التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري

Legal regulation of cybercrime in Algerian legislation

مهداوي حنان*، كلية الحقوق والعلوم السياسية جامعة محمد لمين دباغين سطيف 2

mahdaoui.hanane19000@gmail.com

تاريخ إرسال المقال: 14/ 08/ 2022 تاريخ قبول المقال: 10/ 10/ 2022 تاريخ نشر المقال: 02/ 11/ 2022

الملخص:

أدى الاستخدام المتزايد للأنظمة المعلوماتية إلى الكثير من المخاطر وأظهر أنواعا جديدة من الجرائم تعرف بالجرائم الالكترونية، وتنوعت هذه الجرائم بين تزوير، سرقة معلومات وأموال واختراق للنظم وجرائم ماسة بالأخلاق والآداب العامة، وذلك من خلال الدخول غير المشروع إلى جهاز حاسب آلي أو نظام معلوماتي أو شبكة معلوماتية بهدف تغيير أو إعادة نشر بيانات أو معلومات سرية أو شخصية، إتلاف مستندات أو نظام أو موقع الكتروني.

ونظرا للتطور السريع والانتشار الهائل لهذه الظاهرة الاجرامية المستحدثة وخطورتها، عملت مختلف التشريعات على التصدي لها من خلال وضع النصوص القانونية واستحداث الأجهزة المتخصصة التي تتولى محاربة الجريمة الالكترونية ومكافحتها، وهو ما قام به المشرع كذلك من خلال تعديل التشريعات العقابية واستحداث نصوص جديدة وكذا هيئات متخصصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

الكلمات المفتاحية: جريمة، الكترونية، نظام، معلومات، مكافحة.

Abstract:

The increasing use of information systems has led to many risks and revealed new types of crimes known as electronic crimes, and these crimes varied between forgery, theft of information and money, penetration of systems and crimes against morals and public morals, through illegal entry into a computer. Informational with the aim of changing or re-publishing confidential or personal data or information, or destroying website.

Various legislations worked to address this criminal through the development of legal texts and the creation of specialized agencies that combat electronic crime, which the legislator has also done by amending punitive legislation and introducing new texts as well as specialized bodies for prevention. of crimes related to information and communication technologies and combat them.

Key words: crime, electronic, system, information, combat.

المقدمة:

إن العصر الراهن يعرف بعصر الثورة العلمية والمعلوماتية والتكنولوجية، وعلى الرغم من المزايا الهائلة التي تحققت في مجال تقنية المعلومات على جميع الأصعدة وفي شتى الميادين، فإن هذه الثورة في المقابل

* المؤلف المرسل

رافقتها مجموعة من الانعكاسات السلبية جراء سوء استخدام هذه التقنيات المتطورة، منها تفشي ظاهرة من الظواهر الإجرامية المستحدثة وهي ظاهرة الجرائم المعلوماتية أو الجرائم الالكترونية[1].

أصبحت هذه الجرائم تشكل خطرا كبيرا على جميع الدول نظرا لخطورتها، الأمر الذي دفع إلى ضرورة بحث ووضع قواعد مستحدثة بالإضافة إلى القواعد التقليدية لحماية النظم المعلوماتية وقواعد البيانات وتحقيق الاستخدام المشروع لها ومنه حماية الحياة الخاصة للأفراد والأشخاص والحفاظ على سرية البيانات المخزنة في هذه الأنظمة[2].

وعلى غرار التشريعات المختلفة عمد المشرع الجزائري كذلك إلى وضع مجموعة من النصوص القانونية بهدف مكافحة الجريمة الالكترونية نظرا لتفشيها في الآونة الأخيرة، وذلك انطلاقا من تعديل قانون العقوبات بموجب القانون رقم 04-15[3] الذي استحدث القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، جرم من خلاله الأفعال والسلوكات التي تشكل جرائم المساس بأنظمة المعالجة الآلية للمعطيات ، وقرر لها مجموعة من العقوبات، ثم في فترة لاحقة تبنى المشرع الجزائري مصطلحا آخر للتعبير عن الجرائم الالكترونية وهو " الجرائم المتصلة بتكنولجيات الاعلام والاتصال، وذلك من خلال إصدار القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[4].

ترتيبا عل ما تقدم يمكن أن نطرح الإشكالية التالية: **ما مدى معالجة المشرع الجزائري للجريمة الالكترونية؟**

وللإجابة على هذه الإشكالية ارتأينا تقسيم دراستنا إلى مبحثين أساسيين:

-المبحث الأول: الإطار المفاهيمي للجريمة الالكترونية

-المبحث الثاني مكافحة الجريمة الالكترونية في التشريع الجزائري

1- الإطار المفاهيمي للجريمة الالكترونية:

تعد الجرائم الالكترونية من الجرائم المستحدثة التي ظهرت في العصر الحديث، والسبب في ذلك يرجع إلى ارتباط هذه الجرائم بوسائل التقنيات الحديثة والمتمثلة في أجهزة الكمبيوتر وشبكات الانترنيت والمواقع الالكترونية ، ولقد أدى الانتشار الكبير للتكنولوجيا الحديثة والتفشي المذهل للجريمة الالكترونية الناتجة عن هذه التكنولوجيا إلى زيادة اهتمام الباحثين والمختصين من ميادين عدة كالقانون، الاعلام والاتصال، السياسة، الاقتصاد وغيرها بهذا الموضوع، مما أدى إلى تنوع تعاريفها ومسمياتها، ومن ثم صعوبة إيجاد تعريف جامع مانع لها .

فالجريمة الالكترونية تعتبر من الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطوراتها التي ارتبطت بتقنية المعلومات، فقد اصطلح على تسميتها بداية بإساءة استخدام الكمبيوتر، ثم احتيال الكمبيوتر، الجريمة المعلوماتية، وبعدها جرائم الكمبيوتر والجريمة المرتبطة بالكمبيوتر، ثم جرائم التقنية العالية، إلى جرائم الهاكرز، جرائم الانترنيت، وأخيرا السيبركرايم ، وجدير بالذكر أن مصطلح "الجريمة الالكترونية" استخدم بنسبة قليلة جدا، فالاستخدام الأكثر شيوعا في التشريعات هو "جرائم الكمبيوتر"، "جرائم الاتصالات الالكترونية"، "جرائم تكنولوجيا المعلومات" و"الجريمة ذات التقنية العالية"

وسنحاول من خلال هذه الجزئية من دراستنا تفصيل الإطار المفاهيمي لهذه الجريمة من خلال التطرق لمفهومها وأركانها وذلك فيما يلي.

