وزارة التعليم العالي و البحث العلمي

جامعة عمار ثليجي بالأغواط

كلية الحقوق والعلوم السياسية

قسم : الحقوق

عنوان المذكرة :

التحقيق الجنائي في الجرائم الإلكترونية

مذكرة مكملة لنيل متطلبات شهادة الماستر في تخصص القانون الجنائي و العلوم الجنائية

من اعداد:

–صباح تومي

المشرف:

* الدكتور محمد ذيب

لجنة المناقشة :

الإسم واللقب	الرتبة	الصفة
البروفيسور بوعيشة بوغفالة	أستاذ تعليم عالي	رئيسا
الدكتور محمد ذيب	أستاذ محاضر	مشرفا
الدكتور عبيدي محمد	أستاذ محاضر	مناقشا

السنة الجامعية : 2021/2020


بسم الله الرحمن الرحيم

إهداء

الى من لا يمكن للكلمات ان توفي حقهما، الوالدين الكريمين.

الى سندي في الحياة أخي مصطفى.

الى اعظم هبة وهبها الله لي.

الى أعذب لفظ تلفظت به الشفاه البشرية.

الى من اتلمس خطواتي بوجودهم

الى من تحلو الحياة برفقتهم أولادي (ريتال، و رامي)

أهدي ثمرة جهدي

صباح تومي

شكر وتقدير

في البداية أحمد الله الذي أعطاني القوة و الصبر لإتمام هذا العمل العلمي المتواضع ثم اتوجه بجزيل الشكر و الإمتنان الى الدكتور محمد ذيب لقبوله الاشراف على هذه الأطروحة كما أشكر اعضاء اللجنة الموقرة لقبولهم مناقشة هذه الأطروحة.

مقدمة

مقدمة

قد شهد العقد الأخير من القرن العشرين غزوا تكنولوجيا أدى إلى ظهور اختراعات هائلة على المستوى التقني، من بينها ظهور الحاسبات الآلية التي أصبحت لها قيمة لما تحتوي عليه من معلومات يمكن تخزينها واسترجاعها في ثوان معدودة، مما سهل مختلف المعاملات التي شملت مختلف الميادين منها الميدان الاقتصادي،الاجتماعي،السياسي....الخ بـ إلا انه مع التقدم العلمي والتكنولوجي الذي مس مختلف مجالات الحياة، وجعل من العالم خلية مترابطة بشبكات إلكترونية حطمت الحواجز أمام التواصل بين الشعوب وسهلت المعاملات بين الأفراد من مختلف مناطق العالم، ظهر نوع جديد من الإجرام حيث أصبحت التقنيات الحديثة وسيلة لارتكاب مختلف الجرائم التقليدية في أسرع وقت دون أن تترك أي اثر يدل على المجرم وقد مرت هذه الجريمة بتطور تاريخي مصاحبا لتطور التقنية واستخداماتها حيث ظهر هذا النوع من الجرائم في بداية الستينيات بأول معالجة لما يسمى بالجريمة الإلكترونية على المقالات والمواد الصحافية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والاستخدام غير المشروع للبيانات المخزنة في نظم الكمبيوتر، وقد ثار جدل حول ما إذا كانت هذه الأفعال مجرد سلوكيات غير أخلاقية في بيئة الحوسبة، أم أنها تكتسب الصفة الجرمية وبالتالي تعتبر أفعال يعاقب عليها القانون، ومع بداية السبعينيات اكتسبت الصفة الإجرامية وذلك بعد إجراء عدة دراسات مسحية وقانونية اهتمت بالجرائم الإلكترونية وعالجت عددا من القضايا الفعلية .وتكمن أهمية الموضوع في أن الجريمة الإلكترونية من الجرائم المستحدثة التي توجب الدراسة والتحليل أكثر، والتحقيق فيها يتطلب مهارات فنية وتقنية والخبرة في مجال الحاسب الآلي والانترنيت اللذين اعتبرا وسيلتين أساسيتين لارتكاب الجريمة الإلكترونية،

وما يزيد الموضوع أهمية هو خطورة هذه الجريمة وانتشارها بسرعة رهيبة وعجز القوانين التقليدية على مواكبة هذه السرعة

جرائم الحاسوب بأنها كل عمل او امتناع ياتيه الانسان اضرار في مكانات الحاسوب المادية او المعنوية وشبكات الاتصال الدولية للمعلومات باعتبارها من مصالح الوطنية التى توجب الحماية الجنائية لها ان شبكة المعلومات الدولية عبارة عن اداه للربط والاتصال بمختلف شعوب العالم وان ساء الاستخدام هذه الشبكة او استغلالها على نحو غير مشروع يؤدي الى ظهور طائفة جديدة من الجرائم التى عرفت بالجرائم المعلوماتية وحيث ان جرائم الحاسوب جزء من الجرائم الاقتصادية الحديثة لانها تسبب خسائر مادية تلحق بالمجتى عليه مقابل ما يحققه الفاعل من مكاسب فهي جرائم ضد المال مرتبطة باستخدام المعلومات المخزنة داخل حاسوب كما ان نمو التجارة الالكترونية ادى الى قيام المنافسة غير المشروعة وازدادت من جرائم الاحتيال والغش المعلوماتي وايضا تم استخدام شبكة الانترنت لاهداف سياسية لترويج المعلومات والافكار والاديوجيات التى تتلائم مع مصالحهم مما يؤثر في الافكار السياسية بحيث يؤثر طرف ضد طرف اخر مما يخلق جرائم سياسية قد تمس بأمن الدولة نبعت أهمية الدراسة من تزايد معدلات الجريمة المعلوماتية، بما يمثله ذلك من تهديد للأمن العام يعود بالسلب على الأنظمة الاقتصادية والاجتماعية للدول، وبالنظر إلى الطبيعة الخاصة لتلك الجرائم والمتمثلة في صعوبة إثباتها أو صعوبة التوصل إلى مرتكبيها بأدوات البحث الجنائي التقليدية، الأمر الذي استوجب على سلطات الضبط القضائي مسايرة هذه الأنماط من الجرائم من خلال الاستعانة بالتقنيات العلمية الحديثة خلال مرحلة جمع الاستدلالات، كما تكمن أهمية الدراسة في محاولة إيجاد الحلول التشريعية لمكافحة تلك الجرائم.

انطلاقًا من الأهمية البالغة لهذا الموضوع تبين أن هناك حاجة للبحث المتعمق في المسائل الإجرائية والعملية المتصلة بتحقيق وإثبات جرائم المعلومات، لذا فإن هذه الدراسة تنصب على سبر غور المسائل القانونية والفنية ذات الصلة بسلطة مأمور الضبط القضائي في مواجهة الجريمة بشكل عام وجرائم المعلومات بشكل خاص، وتهدف الدراسة إلى تحديد مفهوم هذه الجرائم وأنماطها وخصائصها، وبيان الأصول الإجرائية والعملية لإجراءات الاستدلال في البيئة الرقمية، كما تسلط الضوء على التحديات التي يواجهها مأمور الضبط القضائي في التعامل مع هذا النمط المستجد من الجرائم

أ- الاشكالية :

ما مدى قابلية تطبيق القواعد التقليدية لإجراءات التحقيق في الجريمة الإلكترونية ؟

وتتفرع عن هذه الإشكالية عدة إشكاليات أخرى:

- ما المقصود بالجريمة الالكترونية ؟
- بما تتميز الجريمة الإلكترونية عن غيرها من الجرائم ؟
- هل توجد أجهزة خاصة بالتحقيق ؟

وللإجابة عن هذه الإشكالية قسمت البحث إلى فصلين:

الفصل الأول بعنوان: جهاز التحقيق في الجريمة الالكترونية للتشريع الجزائري ، حيث عالجت ماهية الجريمة الإلكترونية في المبحث الأول منه والذي قسمته بدوره لمطلبين، خصصت المطلب الأول لدراسة مفهوم الجريمة الإلكترونية، وعرضت الأركان التي تقوم عليها الجريمة الإلكترونية في المطلب الثاني، أما المبحث الثاني من هذا الفصل فقد تناولت فيه التحقيق في الجريمة الإلكترونية من حيث المفهوم في المطلب الأول، والمطلب الثاني ذكرت فيه جهاز التحقيق الجنائي في الجريمة الالكترونية وما يواجهه من صعوبات في سبيل الكشف عنها

اما الفصل الثاني المعنون بحلول الاجرائية لادراك الجريمة الالكترونية عالجت فيه اهم الاجراءات الدولية و الوطنية في مكافحة هذه الجرائم الالكترونية تم المبحث الثاني الدي يتاول التوعية و التحسيس لخطورة هذه الحريمة

ب-**منهج الدراسة** :

قد اعتمدت على المنهج التحليلي في دراستي هذه، لتبيان مفهوم كل من الجريمة الإلكترونية والتحقيق، ومناقشة الإجراءات المتخذة للتصدي لهاته الجريمة المستحدثة.

ت- اسباب اختيار هذه الدراسة :

الأسباب الذاتية:

فإن ما دفعني لاختيار هذا الموضوع هو رغبتي في التعرف على هذا النوع المستحدث من الإجرام الذي انتشر بصورة ملفتة في المجتمع الجزائري مؤخرا، ولأنها ترتبط بالتقنية الحديثة وتعتبر من سلبياتها لابد من أنها تتميز بمجموعة من الخصائص مقارنة مع باقي الجرائم التقليدية، مما يستدعي الوقوف ومعرفة إن كانت هناك إجراءات خاصة في مجال البحث والتحري، ومدى إمكانية تطبيق القوانين التقليدية لمواجهة الجريمة الإلكترونية كذلك دفعني الفضول لمعرفة بما يحكم به القاضي في مثل هذه الجرائم، إن كان يستعين بالنصوص التقليدية أم أن هناك قوانين خاصة يلجأ إليها ورغبتي فيزاالة الغموض عن هذه الجريمة.

الأسباب الموضوعية :

تسليط الضوء على جريمة باتت الحديث الرئيسي في مجالسنا سواء في بيوتنا أو في شوارعنا لكثرة إنتشارها وظهورها بأبشع صورها.

تطور خطورة هذه الجريمة مع تطور تكنولوجي.

