المتسارع لتكنولوجيا الاتصال والمعلومات في الفضاء الرقمي وما صاحبها من اضرار معتبرة على الافراد وعلى مؤسسات الدولة ، ورغبة المشرع الجزائري في التصدي لظاهرة الاجرام الالكتروني، محاولا تدارك الفراغ التشريعي القائم في هذا المجال نتيجة قصور القواعد الاجرائية التقليدية والمتعلقة بالتحريات والتحقيقات لملاحقة مرتكبي الجرائم المتصلة بتكنولوجيات الاعلام والاتصال لما تتطلبه هذه الاخيرة من اجراءات خاصة تتناسب مع التطورات الاجرامية في هذا المجال ، فعمد الى استحداث اليات قانونية تسمح بالحد من انتشار هذه الجرائم والوقاية منها ومكافحتها بشكل فعال من خلال وضع منظومة قانونية متكاملة ترتكز اساسا على تعديل كل من قانوني العقوبات والاجراءات الجزائية تتجاوب مع التطورات الاجرامية في مجال تكنولوجية الاعلام والاتصال، وتم تدعيمها بالقانون رقم 09-04 المؤرخ في 05 اوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ، بالإضافة الى قوانين خاصة لضمان الحماية الجنائية للمعاملات الالكترونية ، وتم ارساء قواعد اجرائية جديدة تتضمن تحكما جيدا في اساليب مكافحة هذ النوع من الجرائم سواء على المستوى الوطني أو الدولي بتعزيز التعاون التشريعي والقضائي بناءا على اتفاقيات ومعاهدات مشتركة لتبسيط الاجراءات لمواجهة الجرائم المعلوماتية ، كما اقر اجهزة ووحدات امنية خاصة لمتابعة ومكافحة هذه الجريمة ، كما استحدث الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ، وأقطاب متخصصة في هذا المجال مجهزة بأحدث الطرق العلمية المتطورة .

لذلك سنتناول في هذا الفصل الاليات القانونية الموضوعية والاجرائية لمكافحة الجريمة الالكترونية في التشريع الجزائري في المبحث الاول ونتعرض للهياكل والهيئات الخاصة لمكافحة الجريمة الالكترونية من خلال المبحث الثاني .

المبحث الاول

الاطار القانوني لمكافحة الجريمة الالكترونية في التشريع الجزائري

عمد المشرع الجزائري التصدي لهذه الجريمة المستحدثة وتوفير حماية جزائية للأنظمة المعلوماتية من خلال انتهاجه سياسة مزدوجة في المكافحة ، حيث ادخل تعديلات كثيرة على قانون العقوبات اثر تعديله سنة 2004 بصدور القانون رقم 04-15 وكذا تعديله الحاصل سنة 2006 بموجب القانون 06-22 المعدل والمتمم لقانون الاجراءات الجزائية التي تعرف بالقواعد العامة للمكافحة لجعله يتجاوب مع التطورات الاجرامية في مجال تكنولوجيا الاعلام والاتصال واستحداث قوانين خاصة تختص بعملية الوقاية والقمع لا سيما منه القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها ، وكذا تعزيزه بالتعاون الدولي في المجال التشريعي والقضائي .

في هذا الاطار سنتناول في المطلب الاول الاليات القانونية الموضوعية لمكافحة الجريمة الالكترونية في قانون العقوبات والقوانين الخاصة، وفي المطلب الثاني الاليات القانونية الاجرائية وفقا لقانون الاجراءات الجزائية وقانون رقم 09- 04 ، اما القواعد القانونية المقررة في اطار التعاون الدولي سندرجها كمطلب الثالث .

المطلب الاول

الاليات القانونية الموضوعية لمكافحة الجريمة الالكترونية

وضع المشرع الجزائري نصوص واليات قانونية واضحة لمكافحة الجريمة المعلوماتية ويتجلى ذلك من خلال تعديل قانون العقوبات بموجب القانون 15/04 المؤرخ في 10 نوفمبر 2004 المتمم لأمر 66-156وخص لهذا النوع من الجرائم قسما كاملا تحت عنوان " المساس بأنظمة المعالجة الالية للمعطيات " ضمن ثمان مواد من المادة 394 مكرر الى 394 مكرر 7 ، نصت على جملة من القواعد الموضوعية جرمت من خلالها الافعال الماسة بنظم المعالجة الالية للمعطيات وما يقابلها من جزاء أو عقوبة .

الفرع الاول :القواعد العقابية المقررة في قانون العقوبات

عرف المشرع الجزائري نظام المعالجة الالية بموجب الفقرة (ب) من المادة 02 من القانون رقم 09-04 بأنه " اي نظام منفصل أو مجموعة من الانظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو اكثر بمعالجة الية المعطيات تنفيذا لبرنامج معين"

والملاحظ ان هذه المادة لم تحدد العناصر التي يتكون منها نظام المعالجة الالية من مدخلات أو مخرجات وغيرها ، وانما اعتمدت على عنصر عملية المعالجة الالية في التعريف باعتبارها تنطوي على مراحل سابقة ولاحقة (الادخال ، والخزن ، والنقل ، والتبادل ....) وهوما يسمح باعتبار عناصر التبادل المتعلقة بالجوانب الاتصالية بالمعلومات ضمن مفهوم المعالجة[1]

ولقد نص المشرع الجزائري على صور الاعتداء على نظام المعالجة الالية للمعطيات والعقوبات المقررة لها في المواد 394 مكرر الى 394 مكرر 7 من قانون العقوبات في ثلاث صور [2] :

-الدخول والبقاء غير المشروع في نظام المعالجة الالية للمعطيات .

- الاعتداءات العمدية على نظام المعالجة الالية للمعطيات .

- الاعتداءات العمدية على سلامة المعطيات الموجود داخل النظام .

اولا : جريمة الدخول والبقاء غير المشروع في نظام المعالجة الالية للمعطيات

نصت المادة 394 مكرر على جريمة الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الالية للمعطيات بنصها " **يعاقب بالحبس من ثلاثة اشهر الى سنة وبغرامة من 50000 الى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الالية للمعطيات أو يحاول ذلك .**

[1] رشيدة بوكر ، المرجع السابق ، ص 52.

[2] المادة 394 مكرر من القانون رقم 09-04 مؤرخ في 05 اوت 2009 ،**يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها**، الجريدة الرسمية 47 الصادرة بتاريخ 16 اوت 2009.

تضاعف العقوبة اذا ترتب على ذلك حذف أو تغيير معطيات المنظومة ، واذا ترتب على الافعال المذكورة اعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة اشهر الى سنتين وبغرامة من 50.000 دج الى 150.000 دج "

01-الدخول غير المرخص : عرفه البعض انه عملية ولوج غير شرعي الى نظام التشغيل في الحاسب من قبل اشخاص لا يملكون سماحيات الدخول بهدف القيام بأعمال غير قانونية مثل التجسس والسرقة والتخريب ، مع الاخذ بعين الاعتبار قدرة هؤلاء الاشخاص على نقل ومسح أو اضافة ملفات وبرامج والقدرة على التحكم بنظام التشغيل أو اصدار اوامر [1].

وعليه يتحقق فعل الدخول بمجرد الوصول الى المعلومات المخزنة داخل النظام دون علم ورضا صاحبه .

ويلاحظ من خلال المادة 394 مكرر ان المشرع الجزائري اعتبر جريمة الدخول غير المرخص به بمثابة جريمة شكلية التي لا يشترط لقيام الركن المادي فيها تحقق النتيجة الاجرامية ، اي انه جرم مجرد الدخول الى نظم المعالجة الالية للمعطيات بأكمله اوالى جزء منه فقط بشرط ان يكون فعل الدخول بدون ترخيص ، كما لا تشترط المادة 394 مكرر لتحقق جريمة الدخول غير المرخص به الى نظام المعالجة ان يكون هذا النظام محاطا بحماية فنية تمنع الاختراق كالتشفير مثلا ، بل جاءت عامة ومطلقة اي تحمي كل الانظمة المعلوماتية من الاعتداء سواء كانت محمية فنيا ام لا ،

01-البقاء غير المرخص : معنى البقاء هو التواجد داخل نظام المعالجة الالية للمعطيات ضد ارادة من له الحق في السيطرة على هذا النظام بتجاوز المدة المسموح به بالبقاء فيها أو عدم الانسحاب فورا وقطع وجوده في النظام رغم علمه بان بقاءه فيه غير مرخص[2] .

[1] رشيدة بوكر،المرجع السابق ، ص 178.
[2] نفس المرجع ،ص 213.

اعتبر المشرع الجزائري فعل البقاء غير مرخص في نظام المعالجة الالية للمعطيات جريمة مثلها مثل جريمة الدخول الغير المرخص به وحدد لهما نفس العقوبة بموجب المادة 94 مكرر من قانون العقوبات.

كما نصت المادة 394 مكرر فقرة 02-03 من قانون العقوبات على ظرفين تشدد بهما العقوبة جريمة الدخول أو البقاء داخل النظام ويتحقق هذان الظرفان عندما ينتج عن الدخول أو لبقاء اما محو أو تعديل البيانات التي يحتويها النظام واما عدم صلاحية النظام لأداء وظائفه ويكفي لتوفر هذا الظرف وجود علاقة سببية بين فعل الدخول غير المشروع أو البقاء غير مباشر وتلك النتيجة الضارة التي حددتها المادة في محو أو تعديل بيانات النظام أو تخريب تشغيل النظام ذاته .

ثانيا : جريمة الاعتداء على معطيات نظام المعالجة الالية للمعطيات

يقصد بالاعتداء على معطيات نظام المعالجة ذلك الاعتداء الذي يهدف الى الاضرار بمعلومات الكمبيوتر، أو وظائفه سواء بالمساس بسريتها، أو المساس بسلامة محتوياتها أو بتعطيل قدرة وكفاءة الانظمة بشكل يمنعها من اداء وظيفتها بشكل سليم ويتخذ الاعتداء احد الشكليين :

01 – الاعتداء على المعطيات الداخلية للنظام : لقد جرم المشرع الجزائري اي اعتداء يقع على المعطيات الموجودة داخل نظام المعالجة الالية من خلال المادة 394 مكرر 1 من قانون العقوبات التي تنص " **يعاقب بالحبس من 06 اشهر الى 03 سنوات وبالغرامة من 50000 دج الى 2000000 دج كل من ادخل بطريق الغش معطيات في نظام المعالجة الالية أو ازال أو عدل بطريق الغش المعطيات التي يتضمنها** "[1]

يلاحظ من خلال احكام المادة المذكورة ان المشرع حدد صور الاعتداء على معطيات النظام الداخلية على سبيل الحصر الادخال أو المحو او التعديل .

[1] المادة 394 مكرر1 من القانون رقم 09-04 مؤرخ في 05 اوت 2009 ،**يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها**، الجريدة الرسمية 47 ،الصادرة بتاريخ 16 اوت 2009.

الادخال : يقصد بفعل الادخال حسب المادة 394 مكرر 1 اضافة معطيات جديدة الى نظام المعالجة الالية أو التعديل من معلومات داخلة مسبقا ويعتبر ادخال البرامج الخبيثة الى نظام المعالجة الالية بهدف اتلاف المعلومات ونشوبها وتدميرها ومن اشهر هذه البرامج الفيروسات والقنابل المنطفية والزمنية.

المحو: يعني ازالة من معطيات مسجلة على دعامة موجودة داخل نظام المعالجة الالية أو تحطيم تلك الدعامة أو نقل جزء من المعطيات من المنطقة الخاصة بالذاكرة .

التعديل : يعني تغيير المعطيات الموجودة داخل نظام المعالجة واستبدالها بمعطيات اخرى.[1]

وتجدر الاشارة الى ان المادة المذكورة لا تشترط اجتماع هذه الصور الثلاثة بل يكفي ان يصدر عن الجاني احداها لكي يكتمل الركن المادي لجريمة الاعتداء على معطيات نظام المعالجة ، مهما كانت الوسيلة المستعملة والطريقة المتبعة لتحقيق ذلك .

02- **الاعتداء على المعطيات الخارجية للنظام :** يقصد بالمعطيات الخارجية لنظام المعالجة تلك المعطيات التي لها دور في تحقق نتيجة معينة تمثل في المعالجة الالية للمعطيات وقد نص المشرع الجزائري في المادة 394 مكرر 02 من قانون العقوبات على النحو التالي " **يعاقب بالحبس من شهرين الى 03 سنوات وبغرامة من 100000 دج الى 200000 كل من يقوم عمدا اوعن طريق الغش بـ :**

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

- حيازة أو افشاء أو نشر أو استعمال لأي غرض كانت المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم "

[1] رشيدة بوكر،المرجع السابق ، ص 251.

فيقصد المشرع بالمعطيات المخزنة اما تلك المفرغة في دعامة مادية خارج النظام كالأقراص أو تلك المخزنة داخل النظام ذاته كذاكرته أو قرصه الصلب .

ويقصد بالمعطيات المعالجة اما تلك التي اصبحت جزء من النظام بعد ان تحولت الى اشارات أو رموز تتمثل المعطيات المعالجة، واما تلك المعطيات المرسلة عن طريق منظومة معلوماتية مثل تبادل ارسال المعلومات بين اجهزة المنظومة المعلوماتية فالأولى تعتبر معطيات داخل النظام والثانية هي معطيات النظام الخارجية [1].

وعليه فأي تلاعب بالمعطيات المذكورة اعلاه واستعمالها عمدا اوعن طريق الغش بإحدى الطرق المحددة في المادة 394 مكرر 2 يعد جريمة اعتداد على المعطيات الخارجية لنظام المعالجة الالية .

ثالثا : جريمة الاعتداء على سير نظام المعالجة الالية للمعطيات

لقد اغفل المشرع الجزائري وضع نص صريح خاص بتجريم الاعتداء على سير نظام المعالجة الالية للمعطيات ، غير انه يمكن استخلاص ذلك من خلال النصوص التي استحدثها بخصوص تجريم الاعتداءات الواقعة على الانظمة المعالجة او على المعطيات داخلية أو خارجية .

فالاعتداء على النظام بتخريبه كما نصت المادة 393 مكرر [2]من شانه ان يعيب عملية سير نظام والاعتداء على معطيات الداخلية للنظام باستعمال برامج الفيروسات وبرامج القنابل المعلوماتية من شانه التأثير في سير أو حسن سير النظام المعلوماتي ، ويمكن ان تتخذ الافعال الماسة بسير النظام عدة صور نذكر منها :

التعطيل : يمكن ان يصيب التعطيل الاجهزة المادية للنظام كتحطيم الاسطوانات أو قطع شبكة الاتصال أو يصيب الكيانات المنطقية للنظام كالبرامج أو المعطيات باستخدام برنامج فيروسي أو قنبلة منطفية مما يؤدي الى عرقلة سير النظام .

---

[1] براهيمي جمال ،**محاضرات في مكافحة الجريمة الالكترونية في التشريع الجزائري**. كلية الحقوق والعلوم السياسية جامعة مولود معمري :بتيزي وزو ،ص 136.

[2] المادة 393 مكرر من القانون رقم 09-04،**المتعلق بالوقاية من تكنولوجيا الاعلام والاتصال ومكافحته** .

الافساد : هو جعل نظام غير صالح للاستعمال بإحداث خلل في نظام سيره وفقدان توازن في اداء وظائفه كان يعطي نتائج غير تلك التي كان من الواجب الحصول عليها ، ومثل هذا الفعل ان لم يؤدي الى تعطل نظام المعالجة كله فانه يحول دون تحقيقه لوظائفه بشكل صحيح [1].

تجدر الاشارة الى ان المشرع الجزائري نص على الاتفاق الجنائي لارتكاب الجريمة الالكترونية واعتبره جريمة كاملة معاقب عليها من خلال المادة 394 مكرر 5 من قانون العقوبات نجد المشرع ينص على ان يعاقب " **كل من شارك في مجموعة أو اتفاق تالف بغرض الاعداد لجريمة أو اكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة افعال 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 الا في الجرائم الواقعة والتامة المكتملة الاركان أو الجرائم التي تقف عند مرحلة الشروع أو المحاولة ، ويعود هذا الاستثناء عن القاعدة العامة في التجريم الى خطورة الجريمة الالكترونية [2].

كما انه جرم كل من واشترك وشرع في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية وجعل العقوبة لهما تساوي العقوبات المقررة للجريمة ذاتها المادة 394 مكرر 7 من قانون العقوبات .

وعليه تشمل هذه العقوبات المذكورة في القسم السابع مكرر من قانون العقوبات ، عقوبات اصلية تتمثل في الحبس والغرامة، بالإضافة الى ذلك نص على جملة من العقوبات التكميلية لهذه الجرائم ،وفي هذا الاطار نصت المادة 394 مكرر 06 بنه " **مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الاجهزة والبرامج والوسائل المستخدمة مع اغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم ، علاوة على اغلاق المحل أو مكان الاستغلال اذا كانت الجريمة قد ارتكبت بعلم مالها** "

---

[1] بدري فيصل ،**مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي**، اطروحة لنيل شهادة الدكتورا علوم تخصص قانون عام ،كلية الحقوق :جامعة الجزائر 2017-2018، ص 171.

[2] دمان ذبيح عماد - بهلول سمية ، **الاليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري**، جامعة محمد لمين دباغين: سطيف 2 تاريخ النشر 2020/01/05، ص143.

وعليه فان العقوبات التكميلية لهذه الجريمة تتمثل في :

01-المصادرة : عرف المشرع الجزائري المصادرة بانها " **الايلولة النهائية الى الدولة لمال أو مجموعة اموال معينة أو ما يعادل قيمتها عند الاقتضاء** "وانطلاقا من المادة 394 مكرر06 اعلاه فانه لا بد من اعمال اجراء المصادرة في مجال الجرائم الالكترونية توافر جملة من الشروط المتمثلة في :

-ان يحكم على المتهم بعقوبة اصلية في احدى الجرائم المنصوص عليها في القسم الخاص بالاعتداء على انظمة المعالجة الالية للمعطيات.