1.1- مفهوم الجريمة الالكترونية:

يمكن تعريف الجريمة عموما بأنها سلوك الفرد عملا كان أو امتناع يواجهه المجتمع عموما بتطبيق عقوبة جزائية وذلك بسبب الاضطرابات التي يحدثها في النظام الاجتماعي، كما يمكن تعريفها بأنها فعل غير مشروع صادر عن إرادة جنائية، يقرر له القانون عقوبة أو تدبيرا احترازيا[5]، أما الجريمة الالكترونية أو المعلوماتية فهي مزيج بين مصطلحي "الجريمة" و" الالكترونية" أو "المعلوماتية" ومما تجب الإشارة إليه ان التعاريف المتعلقة بالجريمة الالكترونية تباينت وتعددت نظرا لتباين المصطلحات التي أطلقت عليها والتي يرى البعض انها نتيجة نشأة وتطور ظاهرة الإجرام المرتبطة بتقنية المعلومات[6]، وفيما يلي نتطرق لتعريف الجريمة الالكترونية وخصائصها وذلك بهدف الإلمام بمفهوم الجريمة الالكترونية.

1.1.1- تعريف الجريمة الالكترونية: نشير من خلال هذه الجزئية من دراستنا إلى التعريف الفقهي والقانوني للجريمة الالكترونية، وذلك على النحو التالي:

1.1.1.1- التعريف الفقهي للجريمة الالكترونية:

انقسم الفقه في تعريفه للجريمة الالكترونية إلى اتجاهين، اتجاه تبنى التعريف الموسع واتجاه تبنى التعريف الضيق، بالنسبة للاتجاه الذي تبنى التعريف الموسع، فقد قدم تعاريف عديدة نذكر منها ما يلي:

" كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية بهدف الاعتداء على الأموال أو الأشياء المعنوية"[7]

" كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الجاني"[8]

" عمل أو امتناع يأتيه الانسان إضرارا بمكونات الحاسوب وشبكات الاتصال الخاصة به التي يحميها القانون ويفرض لها عقابا"[9].

أن التعاريف السابقة تنطوي على توسيع كبير لمفهوم الجريمة الالكترونية، إذ يؤخذ على هذا التوسع أنه من شأنه أن يسقط وصف الجريمة الالكترونية على أفعال قد لا تكون كذلك لمجرد مشاركة الحاسوب في النشاط الإجرامي، فبعض الجرائم كسرقة الحاسوب الآلي أو الأقراص المضغوطة مثلا لا يمكن إعطاؤها وصف الجريمة الالكترونية لمجرد أن الحاسوب أو أحد مكوناته المادية كان محلا لفعل الاختلاس[10].

أما بالنسبة للاتجاه الذي تبنى التعريف الضيق فقد عرف الجريمة الالكترونية بأنها:

"كل فعل غير مشروع يكون العلم بتكنولوجيا الحاس الآلي بقدر كبير لازم لارتكابه من ناحية، لملاحقته وتحقيقه من ناحية أخرى"[11].

" الجريمة التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسيا"[12].

" الجريمة التي يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب"[13].

ما يؤخذ على هذه التعاريف أنها جاءت قاصرة على الإحاطة بأوجه ظاهرة الإجرام الالكتروني، فالبعض من فقهاء الاتجاه ركز على معيار موضوع الجريمة، والبعض الآخر ركز على وسيلة ارتكابها، والبعض الآخر على معيار النتيجة[14].

2.1.1.1-التعريف القانوني للجريمة الالكترونية (تعريف المشرع الجزائري)

استعمل المشرع الجزائري للدلالة على الجريمة الالكترونية بداية مصطلح " جرائم المساس بأنظمة المعالجة الآلية للمعطيات" وذلك بعد استحداثها بموجب القانون 04-15 المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات، ثم بعد ذلك استعمل مصطلح " الجرائم المتصلة بتكنولوجيات الاعلام والاتصال" وذلك بموجب القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، حيث عرفها في **المادة 02 منه كما يلي: " الجرائم المتصلة بتكنولوجيات الاعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية**".

يلاحظ على هذا التعريف أن المشرع الجزائري قد اعتمد على الجمع بين عدة معايير لتعريف الجريمة الالكترونية، أولها معيار وسيلة الجريمة وهي المنظومة المعلوماتية أو نظام للاتصالات الالكترونية، وثانيها معيار موضوع الجريمة وهو المساس بأنظمة المعالجة الآلية للمعطيات، فمن خلال النص القانوني المذكور نجد أن المشرع قد أحال إلى قانون العقوبات، وبالتالي كل الأفعال المجرمة في المواد من 394 مكرر إلى

394 مكرر 8 من قانون العقوبات تشكل موضوعا للجريمة الالكترونية، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليه في قانون العقوبات، كما حدد المشرع نطاق الجريمة الالكترونية وذلك من خلال إقراره بأن الجريمة الالكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع من نطاق الجرائم الالكترونية في القانون الجزائري[15].

بعد عرض التعاريف الفقهية والتعريف القانوني الذي طرحه المشرع الجزائري يمكن القول أن الجريمة الالكترونية أو المعلوماتية هي سلوك غير مشروع يقع على النظام المعلوماتي أو بواسطته، يمس بالأشخاص أو الأموال أو أمن الدولة، وهو ما يبرر تجريم هذا السلوك وتقرير العقوبات المناسبة له.

2.1.1- الخصائص المميزة للجريمة الالكترونية

للجريمة الالكترونية مجموعة من الخصائص التي تنفرد بها عن الجرائم التقليدية، ومن أهم هذه الخصائص أن الجريمة الالكترونية تتطلب وجود جهاز الكتروني ومعرفة كيفية استخدامه، وفيما يلي نفصل أهم هذه الخصائص:

-**صعوبة اكتشاف الجريمة وإثباتها:** تتسم الجرائم الالكترونية بالخفاء، إذ أن هناك صعوبة في اكتشافها والاستدلال على مرتكبيها ومرد ذلك أنها تستهدف المعنويات لا الماديات، فلا يترك الجناة أثرا ماديا يمكن من خلاله التعرف عليهم بخلاف الجرائم التقليدية، كما أن مباشرة التحقيق والاستدلال يحتاج إلى دراية كبرة بتقنية المعلومات مما يتعذر على الأجهزة الضبطية التعامل معها، فعادة ما يتم اكتشاف الجريمة الالكترونية بمحض الصدفة ويرجع السبب في ذلك إلى عدم ترك الجناة أثرا خارجيا مرئيا لأنها من الجرائم التي تتسم باللاعنف، فتنصب على البيانات والمعلومات المخزنة في نظم الحواسيب ووسائط التخزين عبر تغييرها، التلاعب بها، محوها، غتلافها أو نسخها، فيؤدي ذلك إلى محو أي أثر كتابي، فالجريمة الالكترونية لا عنف فيها ولا آثار للاقتحام المادي وإنما هي أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسبات[16].

ومن الصعوبات التي تعترض أيضا اكتشاف الجريمة الالكترونية ضعف رقابة نظم الحواسيب في اكتشاف الجرائم وهو ما يسميه البعض بالدور غير المباشر للمجني عليه في ارتكاب الجريمة، وللحيلولة دون وقوع ذلك يجب تطوير نظم الأمن الخاصة بأنظمة الحاسبات الآلية[17].