ث- اهمية الموضوع :

أهمية الموضوع ولقد قمنا باختيار هذا الموضوع وجعلناه موضوع دراستنا في هذه المذكرة نظرا للأهمية البالغة لموضوع الإثبات الجنائي في الجرائم المعلوماتية، وتظهر هذه الأهمية من خلال اعتبار أن موضوع الجرائم المعلوماتية حديث وكثير

الانتشار حاليا، كما أنه من الموضوعات التي تثير جدلا افقهي لدى فقهاء القانون الجنائي، إضافة إلى تعلق هذا الموضوع بالوسائل الحديثة ذلك أنه كلما تطورت الوسائل الإلكترونية كلما تطور أسلوبراتكاب هذا النمط من الجرائم، وهذا ما شكل عائق ا أمام القائمين على البحث وإثبات الجرائم المعلوماتية ، حيث أن قواعد البحث والتحقيق وأسس الإثبات الجنائي في القوانين 3التقليدية لا تكفي ، بل يحتاج هذا النوع من الجرائم إلى استحداث تشريعات جديدة تتلائم مع طبيعتها الفنية

ج- اهداف البحث :

أهداف البحث إن الغاية المرجوة من هذه الدراسة تتمثل أساسا في تحديد طرق وكيفية الوصول واستخـلاص أدلة الإثبات الجنائية في الجرائم المعلوماتية، كما تهدف هذه الدراسة إلى تقديم رؤية خاصة بشأن التحقيق الجنائي في هذه الجرائم ، كون أن مسرح الجريمة الرقمي هو مسرح افتراضي غير مرئي و كما تناولت الدراسة الصعوبات التي تواجه التحقيق الجنائي، ولفت الانتباه من خلال هذه الدراسة إلى أن الدليل الرقمي و تحديد ماهيته يعتبر من أهم أدلة الإثبات في الجرائم المعلوماتية، وق دـ تعرضت الدراسة أيضا إلى المشكلات التي تعيق تحديد الاختصاص المكاني في هذا النوع من الجرائم العابرة للحدود و مدى سلطة القاضي الجنائي في قبول الدليل الرقمي أمام المحاكم كدليل إثبات جنائي في الجرائم المعلوماتية

لا يفوتنا القول أنه تلقينا صعوبات جمة في اختيار موضوع البحث في حد ذاته، كون أن هذا الموضوع - الإثبات الجنائي في الجرائم المعلوماتية - حديث لم يسبق بحثه بوضوح وتعمق ولو أن هناك مراجع ومقالات تناولت هذا الموضوع ، إلا أنها لم تعالجه من كل جوانبه أو أدرجته بشكل سطحي، إضافة إلى أن الجرائم محل الدراسة ترتبط بالحاسب الآلي مما يتطلب الإلمام بمكوناته بنو ظام المعالجة الآلية

للمعلومات والشبكات الإلكترونية، وكما يحتاج الأمر إلى دراية باللغة والمصطلحات التقنية والفنية، وهذا ما يتطلب جهد كبير ناهيك عن الجهد القانوني.

الفصل الاول :

الجريمة الالكترونية في التشريع الجزائري

تعد الجريمة الإلكترونية ظاهرة إجرامية حديثة نظرا لإرتباطها بالتكنولوجيا الحديثة، فقد ترتب على ذلك إحاطة هذه الظاهرة بكثير من الغموض، لأجل ذلك فقد بدا لنا أنه وقبل الخوض في الإجراءات التي تطبق على الجرائم الإلكترونية، إذا يجب الإلمام الجريمة الإلكترونية وخصائصها وأيضا التطرق إلى الأجهزة المختصة في التحقيق في الجريمة الإلكترونية . وعلى ضوء ذلك سنقسم الفصل الأول إلى الجريمة الإلكترونية وكيفية التحقيق فيها في المبحث الأول أما المبحث الثاني سيكون تحت عنوان السلطات المختصة في الجريمة الإلكترونية.

❖ المبحث الأول: الجريمة الإلكترونية و التحقيق فيها في التشريع الجزائري.

أثيرت العديد من التساؤولات حول تحديد الطبيعة القانونية للجريمة الإلكترونية، ويرجع سبب ذلك إلى تعدد وجهات النظر بخصوص هذا النوع من الجرائم، حيث ظهرت عددتراءاء فقهية في محالة فهم المقصود بالجريمة الإلكترونية . وقد تبنى المشرع الجزائري للدلالة على الجريمة الإلكترونية، مصطلح المساس بالأنظمة المعالجة الآلية للمعطيات، حيث يمثل نظام المعالجة الآلية للمعطيات المسئلة الأولية أو الشرط الأولي الذي يلزم تحقيقه . وذلك فالمشرع الجزائري لم يبعرف نظام المعالجة فأوكل مهمة تعريفه لكل من الفقه والقضاء.

وعليه سنحاول من خلال هذا المبحث أن نتطرق إلى الجريمة الإلكترونية والتحقيق فيها، حيث يتضمن المطلب الأول التعريف بالجريمة الإلكترونية وخصائصها وأنواعها، أما المطلب الثاني سنتطرق إلى التحقيق فيها في التشريع الجزائري

.المطلب الأول: مفهوم الجريمة الإلكترونية

مفهوم الجريمة :

لغة: جرم أي قطع الشئ، يقال الجريم التمر اليابس، جرامة ماسقط من ثمر النخل. الجريمة: النواة للتمر، جرم جريمة و إجرام إليه أو عليه بمعنى أذنب والجرم هو الخطأ.[1]

إصطلاحا: لم يتطرق قانون العقوبات الجزائري إلى تعريف الجريمة حتى لا يحرج الفقهاء من جهة على تأويل حرفية النص طبقا للقاعدة الفقهية التي تقول لا اجتهاد مع صراحة النص الآمر، ومن جهة أخرى فإن المشرع حتى ولو وضع تعريفا شرعيا للجريمة فسوف يخفق في جمع كل معاني مدلول لفظ الجريمة. وعليه

[1] الموسوعة العربية الالكتونية على الرابط :http://droit7.blogspot.com/2019/09/blog-post_15.html #

فقد عرفها فريق أول من الفقهاء بأن الجريمة هي ظاهرة إجتماعية استهجنها الرأي العام فتدخل القانون لحصرها ورصد لها عقوبة أو تدابير أمن، وفريق ثان عرفها بأنها كل سلوك إيجابي أو سلبي يأمر القانون معاقبة مرتكبه، ونحن نميل إلى التعريف التالي: بأن الجريمة هي القيام بعمل أو الامتناع عنه يعتبره القانون غير مشروع إذا لم يبرره إستعمال حق ويقرر له القانون عقوبة أو تدابير[1] .

مفهوم الجريمة الالكترونية :

ظاهرت تعاريف كثيرة حول تعرف الجريمة الإلكترونية ما بين مضيف لمفهومها وموسع كما تعددت المصطلحات المستخدمة للدلالة عليها فالبعض استخدم مصطلح جرائم استخدام الحسابات أو جرائم المعالجة الآلية للبيانات والبعض الآخر أطلق عليها اسم الإجرام المعلوماتي، وفيما يلي: تفصيل لمفهوم هذه الجريمة من حيث التعريف والخصائص

.الفرع الأول: تعريف الجريمة الإلكترونية :

تعتبر الجريمة الإلكترونية من الظواهر الحديثة لإرتباطها بتكنولوجيا الحديثة، ولقد تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لها، حيث لم يتفق الفقه على تعريف محدد بل إذ بعض الفقهاء، ذهب إلى ترجيح عدم وضع تعريف بحجة أن مثل هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب إلكتروني[2]

[1] الموسوعة العربية الالكتونية على الرابط :http://droit7.blogspot.com/2019/09/blog-post_15.html #

[2] خالد ممدوح، أمن الجريمة الإلكترونية، الدار الجامعية، الإلكترونية، الإسكندرية، 2008 ،ص .41

أولا: تعريف الجريمة الإلكترونية لغة.

الجريمة لغة مأخوذة من الجرم وهي الذنب والجناية، جمعها جرائم، وجرم الشيء قطعه ٍ ليهم، ذنب وجنى جنتئة(وجرمه الرجل على قومه [1]

.ثانيا: تعريف الجريمة إصطلاحا : معظم الفقهاء المؤلفين في هذا الباب يردون تعريف الجريمة في الفقه إلى ما قرره الموارديي في الأحكام السلطانية بقوله: " الجرائم محظورات شرعية زجر الله عنها بحد أو تعزير يعني إذا كانت ممن يتعمدراتكابها، أما الإمام أبو زهرة فبعدها ذكر تعريف الماوردي وأيده ساق من بين نصوصه تعريف آخر للجريمة فقال " هي المعصية التي يكون فيها عقاب يقرره القضاء "[2])

.ثالثا: تعريف الجريمة الإلكترونية فقها وقانونا.

ـ أ التعريف الفقهي: انقسم الفقه إلى عدةرااء منهم من ضيق من مفهوم الجريمة الإلكترونية ومنهم من وسع من مفهومها، الاتجاه الذي يضيق من مفهوم الجريمة الإلكترونية . يذهب أنصار هذا الإتجاه إلى حصر الجريمة الإلكترونية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية فيراتكابها ومن التعريفات التي وضعها أنصار هذا الإتجاه أن الجريمة الإلكترونية هي كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لإرتكابه من ناحية وملاحقته وتحقيقه من ناحية أخرى.

وفي هذا الإتجاه أيضا الجانب الفقهي بالنظر إلى معيار نتيجة الإعتداء، إذ يرى الأستاذ MASSأن المقصود بالجريمة الإلكترونية هي اعتداءات ترتكب بواسطة المعلومات بغرض تحقيق ربح

[1] ضياء مصطفى عثمان، السرقة الإلكترونية، دار النفائس، عمان، الطبعة الأولى، 2011 ،ص .32
[2] بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، 2014 ،ص . 9

.كما عرف الأستاذ PARKER الجريمة الإلكترونية بأنها كل فعل إجرامي متعمد أيا كان (صلة بالمعلوماتية ينشأ عنها خسارة تحلق بالمجني عليه أوكسب يحققه الفاعل[1]

.الإتجاه الذي يوسع من مفهوم الجريمة الإلكترونية: عرف أصحاب الإتجاه الموسع الجريمة الإلكترونية بأنها سلوك إجرامي يتم بمساعدة الكمبيوتر أو هي جريمة تتم في محيط أجهزة الكمبيوتر، أو هي كل سلو ك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها،

كما عرفها الفقيهان credo&Michels بأنها سوء استخدام الحاسب أو جريمة الحسابات تسهل استخدام الحاسوب كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه البيانات الخاصة، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية على جهاز الحاسب ذاته أو المعدات المتصلة به، وأيضا الاستخدام غير المشروع أو سرقة جهاز الحاسب في حد ذاته أو أي مكون من مكوناته[2] .

- ب التعريف القانوني: أما بالنسبة للتعريف الذي جاء به المشرع الجزائري للجرائم المتصلة للتكنولوجيات الإعلام والإتصال فإنه يعرفها بأنها «: جرائم المساس بأنظمة المعالجة الآلية للامعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهلراتكابها عن طريق منظومة معلوماتية أو نظام الإتصالات الإلكترونية

وبهذا فقد وفق المشرع برأينا في تعريفه لأنه جمع الحالات التي تكون فيها نضم المعلوماتية وشبكات الإتصال إما موضوعا للجريمة أو وسيلة أو دعامة للجرائم التقليدية. ولول هذه النضم المعلوماتية وشبكات الإتصال ما كان أن نسبغ صفة المعلوماتية على هذه الجرائم

[1] محمد أمنية الشوايكة جرائم الحاسوب والأنترنت (الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2009 ، 8.ص
[2] سميرة معاشي، ماهية الجريمة الإلكترونية، مجلة المنتدى القانوني، العدد السابع، جامعة، بسكرة، ص 276.