-ان تكون الاشياء التي تمت مصادرتها قد استخدمت في ارتكاب الجريمة الصادر بشأنها الحكم القضائي .

- يجب الا تخل المصادرة بحقوق الغير حسن النية ، في حال ما اذا كنت الوسائل المستخدمة في ارتكاب الجريمة ملكا للغير .

-يجب ان يكون الشخص حسن النية جاهلا بكون الوسائل المستخدمة في ارتكاب الجريمة جاهلا بان هذه الوسائل قد تستخدم في ارتكاب الجريمة.

02-الغلق :يعتبر الغلق من ثاني العقوبات التكميلية التي نصت عليها المادة 394 مكرر من قانون العقوبات[1] ، وتشمل عقوبة الغلق في اطار الجرائم الالكترونية غلق المواقع الالكترونية التي تكون محلا للجريمة ، كما يشمل الغلق المحل أو مكان الاستغلال اذا كانت الجريمة قد ارتكبت بعلم مالك المحل ،ولم يحدد المشرع مدة زمنية للغلق للمواقع في الجرائم الالكترونية تارك الامر لتقدير القاضي تطبيقا للقواعد العامة الواردة في احكام المادة 16 مكرر 01 من قانون العقوبات والتي تنص " **يترتب على غلق المؤسسة منع المحكوم عليه من ان يمارس فيها النشاط الذي ارتكبت الجريمة**

[1] القانون رقم 15/04 ،المؤرخ في 10 نوفمبر 2004، **المتمم لقانون العقوبات** الجريدة الرسمية العدد 71، الصادرة بتاريخ 10 نوفمبر 2004.

بمناسبته ويحكم بهذه العقوبة اما بصفة نهائية أو لمدة لا تزيد عن عشر (10) سنوات في حالة الادانة لارتكاب جنحة " [1]

كما ان المشرع ضاعف عقوبة الغرامة المقررة للشخص المعنوي الذي يرتكب احدى الجرائم المعلوماتية بموجب المادة 394 مكرر 4 " **يعاقب الشخص المعنوي الذي يرتكب احدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمسة (05) مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي**" مع اقراره المسؤولية الجزائية للأشخاص الطبعيين بصفتهم فاعلين اصلي أو شركاء في نفس الجريمة التي ارتكبها الشخص المعنوي المادة 394 مكرر 04 من قانون العقوبات .

الفرع الثاني : القـواعـد المقـررة في القـوانين الخاصـة

اولا- القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته :

ان اصدار المشرع الجزائري القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها قام بإرسال قواعد اجرائية جديدة تضمن تحكما جيدا في اساليب مكافحة هذا النوع من الاجرام بما يتوافق وخصائصه .

وباستقراء فحوى هذا القانون يتبين لنا ان المشرع استحدث تدابير جديدة غير مألوفة في القوانين السابقة للتصدي لجرائم المعلوماتية ، تتمثل في تدابير وقائية تساعد على الكشف المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها ورصد مرتكبيها ، وتدابير اخرى اجرائية مكملة لتلك المنصوص عليها في قانون الاجراءات الجزائية .

وقد اورد المشرع في المادة 02 من قانون 09-04 انه "**يقصد بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال جرائم المساس بأنظمة المعالجة الالية للمعطيات**

[1] القانون رقم 09-04 مؤرخ في 05 اوت 2009 ،**يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها**، الجريدة الرسمية 47 ،الصادرة بتاريخ 16 اوت 2009.

المحددة في قانون العقوبات واي جريمة اخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية"

وقد شمل هذا القانون الكثير من الاليات المستحدثة بنصه على انشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته ، كذلك القواعد المتعلق

بالاختصاص الاقليمي للقانون الجزائي الجزائري ، حيث تم التوسع في الاختصاص الاقليمي للسلطة القضائية في متابعة جرائم تمس مؤسسات الدولة الجزائرية أو الدفاع أو المصالح الاستراتيجية للاقتصاد الوطني[1] .

ايضا فان عالمية استغلال تكنولوجيات الاعلام والاتصال وخاصة الانترنت ادت الى حذف الحدود الاقليمية ، واصبحت الجرائم تمتد عبر عدة اقاليم ، ويكون الاختصاص القانون الجزائي لأكثر من دولة ، مما قد ينجر عنه تنازع في الاختصاص أو رفض له

فكان التعاون الدولي في هذا النوع من الجرائم مفيدا وفعال جدا، ولا يتأتى ذلك الا باستعمال الطرق الحديثة للتواصل ما بين السلطات القضائية وهوما تم تشريعه فعلا ضمن هذا القانون .

بالإضافة فان التحري في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ميزاتها الخاصة، والتي تبناها المشرع في القانون 04/09 فالمراقبة الالكترونية للاتصالات وتفتيش نظم المعلوماتية اعطى لها القانون الصفة الشرعية القانونية بتقنينها وادخالها ضمن الترسانة الاجرائية الجزائية في القانون الجزائري .

كما يلعب مقدمو خدمات الانترنت لما لديهم من تقنيات متماشية مع تطور التكنولوجيا الحديثة للإعلام والاتصال دورا مهما في مكافحة هذا النوع من الاجرام وتقديم المساعدة التقنية للسلطات المكلفة بالبحث والتحري عن الجرائم المرتكبة بواسطة هذه التكنولوجيات

[1] القانون رقم 09-04 مؤرخ في 05 اوت 2009 ،**يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها**، الجريدة الرسمية 47، الصادرة بتاريخ 16 اوت 2009.

وايضا الالتزام بما قرره المشرع بحفظ للمعطيات المعلوماتية يسمح للمحققين تتبع الجريمة وحركة المجرمين .

ثانيا- القواعد الخاصة المتعلقة بحماية المؤلف والحقوق المجاورة

ادت القفزة الرقمية التي حدثت في العالم الى احداث اثر بالغ على كافة جوانب الحياة ، وكان لها اثر مباشر على الملكية الفكرية وتحديدا في مجال حق المؤلف ، حيث اصبح نشر وتوزيع وعرض المصنفات غاية في السهولة والسرعة والاتقان وباقل تكاليف [1] الامر الذي ادى الى مسايرة هذه التطورات لظهور ما يسمى بالملكية الرقمية ، والتي تشمل حقوق الملكية الفكرية على الانترنت والتي مضمونها يشمل كل مصنف ابداعي ينتمي الى بيئة تقنية المعلومات يعد مصنفا رقميا .

مما لا شك فيه ان حقوق المؤلف تأثرت بشكل كبير بالتطور التكنولوجي ، واصبحت تتبلور في مصنفات رقمية موجودة على مستوى البيئة الافتراضية الرقمية ، الا ان تداول هذه المصنفات في البيئة الرقمية ادى الى تعرضها الى انتهاكات مست بحقوق المؤلف بالدرجة الاولى ، والتي اصبحت بمثابة المثبط لروح الابداع والابتكار لدى المؤلفين ذلك ان التشريعات التقليدية باتت تقف عاجزة عن حماية صاحب الحقوق في شبكة الانترنت

ولهذا سارع المشرع الجزائري على غرار التشريعات الاخرى الى حماية هذه المصنفات بتطويع النصوص التقليدية الخاصة بحماية الملكية الفكرية ، وذلك بإخضاع المال المعلوماتي (برامج الحاسوب) لقوانين الملكية الفكرية ، حيث اعتبر برنامج الحاسوب الالي ضمن المصنفات الادبية والفنية بموجب المادة الرابعة من الامر رقم 05/03 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة والتي تنص على

انه " تعتبر على الخصوص كمصنفات ادبية أو فنية محمية ما يلي :

[1] عبد الله عبد الكريم عبد الله،**الحماية القانونية لحقوق الملكية الفكرية على شبكة الانترنت** .دار الجامعة الجديدة الازاربطة ،ط 2008 ،ص 19 .

أ – المصنفات الادبية المكتوبة مثل المحاولات الادبية والبحوث العلمية والتقنية والروايات والقصص والقصائد الشعرية وبرامج الحاسوب ... الخ " [1]

وقد بسط المشرع الجزائري حمايته على برامج الحاسبات الالية مدخلا اياها تحت نطاق حقوق المؤلف تماشيا مع اتفاقية " برن " الدولية [2]التي صادقت عليها الجزائر بموجب المرسوم الرئاسي 341/97 المؤرخ في 1997/09/13 منح الحماية للبرامج مدة 50 سنة ابتداء من مطلع السنة الميلادية التي تلي نشر المصنف المادة 01/5 من الامر 05/03 السالف الذكر ، ومدة 50 سنة ابتداء من طلع السنة الميلادية التي تلي تاريخ وفاة المؤلف تماشيا مع نص المادة السابعة من اتفاقية برن .

كما ان المشرع وسع قائمة المؤلفات المحمية ، حيث ادمج تطبيقات الاعلام الالي ضمن المصنفات الاصلية ، حيث عبر عنها بالمصنفات قواعد البيانات وبرامج الاعلام الالي ، والتي تمكن من القيام بنشاط علمي اواي نشاط من نوع اخر أو الحصول على نتيجة خاصة من المعلومات .

وفي سبيل تقرير حماية جنائية فعالة في هذا المجال عدد المشرع مجموعة من الافعال الماسة بالمصنفات وبحقوق مؤلفيها وجرمها وجعل مرتكبيها يشكلون خرقا لحقوق

المؤلف تجب معاقبته من اقترافها ، ومن الجرائم المعلوماتية التي جاء بها الامر رقم 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة ما يلي :[3]

– ارتكاب جنحة التقليد عن طريق الكشف غير المشروع للمصنف أو المساس بسلامة مصنف أو اداء لفنان مؤد أو عازف ، استنساخ مصنف أو اداء باي اسلوب من الاساليب في شكل نسخ مقلدة ، استراد أو تصدير نسخ مقلدة من مصنف أو ا داء ، أو

---

[1] امر رقم 03-05 ،مؤرخ في 19 جمادي الاولى عام 1424 الموافق 19 يوليو2003 ،**المتعلق بحقوق المؤلف والحقوق المجاورة .**

[2] السيد عبد الحميد احمد، **جرائم الشبكة العنكبوتية وغسل الاموال في اطار الملاحقة الامنية والقضائية الدولية** .مكتبة الوفاء القانونية : الاسكندرية 2018، ص 347.

[3] نفس الامر السابق رقم 05/03 المتعلق بحقوق المؤلف .

بيع نسخ مقلدة لمصنف ، أو اداء ، تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف ، أو اداء (المادة 151 من الامر 05/03) .

– ارتكاب جنحة التقليد عن طريق انتهاك الحقوق المحمية بموجب هذا الامر ، فيبلغ المصنف أو الاداء عن طريق اي منظومة معالجة معلوماتية (المادة 152 من نفس الامر).

– الاشتراك بالعمل أو الوسائل الحائز عليها للمساس بحقوق المؤلف اواي مالك للحقوق المجاورة (المادة 154 من نفس الامر) .

اما بالنسبة للعقوبات المقررة على مختلف هذه الاعتداءات ، فقد تضمنتها المواد 153 ، 156 ، 157 ، 158 ، 159 من الامر السالف الذكر ، وتشمل العقوبة لمرتكب جنحة التقليد لمصنف أو اداء فني كما هو وارد في المادتين 151 –152 من ذات الامر بالحبس من 06 اشهر الى ثلاث سنوات وبغرامة من خمسة مئة الف (500.000 دج) الى مليون دينار جزائري (1000.000 دج) سواء كان النشر قد حصل في الجزائر أو خارجها طبقا للمادة 153 من نفس الامر ، كما نص في المادة 154 من نفس الامر على معاقبة الشريك في ارتكاب جريمة التقليد سواء بأعماله أو بالوسائل التي يحوزها للمساس بحقوق المؤلف بنفس العقوبات المقررة في المادة 153 من الامر السالف الذكر ونفس الشيئي بالنسبة لكل من يمتنع عن دفع المكافاة المستحقة للمؤلف (المادة 155 من ذات الامر) .

وقد شدد المشرع العقوبة في حالة العود الى ضعف العقوبة المقدرة في المادة 153 من الامر 03–05 المشار اليه سابقا طبقا للمادة 156 من نفس الامر[1] .

بالإضافة الى هذه العقوبات الاصلية قرر المشرع كذلك لهذه الجرائم العقوبات التكميلية ، التي تتمثل في الغلق لمؤسسة يستغلها المقلد أو شريكه والمصادرة ، سواء مصادرة المبالغ التي تتمثل الايرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو اداء محمي طبقا

[1] امر رقم 03-05 ، مؤرخ في 19 جمادي الاولى عام 1424 الموافق 19 يوليو 2003 ،**المتعلق بحقوق المؤلف والحقوق المجاورة .**

للمادة 157 من الامر 05/03 وكذلك نشر حكم الادانة وفقا لأحكام المادة 158 من نفس الامر [1].

ثالثا – القواعد الخاصة المتعلقة بالبريد والموصلات السلكية و اللاسلكية

سارع المشرع الجزائري الى مواكبة التطور الذي شهدته التشريعات العالمية مسايرة التطور التكنولوجي بإصداره قانون رقم 2000–03 المؤرخ في 05 اوت 2000 المتعلق بالقواعد المتعلقة بالبريد والموصلات السلكية وللاسلكية .

وقد قام هذا القانون بتعريف المواصلات السلكية واللاسلكية ومنها الامواج السلكية وللاسلكية ، الشبكة الخاصة والشبكة العامة وخدمة الهاتف وخدمة التلكس والخدمات البريدية واطرافها من مرسل ومرسل اليه وغيرها من المصطلحات التي تم استخدامها في هذا القانون.

نصت المادة 84 الفقرة 02 منه " **تطبق احكام المادة 89 من هذا القانون عن استعمال حوالات دفع عادية أو الكترونية أو برقية** "

نصت المادة 105 الفقرة الاخيرة على انه "**لا يمكن باي حال من الاحوال انتهاك حرمة المراسلات**" [2].

كما تضمن هذا القانون الجرائم المعلوماتية والعقوبات المقررة والتي تتمثل :

فتح، أو تحويل، أو تخريب البريد، أو انتهاك سرية المراسلات، أو المساعدة على ارتكاب هذه الافعال من قبل كل شخص يقوم بتقديم خدمة البريد السريع الدولي اوكل عون يعمل لديه في اطار ممارستهم لمهامهم ، كل شخص مرخص له بتقديم خدمة مواصلات السلكية وللاسلكية ، وكل عامل لدى متعاملي الشبكات العمومية السلكية وللاسلكية ، واثناء ممارستهم لمهامهم وغيرهم (المادة 127 من هذا القانون) .

[1] نفس الامر السابق رقم 05/03،المتعلق بحقوق المؤلف والحقوق المجاورة.

[2] قانون رقم 2000-03 المؤرخ في 05 اوت 2000،**المتعلق بالقواعد العامة المتعلقة بالبريد والموصلات السلكية وللاسلكية .**

-انشاء أو استغلال شبكة عمومية للمواصلات السلكية واللاسلكية دون رخصة أو مواصلة ممارسة النشاط خرقا لقرار التعليق أو سحب هذه الرخصة (المادة 131 من هذا القانون)

- انشاء أو العمل على انشاء شبكة مستقلة دون ترخيص (المادة 132) .

- اشهار بغرض بيع تجهيزات أو معدات للمواصلات السلكية واللاسلكية دون الحصول على الاعتماد المسبق (المادة 133 من هذا القانون) .

المطلب الثاني

الاليات القانونية الاجرائية لمكافحة الجريمة الالكترونية

في اطار اصلاح المنظومة التشريعية والقضائية ، وضمانا لفعالية وسرعة التحقيق في القضايا المتعلقة بالجرائم المستحدثة ، سارع المشرع الجزائري بتعديل قانون الاجراءات الجزائية تماشيا مع التطور المعلوماتي الذي لحق بالجريمة محاولة منه تطويقها والقضاء عليها أو على الاقل الحد من انتشارها ، وذلك في اطار المكافحة الاجرائية لهذا النوع من الاجرام، حيث وضع قواعد خاصة لسلطة التحري والمتابعة الغرض منها مواجهتها والتصدي لها [1].

الفرع الاول : القواعد الاجرائية المقررة وفقا لقانون الاجراءات الجزائية

ادرك المشرع الجزائري جيدا بان المواجهة الفعالة للإجرام الالكتروني لا تكون بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية فقط، انما لابد من مصاحبة هذه القواعد بقواعد اخرى اجرائية وقائية وتحفظية ، وهوما استدركه بتضمين القانون رقن (06-22) المعدل لقانون الاجراءات الجزائية تدابير ارجائية جديدة تتعلق بالتحقيق في الجرائم الالكترونية تتمثل فيما يلي :

اولا- الاختصـــاص

01-تمديد الاختصاص المحلي :حيث نصت المادة 329 من قانون الاجراءات الجزائية في فقرتها الاخيرة "على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم اخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجريمة الماسة بأنظمة المعالجة الالية للمعطيات "ولعل اعتماد الاختصاص الاقليمي الموسع هو لمواجهة الفعالة لطائفة من الجرائم المنظمة الخطيرة ومنها الجرائم الالكترونية الماسة بأنظمة المعالجة الالية للمعطيات[2] .

---

[1] الملتقى الوطني، **اليات مكافحة الجريمة الالكترونية في التشريع الجزائري**. الجزائر العاصمة، 29 مارس 2017 ص 67.

[2] قانون 06-22، مؤرخ في 20 ديسمبر 2006 ،يتم الامر 66 -156 **المتضمن قانون الاجراءات الجزائية**.

كما انشئت الاقطاب القضائية الجزائية المتخصصة بموجب القانون 04-14 المؤرخ في 10 نوفمبر 2004المعدل لقانون الاجراءات الجزائية[1] من بين الجرائم التي تختص بها الجرائم الماسة بأنظمة المعالجة الالية للمعطيات (المواد 37 و40 و329 من قانون الاجراءات الجزائية).