-**الخبرة الفنية في التعامل مع الجريمة الالكترونية:** تتطلب الجريمة الالكترونية الإلمام بتقنيات الكمبيوتر ونظم المعلومات سواء لارتكابها أو التحقيق فيها أو ملاحقتها قضائيا لذلك يجد مأموري الضبط القضائي أحينا أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذا النوع من الجرائم، فضلا عن صعوبة إجراء التحريات السرية وتتبع مسار العمليات الالكترونية العابرة للحدود، كما أن رجال

الشرطة ومأموري الضبط القضائي قد لا يتعاملون مع ساحة الجريمة خلال المعاينة والدليل الالكتروني بمهارة واحتراف، فقد يتسبب المحقق بدون قصد أو بطريق الخطأ في اتلاف الدليل الالكتروني أو تدميره كما في حالة محو البيانات الموجودة في الأسطوانة الصلبة، وقد يتجاهل المحقق الدليل الالكتروني ظنا منه أنه غير مهم، أو لا يقوم بمصادرة جهاز الكمبيوتر المستعمل في الجريمة أو ملاحقه من طابعة أو ماسح ضوئي[18].

-**خصوصية مجرم المعلومات:** قد لا تتأثر الجرائم التقليدية بالمستوى العلمي للمجرم كقاعدة عامة ولكن الأمر مختلف تمام بالنسبة للمجرم المعلوماتي، والذي يكون عادة من ذوي الاختصاص والمعرفة في مجال تقنية المعلومات، وقد تم تصنيف مجرمي الجرائم الالكترونية إلى المخترقين والمحترفين والحاقدين، فالمخترق مثل الهاكرز يعد شخصا بارعا في استخدام الحاسب الآلي ولديه فضول في استخدام حسابات الآخرين بطرق غير مشروعة[19]، أما المحترفون فهم الأكثر خطورة بين مجرمي الانترنيت، حيث يهدف البعض منهم إلى الاعتداء لتحقيق الكسب غير المشروع المتمثل في الناحي المادية، وذلك عبر الدخول إلى حسابات البنوك، والبعض الآخر يدخل من أجل تحقيق أغراض سياسية والتعبير عن وجهة نظر أو فكرة[20]، وبالنسبة للحاقدين فهم الذين ليس لديهم أهداف للجريمة ولا يسعون لمكاسب سياسية أو مادية ولكن يتحركون لرغبة الانتقام والتأثر كالأمور الطائفية[21].

-**وقوع الجريمة الالكترونية أثناء المعالجة الآلية للبيانات:** من خصائص الجريمة الالكترونية أنها تقع أثناء عملية المعالجة الآلية للبيانات والمعطيات الخاصة بالكمبيوتر، ويمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام أركان الجريمة الالكترونية، ذلك أنه في حالة تخلف هذا الشرط تنتفي الجريمة[22]، وهذه الأخيرة قد تقع أثناء عملية المعالجة الآلية للبيانات في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للبيانات، سواء عند مرحلة إدخال البيانات أو أثناء مرحلة المعالجة أو أثناء مرحلة إخراج المعلومات[23].

-**الجريمة الالكترونية جريمة مستحدثة:** تعد الجرائم الالكترونية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل خطرا جسيما في ظل العولمة، فلا غرابة أن تعد الجرائم التي تتعرض لها أجهزة الكمبيوتر أو التي تسخر هذه الأجهزة في ارتكابها من الجرائم المستحدثة، حيث أن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، والأسوء أن هذا التقدم تجاوز بقدراته وإمكاناته أجهزة الدولة الرقابية، بل إنه أضعف من قدراتها في تطبيق قوانينها بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها[24].

-**احتمال تعدد الاوصاف القانونية لمحل الجريمة الالكترونية:** إن محل الجريمة الالكترونية قد يظهر بمظهرين أحدهما مادي والآخر معنوي كما هو الحال بالنسبة للمعلومات، فقد تكون في حالة انتقال أو موجودة في ذاكرة النظام الالكتروني، أي انها في حالة غير مادية، والشكل الآخر أن تكون المعلومات متجسدة في صورة مادية بتخزينها على دعامة الكترونية، حتى أن المعلومات غير المادية بطبيعتها يمكن أن

تخضع لأكثر من نص قانوني وفقا لما إذا كانت في شكل مادي أو غير مادي، وفي الشكل الأخير يوجد لها أكثر من نص قانوني يمكن أن تخضع له مثال ذلك اعتبارها مصنف أدبي مما يثير مشكلة تعدد الأوصاف القانونية على ذات المحل[25].

2.1- أركان الجريمة الالكترونية :

إن أركان الجريمة عموما هي تلك العناصر التي لا وجود للجريمة بدونها، وتتمثل الأركان العامة في الركن القانوني (الشرعي)، وهو النص الجزائي الذي يحوي النموذج القانوني للفعل أو الامتناع المجرم، ثم العناصر المكونة للركن المادي وأخيرا الركن المعنوي القائم على العلم والإرادة، أما الأركان الخاصة فهي ما يورده المشرع من عناصر في النص لقيام الجريمة بالإضافة إلى الأركان السابقة، وما يميز الجريمة الالكترونية عن غيرها من الجرائم أن وجود نظام المعالجة الآلية للمعطيات يعد بمثابة الشرط الأولي أو الركن الخاص الذي يجب تحققه حتى يمكن البحث في توافر أو عدم توافر أركان أي جريمة من جرائم الاعتداء على هذا النظام[26]، وفيما يلي نفصل في مختلف الأركان التي تقوم عليها الجريمة الالكترونية.

1.2.1- الركن الشرعي المكون للجريمة الالكترونية

يقوم الركن الشرعي على النص التشريعي المجرم للسلوك والمحدد للعقوبة المقررة له تطبيقا لمبدأ شرعية الجرائم والعقوبات، لا جريمة ولا عقوبة إلا بناء على نص تشريعي تضعه السلطة المختصة بالتشريع[27]، ولقد خص المشرع الجزائري الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بقسم خاص ضمن قانون العقوبات وهو القسم السابع مكرر الذي يشتمل على تسعة مواد تهتم بذكر كل أنواع الاعتداءات على الأنظمة المعلوماتية[28].

2.2.1- الركن المادي المكون للجريمة الالكترونية

تتخذ الجرائم الالكترونية عدة أشكال وذلك بتعدد وتنوع صور الاعتداء الواقع على نظام المعلوماتية بحد ذاته، ويمكن تلخيص هذه الصور كما يلي:

1.2.2.1-جريمة الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات: يقصد بفعل الدخول ذلك الدخول المعنوي أو الالكتروني باستعمال الوسائل الفنية والتقنية إلى النظام المعلوماتي، ولا يعد فعل الدخول في حد ذاته سلوكا غير مشروع، وإنما يتخذ وصفه الإجرامي انطلاقا من كونه قد تم دون وجه حق أو دون ترخيص[29]، وهو ما أشار إليه المشرع الجزائري في المادة 394 مكرر من قانون العقوبات التي نصت على ما يلي: "يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة مالية من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك..." .

أما فيما يخص فعل البقاء غير المشروع في نظام المعالجة الآلة للمعطيات فيقصد به استمرارية التواجد داخل النظام دون إذن من صاحبه أو من له حق السيطرة عليه، أي أنه بقاء شخص داخل نظام للمعالجة يكون ملكا للغير وذلك بعد الدخول إليه خطأ أو صدفة رغم علمه أن بقاءه فيه غير مرخص[30].