. وعلى خلاف المشرع الفرنسي الذي لم يعطي تعرفا للجريمة الإلكترونية فإن المشرع الجزائري قد اصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وعرفها بموجب المادة 02 من القانون 09 -04 على أنها «: جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أي جريمة ترتكب أو يسهلراتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية

«.ويلاحظ على هذا التعريف ما يلي -أن المشرع قد اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الالكترونية أولها معيار وسيلة الجريمة وهو نظام الاتصالات الالكترونية، وثانيها معاير موضوع الجريمة المساس بأنظمة المعالجة الآلية للمعطيات، وثالثا معيار القانون الواجب التطبيق أو الركن(الشرعي للجريمة المنصوص عليها في قانون العقوبات [1] .

-كما حدد المشرع الجزائري نطاق الجريمة الإلكترونية وذلك عن طريق إقراره بأن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهلراتكابها عليه، وهذا ما يوسع من نطاق مجال الجرائم الالكترونية في القانون الجزائري

.الفرع الثاني: خصائص الجريمة الإلكترونية وأنواعها

.إذ ما نقصد به ذاتيه الجرائم الإلكترونية هو استقلاليتها وتميزها من غيرها من الجرائم سيما التقليدية منها، وذلك بمجوعة من الخصائص أثرت بشكل مباشر على التشريعات العقابية«. لإجرائية التقليدية القائمة، وسوف نحاول أن تبرز أهم خصائص المجرم الإلكتروني والمجني(عليه الجريمة الإلكترونية وأنواع المجرمين الإلكترونيين وصفاتهم[2]

[1] بوظياف إسماهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، العدد 11 ،سبتمبر 2018 ،ص - 353 . 352

[2] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، 2013 ،ص .31

.أولا: خصائص الجريمة الإلكترونية

.الفرع الأول :خصائص الجرائم المعلوماتية

ما إن نقصد به من ذاتية الجرائم المعلوماتية هو استقلاليتها وتميزها عن غيرها من الجرائم سيما التقليدية منها، وذلك بمجموعة من الخصائص أثرت بشكل مباشر على التشريعات العقابية والإجرائية التقليدية القائمة، وسوف نحاول أن نبرز أهم هذه الخصائص فيما يلي

-أ الجريمة المعلوماتية متعدية للحدود (عابرة للوطنية): إنه وبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال أسفر هذا الأمر إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد، حيث يمكن أن ترتكب الجريمة من مجرم في دولة على مجني عليه في دولة أخرى في وقت يسير .اجد فالجريمة المعلوماتية ذابه الشكل لا تعترف بالحدود بين الدول وهي بذلك شكل جديد من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة، ذلك أن قدرة تقنية المعلومات على إختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم انعكست على طبيعة الأعمالى الإجرامية التي يعتمد فيها ا لمجرمون إلى استخدام هذه التقنيات في خرقهم للقانون، وهو ما يعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا، إذ أن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين المعلومات محل الاعتداء،

فقد يوجد الجاني في ما بلد ويستطيع الدخول الى ذاكرة الحاسب الآلي الموجود في بلد آخر، وهو بهذا السلوك قد يضر شخصا آخر موجود في بلد ثالث، أو القيام بإعداد أحد البرامج ا لخبيثة) Vérus) في ثم ما بلد يتم نسخ هذا البرنامج ويرسل إلى دول مختلفة من العالم.

وتظهر هذه المشكلة بصفة خاصة في التعاملات البنكية عبر شبكات المعلومات الدولية، حيث أدى التوسع الكبير لإجراء التعاملات البنكية عبر شبكات المعلومات الدولية إلى إعطاء بعد دولي لهذه الجرائم ذلك أن ربط وسائل الإتصالات بالحاسبات الآلية ضاعف من المعاملات المالية الدولية والتي أصبحت تتم بواسطة وسائل إلكترونية، وبصفة خاصة من خلال التحويل الإلكتروني للأموال والتبادل الإلكتروني للمعلومات

.ومفاد ما سبق ذكره أن الجرائم المعلوماتية تتميز بالتباعد الجغرافي بين الفاعل والمجني عليه ومن الوجهة التقنية التباعد بين أداة الجريمة ومحلها، وهذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة أو خارجها ليطال دولة أخرى يتواجد فيها نظام الحاسوب المخزنة فيه المعلومات محل الإعتداء

.ولقد أثارت هذه الخاصية الدولية للجريمة المعلوماتية عدة إشكالات قانونية تتعلق أساسا بتحديد الدولة صاحبة الاختصاص القضائي في محاكمة مرتكب هذه الجريمة، فهل هي الدولة التي وقع فيها النشاط الإجرامي أم التي أضيرت مصالحها نتيجة هذا التلاعب، بالإضافة إلى إشكالية مدى فعالية القوانين القائمة في التعامل مع الجريمة المعلوماتية، وبصفة خاصة مسألة جمع الأدلة وقبولها،

إذ تتباين مواقف الدول فيما يتعلق بقبول الأدلة المستخلصة من أنظمة الحاسبات الآلية . وغيرها من المشاكل التي يمكن أن تثيرها الجرائم العابرة للوطنية بشكل .عام لذلك فقد لفتت هذه المشكلات النظر إلى ضرورة إيجاد الوسائل المناسبة

لتشجيع التعاون الدولي لمواجهة الجريمة المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم لمختلف الدول . ومن أجل ذلك فقد تعالت الأصوات الداعية إلى التعاون الدولي المكثف من أجل التصدي لها بحزم، وأن يشمل هذا التعاون تبادل المعلومات وتسليم ا لمجرمين وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى .

ولكن ومع ضرورة هذا التعاون والمناداة به إلا أنه تقف أمام هذا المبدأ عقبات ومعوقات تحول دون تحققه وتجعله صعب المنال، من أهمها انعدام نموذج موحد للنشاط الإجرامي المكون للجريمة المعلوماتية، وأن كثيرا من القوانين لم يتم تعديلها بحيث تتواءم مع هذه الجرائم حتى يتسنى إدراجها ضمن الإتفاقيات الدولية الخاصة بتبادل المساعدة الجنائية في مجال الجرائم المعلوماتية، بالإضافة إلى تنوع واختلاف النظم القانونية والإجرائية. واثباتها- :

ب صعوبة اكتشاف الجريمة المعلوماتية

تقع الجريمة المعلوماتية في بيئة افتراضية تقنية لا تترك أية آثار محسوسة، إذ يغلب عليها أنها تتم في الخفاء لأن الجناة يعمدون في كثير من الأحيان إلى إخفاء نشاطهم الجرمي عن طريق تلاعبهم بالبيانات، والذي يتحقق أحيانا لم إن نقل في الغالب في غفلة من المجني ِواثبا ،تها عليهم . كما أنه من السهل عليهم تدمير الأدلة ومحوها مما يعقد أمر كشف الجريمة ِذا وا ما قورنت حالات اكتشاف الجريمة المعلوماتية على ضوء ما يتم اكتشافه من الجرائم التقليدية فإن عددها قليل، فمعظم الجرائم المعلوماتية تم اكتشافها بالمصادفة وبعد وقت طويل وا هي ِ منراتكابه، ذلك أن هذا النمط الإجرامي لا يحتاج إلى عنف أو جثث أو اقتحام نما معلومات وبيانات تغير أو تعدل أو تمحى كليا أو جزئيا من السجلات المخزونة في ذاكرة الحاسب الآلي فلا تترك أثرا خارجيا مرئيا أو ملموسا فهي كما وصفها بعض الفقهاء بأ نها جريمة هادئة بطبيعتها لا تتطلب سوى عدد من اللمسات الخاطفة على لوحة المفاتيح

حتى تؤدي إلى اختراق المعلومات المخزنة في الحاسب الآلي وهتك سريتها ومحوها أو تشويهها أو تعطيل الأنظمة التي تحتويها . فالجريمة المعلوماتية من الجرائم المستحدثة التي لا تترك شهودا يمكن الإستدلال بأقوالهم ولا أدلة مادية يمكن فحصها نما وا تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بواسطة نبضات إلكترونية غير مرئية .

كما ذهب البعض للقول بأن صعوبة اكتشاف الجريمة المعلوماتية وكذا صعوبة إثبا اته راجع أيضا إلى عدة أسباب، من بينها وسيلة تنفيذها والتي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد ومن ف ثم إنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، إذ أنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات وذلك سواء لارتكابها أو التحقيق فيها أو لملاحقة مرتكبيها .فأحيانا نجد رجال الضبطية القضائية غير قادرين على التعامل بالوسائل الإستدلالية والإجراءات التقليدية مع هذا النوع من الجرائم . بالإضافة إلى صعوبة الإحتفاظ الفني بدليل الجريمة المعلوماتية، إذ للمجرم المعلوماتي القدرة على تدمير الدليل في أقل من ثانية ويمكن اعتبار أنه من بين الأسباب أيضا التي تقف وراء صعوبة اكتشاف الجريمة المعلوماتية ثباتها المجني عليهم وا أنفسهم، ذلك أن هؤلاء قد يلعبون دورا رئيسيا في ذلك من خلال الإحجام عن الإبلاغ عنها في حالة اكتشافها، حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للإنتهاك أو تمنى بخسائر فادحة من جراء ذلك عن عدم الكشف حتى بين موظفيها عما تعرضت له وتكتفي باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهزا للثقة في كفاءتها ويبدو ذلك أكثر وضوحا في المؤسسات المالية مثل البنوك والمؤسسات الإدخارية ومؤسسات الإقراض

.حيث تخشى مجالس إدار تها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها، حيث أن الجانب الأكبر من الجرائم المعلوماتية لا يتم الكشف أو

التبليغ عنه، وهو ما يؤثر سلبا على السياسة التي يمكن أن توضع لمكافحتها . تم وقد طرح عدة اقتراحات تكفل تعاون المجني عليه في كشف هذه الجرائم وبالتالي انقاص حجم الإجرام المعلوماتي الخفي، ومن هذه الاقتراحات التي طرحت لحمل المجني عليه على التعاون مع السلطات في الولايات المتحدة الأمريكية مطالبة البعض بأن تفرض النصوص المتعلقة بجرائم المعلوماتية على عاتق موظفي الجهة المجني عليها بالإبلاغ عما يصل علمهم به من جرائم في هذا المجال مع تقرير جزاء على الإخلال بهذا الإلتزام . وعرض ذات الإقتراح على لجنة خبراء مجلس أوروبا ولاقت الفكرة رفضا باعتبار أنه ليس مقبولا تحويل المجني عليه إلى مرتكب الجريمة

. ثانيا: أنواع الجريمة الإلكترونية

.نظر ا لانتشار الجريمة الالكترونية بشكل كبير فقد تعددت أنواع هذه الجرائم وأهمها ما يلي

الجريمة المادية: هي التي تسبب أظرارا مادية على الضحية أو المستهدف من عملية النصب وتؤخذ واحدة من الأشكال الثلاثة التالية:

-عملية السرقة الإلكترونية كالاستيلاء على ماكنات الصرف الآلي، والبنوك كتلك المنتشرة في الكثير من الدول وبها يتم نسخ البيانات الاكترونية لبطاقة الصراف الآلي ثم استخدامها لصرف أموال حساب الضحية

- . إنشاء صفة إنترنت مماثلة جدا لموقع أحد البنوك الكبرى أو المؤسسات المالية الضخمة

- .الرسائل البريدية الواردة من مصاغدر مجهولة بخصوص طلب المساهمة في تحرير الأموال من الخارج من الوعد بنسبة من المبلغ أو تلك التي توهم صاحب البريد الالكتروني بفوزه بأحدى الجوائز أو الينا صيب

. الجريمة الثقافة : هي استيلاء المجرم على الحقوق الفكرية ونسبتها لهم دون موافقة الضحية وتكون على إحدى الصور الآتية -

قرصنة البرمجيات وهي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية على اصطرانات وبيعها للناس بسعر أقل

- .التعدي على القنرات الفضائية المشفرة واتاحتها عن طريق الانترنت من خلال تقنية - Soft . Copy جريمة لنسخ المؤلفات العلمية والأدبية بالطرق الالكترونية المستحدثة.