كذلك نظم المشرع الجزائري في القانون رقم 09-04 المؤرخ في 05 اوت 2009 احكاما جديدة خاصة بالاختصاص في مجال الجريمة المعلوماتية تتماشى والتطور الذي لحق الجريمة ، ومن هذه القواعد ما نصت عليه المادة 03 التي تضمنت اجراءات جديدة التي تتطلبها التحريات والتحقيقات من ترتيبات تقنية بالإضافة الى ذلك قررت المادة 05 من ق 09-04 " انه زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال المرتكبة خارج الاقليم الوطني عندما يكون مرتكبيها اجنبيا ويستهدف مؤسسات الدولة الجزائرية والدفاع الوطني، أو المصالح الاستراتيجية للاقتصاد الوطني [2].

02-توسيع مجال اختصاص النيابة العامة :

بموجب المادة 37 من قانون الاجراءات الجزائية تم توسيع اختصاص النيابة العامة ليشمل نطاقات اخرى لم يكن مرخصا لها بها من قبل ، حيث نصت هذه المادة على تمديد الاختصاص المحلي لوكيل الجمهورية الى دائرة اختصاص محاكم اخرى عن طريق التنظيم في جرائم المخدرات ،والجريمة المنظمة ،والجرائم الماسة بأنظمة المعالجة الالية للمعطيات ،وجرائم تنبيض الاموال ،والارهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف .

كذلك سحب نظام الملائمة من النيابة العامة في مجال متابعة بعض الجرائم ، اذ يلتزم وكيل الجمهورية بتحريك الدعوى العمومية بقوة القانون [3]، بحيث لا يتمتع بشأنها بسلطة

[1] القانون 04-14 المؤرخ في 10 نوفمبر 2004 ،**المعدل لقانون الاجراءات الجزائية** .

[2] القانون رقم 09-04 مؤرخ في 05 اوت 2009 **يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها** الجريدة الرسمية 47 الصادرة بتاريخ 16 اوت 2009 .

[3] الملتقى الوطني – **اليات مكافحة الجريمة الالكترونية في التشريع الجزائري**، المرجع السابق ص 68 .

الملائمة بين تحريك الدعوى العمومية وعدم تحريكها مثلما فعل في الجرائم المنصوص عليها في المواد 144 مكرر 1 و144 مكرر 2 من قانون العقوبات المعدل والمتمم بالقانون رقم 09/01 المؤرخ في 26 يونيو 2000 .

ثانيا : التسـرب

عرف المشرع الجزائري التسرب بموجب المادة 65 مكرر 12 من قانون العقوبات على انه " قيام ضباط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الاشخاص المشتبه في ارتكابهم جناية ،أ وجنحة بإيهامهم انه فاعل معهم أو شريك "[1]

اذ يلاحظ من خلال هذا التعريف ان التسرب عملية في الغالب معقدة تتطلب ان يدخل العون المكلف بالعملية في اتصال بالأشخاص المعنيين ويربط معهم علاقات ضيقة ويحافظ على السر المهني لغاية تحقيق الهدف النهائي من العملية ، وهي تتطلب على الخصوص المشاركة المباشرة في نشاط الخلية الاجرامية التي تسرب اليها ، والذي يكون احيانا ضرورة لقبوله[2].

ويمكن تصور عملية التسرب في نطاق جرائم الاعتداء على نظم المعالجة الالية في دخول ضابط أو عون الشرطة القضائية الى العالم الافتراضي واشراكه مثلا في محادثات غرفة الدردشة أو حلقات النقاش والاتصال المباشر في كيفية قيام احدهم باختراق شبكات أو بث فيروسات مستخدما في ذلك اسماء وصفات هيئات مستعارة ووهمية ظاهرا فيها بمظهر طبيعي ، وكمثال على ذلك ما قامت به المباحث الفيدرالية الامريكية عندما دست احد اعضائها لكي يتمكن بعد ذلك من ضبط مجموعة من المجرمين يمتهن قرصة البرمجيات والمتاجرة فيها بطريقة غير مشروعة .

[1] قانون 06-22 مؤرخ في 20 ديسمبر 2006يتم الامر 66 -156 المؤرخ في 08 يونيو1966،**المتضمن قانون الاجراءات الجزائية** ،الجريدة الرسمية العدد 84 الصادر بتاريخ 24 ديسمبر 2006 .

[2] رشيدة بوكر،المرجع السابق ،ص434 .

01 : شروط صحة عملية التسرب

لما كان التسرب ممارسة غير مألوفة للضابط أو عون الشرطة القضائية ، بل اخطر الاجراءات انتهاكا لحرمة الحياة الخاصة للمتهم ، احاطه المشرع بجملة من الضمانات يتعين مراعاتها عندما تقتضي ضرورات التحري أو التحقيق في احدى الجرائم المذكورة اللجوء اليه يمكن ايجازها في نوعين من الشروط كما يلي :

-**الشروط الشكلية** :عملا بمبدأ الشرعية يجب ان تتوفر في عملية التسرب الشروط التالية

أ-**صدور بإذن قضائي** : وهذا ما نصت عليه المادة (56 مكرر) من قانون الاجراءات الجزائية " ..... يجوز لوكيل الجمهورية أو قاضي التحقيق بعد اخطار وكيل الجمهورية ان يأذن تحت ...."[1]والجهة المختصة لإصداره كما هو مبين من نص المادة اما وكيل الجمهورية أو قاضي التحقيق ، وذلك حماية للحقوق الاساسية المكرسة دستوريا .

ب- ان يكون مكتوبا : وهذا ما نصت عليه المادة (65 مكرر 15) من قانون الاجراءات الجزائية بقولها " يجب ان يكون الاذن مسلما طبقا للمادة (65 مكرر 11) اعلاه مكتوبا تحت طائلة البطلان "

ج-ذكر اسم الضابط :المشرف على العملية وهويته الكاملة .

هـ- المدة المطلوبة لعملية التسرب :وقد جاءت حسب نص المادة (65 مكرر 15) الفقرة الثالثة من قانون الاجراءات الجزائية على ان لا تتجاوز اربعة اشهر ، ويمكن ان تجدد حسب مقتضيات التحري أو التحقيق ،وفي نفس الوقت اجاز القانون للقاضي الذي رخص باجرائها ان يأمر في اي وقت بوقفها قبل انقضاء المدة المحددة .

[1] قانون رقم 06-22 مؤرخ في 20 ديسمبر 2006 ،يتم الامر 66 -156 المؤرخ في 08 يونيو1966،**المتضمن قانون الاجراءات الجزائية**، الجريدة الرسمية ،العدد 84 ، الصادر بتاريخ: 24 ديسمبر 2006 .

و-ابقاء الاذن بالتسرب خارج ملف الاجراءات الى غاية الانتهاء من العملية : حفاظ على السرية المطلوبة التي حصرها المشرع بين القاضي الامر بها (وكيل الجمهورية أو قاضي التحقيق) وضابط الشرطة القضائية المشرف على العملية وكذا العون المتسرب

م- وجود تقرير مسبق محرر من طرف الضابط عن الجريمة : بشكل مفصل للاطلاع القاضي بشكل تام عن ظروف القضية ومتطلباتها .

ن- الصفة :يستشف من نص المادة (65 مكرر 12) المادة (65 مكرر 14) من قانون الاجراءات الجزائية ان المخولين قانون للعمل بنظام التسرب هم ضباط وكذا اعوان الشرطة القضائية وكذا الاشخاص المسخرين لذلك[1] .

02-الشروط الموضوعية :يمكن ايجاز الشروط الموضوعية لعملية التسرب وفق الاحكام التي نظمها المشرع الجزائري في شرطيين اساسيين :

أ – تسبيب عملية التسرب : يعتبر التسبيب شرط جوهري لمشروعية عملية التسرب ، لذلك اشترط القانون عند اصدار الاذن بالتسرب من السلطات المختصة ذكر السبب أو الدافع الحقيقي الجاد الذي يبرر اللجوء الى هذا الاجراء تحت طائلة البطلان المادة (65 مكرر 15) من قانون الاجراءات الجزائية .

ب – محل التسرب : بمعني ان عملية التسرب يجب ان تنصب على احدي الجرائم السبعة المنصوص عليها في المادة 65 مكرر 5 وهي جرائم المخدرات ، الجريمة المنظمة ، الجرائم الماسة بأنظمة المعالجة الالية للمعطيات ، جرائم تبيض الاموال ، وجرائم المتعلقة بالتشريع الخاص بالصرف وفيما عدى ذلك يعتبر التسرب اجراء باطلا [2].

ثالثا : اعتراض المراسلات وتسجيل الاصوات والتقاط الصور

ان هذا الاجراء قد تم ادراجه من قبل المشرع الجزائري بموجب القانون رقم (06-22) المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الاجراءات الجزائية ، فاستحدث له

[1] رشيد بوكر، المرجع السابق ، ص 436 .
[2] نفس المرجع، ص 437.

الفصل الرابع تحت عنوان " في اعتراض المراسلات وتسجيل الاصوات والتقاط الصور " وقد ضمنه ستة مواد من المادة (65 مكرر) حتى المادة (65 مكرر 10) .

ثالثا : تعريف اعتراض المراسلات السلكية واللاسلكية :

نستشف من نص المادة (65 مكرر 5) من قانون الاجراءات الجزائية ان المقصود باعتراض المراسلات اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهاته المراسلات عبارة عن بيانات قابلة للنتاج والتوزيع والتخريب الاستقبال والعرض .

وفي اجتماع لجنة الخبراء للبرلمان الاوروبي بستراسبورغ بتاريخ 06-10-2006 حول اساليب التحري التقنية وعلاقتها بالأفعال الارهابية نجدها تعرف اعتراض المراسلات بانها " عملية مراقبة سرية المراسلات السلكية واللاسلكية وذلك في اطار البحث والتحري عن الجريمة وجمع الادلة أو المعلومات حول الاشخاص المشتبه فيهم اوفي مشاركتهم في ارتكاب الجرائم"[1].

اما التقاط الصور يكون بالتقاط صورة لشخص أو عدة اشخاص يتواجدون في مكان خاص ويتم استخدام هذه الوسائل في المحلات السكنية والاماكن العامة والخاصة .

اما تسجيل الاصوات فيتم عن طريق وضع رقابة على الهواتف وتسجيل الاحاديث التي تتم عن طريقها ، كما يتم ايضا عن طريق وضع مكروفونات حساسة تستطيع التقاط الاصوات وتسجيلها على اجهزة خاصة .[2]

وقد اشار المشرع الجزائري الى ظروف وكيفية اللجوء هذا الاجراء في المادة 65 مكرر 5 من قانون الاجراءات الجزائية على النحو" اذا اقتضت ضرورات التحري في الجريمة المتلبس بها او التحقيق الابتدائي في ..... الجرائم الماسة بأنظمة المعالجة الالية للمعطيات ..... يجوز لوكيل الجمهورية المختص :

[1] رشيد بوكر، المرجع السابق ،ص ص 441-442.

[2] الملتقى الوطني ،**اليات مكافحة الجرائم الالكترونية في التشريع الجزائري**،المرجع السابق ص 69 .

-باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية .

-وضع الترتيبات التقنية دون موافقة المعنيين من اجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة اشخاص في اماكن خاصة أو عمومية، أو التقاط صور لشخص أو عدة اشخاص يتواجدون في مكان خاص .

فموجب هذه المادة فان المشرع الجزائري يسمح لسلطات التحقيق أو الاستدلال اذا استدعت ضرورة التحري في الجريمة المتلبس بها أو التحقيق في الجريمة الالكترونية ، اللجوء الى اجراء اعتراض المراسلات السلكية واللاسلكية وتسجيل المحادثات والاصوات والتقاط الصور والاستعانة بكل الترتيبات التقنية اللازمة لذلك من اجل الوصول الى الكشف عن ملابسات الجريمة واثباتها دون ان يتقيدوا بقواعد التفتيش والضبط المألوفة [1].

ومع هذا فان المشرع الجزائري لم يطلق حق اللجوء الى هذا الاجراء بل احاطه بمجموعة من الضمانات القانونية التي تحد من تعسف سلطات الاستدلال والتحري وتصون الحقوق والحريات العامة والحياة الخاصة للأفراد والتي يمكن ان تتلخص فيما يلي :

***ترخيص السلطة القضائية ومراقبتها** :السلطة القضائية هي المختصة عموما بإصدار هذا الاذن ويعد ذلك ضمانة لازمة لمشروعية الاعتراض على المراسلات السلكية واللاسلكية في القانون الجزائري فطبقا لنص (المادة 65 مكرر 5) من قانون الاجراءات الجزائية لا يمكن لضباط الشرطة القضائية اللجوء الى اجراء اعتراض المراسلات الا بعد ان يحصل على اذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق .

***نوع الجريمة التي اقتضت ضرورة التحري أو التحقيق القضائي** :وهي محددة على سبيل الحصر بنص المادة (65 مكرر 5) من قانون الاجراءات الجزائية ومن بينها المساس بنظم المعالجة الالية للمعطيات .

* **طبيعة المراسلة والاتصال** : محل الاعتراض أو التنصت .

[1] بوجاني نور الدين،**اساليب البحث والتحري الخاصة واجراءاتها وفقا لقانون رقم 06-22 مداخلة في يوم دراسي حول علاقة النيابة العامة بالشرطة القضائية احترا حقوق الانسان ومكافحة الجريمة**. المديرية العامة للامن الوطني المنعقد: باليزي الجزائر، **المؤرخ في 20-12-2006** ص 26 .

02- **فائدة الاعتراض في اظهار الحقيقة :** تقرر التشريعات المعاصرة ان ضابط فائدة المراقبة في ظهور الحقيقة يعتبر السند الشرعي المبرر للاعتراض بسبب ان هذا الاجراء يتضمن اعتداء جسيما على حرمة الحياة الخاصة وسرية الاتصالات[1] فيباح استثناءا في حدود ضيقة ، وذلك للفائدة المنتظر منه والتي تتعلق بإظهار الحقيقة بكشف غموض الجريمة وضبط الجناة .

03 -الجرائم التي يجوز فيها الاعتراض : بالرجوع الى المادة (65 مكرر 5) من قانون الاجراءات الجزائية نجد ان المشرع الجزائري قد نص صراحة على نوع الجرائم التي يجوز فيها مباشرة الاعتداء ومنها جرائم الاعتداء على نظم المعالجة الالية ، وذلك ادراكا منه على عدم كفاية الوسائل التقليدية لجمع الدليل التقني، نظرا لما تتمتع هذه الجريمة المستحدثة من خصوصية .

04- مدة الاجراء :وهي اربعة اشهر قابلة للتجديد حسب تقدير نفس السلطة مصدرة الامر وفقا لمقتضيات التحري والتحقيق ، وذلك بموجب الفقرة الثانية (2) من المادة (65 مكرر) بقولها " يسلم الاذن مكتوبا بالمدة اقصاها اربعة اشهر قابلة للتجديد ....."

05- مراعاة السر المهني اثناء الاعتراض : اي عند القيام باعتراض المراسلات تلتزم سلطات التحقيق بعدم المساس بالسر المهني المتعلق بالتفتيش المنصوص عليه بالمادة 45 من قانون الاجراءات الجزائية .

الفرع الثاني: القواعد الاجرائية المقررة وفقا لقانون 09-04المتعلق بالوقاية من تكنولوجيات الاعلام والاتصال ومكافحتها

يمثل هذا القانون الاطار القانوني الاكثر ملائمة مع خصوصيات الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت باستقراء فحوى هذا القانون يتبين ان المشرع استحدث تدابير جديدة غير مألوفة في القوانين السابقة للتصدي لجرائم المعلوماتية ، تمثل في تدابير وقائية تساعد على الكشف المبكر للاعتداءات المحتملة والتدخل السريع لتحديد

[1] رشيد بوكر، المرجع السابق ، ص ص 444-445

مصدرها ورصد مرتكبيها ، وتدابير اخرى اجرائية مكملة لتلك المنصوص عليها في قانون الاجراءات الجزائية ، منها مراقبة الاتصالات الالكترونية ، التفتيش ، حجز المعطيات ، مع اقحام مقدمي خدمات الانترنت في مسار الوقاية من الجرائم المعلوماتية سنتناولها بالتفصيل :

اولا- مراقبة الاتصالات الالكترونية

اقر المشرع الجزائري مشروعية المراقبة الاتصالات الالكترونية كإجراء استثنائي لمبدا الحق في الخصوصية المعلوماتية لموجهة الاجرام المستحدث والكشف عن الحقيقة في الجرائم الماسة بتكنولوجيات الاعلام والاتصال عن طريق اجراءات وقواعد خاصة نظمها القانون رقـم 09-04 المؤرخ في 05 اوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها [1].

01- تعريف مراقبة الاتصالات الالكترونية

لم يعرف المشرع الجزائري عملية مراقبة الاتصالات الالكترونية كإجراء مستحدث تاركا المجال للفقه حيث عرفه جانب من الفقه مراقبة الاتصالات" التنصت بغرض الاستماع الى الحديث خلسة ، والذي يتم عن طريق استراق السمع ، كما يتوافر ايضا عن طريق التسجيل للحديث اوفي نقله الى مكان اخر"

وعرفه جانب اخر من الفقه " نوع خاص من استراق السمع يسلط على الاحاديث الشخصية والمحادثات التلفونية خلسة دون علم صاحبها بواسطة اجهزة الكترونية اسفر عنها النشاط العلمي الحديث [2]"

ويمكن تعريف المراقبة بانها اجراء تحقيق يباشر خلسة وينتهك الاحاديث الخاصة تامر به السلطة القضائية في الشكل المحدد قانونا بهدف الحصول على الدليل .

---

[1] القانون رقم 09-04 مؤرخ في 05 اوت 2009 . **يضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها** ،الجريدة الرسمية العدد 47 ،الصادرة بتاريخ 2009/08/16.

[2] ياسر الامير فاروق ،**مراقبة الاحاديث الخاصة في الاجراءات الجنائية دراسة تأصيلية تحليلية ومقارنة للتنصت على المحادثات التليفونية والتي تجرى عبر الانترنت والاحاديث الشخصية نظريا وعمليا** .دار المطبوعات الجامعية: الاسكندرية ، ط 2009 ،ص 140.