وبالرجوع إلى نص المادة 394 مكرر من قانون العقوبات يمكن القول أن المشرع الجزائري قد أورد ظرفين لتشديد عقوبة الدخول والبقاء دون ترخيص في نظام المعالجة الآلية للمعطيات، يتحقق الظرف الأول إذا نتج عن الدخول أو البقاء محو أو تعديل في البيانات التي يحتويها النظام، ويتحقق الظرف الثاني عندما يترتب عن الدخول أو البقاء تخريب نظام اشتغال المنظومة وإعاقته عن أداء وظيفته، فالفقرة 2 من المادة 394 مكرر سالفة الذكر تنص على ما يلي: "تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، وإذا ترتب عن الأفعال المذكورة أعلاه تخريب في نظام اشتغال المنظومة تكون العقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50.000دج إلى 150.000دج.

2.2.2.1-جرائم الاعتداء على المعطيات الموجودة داخل نظام المعلوماتية: نص المشرع الجزائري على هذا النوع من الجرائم في المادتين 394 مكرر1 و394 مكرر2 من قانون العقوبات حيث جاء فيهما ما يلي:

المادة 394 مكرر1: "يعاقب بالحبس من 6أشهر إلى 3 سنوات وبغرامة من 500.000دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

المادة 394 مكرر2: "يعاقب بالحبس من شهر إلى 3 سنوات وبغرامة من 1.000.000دج إلى 5.000.000دج كل من يقوم عمدا وعن طريق الغش بما يأتي:

-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.2-حياز أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم"

يتضح من هذين النصين أن جرائم الاعتداء على المعطيات الموجودة داخل نظام المعلوماتية تتخذ صورتين، الصورة الأولى هي جريمة التلاعب بالمعطيات والصورة الثانية هي جريمة التعامل في المعطيات.

بالنسبة لجريمة التلاعب بالمعطيات فإنها تتحقق طبقا لما ورد في المادة 394 مكرر1 بارتكاب إحدى الصور الثلاث التالية:

-الإدخال بطريق الغش لمعطيات في نظام المعلوماتية.

-المحو بطريق الغش لمعطيات في نظام المعلوماتية.

-التعديل بطريق الغش لمعطيات في نظام المعلوماتية.

أما بالنسبة لجريمة التعامل في معطيات غير مشروعة، فإنها تتحقق طبقا لما ورد في المادة 394 مكرر2 بارتكاب إحدى الصورتين التاليتين:

- التعامل في معطيات صالحة لارتكاب جريمة: يقصد بالتعامل كل سلوك يكشف عن وجود صلة معينة بين شخص ومعطيات غير مشروعة، هذه الصلة تتمثل في القيام بأحد أنواع السلوك، بدءا بتصميم هذه المعطيات والبحث في مضمونها وتجميعها وصولا إلى جعلها في متناول الغير، وتصل ليد الجاني وتكون تحت تصرفه ليرتكب بها جريمته وذلك بتوفيرها أو نشرها أو الاتجار فيها[31].

-التعامل في معطيات متحصلة من جريمة: يتحقق هذا السلوك المجرم بالقيام بأحد الأفعال التي نصت عليها المادة 394 مكرر 2 وهي الحيازة، الإفشاء، النشر والاستعمال للمعطيات المتحصل عليها من جريمة الدخول أو البقاء بطريق الغش أو من جريمة التلاعب بالمعطيات.

3.2.1- الركن المعنوي المكون للجرائم الالكترونية

الركن المعنوي هو المسلك النفسي للجاني باعتباره محور القانون الجنائي، ذلك أنه في إطار هذا الركن تتوافر كافة مقومات المسؤولية الجنائية من علم وإرادة آثمة وقصد جرمي مع إقرار العقاب الذي يبنى على هذه المقومات، لذلك يمكن تعريف الركن المعنوي بأنه العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، وهذه العلاقة يطبق عليها القانون والعقاب الذي يقرره[32].

كما يمكن تعريف الركن المعنوي بأنه العلم بعناصر الجريمة وإرادة ارتكابها، وبالتالي يتكون هذا الركن من عنصرين هما العلم والإرادة، فالعلم هو إدراك الأمور على نحو مطابق للواقع، اما الإرادة فتتمثل في الاتجاه من اجل تحقيق السلوك الإجرامي[33].

ويتخذ القصد الجنائي صورتين، القصد الجنائي العام، والقصد الجنائي الخاص، فالقصد الجنائي العام هو الهدف الفوري والمباشر للسلوك الإجرامي وينحصر في حدود تحقيق الغرض من الجريمة، أي لا يمتد لما بعدها، أما القصد الجنائي الخاص فهو ما يتطلب توافره في بعض الجرائم، فلا يكفي مجرد تحقيق الغرض من الجريمة بل هو أبعد من ذلك لأنه يبحث في نوايا المجرم.

إن المجرم الالكتروني يتوجه من أجل ارتكاب فعل غير مشروع مع علمه بأركان الجريمة، وبالرغم من أن بعض المخترقين يبررون أفعالهم بأنهم مجرد فضوليين وأنهم قد تسللوا صدفة، فلا انتفاء للعلم كركن للقصد الجنائي وأنه كان يجب عليهم أن يتراجعوا بمجرد دخولهم ولا يستمروا في الإطلاع على أسرار الأفراد والمؤسسات لأن جميع المجرمين والأشخاص الذين يرتكبون هذه الأفعال يتمتعون بمهارات عقلية ومعرفية كبيرة، وعليه فالقصد الجنائي العام متوافر في جميع الجرائم الالكترونية دون أي استثناء، ولكن هذا لا يمنع أن هناك بعض الجرائم الالكترونية التي تتطلب أن يتوافر فيها القصد الجنائي الخاص، مثل جرائم تشويه السمعة عبر الانترنيت وجرائم نشر الفيروسات عبر الشبكة، وفي جميع الحالات يرجع الأمر لتقرير هذا العنصر للسلطة التقديرية لقاضي الموضوع[34].

2- مكافحة الجريمة الالكترونية في التشريع الجزائري:

رغبة من المشرع الجزائري في التصدي لظاهرة الجرام الالكتروني وما يصاحبها من أضرار كبيرة على الأفراد ومؤسسات الدولة، ومحاولة منه لتدارك الفراغ التشريعي القائم في هذا المجال عمد إلى تعديل العديد من القوانين الوطنية بما فيها التشريعات العقابية، على رأسها قانون العقوبات لجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجيا الاعلام والاتصال، كما قام باستحداث قوانين أخرى خاصة لضمان الحماية الجنائية للمعاملات الالكترونية[35]، وسنحاول من خلال هذه الجزئية من دراستنا الوقوف على كيفية تصدي المشرع الجزائري للجريمة الالكترونية وذلك على النحو التالي:

1.2- مكافحة الجريمة الالكترونية بموجب النصوص القانونية

نظرا للتطور السريع في التكنولوجيا وتقنيات المعلومات أظهرت الدراسات الجنائية عدم كفاية النصوص التقليدية في تطبيقها على الجرائم المستحدثة في ظل التطور الهائل على مستوى أنظمة معالجة المعلومات ونقلها عبر الشبكات، وباتت الحاجة ضرورية لاستحداث قواعد قانونية جديدة لمواجهة هذه الجرائم المستحدثة[36]، وهو بالفعل ما قام به المشرع الجزائري، فإلى جانب تعديل قانون العقوبات وقانون الإجراءات الجزائية قام المشرع الجزائري بإصدار القانون الخاص للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وهو القانون 09-04 ، وفيما يلي نبين كيف قام المشرع الجزائري بمكافحة الجريمة الالكترونية من خلال النصوص القانونية العامة والخاصة.