الجريمة السياسية والاقتصادية : تستخدم المجموعات الارهابية حاليا تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية وهم لا يتوانون عن استخدام الوسائل المتقدمة مثل: الاتصالات والتنسيق وبث الأخبار المغلوطة وتوظيف بعض صغار السن وتمويل بعض الأموال في سبيل تحقيق أهدافهم - . الاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على نشر الفيروسات - . نشر الأفكار الخاطئة بين الشباب كالإرهاب والادمان والزنة لفساد الدولة لأسباب سياسية واقتصادية بالدرجة الأولى

.الجريمة الجنسية :هذا النوع من الجريمة يمكن أن يتمثل في إحدى الصور الآتية - **الإبتزاز:** من أشهر حوادث الابتزاز عندما يقوم أحد الشباب باختراق جهاز إحدى الفتيات أو الاستيلاء عليه وفيه مجموعة من صورها واجبارها على الخروج معه أو فضحها بما يملكه من صورها

- .**التغرير والاستدراج:** في العادة هذه الصورة عندما يتعرف أحد الشبان على إحدى الفتيات عبر برامج المحادثة يكون مع علاقة معها ثم يستدرجها بالكلام ويوهمها بالزواج لكي تثق به ومن ثم يقوم بتهديدها بما يملكمه من صور وتسجيلات من صوتها إن لم تستجب(لطلباته[1] .

جرائم حسب الأفراد : هي الجرائم التي يتم الوصول فيها إلى الهوية الإلكترونية للأفراد بطرق غير شرعية، كحسابات البريد الإلكتروني وكلمات السر التي تخصهم وقد تصل إلى انتحال شخصياتهم وأخذ صور وملفات المهمة من أجهزتهم بهدف تهديدهم وينطوي تحت هذا القسم من الجرائم كل من[2]

أ- جرائم التشهير بهدف تشويه سمعت الأفراد

ب-جرائم السب والشتم والقذف.

ت- جرائم المطاردة الالكترونية)

لثاثا : المجني عليه في الجريمة الإلكترونية

. المعتدي عليه في الجريمة الإلكتورنية هو من يكون ضحية الإعتداءات غيرالمشروعة على مكونات الحاسوب، وقد يكون شخصا طبيعيا، شركة، أو مؤسسة تتعامل بمجال الحاسوب أثناء ممارسة الأعمال التجارية، الاقتصادية والسياسية التي ينبغي أن يستغل الحاسوب في إدارة أعمالها، وحسب تقديرات بعض خبراء الصندوق الدولي للبنوك، فإنه من المستحيل أن تحدد على نحو دقيق نطاق الجريمة الإلكترونية التي لا يعلم ضحاياها عنها شيئا إلا عندما تكون النظم المعلوماتية المملوكة لهم هدفا للجريمة الإلكترونية، حتى في حالة عملهم بذلك فهم يفضلون عدم إفشاء الفعل لأنه لا يوجد من يريد الإعتراف بأنه تم إنتهاك نظامه المعلوماتي . والجدير بالذكر أن سلبية المجني عليهم أو ضحايا الجريمة الإلكترونية،

[1] نواوي سليمة، دور الدرك الوطني في محاربة الجريمة الالكترونية، جامعة مسيلة، 2019/2018 ،ص . 27 -25

[2] بن سولة نور الدين، الجرائم الالكترونية في ضوء التشريع الجزائري، المجلد التاسع، العدد 1 ،مارس 2018 ،ص272

وخوفهم من الإبلاغ حفاظا على سمعتهم التجارية ومكانتهم المرموقة، غير معين على التمادي في إقتراف ِ لى المواقع الإلكترونية مثل هذه الجرائم،

وتوجد هذه الجرائم بصفة خاصة إلى البنوك، وا للمؤسسات المالية، لأن القطاعات المستهدفة من الجريمة الإلكترونية هي تعتمد أكثر من غيرها ً على أجهزة الحاسوب، وتعتبر البنوك من أهم تلك القطاعات وأكثرها تضرر[1]

.ثالثا: أنواع المجرمين الإلكترونين وصفاتهم.

قد يكون الجاني في الجريمة الإلكترونية، إما شخص يعمل بمفرده أو ضمن منظومة بغض النظر عن هذه الأخيرة، فقد تكون تجارية،(سياسية، أو عسكرية ، ويمكن تقسيم أنواع المجرمين إلى فئتين [2].

الفئة الأولى: صغار نوابغ المعلوماتية

.ويقصد بهم البالغ المفتون بالمعلوماتية والحسابات الآلية، وكثيرا ما لفتوا النظر في الآونة الأخيرة، ويرتكب هؤلاء الأشخاص الجرائم بغرض التسلية والمزاج مع الآخرين دون أن يكون في نيتهم نيتهم إحداث أي ضرر بالمجني عليهم .الفئة الثانية: المحترفون في الجريمة الإلكترونية . ويتمتع أصحابها بخيرة ودراية أكبر ويتقسمون إلى : فئة المتسللين الهوات: Hackers ظهارهم لا يهدفون في حربهم المعلوماتية إلا للمغارات وا القدرات أمام الأقران فلا توجد عادة عندهم هؤلاء أطماع مالية

. فئة القراصنة الخبيثون : MALICIOUSHACERS هم أشخاص هدفهم إلحاق خسائر بالمجني عليهم دون أن يكون الحصول على مكاسب مالية، ويندرج تحت هذه الفئة الكثير من مخترعي فيروسات الحاسبات الآلية وموزعيها

[1] عبد الفتاح البيومي حجازي، مكافحة جرائم الأنترنت، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006 ،ص - 96 97
[2] عبد الفتاح مراد، المرجع السابق، ص .45

.فئة حلالي المشاكل الشخصية: هم الأكثر شيوعا يترتب على إجرامهم في الكثير من الأحيان خسائر كبيرة تحلق بالمجني عليهم، رغبة منهم في إيجاد حلول لمشكلات مادية تواجههم، والتي لا يتم حلها بالوسائل الأخرى وغالبا ما يكون المجني عليه المؤسسة التي يعملون بها . فئة المجرمين المهنيين: وتظم مجرمي الجريمة الإلكترونية الذي يبتغون من وراء نشاطهم الإجرامي تحقيق الربح المادي بطريقة غير مشروعة، ويعمل المنتمون إلى هذه الفئة في أغلب الأحوال بطريقة منظمة بحيث ينطبق على أفعالهم وصف الجريمة المنظمة . فئة أصحاب الدعوة المتطرفة:وتدخل في عدادها الجماعات الإرهابية أم المتطرفة، والتي تتكون بدورها مجموعة أشخاص لديهم معتقدات وأفكار اجتماعية سياسية أو دينية، يرغبون في فرض هذه المعتقدات باللجوء إلى النشاط الإجرامية أحيانا[1]

وقد بدأ اهتمام الجماعات الإرهابية وخاصة التي تتمتع من بينها بدرجة عالية من التنظيم، يتجه إلى نوع جديد من النشاط الإجرامي، ومن الأمثلة الشهيرة في هذا الخصوص قيام إحدى الجماعات الإرهابية المعروفة بأوروبا باسم BRIGADES THEREDبتدمير ما يزيد من 60 مركز للحاسبات الآلية خلال الثمانينات لتلف الأنظار إلى أفكارها ومعتقداتها

.فئة الجناة المقصرية: تضم واحدة من أهم المشكلات التي تتصل بإساءة إستخدام الحاسبات الآلية وهي الإهمال، ولا شك في أن الإهتمام في مجال الحسابات الآلية يمكن أن يترتب عليه في كثير من الأحيان نتائج خطيرة قد تصل إلى حدزاهاق الروح ففي نيوزيلدا مثلا: قام الاثنان من مبرمجي الحسابات الآلية بتغيير في أحد البرامج التي تحدد خط سير إحدى الطائرات ولم يتمكنوا من إبلاغ قائد الطائر بهذا

[1] بخي فاطمة الزهراء، المرجع السابق، ص .25 -23

التغيير، مما أنجم عن مقتل 60 راكب بعد تحطم الطائرة إثر اصطدامها بأحد الجبال وتمت محاكمتها بتهمة القتل الخطأ [1]

.المطلب الثاني: التحقيق في الجريمة الإلكترونية

.إن التحقيق هو إجراء من أهم الإجراءات التي تتخذ بعد وقوع الجريمة، لما له من أهمية قامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف ٍ في التثبت من حقيقة وقوعها وا أنواعها، وهو كما يدل إسمه عليه استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة . والتحقيق في الجرائم الإلكترونية يختلف عن التحقيق في الجرائم العادية من حيث (الإجراءات وذلك لحادثة هذه الجريمة ومهارة مرتكبيها في الإجرام وحو الأدلة [2]

الفرع الأول: تعريف التحقيق الجنائي في الجريمة الإلكترونية.

لا يختلف التحقيق في الجريمة الإلكترونية عن الجرائم الأخرى وسنتناول تعريفه لغة واصطلاحا، ولكي يكتمل هذا التعريف يجدر التطرق إلى تعرف المحقق الذي هو بدوره القائم بجميع وكافة اجراءات التحقيق

.أولا: المقصود بالتحقيق الجنائي في الجريمة الإلكترونية

. يهدف التحقيق إلى جمع الأدلة والتنقيب عليها

- . أ **تعريف التحقيق لغة**: التحقيق مأخوذ من حقق يحقق تحقيقا، حقق الظن بالله صدقه، الأمر أحكمه - مع فلان - في قضيته: أخذ رأيه فيها

[1] نفس المرجع ص25-
[2] سعيد (أبي نعيم)، المرجع السابق، ص 102

- . ب **تعريف التحقيق اصطلاحا**: عرف التحقيق بمعناه العام أنه: اتخاذ جميع الإجراءات والوسائل المشروعة التي توصل إلى كشف الحقيقة وظهورها

. وعرف التحقيق أنه: مجموعة من الإجراءات تستهدف التنقيب عن الأدلة في شأن جريمةراتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها الإحالة المتهم إلى المحاكمة، كذلك هو مجموعة الإجراءات التي تباشرها سلطات التحقيق بالشكل المحدد قانونا، بغية تمحيص الأدلة (والكشف عن الحقيقة قبل مرحلة المحاكمة [1]

.وكذلك عرف التحقيق بأنه: " مجموعة من الإجراءات التي تباشرها السلطة المختصة بالتحقيق طبقا للشروط والأوضاع المحددة قانونا بهذا التنقيب عن الأدلة وتقديرها والكشف عن(الحقيقة في شأن جريمةراتكبت كتقدير لزوم محاكمة المدعي عليه أو عدم لزومها [2]"

ثانيا: تعريف المحقق

. ذهب جانب من الفقه إلى تعريف المحقق بأنه: " كل من عهد إليه القانون بتحري الحقيقة في البلاغات والحوادث الجنائية، وتحقيقها ويسهم بدوره في كشف غوامضها وصولا إلى معرفة حقيقية الحادث وكشف مرتكبيه لمحاكمته أو بصدد المحاكمة التي تجريها المحكمة ." كما عرف البعض المحقق أو الباحث الجنائي بأنه الشخص الذي يتولى ويتكلف بالتحقيق والتحري والبحث وجمع الأدلة لكشف غموض الحوادث ويتحدد دوره بالعمل على منع الجريمة قبل وقوعها أو اكتشافها بعد وقوعها، وضبط مرتكبيها والأدوات التي استعملت فيها .