02- الحالات التي يمكن اللجوء فيها الى المراقبة الالكترونية

لا يجوز اللجوء الى اجراء المراقبة الالكترونية الا في الحالات المذكورة في المادة 04 من القانون 09-04 كما يلي :

أ- للوقاية من الافعال الموصوفة بجرائم الارهاب أو التخريب ،أو الجرائم الماسة بأمن الدولة.

ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني .

ج -لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول الى نتيجة تهم الابحاث الجارية دون اللجوء الى المراقبة الالكترونية.

د- في اطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.[1]

يتضح من خلال استقراء هذه الحالات ان المشرع الجزائري قلص من الحالات التي يمكن اللجوء فيها الى اجراء المراقبة الالكترونية وحصرها في الجرائم التي تمس الامن الوطني وحالات تنفيذ المساعدة القضائية ومقتضيات التحريات والتحقيقات القضائية[2].

الا انه لم يحدد على سبيل الحصر الجرائم المعينة بهذه المراقبة ،مما يمكن تطبيقها على جميع الجرائم في حالة توفر ضرورة التحريات ومستلزمات التحقيقات القضائية .

03- تقييد اجراء المراقبة الالكترونية بمجموعة من الضمانات

حرص المشرع الجزائري على تحديد الضمانات التي تسمح باللجوء لإجراء المراقبة الالكترونية ، للحد من التعسف في استخدامه من طرف السلطة المختصة وحفاظا على الحق في الخصوصية المعلوماتية من كل اعتداء عليه ، فقد اشترط اللجوء الى مراقبة

[1] القانون رقم 09-04 مؤرخ في 05 اوت 2009 ،**يضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها**. الجريدة الرسمية ،العدد 47 الصادرة بتاريخ 2009/08/16.

[2] محمدي برنية امنة ،**اجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية**.(دراسة تحليلية لأحكام قانون الاجراءات الجزائية) وقانون الرقابة من جرائم الاعلام (اعمال الملتقى الوطني اليات مكافحة الجرائم الالكتروني في التشريع الجزائري 29 مارس 2017 مركز جيل البحث العلمي: الجزائر 2017 ،ص 74.

الاتصالات الالكترونية الحصول على اذن من طرف السلطة القضائية واستعمال المعطيات المتحصل عليها عن طريق المراقبة في حدود ضيقة .

أ- ضرورة الحصول على اذن من طرف السلطة القضائية المختصة

يعد الاذن من بين الضمانات التي وضعها المشرع الجزائري لمراقبة الاتصالات الالكترونية حفاظ على خصوصية الافراد بما فيها الخصوصية المعلوماتية ، وبذلك نصت الفقرة 02 من المادة 14 من القانون 09-04 السابق الذكر على انه لا يجوز اجراء عمليات المراقبة الا بإذن مكتوب صادر عن السلطات القضائية المختصة دون تحديد فيما تتمثل هذه السلطة .

ويتبن ان المشرع الجزائري احال بصفة صريحة الى قانون الاجراءات الجزائية بخصوص ما يتعلق بمحتوى المادتين 03-04 من قانون 09-04 وعليه يتمثل اذن السلطة القضائية المختصة في منح الاذن بمراقبة الاتصالات الالكترونية في وكيل الجمهورية قبل فتح تحقيق، أو قاضي التحقيق في حالة فتح تحقيق قضائي كقاعدة عامة .

ويختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته ، اذن لمدة 06 اشهر قابلة للتجديد ، وذلك على اساس التقرير بين طبيعة الترتيبات التقنية المستعملة والاغراض الموجهة لها وهذا عندما يتعلق الامر بجرائم الارهاب أو التخريب أو الجرائم الماسة بأمن الدولة [1]

وعليه لا يتم القيام بمراقبة الاتصالات الالكترونية الا بأذن مكتوب من السلطات القضائية المختصة ، غير انه ما يلاحظ هو سكوت المشرع الجزائري عن تحديد مدة الاذن للقيام بعملية المراقبة مكتفيا فقط بتحديد مدة الاذن الممنوح من طرف النائب العام لدى مجلس قضاء العاصمة بـ 06 اشهر قابلة للتجديد في حالة الوقاية من الافعال الموصوفة بجرائم

[1] القانون رقم 09-04 مؤرخ في 05 اوت 2009 ، **يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها** ، الجريدة الرسمية ،العدد 47،الصادرة بتاريخ 2009/08/16.

الارهاب أو التخريب أو الجرائم الماسة بأمن الدولة ، اما بالنسبة للاذن الممنوح في الحالات الاخرى المنصوص عليها في المادة 04 من قانون 09-04 فتخضع لقانون الاجراءات الجزائية وتحديدا المادة 65 مكرر وما يليها وهذا طبقا لنص المادة 03 من القانون 09-04 .

وعليه يعتبر الاذن من اهم الضمانات المقررة لا جراء مراقبة الاتصالات الالكترونية من اجل تحقيق التوازن بين المصلحة العامة من خلال مواجهة الاجرام المستحدث والمصلحة الخاصة من خلال حماية حقوق وحريات المتهم .

ب- حدود استعمال المعطيات المتحصل عليها عن طريق مراقبة الاتصالات الالكترونية

ينتج عن مراقبة الاتصالات الالكترونية تجميع وتسجيل محتوى هذه الاتصالات سواء تمثلت في محادثات شفوية أو رسائل الكترونية متبادلة عن طريق البريد الالكتروني أو التقاط الصور وذلك باستعمال الترتيبات التقنية المناسبة ، وحفاظ على مثل هذه المعطيات المتحصل عليها عن طريق المراقبة قيد المشرع استعمالها في الحدود الضرورية للتحريات والتحقيقات القضائية تحت طائلة العقوبات المنصوص عليها في قانون العقوبات وهذا ما اكدته عليه المادة 09 من القانون 09-04 .

ويهدف المشرع الجزائري من خلال تقييد اجراء المراقبة التقنية الالكترونية بمجموعة من الضمانات القانونية الى الموازنة بين احترام الخصوصية بما فيها الخصوصية المعلوماتية ومواجهة الاجرام المستحدث حتى لا يتم الاخلال بالأحكام القانونية التي تتضمن سرية المرسلات والاتصالات ولتحقيق هذا الهدف تم انشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال كآلية لتنفيذ المراقبة الالكترونية .

ثانيا - تفتيش المنظومة المعلوماتية

لم يضع المشرع الجزائري تعريفا للتفتيش فقد اعتبره اجراء من اجراءات التحقيق الهدف منه الحصول على الادلة لإثبات الجريمة للوصول للجاني تاركا المجال للفقه .

وقد عرفه جانب من الفقه " ان التفتيش هو اجراء من اجراءات التحقيق يهدف الى ضبط ادلة الجريمة موضوع التحقيق وكل ما يفيد في كشف الحقيقة "

وهناك من يرى " انه اجراء من اجراءات التحقيق تقوم به سلطة حددها القانون يتم بالبحث في مستودع السر عن ادلة الجريمة التي وقعت وكل ما يفيد في كشف الحقيقة "[1]

اما تفتيش الانظمة المعلوماتية، فقد عرفه بعض الفقهاء بانه البحث في مستودع سر المتهم عن اشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها اليه ، أو هو البحث الدقيق والاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه سواء كان مسكنا أو جهاز حاسوب أو انظمة أو الانترنت[2].

ونص المشرع الجزائري على اجراء تفتيش المنظومة المعلوماتية بموجب القانون رقم 09-04 المتعلق بالوقاية من تكنولوجيا الاعلام والاتصال ومكافحتها بموجب المادة 05

تنص " يجوز للسلطات القضائية وكذا ضباط الشرطة القضائية ف اطار قانون الاجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 اعلاه الدخول بغرض التفتيش ولوعن بعد الى :

أ – منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها .

ب –منظومة تخزين معلوماتية [3].

01- محل تفتيش النظم المعلوماتية

يقع التفتيش دائما على مستودع السر الذي يحتفظ به المرء بالأشياء المادية ولامادية التي تتضمن سره ، وينصب محل تفتيش المنظومة المعلوماتية على كل ما له صلة بهذه النظم من برامج والات واجهزة حاسوب وغيرها من الاجهزة الالكترونية ، ويكون التفتيش منصب

---

[1] علي حسن محمد الطوالبة،**التفتيش الجنائي على نظم الحاسوب والانترنت دراسة مقارنة**.عالم الكتب الحديث: الاردن ط 2004، ص ص10-11.

[2] نفس المرجع،ص ص 12-13 .

[3] القانون رقم 09-04 مؤرخ في 05 اوت 2009 ،**يضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها**،الجريدة الرسمية ،العدد 47 الصادرة بتاريخ 2009/08/16.

على كل مكونات المنظومة المعلوماتية سواء الكيان المادي للحاسوب أو المكونات المعنوية له .

أ- المكونات المادية للحاسوب hardware

يقصد بالمكونات المادية للحاسوب "الاشياء الملموسة من اجزائه وادواته التي تعمل بشكل متكامل لأداء مهمة في معالجة البيانات اليا "[1]

وعليه يتكون الحاسوب من عدة وحدات مثل وحدات الادخال كلوحة المفاتيح والقلم الضوئي ووحدة الذاكرة الرئيسية التي تستخدم في الحفظ الدائم أو المؤقت للبيانات والبرامج اضافة الى وحدة المعالجة المركزية التي تقوم بالتنسيق بين الوحدات الاخرى وضبط التعليمات ، واخيرا وسائط اظهار نتائج التشغيل كالشاشة والطابعة والاقراص المرنة والصلبة .

ب- المكونات المعنوية للحاسوب software

يطلق ايضا على المكونات المعنوية للحاسوب بالبرمجيات ويعرف الكيان المنطقي للحاسوب لغة بانه كلمة تستخدم للدلالة على جميع المكونات غير المادية لنظام الحاسوب كنظم التشغيل وبرامج التطبيقات ، كما عرفه التوجه الاوروبي الصادر في 14 ماي 1991 برامج الحاسب الالي " بانها مجموعة من الاوامر التي تؤدي الى انجاز المهام المستهدفة من خلال نظام معالجة المعلومات ويطلق عليه اسم الحاسب ، كما يمكن تقسيم برامج الحاسوب الى نوعين يسمى الاول برامج النظام system program الذي دونه لا يمكن استغلال الحاسوب والثاني برامج التطبيقات application programs التي تقوم بمهام محددة مثل برامج معالجة النصوص .

ويميز المشرع الجزائري في تفتيش المنظومات المعلوماتية بين ما اذا كانت المنظومة متصلة بنظام اخر داخل التراب الجزائري ، أو كانت المنظومة متصلة بمنظومة معلوماتية تقع خارج الاقليم الوطني .

[1] بلال امين زين الدين ،**جرائم نظم المعالجة الالية للبيانات في لتشريع المقارن** . دار الفكر الجامعي :الاسكندرية 2006 ، ص 221.

الحالة الاولى :اذا كانت المعطيات المبحوث عنها مخزنة في منظومة معلوماتية اخرى ويمكن الولوج اليها انطلاقا من المنظومة الاولى فانه يجوز تفتيش هذه المنظومة بسرعة دون استصدار اذن قضائي ، وانما يكفي اعلام السلطة القضائية المختصة حسب المادة 05 فقرة 02 من قانون 09-04 ولعل انتظار صدور الاذن من السلطات المختصة قد يأخذ بعض الوقت ما قد يؤدي الى تلاشي الدليل واندثاره في وقت قياسي ، كان يقوم المشتبه فيه بمحوه واتلافه ، اذ يكفي الضغط على مكان معين لا نهاء وجود المعلومة ومن ثم تتبخر عناصر الاثبات ما يشكل صعوبة في ايجاد دليل حاسم لذلك فان استصدار اذن قضائي في مثل هذه الحالات لا فائدة منه .[1]

02- محل تفتيش النظم المعلوماتية

بحسب نص المادة 05 من قانون 09-04 المتعلق بمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ، فان حالات اللجوء الى تفتيش النظم المعلوماتية هي نفسها الحالات التي تسمح باللجوء الى المراقبة الالكترونية للاتصالات :

أ- للوقاية من الافعال الموصوفة بجرائم الارهاب أو التخريب، أو الجرائم الماسة بأمن الدولة.

ب- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني .

ج -لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول الى نتيجة تهم الابحاث الجارية دون اللجوء الى المراقبة الالكترونية.

د- في اطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة [2].

[1] يزيد بوحليط،**تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري**. مجلة التواصل في الاقتصاد والادارة والقانون، كلية الحقوق والعلوم السياسية جامعة باجي مختار: عنابة ، ص 85

[2] المادة 05 من القانون رقم 09-04 مؤرخ في 05 اوت 2009 ،**يضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها** الجريدة الرسمية العدد 47 الصادرة بتاريخ 2009/08/16

فالمشرع الجزائري من خلال نص المادة 05 من القانون رقم 09-04 اجاز اجراء التفتيش على المنظومة المعلوماتية عن بعد وهذا اجراء جديد ، بحيث يمكن الدخول اليها دون اذن صاحبها في الكيان المنطقي للحاسوب للتفتيش عن ادلة في المعلومات التي يحتوي عليها هذا الاخير ، كما اجاز افراغ هذه المعلومات على دعامة مادية أو نسخها للبحث عن الدليل فيها .

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

كما نص المشرع الجزائري في نفس القانون على اجراء اخر يسهل عملية التفتيش في الفقرة الاخيرة من المادة 05 وهذا الاجراء يتمثل في اللجوء الى الاشخاص المؤهلين كالخبراء والتقنيين والمختصين في الاعلام الالي وفن الحاسوب .[1]

ثالثا – حجز المعطيات المعلوماتية

مما لا شك فيه ان النتيجة الطبيعية التي ينتهي اليها التفتيش هو ضبط الادلة التي يتم الحصول عليها تفيد في كشف الحقيقة عنها وعن مرتكبيها ،وفي جرائم الاعتداء على نظام المعالجة الالية يكون المحل الذي يرد عليه الضبط في هذه الجرائم ذات طبيعة معنوية تتمثل في المعلومات بما تمثله كالمراسلات والاتصالات الالكترونية [2].

وقد تدخل المشرع الجزائري لاستكمال ما تبقى من فراغ تشريعي في المنظومة التشريعية وذلك بموجب القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته .

[1] نفس القانون السابق رقم 09-04 ،**يضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها**.

[2] رشيد بوكر، المرجع السابق، ص419.

حيث استحدثت المادة 06 التي تنص على انه " عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وانه ليس من الضروري حجز كل المنظومة ، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في احراز وفقا للقواعد المقررة في قانون الاجراءات الجزائية[1].

بموجب هذا القانون على السلطة القائمة على التفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية ، ويجوز لها عند الضرورة استعمال الوسائل التقنية قصد جعلها قابلة للاستعمال لأغراض التحقيق شرط ان لا يؤدي ذلك الى المساس بمضمون هذه المعطيات [2].

واذا استحال اجراء الحجز وفقا لما هو منصوص في احكام المادة 07 اعلاه لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول الى المعطيات التي تحتويها المنظومة المعلوماتية وذلك عن طريق ترميزها وتقييدها عن اي وسيلة الكترونية اخرى تمنع الدخول لها ، وكذلك نسخها ووضعها تحت تصرف الاشخاص المرخص لهم باستعمال هذه المنظومة .

ويمكن للسلطة التي تباشر التفتيش ان تامر باتخاذ الاجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة لا سيما عن طريق تكليف شخص مؤهل باستعمال الوسائل التقنية وذلك عن طريق ترميزها وتقييدها عن طريق والمنع الدخول الى هذه المعلومات .

---

[1] نفس القانون السابق رقم 04/09،**يضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها**.

[2] الهادي خضراوي ،**تجربة الجزائر في مكافحة الجريمة الالكترونية** .المؤتمر الدولي لمكافحة الجرائم المعلوماتية كلية العلوم الحاسب ، جامعة الامام محمد بن سعود الاسلامية ،ص 165 .

رابعا– التزامات مقدمي خدمات الانترنت في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال

نظرا لخصوصية الجريمة الالكترونية ولتسهيل عملية البحث والتحقيق ، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وبوضع المعطيات التي يتعين عليهم حفظها تحت تصرف السلطات ،ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها ذلك تحت طائلة العقوبات المقررة لإفشاء اسرار التحري والتحقيق.

01–تعريف مقدمي الخدمات :

عرف المشرع الجزائري مقدمي الخدمات بموجب المادة 02 فقرة" د" من القانون رقم 09–04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته

مقدمي الخدمات اي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام الاتصالات واي كيان يقوم بمعالجة ،أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها [1].

02–التزامات مقدمي خدمات الانترنت :

أ– **حفظ المعطيات المتعلقة بحركة السير:** حفظ المعطيات المقصود بها قيام مزود الخدمات بتجميع المعطيات المعلوماتية وحفظها وحيازتها في الارشيف ، وذلك بوضعها في ترتيب معين والاحتفاظ بها في المستقبل في انتظار اتخاذ اجراءات قانونية اخرى كالتفتيش وغيره[2] .

ويفهم من ذلك ان اجراء الحفظ يتم بعد قيام مقدمي الخدمات بإجراء التجميع والتسجيل ثم الحفظ ليقدم في النهاية الى يد السلطات المكلفة بالتحريات القضائية ، وتكتسي هذه

[1] انفس القانون السابق رقم 09-04 ،**يضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها**.

[2] رشيدة بوكر ،المرجع السابق ،ص 448.

الاجراءات اهمية بالغة من حيث كونها اداة تنقيب وتحري مفيدة من اجل تحديد مصدر الاتصال وماله عن طريق ارقام الهاتف ، كما توفر بيانات مرتبطة بالساعة والتاريخ والمدة المتعلقة بأنواع الاتصالات غير المشروعة .