1.1.2- مكافحة الجريمة الالكترونية من خلال قانون العقوبات الجزائري

قام المشرع الجزائري بتجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة للإجرام والتي لم تشهدها البشرية من قبل، مما دفع المشرع الجزائري إلى تعديل

قانون العقوبات بموجب القانون 04-15، حيث أضاف القسم السابع مكرر تحت عنوان المساس بأنظمة المعاجلة الآلية للمعطيات، وتضمن هذا القسم تسعة مواد (من المادة 394 مكرر إلى 394 مكرر 8)، وقام المشرع من خلال هذه المواد بتجريم مجموعة من الأعمال التي يشكل ارتكابها جريمة ماسة بأنظمة المعالجة الآلية للمعطيات وقرر العقوبة الخاصة بكل فعل إجرامي من خلال النصوص السابقة[37].

ومما تجب الإشارة إليه أن المشرع الجزائري وفي سنة 2016 أدخل تعديلا آخر على قانون العقوبات بموجب القانون 16-02[38]، حيث مس هذا التعديل القسم السابع مكرر و الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، حيث قام المشرع من خلال هذا التعديل بإضافة المادة 394 مكرر 8 والتي شدد من خلالها العقوبة على مقدم خدمات الانترنيت، فيعاقب بالحبس من سنة إلى 3 سنوات وبغرامة من 2.000.000دج إلى 10.000.000 دج أو بإحدى هاتين العقوبتين فقط وذلك في حالة عدم قيامه بالتدخل الفوري لسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا، أو عند قيامه بوضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم السابقة أو لجعل الدخول إليها غير ممكن.

والملاحظ أن هذا التعديل جاء تماشيا مع القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، حيث تضمن هذا الأخير في الفصل الأول منه الذي يشمل الأحكام العامة شرحا لبعض المصطلحات منها مصطلح "مقدمو الخدمات"، حيث يقصد بهم طبقا لما ورد في الفقرة 1 من المادة 02 :

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

2-وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعملها".

وبالتالي يعتبر القانون 02/16 المعدل للأمر 156/66 المتضمن قانون العقوبات مكملا لما جاء به القانون 04/09، فلقد جرم بعض الممارسات التي يقوم بها مقدمو خدمات الانترنيت، حيث يشكل ارتكابها جرائما ماسة بأنظمة معالجة المعطيات وقرر العقوبات المناسبة لها.

2.1.2- مكافحة الجريمة الالكترونية من خلال قانون الإجراءات الجزائية

تتم متابعة الجريمة الالكترونية بنفس الإجراءات التي تتبع بها الجريمة التقليدية كالتفتيش والمعاينة واستجواب المتهم والضبط والشهادة والخبرة[39]، حيث نص المشرع الجزائري على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الالكترونية في المادة 37 من قانون الإجراءات الجزائية، ونص على التفتيش

في المادة 45 الفقرة 7 من نفس القانون، غير أنه اعتبر أن التفتيش المنصب على المنظومة المعلوماتي يختلف عن التفتيش المتعارف عليه في القواعد الإجرائية العامة من حيث الشروط الشكلية والموضوعية، فالتفتيش وإن كان إجراء من إجراءات التحقيق فقد أحاطه المشرع بقواعد صارمة، وبالتالي لا تطبق الأحكام الواردة في المادة 44 من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الالكترونية.

كما نص المشرع على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقر 6 وكذا على اعتراض المراسلات والتقاط الصور في المادة 65 مكرر 5، وبموجب هذه النصوص فإن المشرع الجزائري يسمح لسلطات التحقيق والاستدلال إذا استدعت ضرورة التحري في الجريمة المتلبس بها أو التحقيق في الجريمة الالكترونية اللجوء إلى إجراء اعتراض المراسلات السلكية واللاسلكية وتسجيل المحادثات والأصوات والتقاط الصور والاستعانة بكل الترتيبات التقنية اللازمة لذلك من أجل الوصول إلى الكشف عن ملابسات الجريمة وإثباتها دون التقيد بقواعد التفتيش والضبط المألوفة[40].

مما سبق يمكن القول أن المشرع الجزائري أدرك جيدا أن المواجهة الفعالة للجريمة الالكترونية لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية والتي من شأنها تفادي وقوع الجريمة الالكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها وهو ما استدركه المشرع الجزائري بتضمين قانون الإجراءات الجزائية تدابير إجرائية مستحدثة تتفق وطبيعة الجريمة الالكترونية.

3.1.2-: مكافحة الجريمة الالكترونية من خلال القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها

يحتوي القانون 04/09 على 6 فصول تناولت على التوالي: أحكام عامة، مراقبة الاتصالات الالكترونية، القواعد الإجرائية، التزامات مقدمي الخدمات، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، التعاون والمساعدة القضائية الدولية.

وبذلك يكون القانون04/09 قد تضمن مجموعة من التدابير الوقائية التي يتم اتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع الجرائم الالكترونية أو الكشف عنها وعن مرتكبيها في وقت مبكر[41]، ويمكن تلخيص أهم هذه التدابير كما يلي:

-**مراقبة الاتصالات الالكترونية:** حددت المادة 04 من القانون 04/09 الحالات التي تسمح باللجوء إلى المراقبة الالكترونية، وهي:

أ-للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب–في حالة توافر 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 إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.

د– في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

غير أن المشرع الجزائري ومن خلال نفس النص القانوني أكد على أنه لا يجوز إجراء عمليات المراقبة في الحالات السابقة المذكورة إلا بعد الحصول على إذن مكتوب من السلطة القضائية المختصة.

–**القواعد الإجرائية:** تضمنت المواد من 5 إلى 9 من القانون 04/09 مجموعة من القواعد الإجرائية التي تهدف إلى الوقاية من الجرائم الالكترونية ومكافحتها، وتتمثل هذه الإجراءات في:

–**تفتيش المنظومات المعلوماتية**[42]، حيث يجوز للسلطات القضائية في إطار قانون الإجراءات الجزائية وفي الحالات التي تسمح باللجوء إلى المراقبة الالكترونية التي سبق وأشرنا إليها الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، وإلى منظومة تخزين معلوماتية.