[1] عمر بن إبراهيم بن حماد العمر، إجراءات الشهادة في مرحلة الاستدلال والتحقيق الابتدائي في ضوء نظام الإجراءات السعودي، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمنية، 2007 ،ص22

[2] حسن الجوخندار، التحقيق الابتدائي في قانون الأصول المحاكمات الجزائية، دار الثقافة عمان، الطبعة الأولى، 2008 ، ص .11

.وعرف المحقق بأنه: " ذلك الشخص الذي عهد غليه قانونا باتخاذ كافة الإجراءات القانونية والوسائل المشروعة فيما يصل إلى عمله من جرائم بهدف الكشف عن غموضها(وضبط فاعلها وتقديمه للمحاكمة [1]

. "أما المشرع الجزائري فقد وضع تعرفا لقاضي التحقيق في المادة 68 من قانون الإجراءات الجزائية حيث جاء في نصها ما يلي:

" يقوم قاضي التحقيق وفقا لقانون باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة بالتحري عن أدلة الإتهام وأدلة النفي

" الفرع الثاني: خصائص التحقيق الجنائي في الجريمة الإلكترونية :

تعد مرحلة التحقيق الإبتدائي أو ما يطلق عليها مرحلة جمع الاستدلالات، مرحلة هامة في سبيل البحث والتحري عن الجرائم، وتبلغ هذه المرحلة أعلى مستوياتها عندما يتعلق الأمر بالجريمة الإلكترونية، لأنها تعد حجر الزاوية الذي سيتم على أساسه بناء الدعوة برمتها، فما يتم جمعه من معلومات وأدلة رقمية في المرحلة التي تعقبراتكاب الجريمة مباشرة قد لا يبق متاحا بعد مرور وقت قصير علىراتكابها والسبب في ذلك يعود إلى الطبيعة التقنية لهذه الجرائم، ففي كثيرا من الجرائم المعلوماتية لم يترك الجاني ورائه سوى ذلك التعبير الذي يعتري وجوه(القائمين على تعقبه والممزوج بالإعجاب والإحباط معا[2]

.أولا: خصائص التحقيق

.التحقيق الجنائي عموما هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى، فله قواعد ثابتة وراسخة بدونها ما كان ليتمتع التحقيق بتلك الصفة . ٍما فنية، فالأو

[1] بخي فاطمة الزهراء، المرجع السابق، ص . 40
[2] محمد طارق عبد الرؤو ف، جريمة الإحتيال عبر الإنترنت الأحكام الموضوعية والأحكام الإجرائية، منشورات الحلبي الحقوقية، الطبعة الأولى، 2011 ،ص 230

وهذه القواعد إما قانونية وا لى لها صفة الثبات التشريعي لا يملك المحققزاءها شيئا سوى الخضوع والامتثال، أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته وفطنته ومهارته[1] .

ذلك أن الفكر البشري المتعلق بالجرم الإلكتروني يجب أن يقابله فكر بشري من قبل المحقق الجنائي، وبالتالي فإن أسلوب التحقيق وفكر المحقق الجنائي يجب أن يكون متغيرا أو متطورا أيضا، وذلك كنتيجة طبيعية لمواجهة المجرم الإلكتروني/أسلوب التحقيق الإبتدائي في الجر يمة الإلكترونية : التحقيق عموما هو مجموعة الإجراءات التي يقوم بها المحقق وتؤدي إلى إكتشاف الجريمة ومعرفة مرتكبيها تمهيدا لتقديمهم للمحاكمة،

وقد تكون هذه الإجراءات عملية كالتفتيش أو فنية كمظاهات البصمات أو برمجية كتحديد كيفية الدخول إلى المعطيات المخزنة في النظام المعلوماتي .والهدف من التحقيق الإبتدائي هو التأكد أولا من وقوع الجريمة يعاقب عليها القانون، ومن ثمة معرفة نوع هذه الجريمة ومن هو الجاني ومن هو المجني عليه، وكذا معرفة وقوعها وما هي الوسائل التي استعملت فيراتكابها، ويكون ذلك في الجريمة المعلوماتية وفقا لمنهج تحقيقي يختلف عن غيره بالنسبة للجرائم الأخرى

. أ/ وضع خطة عمل التحقيق: يبدأ المحقق عند تجميع الاستدلالات المتعلقة بالجريمة المعلوماتية بوضع خطة العمل اللازمة على ضوء المعلومات المتوافرة لديه، وتحديد الفريق الفني اللازم للقيام بمساعدته في أعمال التحقيق وذلك على النحو الآتي

-وضع الخطة المناسبة والتي لا تبدأ إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الخطر ووضع التصورات الكفيلة للتصدي للجريمة

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، 2009 ،ص . 56

- .التخطيط الفني للتحقيق وذلك من أجل الوصول إلى أفضل الطرق والأساليب للتعامل مع هذه الجرائم

-عمل دراسة جادة لكافة الإجراءات التحقيق خطة مسبقة التي يتم وضعها وناقاشها العاملون في فريق التحقيق

- .تنسيق جهود الفريق القائم بالتحقيق لتسهيل مهمتهم وعملهم وتقليل الآثار السلبية والإسراع في انجاز العمل من أجل ضمان مستوى جيد من الأداء

- .تحديد الإجراءات المسبقة والتي من شأنها التقليل من الأخطار الفردية التي قد تنتج عن قلة الخبرة أنقص المعرفة، والتي تساعد في التقيد بالمستوى المطلوب والتي تضمن الخطوات التي يقوم بها المحقق خلال مراحل التحقيق[1] .

ب/ تشكيل فريق التحقيق: إن التحقيق الإبتدائي في الجرائم المعلوماتية يكون غالبا أكبر من أن يتولاه شخص واحد بمفرده، حتى ولو كانت المضبوطات هي مجرد حاسب شخصي واحد، ولذلك فإنه يفضل أن يتعاون عدة محققين في انجاز مهمة التحقيق والعثور على الأدلة، ويجب أن يتشكل فريق التحقيق من فنيين أخصائيين ذوي خبرة في مجال الحاسوب الأنترنت، ويمتازون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الجنائي الإلكتروني وفي شكل خاص، ولهؤلاء المحققين أن يستعينوا بخبراء في مجال الحاسوب و الانترنت ليتمكنوا من فك التعقيدات التي تفرقها ظروف وملابسات كل جريمة [2].

ان كان أسلوب عمل الفريق يستخدم في التحقي وا ق في كثير من أنواع الجرائم إلا أنه يأخذ أهمية خاصة في الجرائم المعلوماتية لما تطلبه من مهارات وخبرات

[1] محمد نصير السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004 ،ص 72.

[2] عبد الله حسين محمود، إجراءات جمع الأدلة في الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، 2003 ،ص 612

متنوعة قد لا تتوافر لدى المحققين، وبذلك يكون تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم أمرا ضروريا ومن الناحية العملية غالبا ما يتكون فريق التحقيق من[1]

-خبراء الحاسوب وشبكات الأنترنت الذين يعرفون ظروف الحادثة وكيفية التعامل مع هذه الجرائم.

- خبراء ضبط وتحرير الأدلة الرقمية العارفين بأمور تفتيش الحاسوب.

- خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية

- .خبراء التصوير والبصمات والرسم التخطيطي

.وفي هذا الإطار نجد أن المشرع الجزائري إلى مسألة إمكانية إستعانة الجهات المكلفة بالتحقيق بالخبراء المتخصصين في مجال الحاسوب والنظم المعلوماتية، ومن الذين لهم دراية بعمل المنظومة المعلوماتية أو ممن لهم دراية بالتدابير المتخذة لحماية المعطيات المعلوماتية، وذلك بغض مساعدة جهات التحقيق في إنجاز مهمتها وتزويدها بالمعلومات(الضرورية لذلك [2]

/ 2العناصر الأساسية للتحقيق الإبتدائي في مجال البرمجة الإلكترونية:

نقصد بها تلك الإجراءات التي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة والمحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبيها، وهناك إجراءات واحتياطات يتعين على اجراءات أخرى يجب الضبطية القضائية مراعاتها

[1] عبد الله حسين محمود، المرجع السابق، ص 613

[2] أنظر المادة 05 الفقرة الأخيرة من القانون /09 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المعدل والمتمم في 2019

قبل البدء في عمليات التحقيق الإبتدائي(على الضبطية القضائية مراعاتها أثناء التحقيق الإبتدائي[1]

/ .أ الإجراءات التي يجب مراعاتها قبل البدء في التحقيق

- .تحديد نوع نظام المعالجة الأولية للمعطيات فهل هو كمبيوتر معزول أم متصل بشبكة معلومات

- .وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي عن المسؤولين بها ودور كل منهم

- .إذا وقعت الجريمة على شبكة فإنه يجب حصر طرفيات الإتصال بها أو منها لمعرفة الطريقة التي تمت بها عملية الإختراق من عدمه – .

مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة المعلوماتية.

- مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة.

- يجب فصل التيار الكهربائي عن موقع المعاينة أو جمع الاستدلالات لشل فاعلية الجاني في أن يقوم بطريقة ما بمحو آثار الجريمة.

- فصل خطوط الهاتف حتى لا يسيئ الجاني استخدامها، والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق لأنهم قد يسيؤون استخدامها لطمس البيانات .

[1] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي، دار الكتب القانونية المجلة الكبرى، الطبعة الأولى، ص 84

-التأكد من أن خط الهاتف يخص الحاسوب محل الجريمة، ذلك أنه من الخدع التي يستعملها الجاني عند الاختراق أن يتم ذلك بخط هاتيفي مسروق عن طريق الدخول إلى شبكة الهاتف والتلاعب فيها وتقليل أجهزة المراقبة وأجهزة التحقيق بعد ذلك.

إبعاد الموظفين عن أجهزة الحاسوب الآلي بعد الحصول منهم على كلمة السر وكذا الثغرات في حالة وجودها

- .تصوير الأجهزة المستهدفة من أمام والخلف لإثبات بأنها كانت تعمل.

ب/ الإجراءات التي يجب مراعاتها أثناء التحقيق :

- عمل نسخة احتياطية من الأقراص الصلبة قبل استخدامها والتأكد فنيا من دقة النسخ

- . نزع غطاء الحاسب الآلي المستهدف والتأكد من عدم وجود أقراص صلبة إضافية

- . العمل على فحص العلاقة بين برامج التطبيق والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها.