ويعتبر اجراء الحفظ اجراء وقتي ، اذ حدده المشرع الجزائري في نفس المادة من ذات القانون في فقرة الثالثة لمدة سنة ابتداء من تاريخ التسجيل ، ويأتي تحديد هذه المدة احتراما للحق في الخصوصية اذ يلزم مقدم الخدمات بمسح المعطيات التي يتم حفظها .

ب- التزامات مزودي الخدمات لسحب المعطيات:

يلزم المشرع الجزائري وفقا للمادة 12 من قانون سابق الذكر مقدمي خدمة الانترنت الى جانت الالتزام بحفظ المنصوص عليه في المادة 11 ما يلي :

-التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة لمخالفتها للقوانين وتخزينها أو جعل الدخول اليها غير ممكن .

- وضع ترتيبات تقنية تسمح بحصر امكانية الدخول الى موزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة واخبار المشتركين لديهم بوجودها [1].

وقد حدد المشرع الجزائري المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمات بمعطيات المرور أو كما سماها "حركة السير " وقد عرف هذا الاخير بموجب الفقرة هـ من المادة 02 من نفس القانون بانها " اي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الاخيرة باعتبارها جزءا في حلقة الاتصالات توضح مصدر الاتصال والوجهة المرسلة اليها والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة .

[1] المادة 12 من القانون رقم 09-04 ،**يضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها**.

ومن ضمن معطيات المرور نجد ان المشرع الجزائري في المادة 11 قد حدد عدة طوائف منها ، والتي تخضع لنظام قانوني واحد لما يعني دخولها في نطاق الالتزام بالحفظ من طرف مزود الخدمة وحصرها في :

أ – المعطيات التي تسمح بالتعرف على مستعملي الخدمة .

ب – المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

ج– الخصائص التقنية وكذا تاريخ وقت ومدة كل اتصال .

د– المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها .

هـ – المعطيات التي تسمح بالتعرف على المرسل اليه أو المرسل اليهم الاتصال وكذا عناوين المواقع المطلع عليها .

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

تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة ابتداء من تاريخ التسجيل[1]

03– مسؤولية مقدمي الخدمات عن اخلالهم بالالتزامات القانونية المفروضة عليهم

يتحمل مقدمي الخدمات المسؤولية الجنائية وتطبق عليهم العقوبات المنصوص عليها في قانون العقوبات اذا لم يلتزم بكتمان اسرار التحري والتحقيق ، كما يتحملون المسؤولية الجنائية عن اخلالهم بالالتزام الحفظ ، حيث وفقا للفقرة الرابعة من المادة 11 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته " دون الاخلال بالعقوبات الادارية المترتبة على عدم احترام التزامات المنصوص عليها في هذه المادة تقوم المسؤولية الجزائية للأشخاص الطبعيين والمعنويين عندما يؤدي الى عرقلة حسن سير التحريات القضائية ، ويعاقب الشخص الطبيعي بالحبس من ستة (6) اشهر الى خمس (5) سنوات وبغرامة من 50.000 دج الى 500.000 دج .

[1] المادة 11 من القانون رقم 09-04 ،**المتعلق بالوقاية من تكنولوجيا الاعلام والاتصال ومكافحتها**.

ويعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات [1].

اذ ان مقدمي الخدمات يتعاملون مع هيئات وتفرض عليهم هذه الاخيرة عدة التزامات تقيد في دفتر الشروط وفي حالة اخلالهم بها تطبق عليهم جزاءات كسحب رخصة اضافة الى عقوبات ادارية اخرى .

ومع هذا ينبغي الاعتراف بحقيقة وهي انه رغم الجود الجبارة التي بذلها المشرع الجزائري في سبيل التصدي لظاهرة الاجرام الالكتروني ، الا انها تبقى غير كافية لبلوغ الهدف المنشود ، نظرا للتطورات السريعة والمستمرة التي تعرفها ظاهرة الاجرام الالكتروني من جهة ، نظرا للطابع العالمي والعابر للحدود الذي يتميز بها هذه الظاهرة من جهة اخرى ، لذا لا بد من التوجه الى التنسيق التشريعي والقضائي مع الدول العربية ، وكذا الدول الغربية الاكثر دراية بالجرائم الالكترونية والاستفادة من خبراتها في مجال مكافحة هذه الجرائم .

الفرع الثالث : القواعد القانونية المقررة في اطار معاهدات دولية خاصة

ان قصور التشريعات الداخلية في مواجهة الجريمة الالكترونية بسبب طبيعتها عبر الوطنية جعل المجتمع الدولي يقتنع بان توحيد جهوده وحشد قواه هو الحل الامثل لمكافحة هذا الاجرام ، خاصة ان جهود الفردية للدول غدت لا تجدي نفعا كونها جريمة عابرة للحدود ، وهوما يجعل من التعاون الدولي مطلب الجميع[2] ، لهذه سارعت الجزائر كغيرها من الدول الى النص على ضرورة التعاون الدولي في مجال اجراءات المتابعة والتحقيق لتعقب مرتكبي هذه الجرائم وملاحقتهم والقبض عليهم ومحاكمتهم ، وذلك بإبرام اتفاقيات ومعاهدات دولية لتبسيط هذه الاجراءات وتوحيد القواعد العامة .

وقد نصت الاتفاقية العربية لمكافحة الجريمة المعلوماتية التي صادقت عليها الجزائر على مسالة التعاون الدولي في المادة 32 منها بقولها "على جميع الدول الاطراف تبادل المساعدة فيما بينها بأقصى مدى يمكن لغايات التحقيقات او الاجراءات المتعلقة بجرائم

[1] القانون رقم 09-04 ،**المتعلق بالوقاية من تكنولوجيا الاعلام والاتصال ومكافحتها**.

[2] لينا محمد الاسدي ،**المرجع السابق** ، ص 87.

المعلومات وتقنية المعلومات او لجمع الادلة الالكترونية في الجرائم ...." وتتجلي مظاهر التعاون الدولي في محاربة الجريمة الالكترونية فيما يلي :

اولا: المساعدات القضائية الدولية :

المساعدة القضائية الدولية بانها كل اجراء قضائي تقوم به الدولة في سبيل تسهيل المحاكمة في دولة اخرى بصدد جريمة من الجرائم الواقعة في بيئة الاعمال الالكترونية[1]

وقد تنبه المشرع الجزائري الى اهمية هذا الاجراء ، فسمح في اطار التحريات أو التحقيقات القضائية بخصوص الجرائم الواقعة في بيئة الاعمال الالكترونية وبالتحديد تلك المتعلقة بأنظمة المعالجة الالية للمعطيات ، والتي تعتبر من صور الجريمة المعلوماتية تسمح للسلطات المختصة بتبادل المساعدة القضائية الدولية بخصوص جمع الادلة الالكترونية ، بل يمكن في حالة الاستعجال قبول طلبات المساعدة القضائية اذا وردت عن طريق وسائل الاتصال السريعة لما في ذلك اجهزة الفاكس أو البريد الالكتروني ، وذلك بقدر ما توفره هذه الوسائل من شروط امن كافية للتأكد من صحتها .

ويمكن حصر المساعدات الدولية المتبادلة في الصور التالية :

01- تبادل المعلومات ونقل الاجراءات بين الدول :

بالرجوع الى المادة 17 من قانون 09-04 المتعلق بالوقاية من جرائم المتصلة بتكنولوجيات الاعلام والاتصال انه " تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ اجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة أو الاتفاقيات الدولية الثنائية ومبدا المعاملة بالمثل " [2].

فيقصد بتبادل المعلومات تقديم المعلومات والوثائق التي تطلبها سلطة قضائية اجنبية بصدد جريمة من الجرائم عن الاتهامات التي وجهت الى رعاياها في الخارج والاجراءات

[1] عادل عبد العال ابراهيم خراشن ،**اشكالية التعاون الدولي في مكافحة الجريمة المعلوماتية وسبيل التغلب عليها** .2015 دار الجامعة الجديدة :الاسكندرية، 2015 ، ص30 .

[2] نفس المرجع ،ص ص 34-35.

التي اتخذت ضدهم ، كما ان هناك مظهر اخر لتبادل المعلومات يتعلق بالسوابق القضائية للجناة والتي تساعد في تقرير الاحكام الخاصة بالعود .

اما نقل الاجراءات قيام احدى الدول باتخاذ الاجراءات الجنائية شكل جريمة ارتكبت في اقليم دولة اخرى لمصلحة هذه الدولة بناء على اتفاقية وذلك اذا توفرت شروط معينة اهمها :

* ان يكون الفعل المنسوب الى الشخص يشكل جريمة في الدولة الطالبة والمطلوب منها.

* ان تكون الاجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب منها على ذات الجريمة.

*ان يكون الاجراء المطلوب اتخاذه يؤدي الى الوصول الى الحقيقة ، كان تكون ادلة الجريمة موجودة بالدولة المطلوب منها .

وبالرجوع الى الاتفاقية العربية السالفة الذكر نجدها تنص على مثل هذا الاجراء في نص المادة 39 منها بحيث جاء فيها :

* يجوز لأي دولة طرف ان تطلب من دولة طرف اخرى البحث أو الوصول أ والضبط أو التام أو الكشف لمعلومات تقنية ، المعلومات المخزنة والواقعة ضمن اراضي الدولة الطرف المطلوب منها لما في ذلك المعلومات التي حفظها بحسب المادة 37 .

* تتم الدولة الطرف المطلوب منها بان تستجيب للدولة الطرف الطالبة وفقا لأحكام الواردة في هذه الاتفاقية .

* تتم الاجابة على الطلب على اساس عاجل اذا كانت المعلومات ذات العلاقة عرضة للفقدان أو التعديل .

ثانيا –الانابــة القضائيــة:

يقصد بالإنابة القضائية الدولية طلب اتخاذ اجراء قضائي من اجراءات الدعوى الجنائية ، تتقدم به الدولة الطالبة الى الدولة المطلوب اليها لضرورة ذلك للفصل في مسالة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها .

فالإنابة القضائية تعبر عن قيام دولة ما بمباشرة اجراء قضائي يتعلق بدعوى قيد النظر داخل الحدود الاقليمية لدولة اخرى نيابة عنها بناء على طلب تلك الدولة المناب عنها وفقا لما تقرره بنود الاتفاقية الدولية بين الدولتين في هذا الشأن [1].

نظم المشرع الجزائري اجراءات الانابة القضائية في المواد 721 و722 من قانون الاجراءات الجزائية ، حيث جاء في المادة 721 انه " في حالة المتابعات الجزائية غير السياسية في بلد اجنبي تسلم الانابات القضائية الصادرة من السلطة الاجنبية بالطريق الديبلوماسي وتنفيذ الانابات القضائية وفقا للقانون الجزائري ومبدا المعاملة بالمثل " [2]

ويمكن ان نستشهد هنا باتفاقية تبادل الانابة القضائية الدولية المبرمة بين الجزائر وفرنسا في 1962/08/28 والتي نصت على ان البلدين " يتعاونان لتقديم المعونة أو المساعدة القضائية التي تطلبها كل دولة " كما تضمنت شروط تنفيذ الانابة القضائية .

وتهدف الانابة القضائية نقل الاجراءات في المسائل الجنائية لمواجهة الجرائم المستحدثة وتذليل العقبات التي تعترض سير الاجراءات الجنائية المتعلقة بقضايا ممتدة خارج الحدود الوطنية .

ثالثا – تسليم المجرمين :

يعد تسليم المجرمين دربا قويما من دروب التعاون الدولي في مجال مكافحة الاجرام المعلوماتي والذي تناولته بالتنظيم ترسانة ضخمة من القوانين الوطنية والاتفاقيات الدولية.

---

[1] عادل عبد العال ابراهيم ، المرجع السابق ،ص ص36-37.

[2] قانون رقم (06-22) مؤرخ في 2006/12/20 يعدل ويتمم الامر رقم 66-155،**يتضمن قانون الاجراءات الجزائية** جريدة رسمية، العدد 84 صادر بتاريخ 2006/12/24 معدل ومتمم .

ويعرف تسليم المجرمين بانه الاجراء الذي تسلم به دولة استنادا الى معاهدات أو الاتفاقيات السياسية تأسيسا على المعاملة بالمثل ،عادة الى دولة اخرى شخصا تطلبه الدولة الاخيرة لاتهامه أو لأنه محكوم عليه بعقوبة جنائية [1].

لذا يعد الاتفاق على تبادل تسليم المجرمين بين الدول حول هذه الجرائم ضرورة ملحة وهوما نصت عليه اتفاقية بودابست في المادة 24 منها ، حيث اكدت على ضرورة ان تلتزم الاطراف المتعاقدة بإدراج هذه الجرائم بوصفها جرائم تستوجب تسليم المجرمين .

وكذا نص المشرع الجزائري الذي اعترف بإمكانية تسليم المجرمين كإحدى تدابير المساعدة القضائية وجعل منه مبدا دستوري وذلك بنصه في المادة 82 من الدستور على " **مبدا جواز تسليم شخص بناءا على قانون تسليم المجرمين وتطبيقا له** "[2]

وقد نظم المشرع الجزائري مسالة تسليم المجرمين في قانون الاجراءات الجزائية من المواد من 694 الى 719 ومن بين ما جاء في هذه المواد، انه يجوز للحكومة الجزائرية ان تسلم شخصا غير جزائري الى حكومة اجنبية بناءا على طلبها اذ وجد في اراضي الجمهورية وكانت قد اتخذت في شانه اجراءات متابعة باسم الدولة الطالبة أو صدر حكم ضده من محاكمها .

ولا يجوز تسليم المجرمين الا اذا كانت الجريمة محل الطلب قد ارتكبت في اراضي الدولة الطالبة اومن رعاياها .

ويشترط المشرع الجزائري ان تكون الجريمة محل الطلب تشكل جناية أو جنحة تزيد عقوبتها عن سنتين ولا يجوز التسليم في الحالات الاخرى الا اذا كان المتهم قد عوقب بالحبس لأكثر من شهرين عن جريمة سابقة في تلك الدولة ، وعليه فان تسليم المجرمين المتهمين بارتكاب احد الجرائم الماسة بالمعاملات التجارية الالكترونية متوقف على تكييف

[1] عادل عبد العال ابراهيم خراشن ،المرجع السابق ، ص ص 41-42.

[2] المادة 82 من القانون رقم (16-01) المؤرخ في 06 مارس 2016 **يتضمن التعديل الدستوري**.

الدولة الطالبة لهذه الجرائم ،وكان من الافضل لو نص المشرع على ان تسليم المجرمين يشمل كافة الجرائم الواقعة في البيئة الالكترونية كونها جرائم عابرة للحدود [1].

رابعا- تكثيف التعاون الفني الدولي :

لا يكفي التعاون التشريعي على المستوى الدولي لا بد تعزيزها بالمساعدة الفنية وتبادل الخبرات والمعارف بين الدول ، كون ان سلطات الامن واجهزة العدالة ليست بذات الجاهزية والكفاءة لمواجهة الجريمة الالكترونية في جميع الدول انما تختلف من دولة الى اخرى بحسب درجة تقدمها ورقيها [2]، ومن هنا كانت الحاجة الملحة الى التعاون الدولي في مجال تدريب وتكوين رجال الامن والقضاء للاستفادة من مهارات وتجارب الاخرين من ذوي الكفاءة العلمية ،عن طريق تنظيم تدريبات تكوينية عالية المستوى للعاملين في اجهزة القضاء والمعنيين بمكافحة الجرائم الالكترونية [3]،وفي هذا الشأن قامت وزارة العدل مند سنة 2003 في اطار اصلاح العدالة ، بإطلاق برنامج تكوين خاص بسلك القضاة ، هدفه رفع مستوى اداءهم ليواكب التطور القانوني الجاري في نظام الاجرام الالكتروني ومن خلاله تم ادراج مادة " الجريمة الالكترونية " في برنامج تكوين طلبة المدرسة الوطنية للقضاء يتم دراستها على شكل ملتقيات ينشطها خبراء واشراكهم في الدورات التكوينية في مختلف الجرائم الالكترونية التي تنظم بالخارج خصيصا للسادة القضاة واطارات وزارة العدل في اطار التعاون الثنائي.

---

[1] الهادي خضراوي، **تجربة الجزائر في مكافحة الجريمة المعلوماتية المؤتمر الدولي** ، ص 168.

[2] امر فرج يوسف ،**الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت** . مكتبة الوفاء القانونية :الاسكندرية 2011 ص 430.

[3] إقلولي محمد ،**التحقيق الجنائي في الجرائم الالكترونية** .أطروحة لنيل شهادة الدكتوراه في العلوم ،تخصص القانون جامعة مولود معمري :تيزي وزو 2018 ص ص 310-311.

المبحث الثاني

الهياكل الخاصة لمواجهة الجرائم الالكترونية

مما سبق تبين لنا أن الجرائم الالكترونية هي من أخطر التحديات الامنية التي تواجه أعضاء المجتمع الدولي ، فهي جرائم معقدة ترتكب بوسائل تقنية حديثة من قبل مجرمين على مستوى عال من الذكاء والخبرة ، بحيث ان الصورة التقليدية لإجراءات التحقيق التي تقوم بها الجهات المكلفة بالبحث والتحري عن الجريمة لا تتماشى وطبيعة الجرائم الالكترونية ، لذلك استحدث المشرع الجزائري قانون 09-04 المتعلق بالجرائم المتصلة بتكنولوجيا الاعلام والاتصال ،وكذا تعديل قانون الاجراءات الجزائية خاصة فيما تعلق باستحداث هيئات معينة تتعامل مع هذه الجريمة من الناحية الاجرائية في اطار الاقليم الجزائري كله مع مراعاة الاختصاص الداخلي والخارجي من أجل المكافحة الفعالة للجريمة الالكترونية ومحاصرتها ،وعلى اثره تطرح الاشكالية التالية :

ماهي الهيئات الخاصة التي استحدثها المشرع الجزائري لمواجهة الجرائم الالكترونية ؟

وللإجابة عن هذه الإشكالية قسمنا هذا المبحث إلى مطلبين نتطرق فيهما إلى الهيئات الفنية المتخصصة في البحث والتحري عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال كمطلب أول نتحدث فيه عن الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في فرعه الأول ثم نتطرق إلى الوحدات التابعة للأمن الوطني وللدرك في الفرع الثاني .