وإذا تبين أن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل، كما يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

–**حجز المعطيات المعلوماتية**[43]: عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم ومرتكبيها يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية، وإذا استحال إجراء الحجز لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية والموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

وفي إطار ممارسة سلطة التفتيش يمكن للسلطة التي تباشر هذه الإجراءات أن تأمر باتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة، وتستعين في ذلك بالأشخاص المؤهلين لاستعمال الوسائل التقنية المناسبة لذلك[44].

-**إلزام مقدمي الخدمات بضرورة المساهمة في الوقاية من الجرام الالكترونية:** فرض القانون 04/09 على مقدمي الخدمات مجموعة من الالتزامات تساهم بدورها في الوقاية من الجرائم الالكترونية ومكافحتها، وتتمثل أهم هذه الالتزامات:

-**تقديم المساعدة للسلطات،** حيث يجب على مقدمي الخدمات تقديم المساعدة اللازمة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات، وبوضع المعطيات التي يتعين حفظها تحت تصرف السلطات المكلفة بالتحريات القضائية، كما يتعين على مقدمي الخدمات في إطار هذه المساعدة كتمان سرية العمليات التي ينجزونها بطلب من المحققين، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق[45].

-**حفظ المعطيات المتعلقة بحركة السير[46]:** يلتزم مقدمو الخدمات بحفظ ما يلي:

-المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

- المعطيات المتعلقة بالتجهيزات المستعملة للاتصال.

-المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

-المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم بالاتصال وكذا عناوين المواقع المطلع عليها.

إضافة إل ما سبق خص المشرع الجزائري مقدمي خدمة الانترنيت بالتزامات معينة تهدف كذلك إلى الوقاية من الجرائم الالكترونية ومكافحتها، وتتمثل هذه الالتزامات في[47]:

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

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

-**إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته:** نفصل مهام الهيئة ودورها في الوقاية من الجرائم الالكترونية ومكافحتها في جزئية لاحقة من دراستنا والمتعلقة بمكافحة الجريمة الالكترونية بموجب الهياكل الخاصة.

-**التعاون والمساعدة القضائية الدولية:** أقر المشرع الجزائري من خلال القانون 04/09 أن المحاكم الجزائرية تختص بالنظر في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني[48].

وفي إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم الالكترونية وكشف مرتكبيها يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني[49]، غير أنه يرفض تنفيذ طلبات المساعدة القضائية الدولية إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام كما يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب[50].

2.2- مكافحة الجريمة الالكترونية بموجب الهياكل الخاصة:

تصدى المشرع الجزائري للجريمة الالكترونية من خلال مجموعة من النصوص القانونية التي منحت بدورها الاختصاص لمجموعة من الهياكل الخاصة، تتولى مكافحة الجرائم الالكترونية والوقاية منها، ومن خلال هذه الجزئية من دراستنا نحاول التطرق لهذه الهياكل وذلك على النحو التالي:

1.2.2- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال

استحدث المشرع الجزائري هذه الهيئة بموجب القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، حيث نصت المادة 13 منه على: تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته، تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم".

وسنفصل تنظيم الهيئة وتشكيلتها ومهامها فيما يلي:

1.1.2.2-تنظيم الهيئة وتشكيلتها وكيفية سيرها: أحال المشرع الجزائري من خلال نص المادة 13 السالف الذكر بخصوص تشكيلة الهيئة وتنظيمها وكيفية سيرها إلى التنظيم، وهو فعلا ما قام به المشرع في وقت لاحق من خلال المرسوم الرئاسي 172/19[51] بعد أن كانت تخضع لأحكام المرسوم الرئاسي رقم

261/15 والملغى بموجب المرسوم 172/19، اعتبر من خلاله المشرع الجزائري الهيئة مؤسسة عمومية ذات طابع إداري، تتمتع بالشخصية المعنوية والاستقلالية المالية، توضع تحت سلطة وزارة الدفاع الوطني[52].

وبخصوص تنظيم الهيئة أشارت المادة 4 من المرسوم الرئاسي 172/19 أن الهيئة تتشكل من مجلسين، مجلس توجيه ومديرية عامة، مجلس التوجيه يرأسه وزير الدفاع أو ممثله، كما تشير المادة المذكورة إلى أن الهيئة تتشكل من الوزارات التالية: وزارة الدفاع الوطني، الوزارة المكلفة بالداخلية، وزارة العدل، الوزارة المكلفة بالمواصلات السلكية واللاسلكية.

أما عن كيفية سير عمل الهيئة، فتنص المادة 7 من المرسوم 172/19 على أن مجلس التوجيه يجتمع في دورة عادية مرتين في السنة بناء على استدعاء من رئيسه، ويمكنه أن يجتمع في دورة غير عادية كلما كان ذلك ضروريا بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة.

2.1.2.2-مهام الهيئة: تمارس الهيئة المهام المنصوص عليها في المادة 14 من القانون 04/09 تحت رقابة السلطة القضائية طبقا لأحكام قانون الإجراءات الجزائية وكذا القانون 04/09، وحددت المادة 14 مهام الهيئة وصلاحياتها كالآتي:

-مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الاعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

-تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم الالكترونية وتحديد مكان تواجدهم.

ما يمكن ملاحظته أن مضمون المادة 14 جاء بصيغة العموم، غير مفصل لمهام الهيئة، الأمر الذي دفع المشرع إلى تفصيل مهامها في المرسوم 172/19 وتقسيمها بين مجلس التوجيه والمديرية العامة للهيئة[53]، حيث تولى المشرع تفصيل هذه المهام في المواد 6، 9، 11، 13، 14 من المرسوم 172/19.

2.2.2- المعهد الوطني للأدلة الجنائية على الإجرام

يتكون هذا المعهد من إحدى عشر دائرة متخصصة في مجالات مختلفة، جميعها تتضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية ومن بين هذه الدوائر توجد دائرة الاعلام الآلي والالكتروني التي تتولى معالجة وتحليل وتقديم كل دليل رقمي يساعد للعدالة، كما تقدم المساعدة التقنية للمحققين في المعاينات[54].

3.2.2- الهيئات القضائية الجزائية المتخصصة

إن السلطة القضائية تتعامل في قضايا الإجرام المتصلة بتكنولوجيات الاعلام والاتصال ولا سيما بعد اللجوء الواسع والمتزايد إلى الشبكات الرقمية والنظام القضائي الجزائي يتجه نحو إرساء فكرة القضاء المتخصص وما يؤكد ذلك ما نص عليه القانون 14/04 المؤرخ في 10 نوفمبر 2010 المعدل والمتمم لقانون الإجراءات الجزائية من إمكانية تمديد دائرة الاختصاص للمحكمة وكذا لوكيل الجمهورية وقاضي التحقيق عن طريق التنظيم، وذلك فيما يتعلق بجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

حيث نصت المادة 40 مكرر من قانون الإجراءات الجزائية على: "تطبق قواعد هذا القانون المتعلقة بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي يتم توسيع اختصاصها المحلي طبقا للمواد 40، 37، 329 من هذا القانون مع مراعاة أحكام المواد من 40 مكرر 1 إلى 40 مكرر5 أدناه"، وتطبيقا لذلك صدر المرسوم التنفيذي رقم 348/06[55] الذي يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، حيث نصت المادة 01 منه على: " تطبيقا لأحكام المواد 37 و 40 و329 من الامر رقم 156/66 ...والمتضمن قانون الإجراءات الجزائية يهدف هذا المرسوم إلى تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق إلى دوائر اختصاص محاكم أخرى كما هو محدد في المواد 2 و3 و 4 و5 أدناه في الجرائم المتعلقة بالمتاجرة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف".