- حفظ المعدات والأجهزة التي تضبط بطريقة فنية وسليمة.

- العمل على فحص وتطبيقاتها مثل البرامج الحسابية التي تكون قد استخدمت في جريمة اختلاس معلومات .

-أن يكون الهدف من نسخ محتوى الأسطوانة والأقراص وتحليل المعلومات الموجودة بها بغرض التوصل إلى معرفة المعلومات والملفات الممسوحة، وكذلك معرفة الملفات الخفية (المخزنة في ذاكرة الحاسوب [1].

ثانيا: الخصائص الفنية للمحقق

. تلعب الأجهزة الفنية دروا أساسيا في صيانة أمن المجتمع وذلك إما بالقيام بدور وقائي،ما القيام بدور يهدف إلى منعراتكاب الجرائم والحيلولة دون وقوعها وتقليل فرص إقترافها، وا قضائي في ضبط الجرائم ومرتكبيها بعد حدوثها . ولقد أصاف ظهور الجرائم المعلوماتية النابعة من التطور الإلكتروني أعباء جديدة على أجهزة التحقيق لما يتطلب التصدي لهذه الجرائم من قدرات فيه لم يألفها رجال الضبطية القضائية ولم يتعودو عليها، ما يستلزم ضرورة توفير المهارات المطلوبة في هذا المجال.

والمشكلة الأساسية التي تواجب المحققين في جرائم نظم المعلومات هي خلفية المحقق نفسه فمتخصصوا الحاسب الآلي قد تكون لديهم المعرفة التقنية اللازمة ولكنهم ليسوا مدربيين على تفهم دوافع الجريمة وجمع الأدلة التقديم المتهم للمحاكة، وفي كثير من الحالات نجد أن متخصص الحاسب يعتقد أن لديه الدليل الحاسم حول الجريمة الإلكترونية، ولكن من الناحية يتضح فيما بعد أن هذا الدليل لا يصلح لإقامة الدعوى، بينما المحققون ذوي الخلفية القانونية قد تكون لديهم خبرة واسعة في التحقيق ولكنهم يفتقدون المعرفة الكافية بتقنيات الحاسب الآلي التي(يستخدمها المجرمون في هذا النوع من الجرائم[2]

اذا كانت مهارات التعامل مع مس وا رح الجريمة والتحفظ على الأدلة و مناقشة الشهود وغير تعتبر من أساسيات التحقيق التي لا يتوقع أحد عدم توافرها لدى

[1] سعيداني نعيم، المرجع السابق، ص 112-114
[2] سعيداني نعيم، المرجع السابق، ص 115

المحقق، إلا أنه يلزمه عند مباشرته التحقيق في الجريمة الإلكترونية معرفة العديد من الجوانب الفنية يقوم بعمله على أحسن وجه ونذكره منها :معرفة الجوانب الفنية والتقنية لأجهزة الأجهزة الحاسوب الانترنت والتي تتعلق بالجريمة المرتكبة ذلك أن إفتقار ضابط الشرطة القضائية للتأهيل الكافي في الميدان التقي قد يغطي إلى إتلاف وتدمير الدليل، على اعتبار أن جهله بأساليبراتكاب الجريمة المعلوماتية يجعله يقع في كثير من الأحيان في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية وتدميرها مثل إتلاف محتويات الأقراص الممغنطة وأوعية المعلومات التي تخزن بها البيانات، وبالتالية فإن الكشف عن هذه الجرائم يقتضي أن تكون الأجهزة المعنية على دراية كافية بأساسيات التعامل مع هذه (الجرائم وكيفية تقصيها وضبطها وصولا إلى مرتكبيها[1] .

كما يتوجب على المحقق معرفة آلية عمل تشكيلات الحاسوب والانترنت، وتبرز أهمية فهم المحقق لهذه المبادئ في كونها ضرورية لتصور كيفيةراتكاب الفعل الإجرامي في العالم لافتر عتراض اضي من اختراق للشبكات وا حزم البيانات أثناء انتقالها عبر الشبكة والتجسس عليها وتحويلها عن مسارها، كما أنها تعطي للمحقق تصورا جيدا عن مدى إمكانية متابعة مصدر الإعتداء على الشبكة والمعوقات التي تحول دون ذاك[2]

[1] جميل عبد الباقي صغير أدلة الإثبات الجنائي والتكنولوجي الحديثة، دار النهضة العربية، القاهرة، 2002 ،ص 115

[2] حسين سعيد بن سيف الغافري، الجهود الدولية، في مواجهة جرائم الأنترنت، ورقة مقدمة للاتحاد العربي للتحكيم الإلكتروني، 2007 ،ص . 02

❖ .المبحث الثاني: السلطات المختصة بالتحقيق في الجريمة الإلكترونية

.المطلب الأول: جهاز التحقيق الجنائي في الجريمة الإلكترونية وأقسامه

.نظرا لانتشار الجريمة الإلكترونية بشكل ملفت للإنتباه، ولأن أجهزة التحقيق في الجرائم التقليدية لم تكن كافية للتصدي لهذا النوع من الإجرام، أنشئت أجهزة خاصة بالتحقيق فيها . الفرع الأول: تعريف جهاز التحقيق في الجريمة الإلكترونية . جهاز التحقيق في الجريمة الإلكترونية هو عبارة عن الوظائف المتخصصة إلكترونيا وقانونيا، التي يصدر بها قرار إداري وتشغل بنوعين من الأفراد الضباط وضباط الصف والمدنيين وتحكم علاقاتهم الوظيفية التسلسل النظامي للرتب العسكرية وقانون الخدمة المدنية للمدنيين وقواعد الأمن ويستخدمون التقنية الإلكترونية وضبطها والتي يكون محلها التقنية(الإلكترونية الرقمية ونظامها وبرامجها وشبكاتها1 .

الفرع الأول: أقسام جهاز التحقيق الجنائي في الجريمة الإلكترونية

.أصبحت الجرائم في عصر التقنية الحديثةرابعة أنواع، جرائم الإعتداء على النفس، جرائم الإعتداء على المال، جرائم الإعتداء على المصلحة العامة، والجرائم الإلكترونية بعد أن كانت ثلاثة أنواع فقط

.وعلى هذا الأسس قسمت الأجهزة التي تتولى التحقيق في هذه الجرائم إلى:

اولا: أجهزة الأمن العام:[2]

وتختص بالتحقيق في جرائم الإعتداء على النفس والمال

[1] محمد مصطفى موسى، التحقيق في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، 2009 ،ض286
[2] محمد مصطفى، المرجع السابق، ص286

- .أ الجرائم الواقعة على الأشخاص : إن للحياة الشخصية خصوصية وحرمة لا يجوز لأي شخص أن يقتحمها، ومثال على ذلك الإعتداء على المعلومات الإلكترونية الخاصة بالمحامين أو الأطباء أو المحاسبين أو غيرهم من المهنيين، وقد تتم هذه الجريمة من خلال الإطلاع على البيانات والمعلومات الخاصة . ويتمثل الركن المادي في جريمة نشر مواد إباحية بالسوك الذي يتخذه الفاعل بتهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة، ويقوم بنشرها على الانترنت، أما الركن المعنوي وهو الحالة النفسية للجاني أي أنه كان يقصد نشر الصور ولديه العلم والإدارة على(ذلك [1]

.ب - الجرائم الواقعة على الأموال : لقد صاحب ظهور شبكة الانترنت تطورات في شتى المجالات، حيث أصبحت معظم المعاملات التجارية تتم من خلال هذه الشبكة، مثل البيع والشراء، مما إنجر عنه تطور وسائل الدفع والوفاء وأصبحت جزء لا يتجزء من هذه المعاملات . وفي ظل التحول من المعاملات التجارية التقليدية إلى المعاملات التجارية الإلكترونية وما أنجز عنه من تطور ووسائل الدفع والوفاء، وفي خضم التداول المالي عبر الانترنت، أصبحت هذه المعاملات عرضة لشتى أنواع الجرائم ومنها[2]

-السطو على بطاقات الإئتمان والتحويل الإلكتورني وفي غير المشروع.

القمار وغسل الأموال عبر الانترنت

- . جريمة السرقة والسطو على أموال البنوك

- .تجارة المخدرات عبر الانترنت

[1] يوسف خليل يوسف العطيفي، الجرائم الإلكترونية في التشريع الفلسطيني، غزة، 2013 ،ص . 13
[2] صغير يوسف، الجريمة الإلكترونية، عبر الانترنت، تيزي وزوو، 2013 ،ص .44.

. **ثانيا: أجهزة التحقيق في الجرائم المخلة بأمن الدولة.**

وتنقسم إلى :[1]

-أجهزة تختص بالتحقيق في الجرائم المضرة بأمن الدولة من جهة الداخل وتتولها أجهزة (

(متخصصة مثل مباحث أمن الدولة في مصر، فرنسا والكويت .

- أجهزة تختص بالتحقيق في الجرائم المضرة بأمن الدولة من جهة الخارج وتتولاها أجهزة (متخصصة مثل المخابرات العامة في مصر[2] .

وقد اشتغل الكثير من الجماعات المتطرفة الطبعة الاتصالية للانترنت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها، خاصة المتمثلة في الإرهاب والجريمة المنظمة، اللذان أخذا معنى آخر في استعمال الانترنت التي سمحت لهم فيراتكاب جرائم غاية الشلك في حق المجتمعات والدول، بل الأخطر من ذلك أتاحت الانترنت الكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالإطلاع على مختلف الأشرار العسكرية الاقتصادية لهذه الأخيرة، خاصة فيما يتعلق بالدول التي يكون فيها((نزاعات، ويبقى المساس بالأمن الفكري من بين أخطر الجرائم المرتكبة عبر الانترنت[3]

[1] محمد مصطفى، المرجع السابق، ص286
[2] محمد مصطفى، المرجع السابق، ص287
[3] بوظياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11 سبتمبر 2018 ،ص 258

ثالثا: جهاز التحقيق في الجرائم الإلكترونية

ٍ[1]ان كانت بعض الدول قد أنشأته وهذا النوع من الأجهزة لم ينشأ بعد في كل الدول العربية وا منذ أن استخدمت الحاسب الآلي وشبكات المعلومات، ويرجع السبب الرئيسي لإنشاء جهاز متخصص للتحقيق الجنائي في الجرائم الإلكترونية إلى تحقيق الضبط الإجتماعي الإلكتروني حماية للمجتمع من الجرائم الإلكترونية وذلك للحد منها وضبطها بعد وقوعها، وذلك بالعمل على الحصول على الدليل الإلكتروني من أجل إثبات الجريمة .ويضاف إلى هذا السبب زيادة تفاعل المجرمين مع تقنية المعلومات، فقد وضح أن تقنية المعلومات ستزيد التفاعل بين الإرهابيين، ومهربي المخدرات والأسلحة وجماعات الجريمة المنظمة، فمن خلال عالم مرتبط شكليا سيكون هناك مدخل للمعلومات والتقنية والتمويل إذا تم استخدام تلك سواء عن طريق الد والخداع المعقد وتقنيات الأفكار الهدامة، وا ول أو فاعلين غير دوليين سيصبح ذبك بمثابة الخاصية الرئيسية لمعظم التهديدات من الداخل للدول. [2]

أما الجزائر فلا زالت إلى الآن تفتقر لجهاز خاص بالتحقيق في الجريمة الإلكترونية إلا أنه انعقدت عدة ملتقيات حول مخاطر هذه الجريمة وناشدت بإنشاء جهاز خاص بالتحقيق في الجريمة الإلكترونية في الجزائر، منها الملتقى الوطني للجريمة الإلكترونية الذي يضم بدائرة قديل بمبادرة من نقابة المحامين لولاية وهران، حيث أختتم بمجموعة من التوصيات منها: أنه لابد من الإسراع في إنشاء الهيئة الوطنية المكلفة بتنشيط وتنسيق عمل السلطات المكلفة بمكافحة الجريمة الإلكترونية، ومدها بالمساعدة والاستشارة اللازمة، وحث الخبراء غلى ضرورة الإسراع في إنشاء هذه الهيئة الوطنية التي ينص على استحداثها القانون رقم 04 -

[1] محمد مصطفى، المرجع السابق، ص287
[2] محمد مصطفى، المرجع السابق، ص287

09 الصادر في 05 أوت 2009 والخاص بالوقاية من الجرائم الإلكترونية ومحاربتها والمكافحة ضدها(والقضاء عليها[1] .