أما المطلب الثاني فقد خصصناه للهيئات القضائية المختصة للبت في الجرائم الالكترونية من خلال دراسة الأقطاب المتخصصة في ظل مرسوم 16-267 في الفرع الأول ،والقطب الجزائي المتخصص في جرائم المعلوماتية في ظل المرسوم 21-11 في الفرع الثاني .

المطلب الأول

الهيئات الفنية المتخصصة في البحث والتحري عن الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال

دعمت الجزائر منظومتها القانونية سنة 2009 بالقانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال والحد منها ، وعليه سنتطرق من خلال هذا القانون الى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ثم الى الوحدات التابعة للدرك والامن الوطني في الفرع الثاني .

الفرع الأول :الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال

نص قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال والحد منها في الفصل الخامس منه على انشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ،ويعتبر هذا التشريع نقلة نوعية في النصوص الاجرائية الجزائية من خلال مراقبة الاتصالات السلكية واللاسلكية والمراسلات الالكترونية والاتصالات الهاتفية وكذا مراقبة المعطيات الشخصية على الانترنت مع مراعاة الحق الدستوري للمواطن في حرمة حياته ومراسلاته من المساس بها بداعي مكافحة الجرائم، وبغرض تفعيل نص المادة 13 من القانون 09-04 فقد صدر في البداية المرسوم الرئاسي 15-261 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ، ثم صدر بعد ذلك مرسوم رئاسي 19-172 المؤرخ في 2019/06/06 المعدل بالإلغاء لأحكام المرسوم الرئاسي السابق بسبب الظروف السياسية والأمنية التي عرفتها البلاد خاصة المخاطر التي تعرض لها الأمن العمومي وكذا المؤسسات الدستورية حيث تم بموجب هذا القانون نقل الهيئة من اشراف وزارة العدل الى وزارة الدفاع وتحولها بالنتيجة الى هيئة ذات طابع أمني ، ثم جاء المرسوم الرئاسي 21-439 المؤرخ في 2021/11/07 المتضمن اعادة تنظيم الهيئة .

أولا : تعريف الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال :تعتبر الهيئة حسب المرسوم الرئاسي رقم 15-261 سلطة ادارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى وزير العدل، لكن الامر تغير سنة 2019 حيث تراجع المشرع عن تكييف هذه الهيئة وحولها الى مؤسسة عمومية ذات طابع ذات طابع اداري تتمتع بالشخصية المعنوية والاستقلالية المالية تحت وصاية وزارة الدفاع الوطني بموجب المرسوم الرئاسي 19-172 المؤرخ في 2019/06/06 .[1]

وبالرجوع الى المرسوم الرئاسي 21-439 في مادتيه الثانية والثالثة حيث تنص المادة الثانية : الهيئة سلطة ادارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي ، توضع لدى رئيس الجمهورية .

المادة الثالثة : يحدد مقر الهيئة بمدينة الجزائر ويمكن نقله الى أي مكان آخر من التراب الوطني بموجب مرسوم رئاسي . [2]

فالمشرع الوطني كان يعتبرها أول مرة مؤسسة مدنية ثم اصبحت مؤسسة تخضع لوصاية وزارة الدفاع الوطني ، ثم عاد وجعلها تحت وصاية رئيس الجمهورية ، نتيجة للظروف السياسية والامنية التي عرفتها البلاد في تلك الفترة مما أدى الى ظهور مخاطر فعلية على الامن القومي والمؤسسات الدستورية هذا ما حتم ان تصبح هيئة ذات طابع أمني ،سيما وأنها تهدف للوقاية من الأفعال الموصوفة بأعمال ارهابية أو تخريبية والمساس بأمن الدولة ، ثم عاد وأتبعها لرئيس الجمهورية [3]،وأخضعها للرقابة القضائية باعتبار السلطة القضائية الضامنة للحقوق والحريات وهذا ما نصت عليه المادة الرابعة من المرسوم أعلاه.

---

[1] خرشي الهام، **النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها**، مجلة الابحاث القانونية والسياسية ، مجلد04 العدد01 جامعة محمد لمين دباغين سطيف 2 ، سنة 2022، تاريخ قبول المقال 2022/03/18 ،ص 60 .

[2] المرسوم الرئاسي 21-439المؤرخ في 07 نوفمبر 2021،**المتضمن اعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها** ، الجريدة الرسمية للجمهورية الجزائرية عدد 86 .

[3] عمارة زينب ، **الوقاية من الجرائم الالكترونية** .ملقاة على طلبة السنة الثانية ماستر ، تخصص اعلام آلي وانترنت ، ،كلية الحقوق والعلوم السياسية ،جامعة محمد البشير الابراهيمي: برج بوعريريج .2021-2022.

ثانيا : مهام الهيئة : رغم أن قانون 09-04 قد نص في المادة 14 منه على مهام الهيئة بصفة واضحة الا أن المرسوم الرئاسي 21-439 فصل في هذه المهام ووزعها على مجلس التوجيه ، المديرية العامة ، مديرية المراقبة الوقائية واليقظة الإلكترونية وقد نصت المادة الرابعة منه على [1]: تكلف الهيئة بما يلي :

– تحديد الاستراتيجية الوطنية للوقاية من المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ووضعها حيز التنفيذ .

– تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها .

– ضمان المراقبة الوقائية للاتصالات الالكترونية ،تحت سلطة القاضي المختص ، قصد الكشف عن الجرائم المتصلة بالأعمال الارهابية أو التخريبية أو التي تمس بأمن الدولة .

– كما تضمن الهيئة بالتنسيق مع المصالح المختصة لوزارة الدفاع الوطني المراقبة الالكترونية عندما يتعلق الامر بأمن الجيش ، وفقا لنفس الشروط المنصوص عليها في التشريع الساري المفعول .

– تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل استعمالها في الاجراءات القضائية .

– المساهمة في تكوين المحققين المختصين في مجال التحريات التقنية المتصلة بتكنولوجيات الاعلام والاتصال.

– المساهمة في تحيين المعايير القانونية في مجال اختصاصها .

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، عن طريق جمع المعلومات والتزويد بها وانجاز الخبرات القضائية.

[1] المرسوم الرئاسي 21-439 **المتضمن اعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها .**

– تطوير التعاون مع المؤسسات والهيئات الوطنية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

– السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها ، وفقا لأحكام المادتين 17 و18 من القانون رقم 09–04 المؤرخ في 05 غشت 2009 والمذكور أعلاه .[1]

ثالثا: تشكيلة الهيئة وتنظيمها :اختلف تنظيم الهيئة ما بين المرسوم الرئاسي رقم 15–261 والمرسوم الرئاسي رقم 21–439فيما يتعلق بتشكيلها ، حيث كانت الهيئة في ظل المرسوم الرئاسي رقم 15–261 تضم مجموعة من الهياكل تمثل في : اللجنة المديرة ، مديرية عامة ، مديرية للمراقبة الوقائية واليقظة الالكترونية ، مديرية للتنسيق التقني ، مركز العمليات التقنية ، ملحقات جهوية .

أما بعد صدور المرسوم الرئاسي رقم 21–439 فقد أصبحت الهيئة مكونة من جهازين اثنين هما : مجلس التوجيه ومديرية عامة طبقا لنص المادة 05 من هذا المرسوم .

1– **مجلس التوجيه :**حددت المادة 06 من المرسوم الرئاسي 21–439 تشكيلة مجلس التوجيه من ممثلي الوزارات الآتية : الامين العام لوزارة الشؤون الخارجية والجالية الوطنية بالخارج ، الامين العام لوزارة الداخلية والجماعات المحلية والتهيئة العمرانية الأمين العام لوزارة العدل ، الامين العام لوزارة البريد والمواصلات السلكية واللاسلكية قائد الدرك الوطني ، المدير العام للأمن الداخلي ، المدير المركزي لأمن الجيش لأركان الجيش الوطني الشعبي ، المدير العام للأمن الوطني ، رئيس مصلحة الدفاع السيبيراني ومراقبة أمن الأنظمة لأركان الجيش الوطني الشعبي ، ممثل عن رئاسة الجمهورية يعينه رئيس الجمهورية .

2– **المديرية العامة :**بموجب المادة 09 من المرسوم الرئاسي 21–439 اكتفى بوضعها تحت ادارة مدير عام وتضم حسب المادة 11 منه: مديرية المراقبة الوقائية واليقظة

[1] المادة 04 من المرسوم الرئاسي رقم 21-439 ،**المتضمن اعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها .**

الالكترونية ،مديرية الادارة والوسائل ، مصلحة للدراسات والتلخيص ، مصلحة للتعاون واليقظة التكنولوجية ، ملحقات جهوية .

رابعا :كيفية سير الهيئة :حسب ما نصت عليه المـــادة 20 من المرسوم الرئاسـي 21-439 فقد تم الحاق القضاة بالهيئة لتسييرها وكذلك ضباط وأعوان للشرطة القضائية مؤهلون من المصالح العسكرية للأمن والدرك الوطني والامن الوطني ، مستخدمو الدعم التقني والاداري للمصالح العسكرية للأمن الوطني والدرك الوطني . وأضافت المادة 21 من نفس المرسوم أنه يمكن للهيئة ان توظف فئات أخرى من المستخدمين حسب الحاجة

يؤدي مستخدمو الهيئة الذين يدعون الى الاطلاع على المعلومات السرية اليمين القانونية أمام المجلس القضائي المختص اقليميا قبل تنصيبهم حسب القسم الذكور في المادة 22 من نفس المرسوم . ويلتزمون بذلك بالسر المهني وبواجب التحفظ[1] .

وهذ قصد الوقاية من الأفعال الموصوفة بجرائم الارهاب أو التخريب أو التي تمس بأمن الدولة ومكافحتها ، تكلف الهيئة حصريا في مجال اختصاصها بمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها داخل منظومة معلوماتية تحت سلطة قاض لدى الهيئة وفقا للأحكام المنصوص عليها في المادة 04 من القانون 09-04 كما تخضع اجراءات التفتيش والحجز لأحكام قانون الاجراءات الجزائية وقد فصلنا في هذه النقطة سابقا .

الفرع الثاني : الوحدات التابعة للأمن الوطني والدرك

من أجل تحقيق المواجهة الفعالة لظاهرة الإجرام الالكتروني فقد قام المشرع الجزائري بموجب المادة 16الفقرتين 7- 8والمادة 16 مكرر من قانون الإجراءات الجزائية المعدل بالقانون 06-22 بتمديد الاختصاص الكلي لضباط الشرطة القضائية إلى كامل الإقليم الوطني[2]، وبناءا على هذا النص أصبح بمقدور الضبطية القضائية ممارسة جميع

[1] المادة 04 من نفس المرسوم الرئاسي رقم 21- 439 ،**المتضمن اعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.**

[2] قانون 06-22 مؤرخ في 20 ديسمبر 2006يتم الامر 66 -156 المؤرخ في 08 يونيو1966 **المتضمن قانون الاجراءات الجزائية**، الجريدة الرسمية، العدد 84 الصادر بتاريخ 24 ديسمبر 2006.

إجراءات البحث والتحري التي تدخل ضمن صلاحياتها عبر كافة الإقليم الوطني إذا تعلق الأمر بالجرائم الماسة بالمعالجة الآلية للمعطيات .[1]

حيث سعت المديرية العامة للأمن الوطني وكذا جهاز الدرك الوطني الى إنشاء فرق خاصة لمكافحة الجرائم المعلوماتية ،وكذا تكوين عناصر متخصصة في هذا المجال سواء على المستوى الداخلي أو الخارجي ، بالإضافة إلى توافر هذين الجهازين على مخبرين علميين للشرطة العلمية والتقنية يتوفران غل احدث الأجهزة التكنولوجية المتطورة لكشف هذا النوع من الإجرام [2].

أولا: الوحدات التابعة لسلك الأمن الوطني : تضع مديرية الامن الوطني في اطار تحديد سياسة أمنية فعالة ، كافة الامكانيات البشرية والتقنية الفعالة المتاحة لديهم من أجل التصدي لكل أنواع الجرائم بالخصوص تلك المستحدثة منها كالجرائم الالكترونية والتي تعتبر نتاج القصور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات الاعلام والاتصال ، بهدف حماية المصلحة العامة وكذلك المصالح الخاصة .

توجد على مستوى جهاز الامن الوطني ثلاث وحدات مكلفة بالبحث والتحقيق في الجرائم المعلوماتية وهي كالآتي : المخبر المركزي للشرطة العلمية بالجزائر العاصمة ، المخبر الجهوي للشرطة العلمية بقسنطينة ، المخبر الجهوي للشرطة العلمية بوهران .

ثانيا : الوحدات التابعة للقيادة العامة للدرك الوطني :إضافة للهيئات التابعة للأمن الوطني، هناك هيئات تابعة للدرك الوطني حيث تلعب مختلف المصالح الجهوية للشرطة القضائية التابعة للدرك الوطني دورا هاما في مجال مكافحة الجريمة المعلوماتية ،وتتميز مختلف الفصائل بخبرة وكفاءة عالية في مكافحة الجريمة المعلوماتية كما يوجد على المستوى المركزي هيئات تتكفل بمكافحة الجريمة المعلوماتية يمكن إجمالها في :

[1] براهيمي جمال ،**التحقيق الجنائي في الجرائم الالكترونية** . أطروحة لنيل شهادة الدكتوراه في العلوم تخصص قانون، جامعة مولود معمري تيزي وزو ، تاريخ المناقشة 2018/06/27 ، ص ص 261-262 .

[2] محمد بوعمرة– سيد علي بنينال،**جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري** ، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية تخصص قانون الاعمال جامعة آكلي محند اولحاج :البويرة ، 2020/2019 ، ص 33 .

1- **المعهد الوطني للأدلة الجنائية وعلم الاجرام :**أنشأ المعهد بموجب المرسوم الرئاسي 04-183 ،ويعتبر هذا المعهد مؤسسة عمومية ذات طابع اداري تحت الوصاية المباشرة لوزير الدفاع الوطني مكلف بإجراء الفحوص العلمية في اطار التحريات الاولية ،واجراء بحوث متعلقة بالكشف عن الإجرام ، باللجوء الى التكنولوجيا الدقيقة ويحتوي على مجموعة من المصالح : مصلحة البصمات ،ومصلحة الإعلام الآلي حيث يتم على مستوى هذه المصلحة رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية وتفكيك البرامج المعلوماتية .

2- **مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني :**أنشأ هذا المركز سنة 2008 ويهدف الى تحليل معطيات وبيانات الجرائم المعلوماتية ،وتحديد هوية أصحابها سواء كانوا فرادى أو جماعات ،والتي قد تستهدف خاصة المؤسسات الرسمية ، البنوك ،وحتى الأفراد ، كما يهدف الى مساعدة باقي الأجهزة الاخرى في أداء مهامها ، خاصة فيما يلي : ضمان المراقبة الدائمة والمستمرة على شبكة الانترنت ، القيام بمراقبة الاتصالات الالكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية ، مساعدة الوحدات الاقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الاعلام والاتصال والبحث عن الادلة ، المشاركة في عمليات التحري والتسرب عبر شبكات الانترنت لفائدة وحدات الدرك الوطني والسلطات القضائية ، المشاركة في قمع الجرائم المعلوماتية من خلال التعاون مع مختلف مصالح الامن والهيئات الوطنية .[1]

3- **مديرية الامن العمومي والاستغلال :**وهي الهيئة التي تعمل على التنسيق بين مختلف الوحدات الاقليمية والمركز التقني العلمي في مجال أعمال البحث والتحري في الجرائم المعلوماتية .

4- **المصلحة المركزية للتحريات الجنائية :**وهي هيئة ذات اختصاص وطني من بين مهامها مكافحة الجريمة المرتبطة بتكنولوجيا الاعلام والاتصال .

[1] رابح سعاد، **ضوابط مكافحة الجريمة المعلوماتية** .مجلة القانون العام الجزائري والمقارن ، مجلد07 العدد01 جامعة جيلالي اليابس - سيدي بلعباس الجزائر 2021، تاريخ قبول المقال 2021/05/21 ،ص ص 280-281 .

المطلب الثاني

الهيئات القضائية

مفهوم القطب :القطب أو الاستقطاب في اللغة هو الجذب أو التجميع نحو نقطة أو مكان واحد

وفي الاصطلاح القانوني بالخصوص في مجال التنظيم القضائي الحديث هو تركيز اختصاصات اقليمية لجهات قضائية متفرقة على عديد المناطق في يد جهة قضائية واحدة، شريطة ان يتعلق الامر بتشكيلة من الاختصاصات النوعية المحددة على سبيل الحصر وبعبارة أخرى أضحى يعرف ذلك بالتخصص القضائي ،وتزود هذه الجهات بالوسائل المادية والبشرية والقانونية اللازمة بغية اعطاء للعملية القضائية المستوى المطلوب من المعالجة لبلوغ حد من النجاعة وتحقيق العدالة[1] .

الفرع الأول : الاقطاب المتخصصة في ظل مرسوم 16-267

عكف المشرع الجزائري وقبله التشريعات المقارنة خاصة المشرع الفرنسي الى استحداث الأقطاب الجزائية المتخصصة وهي محاكم ذات اختصاص اقليمي موسع بموجب القانون 04-14 المؤرخ في 10نوفمبر 2004 المعدل والمتمم لقانون الاجراءات الجزائية الجزائري الذي أجاز توسيع اختصاص بعض المحاكم ووكلاء الجمهورية وقضاة التحقيق في جرائم محددة على سبيل الحصر وتوصف أنها خطيرة وعلى درجة عالية من التعقيد والتنظيم وهي : جرائم المخدرات ، الجريمة المنظمة العابرة للحدود الوطنية ، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، تبييض الأموال ، الجرائم الإرهابية والتخريبية وجرائم مخالفة التشريع الخاص بالصرف .