لقد سعى المشرع الجزائري من وراء إنشائه للأقطاب الجزائية إلى سد العجز القائم على فكرة غياب هيئات قضائية متخصصة مؤهلة لمكافحة الإجرام المستحدث أو على الأقل التقليل من آثاره وأبعاده الوخيمة على الصعيدين المحلي والدولي خاصة بعد إثبات عجز القضاء العادي وعدم قدرته على التكفل بهذا النوع من الجرائم، فلقد أصبحت الأقطاب المتخصصة بطريقة العمل التي تنتهجها والمعتمدة على عامل التخصص والمهارة والكفاءة النموذج المتطور للممارسة القضائية، لذلك أضحت ضرورة لا يمكن الاستغناء عنها لمكافحة الإجرام المستحدث الذي يشمل الجرائم الالكترونية[56].

الخاتمة:

في الوقت الذي تقدم فيه تكنولوجيات الاعلام والاتصال لأجهزة الأمن وللدول الكثير من التسهيلات التي تساهم في رفع إمكاناتها للقضاء على الجريمة، إلا أنها وفي الوقت نفسه أدت إلى تطوير وتحديث

الجريمة، فلم يعد المجرم ذلك الشخص الذي يشهر السلاح في وجه الآخرين، بل أصبح شخصا ذا علم، يستخدم علمه للاعتداء على التقنيات المعلوماتية أو يسيء استخدامها وهو ما جعل الجريمة تتحول من صورتها التقليدية إلى صورة أخرى الكترونية يصعب التعامل معها لارتباطها بالتكنولوجيا.

ومن خلال ما تقدم من دراستنا توصلنا إلى مجموعة من النتائج يمكن تلخيصها كما يلي:

-عدم وجود تعريف موحد للجريمة الالكترونية، حيث اختلف الفقه بين متبن للتعريف الضيق ومتبن للتعريف الموسع، غير أن كلا الاتجاهان يشتركان في كون الجريمة الالكترونية جريمة مستحدثة تتصل بالنظام المعلوماتي، فهي عبارة عن عمل غير مشروع يقع على النظام المعلوماتي أو يتحقق بواسطته.

-اختار المشرع الجزائري للتعبير عن الجرائم الالكترونية مصطلحين هما "جرائم المساس بأنظمة المعالجة الآلية للمعطيات" والذي استحدث بموجب القانون رقم 15/04 المتضمن تعديل قانون العقوبات و" الجرائم المتصلة بتكنولوجيات الاعلام والاتصال" وهو ما أشار إليه القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال الذي عرف الجريمة الالكترونية في المادة 02 منه بأنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام لاتصالات الالكترونية.

-تنفرد الجريمة الالكترونية بمجموعة من الخصائص التي تميزها عن الجريمة التقليدية فهي صعبة الاكتشاف والإثبات، لارتكابها لابد من الالمام بتقنيات الكمبيوتر ونظم المعلوماتية وهو ما يضفي بدوره خصوصية على المجرم الالكتروني، التحقيق فيها وملاحقتها كذلك يستدعي نفس الضرورة ألا وهي الإلمام بتقنيات الكمبيوتر ونظم المعلومات، وبما أن الجريمة الالكترونية تتطلب ضرورة الإلمام بتقنيات المعلوماتية فإن ذلك يجعلها تقع أثناء المعالجة الآلية للمعطيات والبيانات وهو ما يجعلها من الجرائم المستحدثة.

-الجريمة الالكترونية كأي جريمة أخرى لا تقوم إلا إذا توافرت أركانها والمتمثلة في الركن الشرعي، الركن المادي، والركن المعنوي، بالنسبة للركن الشرعي والمقود به النص القانون الذي يجرم ويقرر العقوبة، فنجده في قانون العقوبات أين خص المشرع الجزائري الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بقسم خاص وهو القسم السابع مكرر الذي يشمل مجموعة من المواد تحدد كل أنواع الاعتداءات على الأنظمة المعلوماتية، تجرمها وتقرر العقوبة المناسبة لها، أما الركن المادي فيقصد به الأفعال والممارسات التي تشكل اعتداء وجريمة ماسة بأنظمة المعالجة الآلية للمعطيات، وقد حددها المشرع كذلك في قانون العقوبات انطلاقا من نص المادة 394 مكرر ولى غاية المادة 394 مكرر2، وأخيرا لقيام الجريمة الالكترونية لا بد من علم الجاني بعناصرها واتجاه إرادته لارتكابها، وهو ما يعرف بالقصد الجنائي.

-تصدى المشرع الجزائري لظاهرة الإجرام الالكتروني من خلال تعديل التشريعات العقابية لجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجيا الاعلام والاتصال، كما قام باستحداث نصوص قانونية أخرى تضمن الوقاية من الجريمة الالكترونية.

-أبرز التعديلات التي مست التشريعات العقابية هي تعديل قانون العقوبات بموجب القانون 15/04 والذي أضاف القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، أما بالنسبة للقوانين المستحدثة فقد وضع المشرع القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والذي تضمن مجموعة من القواعد التي تساعد في الوقاية من الجريمة الالكترونية ومكافحتها، أبرز هذه القواعد مراقبة الاتصالات الالكترونية، تفتيش المنظومات المعلوماتية، حجز المعطيات المعلوماتية، إلزام مقدمي الخدمات بضرورة المساهمة في الوقاية من الجرائم الالكترونية، إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الالام والاتصال ومكافحته، تقرير التعاون والمساعدة القضائية الدولية لمواجهة الجريمة الالكترونية.

-إضافة إلى سن مجموعة من النصوص القانونية الخاصة بمحاربة الجريمة الالكترونية فقد وضع المشرع الجزائري قاعدة هيكلية تتولى مكافحة ومحاربة هذه الجريمة المستحدثة، وتشمل هذه القاعدة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، المعهد الوطني للأدلة الجنائية على الاجرام، الهيئات القضائية المتخصصة.

بعد عرضنا لأهم النتائج المتوصل إليها نختم بحثنا بمجموعة من التوصيات والاقتراحات التي من شأنها أن تساهم في مواجهة الجريمة الالكترونية وذلك فيما يلي:

-بالرغم من سعي المشرع الجزائري إلى وضع دعامة قانونية تتصدى للجريمة الالكترونية إلا أنها ومع تزايد تطور هذه الظاهرة الإجرامية لم تعد كافية لمواجهتها بالشكل المطلوب، لذلك نقترح في هذا الخصوص ضرورة التعاون في المجال التشريعي والقضائي والأمني مع دول أخرى سبقت الجزائر من حيث الخبرة بالجرائم الالكترونية من أجل الاستفادة من هذه الخبرة واستغلالها في تحسين وتطوير آليات مواجهة الجريمة الالكترونية، فلا بد من توحيد مجهودات المجتمع الدولي وكل المختصين في هذا المجال للحد من تفشي هذه الجرائم التي تعرف تطورا مستمرا.