الفرع الثالث: معوقات وصعوبات التحقيق في الجريمة الإلكترونية

.يتسم التحقيق في الجريمة الإلكترونية بالعديد من المعوقات والصعوبات التي تؤثر على عملية التحقيق التي تؤدي بها إلى الخروج بنتائج تنعكس على نفسية المحقق بفقدانه الثقة في نفسه وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون غير القادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها، وانعكاسها أيضا على المجرم نفسه، حيث يشعر أن الجهات القضائية غير قادرة على اكتشاف أمره وأن خبرة القائمين على المكافحة والتحقيق، لا تجاري خبرته وعلمه بالأمر الذي يعطيه ثقة كبيرة فيراتكاب المزيد من الجرائم التي تكون أكثر فداحة ا على المجتمع ً وأشد ضرار

. **أولا: قلة خبرة القائمين بالتحقيق في الجرائم** .توجد معوقات للتحقيق في الجريمة الإلكترونية تتعلق بالسلطة القائمة بالتحقيق وتجمع لعدة أسباب نذكرها كالآتي

-أ قلة خبرة القائمين بالتحقيق في هذه الجرائم : لقلة المهارات الفنية المطلوبة للتحقيق في هذا النوع من الجرائم وتقص المهارات في استخدام جهاز الحاسوب والانترنت وعدم توافر المعرفة بأساليبراتكاب الجريمة الإلكترونية، وقلة الخبرة في مجال التحقيق في جرائم الحاسوب و الانترنت وقلة المعرفة باللغة الأجنبية لاسيما أن للعاملين في مجال الحاسوب مصطلحات عملية خاصة أصبحت تشكل الطابع المميز لمحادثاتهم وأساليب التفاهم بينهم، وليس هذا فحسب بل اختصر العاملون في

[1] بخي فاطمة الزهراء، المرجع السابق، ص .51 -50

هذا المجال تلك (المصطلحات والعبارات بالحروف الأولى لديهم تعرف بلغة المختصرات[1]

ب - الصعوبات التقنية لاستخدام بروتوكول IP/TCP في الإثبات : هناك تحديات عند استخدام المحقق بروتوكول IP/TCP كدليل إلكتروني في الإثبات وهي :

بروتوكول IP وحدة معلوماتية تحتوي على معلومات عن الحاسوب وليس عن الأشخاص، لذلك فمن الصعوبة إثبات أن شخصا محدد أحدث الفعل غير المشروع، ومع ذلك يمكن أي يستخدم كقرينة قضائية ضد مالك الجهاز غلى أن يثبت العكس .

-الجاني يعمد إلى استخدام عناوين ومعلومات غير صحيحة أو غير قانونية باستخدام حاسوبه الشخصي في ملف خدمات عامة لتجنب التعرف عليه، ويستخدم عنوان IP لهّ هم استخدام نفس العنوان، وبعد مرور فترة زمنية يقوم بغلق الإتصال، مستخدمين كثر ويمكن وبعد فترة يعاود الاتصال مما يجعل النشاط الإجرامي غالبا موزعا على عدة عناوين

- .تكون المعلومات المحلية لمصدر عنوان IP غير حقيقية أو زائفة وهدا ممكن باستخدام مصدر زائف لمصدر IP بحيث يظهر بأن المعلومات جاءت من حاسوب محدد وفي الحقيقة جاءت من حاسوب آخر

ج -راتفاع تكاليف جمع الأدلة :إن التحقيق في هذه الجرائم يحتاج إلى خبراء متخصصين وهؤلاء يحتاجون إلى دورات مستمرة متزامنة مع تطور التقنية الإلكترونية، وهذا الأمر مرتبط بالتكاليف باهظة، وكذلك التفتيش عن الأدلة يحتاج إلى فحص آلاف الصفحات خصوصا عندما لا تثبت تلك الصفحات(شيئا [2]

[1] يوسف جفال، التحقيق في الجريمة الإلكترونية، 2017/2016 ،ص -41. 42
[2] يوسف جفال، المرجع السابق، ص .43 -42

ثانيا: عوائق تتعلق بالجريمة والجهة المتضررة منها

.المعوقات المتعلقة بالجريمة الإلكترونية تتمثل في -

- اخفاء الجريمة وغياب الدليل المرئي وصعوبة التعرف عليه
- الإعاقات المتعلقة بالوصول إلى الدليل لإحاطته بوسائل الحماية الفنية.
- سهولة محو الدليل أو تدميره في زمن فصير جدا.

الجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها في زمن ا قصير جد بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي هذه الحالة التي قد تعمل بها فإنه يستهدف بالمحو السريع عدم استطاعة السلطات إقامة الدليل ضده، وبالتالي تملصه. رجاعه إلى خطأ نظام الحاسوب الآلي أو الشبكة أو في الأجهزة من مسؤولية هذا الفعل وا

. أما المعوقات المتعلقة بالجهات المتضررة من جرائم الحاسوب والانترنت، وهي عدم إدراك خطورة جرائم الحاسوب والانترنت من قبل المسؤولين بالمؤسسات المجني عليها التي تعد من معوقات التحقيق، وكذلك إغفال الجانب الإرشادي للمستخدمين إلى خطورة الجرائم المتعلقة بالأنترنت، وتسابق الشركات في تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحاتها واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمني، وهذا يؤدي إلى الإحجام عن الإبلاغ عن الجريمة التي تعتبر من أهم وأخطر الإشكالات التي تتعلق بعملية الإبلاغ عن الجريمة الإلكترونية، حيث يحجم البعض عن إبلاغ السلطات المختصة بالجرائم التيراتكبت إذا تعلق الأمر بالمؤسسات المالية أو ما شابهها (بحقهم خاصة [1]

[1] يوسف جفال، المرجع السابق، ص -43. 44

.المطلب الثاني: أجهزة التحقيق في الجريمة الإلكترونية.

لتفاقم الظاهرة الإجرامية المعلوماتية من يوم لآخر ونظر ا إلى الطبيعة الخاصة التي تتميز بها هذه الجرائم، كان من الضروري تطوير أجهزة الشرطة القضائية لتواكب التطور الحاصل في مجال الجريمة الإلكترونية (المعلوماتية)،

لهذا عمدت معظم الدول إلى استحداث وحدات خاصة لمكافحة هذا النوع من الجرائم كما تم إنشاء أجهزة متخصصة على المستوى الدولي مهمتها البحث والتحري في العالم الافتراضي على غرار هيئة الانتربول واليوربول والأنريبول.

أما في الجزائر فقد تم تسخير هيئات ووحدات متخصصة أبرزها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال إضافة إلى وحدات قضائية تابعة لسلك الأمن والدرك الوطني

. الفرع الأول: الهيئات الفنية المتخصصة في البحث والتحري عن الجرائم الإلكترونية

.الهيئات المتخصصة في مجال مكافحة الجريمة المعلوماتية هي وحدات تستند مهام الوقاية ومكافحة الجرائم الإلكترونية بالنظر إلى تشكيلتها البشرية الخاصة التي تضم محققين من نوع خاص تجمع لديهم صفة الشرطة القضائية إضافة إلى المعرفة الواسعة بالنظم(المعلوماتية والمجرم الإلكتروني [1]

.أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال .

وقد استحدثها المشرع الجزائري بموجب قانون رقم 09 -04 المؤرخ في 05 أوت

[1] ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، جامعة باتنة، 2015 -2016 ،ص 171

2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها(وتم تنظيم عملها بموجب المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015[1] ،

ومن مهامها تفعيل التعاون القضائي والأمني الدولي وغدارة وتنسيق العمليات الوقائية والمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكاليفها بالقيام بخبرات قضائية في حال الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني[2]

الهيئة الوطنية تعد سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل، وتظم أساسا أعضاء من الحكومة معنيين بالموضوع، ومسؤولي مصالح الأمن، وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء .تظم الهيئة قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك والأمن الوطنيين، وفقا لأحكام قانون الإجراءات الجزائية تكلف بتجميع وتسجيل وحفظ المعلومات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية وضمان المراقبة والوقاية للإتصالات الإلكترونية

.وذلك قصد الكشف عن الجرائم المنصوص عليها في قانون العقوبات أو الجرائم الأخرى تحت سلطة القاضي المختص

.للإشارة هنا تمكنت الجزائر ممثلة أساسا في أجهزتها الأمنية التابعة للدرك الوطني والأمن الوطني وبالتعاون مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا

[1] مرسوم الرئاسي رقم -15 261 المؤرخ في 08 أكتوبر 2015 المتضمن تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، الصادر في الجريدة الرسمية للجمهورية الجزائرية، عدد /08 /10 2015 . في، 53

[2] جريمة الإلكترونية واجراءات مواجهتها من خلال التشريع الجزائري، دراسة منشور بكتاب أعمال الملتقى _فضيلة عاقلي، ال الدولي الرابع عشر الجرائم الإلكترونية، المنعقدة خلال 24 إلى 25 مارس 2017 ،طرابلس

الإعلام والإتصال من معالجة أكثر من 100 جريمة إلكترونية منها 30 %على مواقع التواصل الاجتماعي، هذا وقد سجلت مديرية الشرطة القضائية بالمديرية العامة للأمن الوطني خلال السداسي الأول من عام 2016 وجود 11 قضية متعلقة بالإرهاب الإلكتروني أغلبها خاصة بالتهديدات الإرهابية باسم تنظيم داعش الإرهابي لتسفر جهود البحث والتحري والتنسيق بين مختلف القطاعات المختصة توقيف 58 شخصا متورطا في قضاياراهاب الكتروني تمت إحالتهم على القضاء

. هذا وقد استطاعت الشرطة الجزائرية المتخصصة من توقيف ما يزيد عن 160 جزائري لهم علاقة مباشرة مع تنظيم داعش في العراق، سوريا وليبيا كما تمكنت من فك شفرات الرسائل المتبادلة وما يزيد عن 30 خلية تسعى لاستقطاب الشباب لتجميده عبر مواقع الأنترنت ومنصات التواصل الاجتماعي خاصة الفيس بوك والتويتر لصالح التنظيمات الإرهابية نتيجة استعمالها لأنظمة تكنولوجية حديثة وتلقيها معلومات تفيد بوجود منشوراتراهابية داعمة وتدعو (للمشاركة في منتدياتراهابية غلى جانب اتصالات محلية ودولية[1] .