ولقد تم بالفعل صدور النص التنظيمي الخاص الذي مدد الاختصاص لأربع جهات قضائية المرسوم رقم 06-348 المؤرخ في 2006/10/05 المعدل والمتمم بالمرسوم التنفيذي 16-267 المؤرخ في 2016/10/17 والذي تم بموجبه تحديد هذه المحاكم مع

[1] محمد بكرارشوش، **الاختصاص الاقليمي الموسع في المادة الجزائية في التشريع الجزائري** ،العدد 14 كلية الحقوق والعلوم السياسية جامعة قاصدي مرباح ورقلة 2016،ص 305 .

تعديل طفيف في المرسوم بحيث شمل التقسيم اضافة بعض المجالس القضائية بمقتضى المواد 3-4-5 المعدلة للمواد 3-4-5 من المرسوم السابق ،وجاء التقسيم كالتالي :

- محكمة سيدي محمد الجزائر العاصمة ،ويمتد اختصاصها الإقليمي إلى المجالس القضائية التالية : الجزائر، الشلف ،الأغواط ،البليدة ، تيزي وزو، الجلفة، المدية، المسيلة وبومرداس .

- محكمة قسنطينة ،ويمتد اختصاصها الإقليمي إلى المجالس القضائية التالية : قسنطينة أم البواقي ، باتنة ، بجاية ،تبسة ، جيجل ، سطيف ،سكيكدة ، عنابة ،قالمة ، برج بوعريريج ، الطارف ، خنشلة ، سوق أهراس وميلة .

- محكمة ورقلة ،ويمتد اختصاصها الإقليمي إلى المجالس القضائية التالية : ورقلة ،ادرار ،تمنغاست، اليزي ، بسكرة ،الوادي وغرداية .

- محكمة وهران ،ويمتد اختصاصها الإقليمي إلى المجالس القضائية التالية : وهران بشار، تلمسان ، تيارت ، تندوف ، سعيدة ، سيدي بلعباس ، مستغانم ، معسكر، البيض تيسمسيلت ،النعامة ،عين تموشنت وغليزان .

بحيث يشمل اختصاص كل جهة قضائية مجموعة من المجالس القضائية تقع في منطقة جهوية من الجزائر ،شمالا ، جنوبا ، شرقا وغربا ،وذلك لدى أربع محاكم تسمى أقطابا جزائية ، كما تم تدعيم عمل هذه الأخيرة باستحداث وسائل التحري الخاصة لمواجهة الإجرام المنظم بما فيها الجريمة الالكترونية .[1]

الفرع الثاني : القطب الجزائي المتخصص في ظل أمر 21-11 المؤرخ في 25غشت 2021

إن اعتماد الجرائم الالكترونية في ارتكابها على تكنولوجيات التواصل والاتصال وتميزها بالطابع التقني وارتكابها في بيئة غير مادية ، بالإضافة إلى الانتشار الواسع لوسائل الإعلام والاتصال وتطورها السريع قد دفع إلى تدخل المشرع سنة 2021 لإنشاء قطب

[1] سعيدة بوزنون، **مكافحة الجريمة الالكترونية في التشريع الجزائري** ، مجلة العلوم الانسانية ، مجلد30 العدد03 جامعة الاخوة منتوري :قسنطينة الجزائر، 2019، تاريخ قبول المقال 2019/07/09 ،ص ص 54-55.

جزائي ذو اختصاص وطني يعنى بمكافحة جرائم تكنولوجيات الإعلام والاتصال ،وذلك من خلال تعديله قانون الإجراءات الجزائية بموجب الأمر رقم 21-11 المؤرخ في 25 غشت 2021 يتمم الأمر رقم 66-155 المؤرخ في 8يونيو1966 والمتضمن قانون الإجراءات الجزائية، بباب سادس عنوانه القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[1] .

جاء هذا القطب الجزائي في إطار تفعيل الجهاز القضائي، أو بالأحرى دعم جهاز العدالة للتمكن من متابعة هذه الجرائم التي أصبحت تشكل خطرا محدقا بالمجتمع وتمس بنسيجه الداخلي ، ولقد أفرد الأمر 21-11 بابا كاملا للقطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال موضحا جملة من الأحكام المتعلقة باختصاصاته .

أولا : دواعي انشاء القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال :ان استحداث قطب جزائي متخصص في جرائم الإعلام والاتصال يندرج ضمن دوافع موضوعية تتمثل في : الطبيعة الخاصة لهذا النوع من الجرائم وقد تطرق إليها المشرع الجزائري بموجب قانون 09-04 في الفقرة أ من المادة 02 كما فصلنا فيها سابقا والذي يستدعي نوعا من التخصص القضائي ،وكذا ضمن دوافع إجرائية تتعلق بالحاجة إلى تفعيل الجهاز القضائي الجزائري إذ أن النصوص الإجرائية الجزائية قد واجهت صعوبات جمة بخصوص المتابعة والتحقيق للكشف عن الجرائم الالكترونية ومعاقبة مرتكبيها .

ثانيا : اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال :نص الأمر 21-11 السلف ذكره على الأحكام المتعلقة بتحديد صلاحيات هذا القطب بما يساعده في رفع أداءه توافقا مع التطورات الحاصلة ،ومن ذلك قام المشرع بتوسيع الاختصاص المحلي لدى القطب ومنحه قواعد إجرائية خاصة من شأنها تفعيل التصدي للجرائم المتصلة بتكنولوجيات الإعلام ولاتصال ،وعلى ذلك سنتطرق إلى دراسة

[1]أمر رقم 21-11 المؤرخ في 25 غشت 2021 يتمم الامر رقم 66-155 المؤرخ في 8يونيو1966 **المتضمن قانون الإجراءات الجزائية** ، الجريدة الرسمية للجمهورية الجزائرية عدد 65 .

اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[1] .

1-الاختصاص المحلي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال :بالرجوع الى نص المادة 329 فقرة 05 من قانون الإجراءات الجزائية نجد أن المشرع الجزائري قام بتمديد الاختصاص المحلي لكل من وكلاء الجمهورية ، قضاة التحقيق ، محاكم مجالس قضائية ، في جرائم محددة تم ذكر من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .

ويبرر الخروج عن معايير الاختصاص الأصلية بخصوص الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب اختصاص محلي موسع مرده إلى اتساع مكان ارتكاب هذه الجرائم خارج حدود الاختصاص المحلي التقليدي من جهة ،وانتشار المكونة لعناصر هذه الجرائم الذي قد يكون عبر كامل التراب الوطني وقد يتعدى حدود الدولة نفسها من جهة أخرى ، الأمر الذي يجعل التمسك بالمعايير التقليدية للاختصاص يشكل عائقا أمام السيطرة على هذا النوع من الجرائم ومكافحته .

وهذا ما أكد عليه المشرع في نص المادة 211مكرر23 من الامر رقم 21-11 السابق ذكره ،والتي جاء فيها ما يلي : **يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، كذا قاضي التحقيق ورئيس ذات القطب صلاحيات في كامل الإقليم الوطني .**

غير أن هذا الاختصاص الموسع الى كامل التراب الوطني فصل فيه المشرع بشيء من الدقة في قيام اختصاص القطب المعني ،وذلك كالآتي :

- اختصاص حصري للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بموجب نص المادة 211مكرر26 من الأمر 21-11 ، خول المشرع

[1]بن عمير أمينة –بوحلايس الهام، **القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ،** مجلة البحوث في العقود وقانون الأعمال ، مجلد07 العدد01 جامعة الإخوة منتوري: قسنطينة 1 الجزائر، 2022، تاريخ قبول المقال 2022/01/18 ، ص ص ص 73-74-75 .

لهذا القطب اختصاصا حصريا في ما يخص الجرائم التي حددتها المادتين 211 مكرر24، و211 مكرر25 ، في كافة أنحاء التراب الوطني دون سواه، وذلك بالنظر الى خصوصية تلك الجرائم التي وجد من أجلها وبموجب تشكيلة خاصة من القضاة .

- **اختصاص مشترك للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال :** يمارس وكيل الجمهورية وكذا قاضي التحقيق ورئيس ذات القطب حسب نص المادة 211 مكرر27 اختصاصا مشتركا مع الاختصاص الناتج عن تطبيق المواد 37، 40، 329 من قانون الإجراءات الجزائية بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها .

- **اختصاص وجوبي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:** وهذا ما نصت عليه المادة 211 مكرر 28 في حالة ما إذا تزامن اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مع اختصاص القطب الاقتصادي والمالي ، يؤول الاختصاص وجوبا لهذا الأخير .

- وقد نصت المادة 211 مكرر 29 من الأمر 21-11 ،على حالة ما إذا تزامن اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مع اختصاص محكمة مقر مجلس قضاء الجزائر طبقا لأحكام المواد 211 مكرر 16 الى 211 مكرر 21 من نفس الأمر ، يؤول الاختصاص وجوبا لهذه الأخيرة[1]

2-الاختصاص النوعي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال :منح المشرع الجزائري لهذا القطب صلاحية الفصل بشكل حصري في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكذا الجرائم المرتبطة بها ،وذلك من خلال نص المادة 211 مكرر24 من الأمر 12-11 التي جاء فيها :**مع مراعاة أحكام الفقرة 2 من المادة 211 مكرر 22 أعلاه ، يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وقاضي**

[1] نص المادة 211 مكرر 29 من نفس الأمر السابق رقم 21-11.

التحقيق ورئيس ذات القطب، حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المذكورة أدناه وكذا الجرائم المرتبطة بها :

- الجرائم التي تمس بأمن الدولة او بالدفاع الوطني ، جرائم المساس بالأمن أو السكينة العامة أو استقرار المجتمع ،جرائم الاتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين ،جرائم التمييز وخطاب الكراهية .

بالإضافة إلى ما سبق مدد المشرع اختصاص القطب الجزائي الحصري إلى النظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا أو المرتبطة بها ايضا وذلك على أساس تعدد الفاعلين أو الشركاء ، أو المتضررين بسبب اتساع ارتكابها ، أو لطابعها المنظم الذي قد يكون عابرا للحدود الوطنية أو لمساسها بالنظام والامن العموميين والتي تستوجب المساعدة والتعاون القضائي الدولي لما تتطلبه من وسائل تحري خاصة وفنية ، حيث أنه سبق وان وسع الاختصاص في مجال المساعدة والتعاون القضائي الدولي في النظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للجهة القضائية المختصة بها والمرتكبة خارج الحدود الوطنية متى كان مرتكبها أجنبيا وتستهدف مؤسسات الدولة والدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني وهذا بموجب نص المادة 25 من القانون رقم 09-04 السابق الذكر .

خلاصة الفصل الثاني :

ختاما لهذا الفصل نجد أن المشرع الجزائري تدارك خطورة الجرائم الواقعة في البيئة الافتراضية باعتبارها دولة نامية، وعدم تحكمها النوعي في التكنولوجيا المتطورة ، سهل ارتكاب الجريمة الالكترونية ،وبالتبعية الإفلات من العقاب .

وعلى هذا الاساس تبني المشرع الجزائري سياسة مزدوجة للتصدي لظاهرة الإجرام المعلوماتي بحيث اهتدى من جهة إلى تعديل الجوانب الموضوعية والإجرائية للتشريعات العقابية العامة بما فيها قانون العقوبات وقانون الإجراءات الجزائية ، وجعلها تواكب التحديات الجديدة الناتجة عن التطور الهائل للتكنولوجيات الحديثة ، وقام من جهة ثانية باستحداث قوانين أخرى خاصة أكثر تجاوبا مع الطبيعة الخاصة للجرائم الالكترونية تجمع بين هدف الوقاية وذلك بالرصد المبكر للاعتداءات المحتملة ، وهدف المواجهة بالتدخل السريع لتحديد مصدرها ، كما عززه بالتعاون التشريعي والقضائي على المستوى الدولي بناءا على اتفاقيات دولية لمكافحة هذا النوع من الإجرام العابر للحدود .

كما دعمت الجزائر أساليب المواجهة من خلال استحداث وحدات وهيئات متخصصة أبرزها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ، بالإضافة الى وحدات تابعة لسلك الامن والدرك الوطني ، وانشاء الأقطاب القضائية المتخصصة في ظل المرسوم الرئاسي 16-267 وكذا القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب الأمر 21-11 المتمم للأمر رقم 66-155 المؤرخ في 08 يونيو 1966 والمتضمن قانون الإجراءات الجزائية يعد نقلة قانونية نوعية وجب تثمينها ، فمن خلال توسيع الاختصاص المحلي لهذا القطب ليشمل كامل التراب الوطني يعتبر اتجاها سليما وايجابيا من شانه أن يساهم بشكل فعال في الحد من تفاقم الإجرام الالكتروني الذي يحمل في طياته جرائم اقتصادية ومالية ،وكذلك الحال بالنسبة للإرهاب والجرائم الماسة بأمن الدولة .

خـاتمـــة :

بينا من خلال دراستنا انه بالرغم من النواحي الايجابية للأنظمة المعلوماتية ، الا انه ترتب عنها جوانب سلبية نجمت عن استغلال بعض الافراد والجهات للتقنيات المعلوماتية لتسهيل ارتكاب العديد من الجرائم ، كما اصبح النظام المعلوماتي ذاته محلا للاعتداء عليه واساءة استخدامه .

وقد اتضح لنا ان الجرائم الالكترونية ظاهرة اجرامية مستجدة تستهدف الاعتداء على المعلومات المخزنة أو المعالجة في نظام الحاسب الالي او المتبادلة عبر الشبكات ، فان طبيعتها المنفردة ادت الى صعوبة ادراجها ضمن الاوصاف التقليدية في القوانين الجنائية الوطنية نظرا للتطور السريع للجريمة الالكترونية من جهة، وللطابع العالمي والعابر للحدود من جهة اخرى، يتعين معه مواجهة هذه الجريمة بنصوص تجريمية جديدة.

وقد بينا من خلال ما سبق حرص المشرع الجزائري على مواكبة النهضة التكنولوجية والمعلوماتية من اجل تغطية وتلافي القصور التشريعي، وتفادي افلات المجرم الالكتروني من العقاب، فادخل تعديلات على قانون العقوبات لجعله يتجاوب مع هذه التطورات بموجب قانون رقم 04-15المؤرخ في 10-11-2004 المعدل والتمم للأمر رقـــم 66-156 المتضمن قانون العقوبات الذي تناول فيه بالتجريم مختلف الاعتداءات على نظم المعالجة الالية ، وتم تعزيزه بالقانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ، الذي جاء في وقته مسايرا للتطورات التكنولوجية، فضلا عن استحداث قواعد اجرائية اخرى تتلاءم مع الطبيعة الخاصة لهذا النوع من الجرائم كالمراقبة الالكترونية، واعتراض المراسلات والتسرب الالكتروني من اجل ضمان الفعالية في توقيع العقاب .

ولقد توصلنا من خلال هذه الدراسة الى النتائج التالية :

- عدم وجود اجماع فقهي بخصوص تعريف الجريمة الالكترونية، حيث تباينت التعريفات بين المفهوم الواسع والمفهوم الضيق .

-صعوبة حصر الجرائم في انواع محددة نتيجة التطور السريع التي تشهده مثل تلك الجرائم .

– بالنسبة لنطاق العقوبة فان المشرع الجزائري تدارك النقص الذي كان موجود في التشريع العقابي ، ورغبة منه في القضاء على الجريمة الالكترونية وتقديرا منه لخطورة هذا النوع من الجنح ، وسع نطاق العقوبة لتشمل من حيث الافعال اعمال الشروع في التنفيذ ومن حيث الاشخاص المشاركين في التحضير لجنح الجرائم المعلوماتية في اطار الاتفاق الجنائي .

– بالنسبة للعقوبات التكميلية ،تبين لنا ان المشرع الجزائري قد نص على المصادرة والغلق كعقوبة تكميلية وجوبية للعقوبة السالبة للحرية في جرائم الاعتداء على النظم المعلوماتية فقد كانت لها الفعالية في مواجهتها ، وتحقيقا لمبد تفريد العقوبة .

–ان المشرع الجزائري اعتمد على العقاب كأسلوب وقائي رادع من خلال تبينه ترسانة عقابية رادعة واسعة النطاق ، يعتبر جزء من الحل ولا يكفي وحده لإبعاد هذا الخطر بل لا بد من تدعيمه بوسائل وقائية اخرى تتناسب والطبيعة التقنية لهذه الجرائم، ويتجلى هذا من خلال الاجراءات المنصوص عليها في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته كمراقبة الاتصالات الالكترونية ، التفتيش ، حفظ المعطيات

– اظهر البحث انه رغم الجهود التي يبذلها المشرع الجزائري في سبيل التصدي لظاهرة الاجرام الالكتروني، الا انها غير كافية نتيجة القصور الذي يعتري النصوص العقابية القائمة، وبسبب التطورات السريعة والمستمرة التي تعرفها هذه الظاهرة ومن جهة اخرى الطابع العالمي والعابر للحدود.

وعليه على ضوء النتائج توصلنا إلى المقترحات التالية :

– حوكمة المنظومة التشريعية الوطنية لمواجهة الجريمة المعلوماتية ، وذلك بالمراجعة الدورية والمستمرة بما يضمن مواكبة وتطورات هذه الجريمة ،وارساء قواعد قانونية جديدة خاصة تواجه المشكلات المعاصرة التي اسفرت عليها هذه الجريمة المستحدثة وتطوراتها اللامتناهية .

– ضرورة تشديد الوصف الجنائي والعقوبات المقررة للأنماط الاجرامية للجريمة المعلوماتية ، بغية تحقيق الردع والقضاء على الاجرام المعلوماتي .

– العمل على وضع مواقع الكترونية مخصصة للتبليغ عن جرائم تقنية المعلومات بصفة عامة وارسالها الى الجهات المختصة وهوما يصطلح عليه " البلاغ الرقمي" .