-مكافحة الجريمة الالكترونية والوقاية منها ليست دورا حكرا على الدولة وأجهزتها القضائية والأمنية فقط، بل يجب على كل مواطن المساهمة في هذه العملية من خلال تنمية ثقافته ووعيه الكافي بما يحيط به، وما يساهم في تحقيق ذلك هو ضرورة التحسيس بمخاطر الجريمة وكيفية تجنبها والحماية منها، وتفعيل أسلوب التوعية والتهذيب لدى مستخدمي شبكات الانترنيت وحثهم على الاستخدام الأمثل لهذه التقنيات.

-تفعيل دور الأجهزة المختصة في مواجهة الجريمة الالكترونية من خلال عقد دورات تكوينية وتدريبية مكثفة للعاملين على مستوى هذه الأجهزة لا سيما ما يتعلق بضرورة الإحاطة والإلمام بتقنيات الكمبيوتر ونظم المعلومات لا سيما في مجال التحري والتحقيق والمحاكمة.

-تشجيع الجامعات والمراكز البحثية على تنظيم الملتقيات الوطنية والدولية لتبادل الخبرات، معالجة تطور الإجرام المعلوماتي واقتراح الحلول المناسبة وكيفية الحد من هذه الظاهرة الإجرامية المستحدثة ومكافحتها.

التهميش:

[1] – عبد النبي مصطفى، قراءة في النصوص القانونية المنظمة للهيئة الوطنية للوقاية من جرائم تكنولوجيا الاعلام والاتصال ومكافحتها، دفاتر السياسة والقانون، المجلد 13، العدد 3، 2021، ص401.

[2] – حكيمة بوكحيل، سامية بن عديد، الهيئة الوطنية للوقاية من جرائم الاعلام وتكنولوجيا الاتصال ودورها في تفتيش نظم المعلوماتية، مجلة الدراسات القانونية المقارنة/ المجلد 7، العدد 1، 2021، ص1543.

[3] – القانون رقم 04-15 مؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، ج.ر عدد 71 الصادرة في نوفمبر 2004.

[4] – القانون 09-04 مؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج.ر عدد 47 الصادرة بتاريخ 16 أوت 2009.

[5] – بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2012-2013، ص7.

[6] – معاشي سميرة، الجريمة المعلوماتية، دراسة تحليلية لمفهوم الجريمة المعلوماتية، مجلة المفكر، العدد 17، جوان 2018، ص400.

[7] – نهلا عبد القادر المومني، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، 2008، ص49.

[8] – نفس المرجع، ص49.

[9] – ونوغي نبيل، زيوش عبد الرؤوف، المرجع السابق، ص131.

[10] – ونوغي نبيل، زيوش عبد الرؤوف، المرجع السابق، ص131.

[11] – نهلا عبد القادر المومني، المرجع السابق، ص48.

[12] سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنيت، دار الفكر الجامعي، الإسكندرية، 2008، ص40.

[13] – نفس المرجع، ص40.

[14] – ونوغي نبيل، زيوش عبد الرؤوف، المرجع السابق، ص130.

[15] – نمديلي رحيمة، خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة، المؤتمر الدولي الرابع عشر، طرابلس، 24-25 مارس 2017، ص100.

[16] – معاشي سميرة، المرجع السابق، ص412.

[17] – نفس المرجع، ص413.

[18] – معاشي سميرة، المرجع السابق، ص413.

[19] – نائلة عادل قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، 2012، ص178.

[20] – إبراهيم خالد ممدوح، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009، ص78.

[21] – نفس المرجع، ص79.

[22] – نائلة عادل قورة، المرجع السابق، ص55.

[23] – عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الالكترونية، دراسة قانونية، رسالة ماجستير ف القانون العام، جامعة الشرق الأوسط، 2014، ص24.

[24] – إبراهيم خالد ممدوح، المرجع السابق، ص86.

[25] – نفس المرجع، ص87، 88.

[26] – بوخبزة عائشة، المرجع السابق، ص62.

[27] – بوخبزة عائشة، المرجع السابق، ص62.

[28] – المواد من 394 مكرر إلى 394 مكرر 8 من قانون العقوبات.

[29] – ونوغي نبيل، زيوش عبد الرؤوف، المرجع السابق، ص133.

[30] – قارة أمال، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجستير في القانون، كلية الحقوق، جامعة الجزائر، 2001، ص44.

[31] – بوخبزة عائشة، المرجع السابق، ص82.

[32] – حسني محمود نجيب، النظرية العامة للقصد الجنائي، دار النهضة العربية، 1971، ص90.

[33] – ونوغي نبيل، زيوش عبد الرؤوف، المرجع السابق، ص136.

[34] – فضيلة عاقلي، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر "الجرائم الالكترونية"، طرابلس، 24، 25 مارس 2017، ص120.

[35] – بوضياف اسمهان، المرجع السابق، ص361.

[36] – رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الانترنيت، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة أبي بكر بلقايد، تلمسان، 2011–2012، ص88.

[37]– راجع الصفحة 5 و6 من هذه الدراسة.

[38] – القانون 16–02 المؤرخ في 19 جوان 2016 المعدل والمتمم للأمر 66–156 المتضمن قانون العقوبات

[39] – فضيلة عاقلي، المرجع السابق، ص130.

[40] – بوضياف اسمهان، المرجع السابق، ص364.

[41] – بوضياف اسمهان، المرجع السابق، ص366.

[42] – المادة 05 من القانون 04/09

[43] – المواد 6، 7، 8 من القانون 04/09.

[44] – المادة 8 من القانون 04/09.

[45] – المادة 10 من القانون 04/09.

[46] – المادة 11 من القانون 04/09.

[47] – المادة 12 من القانون 04/09.

[48] – المادة 15 من القانون 04/09.

[49] – المادة 16 من القانون 04/09.

[50] – المادة 18 من القانون 04/09.

[51] – المرسوم الرئاسي 172/19 المؤرخ في 6 جوان 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج.ر عدد 37 الصادرة بتاريخ 9 جوان 2019.

[52] – المادة 2 من المرسوم الرئاسي 172/19.

[53] – مصطفى عبد النبي، المرجع السابق، ص405.

[54] – بوضياف اسمهان، المرجع السابق، ص370.

[55] – المرسوم التنفيذي 348/06 مؤرخ في 5 أكتوبر 2005، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج.ر عدد 63، الصادرة بتاريخ 8 أكتوبر 2006.

[56] – إيمان رتيبة شويطر، الأقطاب الجزائية المتخصصة كتوجه لمكافحة جرائم الأعمال، مجلة البحوث في العقود وقانون الأعمال، المجلد 7، العدد1، 2022، ص51.