– تفعيل دور وسائل الاعلام في توعية مستخدمي الوسائط الالكترونية بمعدلات حدوث الجرائم الواقعة عليه ، كيفية حدوثها ، طبيعتها ، مخاطرها وحجم الخسائر واضرارها .

– الاعتماد على نظام التكوين والتدريب المستمرين لرجال القانون في مجال الجرائم المعلوماتية حتى يتسنى الالمام بكافة النصوص والاجراءات المتبعة في هذا النوع من الجرائم، وتنشيط دورات تكوينية مستمرة من قبل خبراء ومختصين لمواكبة ودراسة ومتابعة المستجدات على الساحة العالمية .

– تعزيز وتدعيم التعاون العربي في مجال التشريعي والقضائي والامني لمكافحة الجريمة الالكترونية ، ولما لا مع الدول الغربية الاكثر دراية في هذا المجال والاستفادة من تجاربها كونها الاسبق في المكافحة .

– ابرام اتفاقيات ومعاهدات دولية ثنائية او متعددة الاطراف في مجال التعاون الدولي، التي تهدف من وراء ذلك التقريب بين القوانين الجزائية الوطنية في اطار مكافحة الجرائم العابرة للقارات .

– ضرورة توحيد النظام التشريعي في قانون خاص لمكافحة الجرائم الالكترونية ، يلم بكل النصوص الموضوعية والاجرائية والتنظيمية وهوما يسهل عمل الهيئات القضائية والجهاز الامني .

أسمـاء المراجـع :

الكتـب

01-ابراهيم خالد ممدوح، فن التحقيق الجنائي في الجرائم الالكترونية 2009 ،دار الفكر الجامعي الاسكندرية.

02-ابراهيم خالد ممدوح ،الجرائم المعلوماتية، الطبعة الثانية 2019 ،دار الفكر الجامعي الاسكندرية.

03-أحمد طه محمود ، المواجهة التشريعية لجرائم الكمبيوتر والأنترنت ، دار الفكر والقانون 2013 المنصورة.

04-أحمد السيد عبد الحميد ،جرائم الشبكة العنكبوتية وغسل الاموال في اطار الملاحقة الامنية والقضائية الدولية ،مكتبة الوفاء القانونية 2018 الاسكندرية .

05-أحمد لطفي خالد حسن ، جرائم الانترنت بين القرصنة الالكترونية وجرائم الابتزاز الالكتروني، دراسة مقارنة، ، دار الفكر الجامعي، 2018الإسكندرية .

06-الشمري غانم مرضى الجرائم المعلوماتية (ماهيتها خصائصها ، كيفية التصدي لها قانون طبعة 2016 الدار العملية الدولية للنشر والتوزيع .

الأسدي لينا محمد ، مدى فعالية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية دراسة مقارنة، طبعة 2015 ، دار ومكتبة الحامد للنشر والتوزيع ، عمان.

07-الشوابكة محمد امين، جرائم الحاسوب والانترنت (الجريمة المعلوماتية) ، طبعة 2009 دار الثقافة عمان.

08-الطوالبة علي حسن، الجريمة الالكترونية ،جامعة العلوم التطبيقية، طبعة 2008 مملكة البحرين.

09-الطوالبة علي حسن، التفتيش الجنائي على نظم الحاسوب والانترنيت دراسة مقارنة ، طبعة 2004 عام الكتب الحديث الاردن .

10-بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الالية في التشريع الجزائري المقارن طبعة 2012منشورات الحلبي الحقوقية ، مستغانم الجزائر.

11-خراشن عادل عبد العال ابراهيم ،اشكالية التعاون الدولي في مكافحة الجريمة المعلوماتية وسبيل التغلب عليها، طبعة 2015 ،دار الجامعة الجديدة الاسكندرية .

12- زين الدين بلال امين ،جرائم نظم المعالجة الالية للبيانات في لتشريع المقارن، طبعة 2006 دار الفكر الجامعي الاسكندرية.

13-عبد الله عبد الله عبد الكريم، الحماية القانونية لحقوق الملكية الفكرية على شبكة الانترنت، طبعة 2008 دار الجامعة الجديدة الازاربطة .

14- فاروق ياسر الامير، مراقبة الاحاديث الخاصة في الاجراءات الجنائية دراسة تأصيلية تحليلية ومقارنة للتنصت على المحادثات التليفونية والتي تجرى عبر الانترنت والاحاديث الشخصية نظريا وعمليا، طبعة 2009، دار المطبوعات الجامعية الاسكندرية.

15-موسى مصطفى محمد ،التحقيق الجنائي في الجرائم الالكترونية، طبعة 2008 مطابع الشرطة – شارع المرور القاهرة.

16-فرج يوسف امر، الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، طبعة 2011مكتبة الوفاء القانونية الاسكندرية.

17-الملطأحمد خليفة، الجرائم المعلوماتية، الطبعة الثانية2006، دار الفكر الجامعي الاسكندرية.

18-يوسف امير فرج، الجرائم المعلوماتية على شبكة الانترنت، طبعة 2011دار المطبوعات الجامعية الاسكندرية.

المقـالات

01-الهام خرشي، النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ، مجلة الابحاث القانونية والسياسية ، مجلد04 العدد01 جامعة محمد لمين دباغين سطيف 2 ، 2022، تاريخ قبول المقال 2022/03/18 .

02-أمينة بن عميور– الهام بوحلايس، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ، مجلة البحوث في العقود وقانون الأعمال ، مجلد07 العدد01 سنة 2022،جامعة الإخوة منتوري قسنطينة 1 الجزائر، تاريخ قبول المقال 2022/01/18 .

03-بشرى غريبي، خصوصية المجرم المعلوماتي ودوافعه ، مجلة نوميروس الاكاديمية مجلد02 العدد02 سنة2021، جامعة أبوبكر بلقايد تلمسان ، تاريخ قبول المقال 2021/05/09 .

04-بكرارشوش محمد الاختصاص الاقليمي الموسع في المادة الجزائية في التشريع الجزائري دفاتر السياسة والقانون، العدد 14 سنة 2016 كلية الحقوق والعلوم السياسية جامعة قاصدي مرباح :ورقلة ، سعيدة

05- بوزنون سعيدة ، مكافحة الجريمة الالكترونية في التشريع الجزائري ، مجلة العلوم الانسانية مجلد30 العدد03 جامعة الاخوة منتوري قسنطينة الجزائر 2019، تاريخ قبول المقال 2019/07/09.

06-زينب عمارة محاضرات ملقاة على طلبة السنة الثانية ماستر ، تخصص اعلام آلي وانترنت ، الوقاية من الجرائم الالكترونية ،كلية الحقوق والعلوم السياسية ،جامعة محمد البشير الابراهيمي برج بوعريريج .2021-2022.

07- سعاد رابح ،جامعة جيلالي اليابس ، ضوابط مكافحة الجريمة المعلوماتية ،مجلة القانون العام الجزائري والمقارن ، مجلد07 العدد01 سنة 2021، سيدي بلعباس الجزائر تاريخ قبول المقال 2021/05/21 ،صفحة 280-281 .

08-سهام خليلي ،خصوصية المجرم الالكتروني. مجلة المفكر مجلد02 العدد15 جامعة أمحمد لمين دباغين سطيف، جوان 2017 .

09-محمد رحموني ،خصائص الجريمة الالكترونية ومجالات استخدامها ، مجلة الحقيقة العدد 41 ، جامعة أحمد دراية : أدرار تاريخ قبول المقال للنشر 2018/01/10

10-محمد أمينبكوش-هروال نبيلة هبة ، خصوصية المجرم الالكتروني-مجرم الأنترنت نموذجا-مخبر البحث في تشريعات حماية النظام البيئي، مخبر البحث في تشريعات حماية الوظيفة العامة ، مجلة البحوث في الحقوق والعلوم السياسية ، مجلد 07 العدد 01 سنة 2021،جامعة تيارت الجزائر تاريخ قبول المقال للنشر 2021/05/25.

المذكـرات والاطـروحات العلميـة

01-بوعمرة محمد- بنينال سيد علي ، جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية تخصص قانون الاعمال جامعة آكلي محند اولحاج البويرة ،السنة الجامعية 2019/.2020

02- عائشة بوخبزة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري. مذكرة ماجستير في القانون الجنائي، كلية الحقوق جامعة وهران الجزائر 2012-2013.

03-فيصل بدري ،مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي اطروحة لنيل شهادة الدكتورا علوم تخصص قانون عام، كلية الحقوق جامعة الجزائر 2017-2018 .

04-محمد إقلولي، التحقيق الجنائي في الجرائم الالكترونية، اطروحة لنيل شهادة الدكتوراه في العلوم تخصص القانون، جامعة مولود معمري تيزي وزو سنة 2018 .

القـوانيـن

01/القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المتمم لقانون العقوبات الجريدة الرسمية العدد 71 الصادر بتاريخ 10 نوفمبر .2004

02/ قانون 06-22 مؤرخ في 20 ديسمبر 2006يتم الامر 66 -156 المؤرخ في 08 يونيو1966، المتضمن قانون الاجراءات الجزائية الجريدة الرسمية العدد 84 الصادر بتاريخ 24 ديسمبر 2006 .

03-قانون 04-14 مؤرخ في 10نوفمبر2004،المعدل لقانون الاجراءات الجزائية.

04/امر رقم 03-05 مؤرخ في 19 جمادي الاولى عام 1424 الموافق 19 يوليو2003 يتعلق بحقوق المؤلف والحقوق المجاورة .

05/ القانون رقم 09-04 المؤرخ في 05 اوت 2009، المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها الجريدة الرسمية العدد 47 بتاريخ 16 اوت 2009.

06/القانون رقم 01/16 مؤرخ في 06 مارس يتضمن التعديل الدستوري جريدة رسمية العدد 14 الصادرة في 07 مارس 2016.

07/قانون رقم 2000-03 المؤرخ في 05 اوت 2000 ،المتعلق بالقواعد العامة المتعلقة بالبريد والموصلات السلكية وللاسلكية .

08/المرسوم الرئاسي 21-439 المؤرخ في 07 نوفمبر 2021 المتضمن اعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ، الجريدة الرسمية للجمهورية الجزائرية عدد 86 .

المحاضرات

01- بوحليط يزيد ،تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري ، مجلة التواصل في الاقتصاد والادارة والقانون ،كلية الحقوق والعلوم السياسية، جامعة باجي مختار عنابة .

02- جمال براهيمي ،محاضرات في مكافحة الجريمة الالكترونية في التشريع الجزائري ، كلية الحقوق والعلوم السياسية ،جامعة مولود معمري بتيزي وزو.

03-عماد دمان ذبيح- سمية وبهلول ،الاليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري ،جامعة محمد لمين دباغين سطيف 2 تاريخ النشر 2020/01/05.

المداخلات العلمية

01-أمنة محمدي برنية، اجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الاجراءات الجزائية (وقانون الرقابة من جرائم الاعلام) .

02-الملتقى الوطني- اليات مكافحة الجريمة الالكترونية في التشريع الجزائري الجزائر العاصمة 29 مارس 2017 .

03-خضراوي الهادي ،تجربة الجزائر في مكافحة الجريمة الالكترونية ،المؤتمر الدولي لمكافحة الجرائم المعلوماتية كلية العلوم الحاسب، جامعة الامام محمد بن سعود الاسلامية

04-مسعود موسى،ارجومة الاشكاليات الاجرامية التي تثيرها الجريمة المعلوماتية عبر الوطن المؤتمر المغاربي اول.

05-نور الدين بوجاني، اساليب البحث والتحري الخاصة واجراءاتها وفقا لقانون رقم 06-22 المؤرخ في 20-12-2006 مداخلة في يوم دراسي حول علاقة النيابة العامة بالشرطة القضائية احترا حقوق الانسان ومكافحة الجريمة المديرية العامة للأمن الوطني المنعقد باليزي الجزائر .

فهـرس الموضــوع	رقم الصفحة
مقــدمــة	**02**
الفصل الاول : ماهية الجريمة الالكترونية	**09**
المبحث الاول : مفهوم الجريمة الالكترونية	**10**
المطلب الاول :تعريف الجريمة الالكترونية	**10**
الفرع الاول : التعريف اللغوي والاصطلاحي للجريمة الالكترونية	**11**
الفرع الثاني :تعريف المشرع الجزائري للجريمة الالكترونية	**16**
المطلب الثاني :خصائص الجريمة الالكترونية	**17**
المطلب الثالث :اركان الجريمة الالكترونية	**23**
الفرع الاول :الركـن الشرعــي	**23**
الفرع الثاني :الركـن المــادي	**24**
الفرع الثالث: الركـن المعنـوي	**26**
المبحث الثاني :أنواع الجرائم الالكترونية ومرتكبيها	**27**
المطلب الأول: تصنيف الجرائم الالكترونية	**27**
الفرع الأول : الجرائم الالكترونية الواقعة بواسطة النظام المعلوماتي	**29**
الفرع الثاني :الجرائم الالكترونية الواقعة على النظام المعلوماتي	**36**
المطلب الثاني :المجرم المعلوماتي	**39**
الفرع الأول :السمات الخاصة بالمجرم المعلوماتي	**39**
الفرع الثاني :تصنيفات المجرم المعلوماتي	**43**

الفصل الثاني :الاليات التشريعية لمكافحة الجريمة الالكترونية في القانون الجزائري	**52**
المبحث الاول :الاطار القانوني لمكافحة الجريمة الالكترونية في التشريع الجزائري	**53**
المطلب الاول :الاليات القانونية الموضوعية لمكافحة الجريمة الالكترونية	**53**
الفرع الاول : القواعد المقررة في قانون العقوبات	**54**
الفرع الثاني : القواعد المقررة في القوانين الخاصة	**61**
اولا– القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته	**61**
ثانيا– القواعد الخاصة المتعلقة بحماية المؤلف والحقوق المجاورة	**63**
ثالثا – القواعد الخاصة المتعلقة بالبريد والموصلات السلكية واللاسلكية	**66**
المطلب الثاني :الاليات القانونية الاجرائية لمكافحة الجريمة الالكترونية	**68**
الفرع الاول : القواعد الاجرائية المقررة وفقا لقانون الاجراءات الجزائية	**68**
اولا– الاختصاص	**68**
ثانيا –التسرب	**70**
ثالثا– اعتراض المراسلات تسجيل الاصوات والتقاط الصور	**72**
الفرع الثاني: القواعد الاجرائية المقررة وفقا لقانون 09–04المتعلق بالوقاية من تكنولوجيات الاعلام والاتصال ومكافحتها	**75**
اولا– مراقبة الاتصالات الالكترونية	**76**
ثانيا –التفتيش	**79**
ثالثا – حجر المعطيات	**83**
رابع–التزامات مقدمي خدمات الانترنت في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال	**84**

الفرع الثالث : القواعد القانونية المقررة في اطار معاهدات دولية خاصة	**88**
اولا– المساعدات القضائية الدولية	**89**
ثانيا – الانابـة القضائيـة	**90**
ثالثا – تسليم المجرمين	**91**
رابعا – تكثيف التعاون الفني الدولي	**92**
المبحث الثاني :الهياكل الخاصة لمواجهة الجرائم الالكترونية	**94**
المطلب الأول :الهيئات الفنية المتخصصة في البحث والتحري عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال	**95**
الفرع الأول : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال	**96**
الفرع الثاني : الوحدات التابعة للأمن الوطني والدرك	**99**
المطلب الثاني :الهيئـات القضائيـة	**102**
الفرع الأول: الاقطاب المتخصصة في ظل مرسوم 16–267	**102**
الفرع الثاني: القطب الجزائي المتخصص في ظل أمر 21–11 المؤرخ في 25غشت 2021	**103**
خـاتمــة	**109**
المراجـع	**112**
الفهـرس	**117**

ملخـص

تعد الجرائم الالكترونية من الأنماط الإجرامية الجديدة التي أفرزتها تكنولوجيات الإعلام والاتصال الحديثة ، فهي تختلف تماما عن الجرائم التقليدية ، في ذاتية أركانها وأساليب ارتكابها والبيئة الافتراضية واللامادية التي ترد عليها وخصوصية مرتكبيها .

مما جعلها ظاهرة غريبة عن نصوص قانون الجزائي التقليدي بشقيه الموضوعي والإجرائي ،من ثمة فأية محاولة إخضاع هذا النمط الإجرامي الجديد لإجراءات التحقيق والإثبات المألوفة سيؤدي حتما إلى عدم الوفاء بمتطلبات مبدأ الشرعية الإجرائية ، وينجر عنه عقبات كثيرة أمام سلطات التحقيق .

وهوما استدعى تدخل المشرع لوضع حد لهذا التنامي الخطير في ميدان الإجرام المعلوماتي ، عن طريق سن نصوص قانونية موضوعية دولية وحتى داخلية ، تجرم وتعاقب الأفعال التي تشكل اعتداءا أو تهديدا للأمن المعلوماتي، مع استحداث هيئات تعمل على المستوى الميداني من أجل مكافحة هذا النوع من الإجرام .

فما هي الآليات العقابية التي تبناها المشرع الجزائري لمكافحة الجريمة الالكترونية والتصدي لها ، تلك هي الإشكالية التي حاولنا الإجابة عنها في هذه الدراسة.

Abstract:

Cybercrime is one of the new criminal patterns created by modern information and communication technologies. They are quite different from traditional crimes, in their subjectivity, their methods of commission, the virtual and non-material environment to which they respond and the privacy of the perpetrators.

This makes it a phenomenon that is alien to the provisions of the traditional Penal Code in both substantive and procedural terms. Any attempt to subject this new criminal pattern to the usual investigative and evidentiary procedures will inevitably result in failure to meet the requirements of the principle of procedural legality. It has many obstacles to the investigative authorities.

This has necessitated the legislator's intervention to put an end to this dangerous growth in the field of information crime, through the enactment of international and even internal substantive legal texts Offences that constitute an attack or threat to information security shall be criminalized and punished, with bodies established at the field level to combat such offences.

What punitive mechanisms the Algerian legislature has adopted to combat and address cybercrime are the problems that we have tried to answer in this study.