ثانيا: جهازي الأمن الوطني والدرك الوطني

.حيث سعت المديرية العامة للأمن الوطني وكذا جهاز الدرك الوطني في إنشاء فرق خاصة لمكافحة الجرائم المعلوماتية، وكذا تكوين عناصر متخصصة في هذا المجال سواء على المستوى الداخلي أو المستوى الخارجي، بالإضافة إلى توافر هاذين الجهازين من مخبرين علميين للشرطة العلمية والتقنية يتوفرون على أحدث الأجهزة ذات تكنولوجيا متطورة لكشف هذا(النوع من الإجرام[2] .

[1] آمال بن صوليح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني وفي الجزائر، مداخلة الملتقي الدولي حول " الإجرام الييبرالي المفاهيم والتحديات ، " 12 -11 أفريل 2017

[2] محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إيليزا للبحوث والدراسات، العدد الثاني، ديسمبر 2017 ،المركز الجامعي إليزي، الجزائر، ص .35 -34

- أ الوحدات التابعة لسلك الأمن الوطني : تضع مديرية الأمن الوطني في إطار تحديد سياسة أمنية فعالة، كافة الإمكانيات البشرية والتقنية المتاحة لديهم لأجل التصدي لكل أنواع الجرائم بالخصوص تلك المستحدثة منها كالجرائم الإلكترونية، والتي تعتبر نتاج القصور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات الإعلام والإتصال، وذلك بهدف حماية المصلحة العامة وكذلك المصالح(الخاصة المرتبطة باستعمال هذا النوع من التكنولوجيات[1] .

توجد على مستوى جهاز الأمن 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

.في سبيل تدعيم المصالح الولاية للشرطة القضائية قامت المديرية العامة للأمن الوطني سنة 2010 بخلق ما يقارب 23 خلية لمكافحة الجريمة المعلوماتية على مستوى ولايات الوسط، الشرق، الغرب، الجنوب، لتقوم فيما بعد بتعيم الخلايا على جميع مصالح الأمن ولايات (الوطن[2] .

ب - الوحدات التابعة للقيادة العامة للدرك الوطني : يضع الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن الوطني والنظام العام ومحاربة الجريمة بكافة أنواعها، وحدات متنوعة وعديدة على مستوى القيادة العامة، أو على مستوى القيادات الجهوية والمحلية نذكر منها

[1] يوسف جفال، التحقيق في الجريمة الإلكترونية، 2017/2016 ،ص .20
[2] سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، المجلد ب، عدد 52 ديسمبر .53ص، 2019

-المصالح والمراكز العلمية والتقنية

- .هياكل التكوين

- . المصلحة المركزية للتحريات الجنائية.

- المعهد الوطني لعلم الإجرام.

يوجد بالعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع لقيادة العلمية للدرك الوطني قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، حيث يقوم بتحليل الأدلة نجاز ٍ الخاصة بالجرائم الإلكترونية، وذلك بتحليل الدعامات الإلكترونية، وا المقاربات الهاتفية، وتحسين التسجيلات الصوتية والفيديو والصورة وذلك لتسهيل استغلالها بالإضافة إلى مراكز الرقابة من جرائم الإعلام الآلي والجرائم المعلوماتية ومكلفحتها ببئر مراد (رايس والتابع لمديرية الأمن العمومية للدرك الوطني وهو قيد الإنشاء[1]

الوظيفة الأساسية للوحدة هي خدمة العدالة ودعم وحدات التحري في إطار مهام الشرطة القضائية في مجال مكافحة شتى أنواع الجرائم بما فيها الجريمة المعلوماتية حيث يوجد بهذا(المركز قسم الإعلام الآلي والإلكترو نيك الذي يختص بالتحقيق في الجرائم المعلوماتية[2]

[1] يوسف جفال، المرجع السابق، ص .21
[2] سعيدة بوزنون، المرجع السابق، ص .54 -53

.الفرع الثاني: الهيئات القضائية الجزائية المتخصصة.

يقصد بها الأقطاب الجزائية المتخصصة المنشأة بموجب القانون[1] رقم 04 -14 المؤرخ في ، 2004نوفمبر) 1 à وتختص هذه الجهات القضائية بموجب المواد 37-40-329 م ن قانون الإجراءات الجزائية بالنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بالإضافة إلى الصلاحيات الأخرى الممنوحة للجهات القضائية أو للضبطية القضائية في إطار (معالجة مثل هذه الجرائم .

[2]ولقد أثمر مسار إصلاح العدالة الذي شرعت فيه الجزائر منذ سنة 2000 والذي انصب ِ دعم حقوق الإنسان وتسهيل حق اللجوء غلى القضاء واعادة على دراسة ثلاث نقاط أساسية :الإعتبار لنظام التكوين والتأهيل، بإحداث تغييرات جذرية في قطاع العدالة خاصة تعديل واستحداث قوانين تنسجم والالتزامات الدولية للجزائر وكذلك تحسين خدمات قطاع العدالة، ولعل أهم ما جاءت به توصيات لجنة إصلاح العدالة تعديل القانون الجزائري بشقيه الموضوعي والإجرائي في مواجهة الظواهر الإجرامية الخطيرة وتزايد المنظمات الإجرامية وتزايد مخاطر التقنية المعلوماتية على حياة الأشخاص وخصوصياتهم إضافة إلى أن هذا النوع من الجرائم تمتد آثاره خارج حدود الدولة الواحدة مهددة بذلك اقتصاديات الدول وأمنها، حيث شهدت ًا في أعمال المنظمات الإجرامية واستعمالها السنوات الأخيرة تزايد في العلميات الإرهابية وتزايد القضائي الافتراضي للاستفادة من خصائص الجريمة المعلوماتية.

من أجل كل هذا عكف المشرع الجزائري وقبله التشريعات المقارنة خاصة المشرع الفرنسي إلى استحداث الأقطاب الجزائية المتخصصة وهي محاكم ذات اختصاص

[1] لقانون -04 14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم - 66 155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية، الصادر بالجريدة الرسمية، عدد 71 ،بتاريخ ن 10 وفمبر 2004

[2] بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، دراسة مقارنة، 2016 ،ص . 52

إقليمي موسع بموجب القانون 04 -14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري الذي أجاز توسيع اختصاص بعض المحاكم ووكلاء الجمهورية وقضاة التحقيق في جرائم محددة على سبيل المثال لا الحصر وتصف بأنها خطيرة وعلى درجة عالية من التعقيد والتنظيم، وهي: جرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تبييض الأموال، الجرائم الإرهابية والتخريبية وجريمة مخالفة التشريع(الخاص بالصرف[1] .

ولقد تم بالفعل صدور النص التنظيمي الخاص الذي مدد الاختصاص لأربع جهات قضائية المرسوم رقم 06-348 المؤرخ في 05-10-2006 المعدل والمتمم بالمرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016 والذي تم بموجبه تحديد هذه المحاكم مع تعديل طفيف في المرسوم بحيث شمل التقسيم إضافة بعض المجالس القضائية بمقتضى المادة 3 - 5-4 -المعدلة للمواد 3-4 -5 من المرسوم السابق وجاء التقسيم كالتالي [2]: (

:)محكمة سيدي أمحمد الجزائر العاصمة ويمتد اختصاصها الإقليمي إلى المجالس القضائية التالية: الجزائر، الشلف، الأغواط، البليدة، تيزي وزوو، الجلفة، المدية، المسيلة، وبومرداس، البويرة، وعين الدفلى

. محكمة قسنطينة ويمتد اختصاصها للمجالس القضائية: قسنطينة، أم البواقي، باتنة، بجاية، تيسة، جيجل، سطيف، سكيكدة، عنابة، ثالمة، برج بوعريريج، الطارف، خنشلة، سوق أهراس، وميلة.

[1] كريمة علة، الجهات القضائية الجزائية ذات الاختصاص الموسع، المجلة الأكاديمية للبحث القانوني، المجلد 11 عدد 117 .ص، 01 2015

[2] سعيدة يوزنون، المرجع السابق، ص .54

حكمة ورقلة ويمتد اختصاصها للمجالس القضائية التالية: ورقلة، أدرار، تمنراست، إليزي، بسكرة، الوادي، وغرداية . محكمة وهران ويمتد الاختصاص بها إلى المجالس القضائية التالية: وهران، بشار، تلمسان، تيارت، تندوف، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تيسنمسلت، النعامة، عين تيموشنت، وغليزان . بحيث يشمل اختصاص كل جهة فضائية مجموعة من المجالس القضائية تقع في منطقة جهوية من الجزائر شمالا، جنويا، شرقا، وغربا، وذلك لدرابع محاكم تسمى أقطابا جزائية، كما تم تدعيم عمل هذه الأخيرة باستحداث وسائل التحري الخاصة لمواجهة الإجرام المنظم يما(فيه الجريمة الإلكترونية[1]

والموائمة بينها وبين تشريعات الدول الأخرى الراغبة في التعاون معها، والسعي إلى تكوين رضية قانونية تعمل على الكفاح الدولي المشترك ضد هذا الإجرام

[1] سعيدة بوزنون، المرجع السابق، ص .55

الفصل الثاني :

آليات التحقيق في الجرائم الالكترونية

لقداينا كيف أن عملية البحث والتحقيق في الجرائم الالكترونية وملاحقة مرتكبيها يتخللها العديد من المعوقات والعقبات الإجرائية، فمنها ما يتعلق بالطبيعة المتميزة للجريمة الالكترونية، أو بالجهات المتضررة، ومنها ما يتعلق بجهات التحقيق،

وأخرى تتعلق بإجراءات الحصول على الدليل الالكتروني لارتباطها ببيانات معالجة الكترونيا وكيانات منطقية غير مادية. وأن كثرة وتشعب هذه العقبات قد انعكس سلبا على مردود سلطات التحقيق والعدالة الجنائية في ملاحقة مرتكب الجريمة، بل وشجعراتفاع معدل الجريمة فيّ العالم بسبب إدراك المجرم الالكتروني أن وجود كل تلك العقبات سيعيق حتما الجهات الأمنية من اكتشاف أمره أو ملاحقته، ما يعطيه ثقة اكبر فيراتكابه المزيد من هذه الجرائم .ولتدارك هذا الخطر باتت عملية البحث عن الحلول المناسبة للقضاء على ما تثيره مكافحة الجريمة الالكترونية من مصاعب ضرورة حتمية، خاصة وقد وجدت الدول نفسها عاجزة عن أداء واجبها الدستوري والقانوني لحماية الأفراد وتحقيق الأمن والاستقرار الاجتماعي المنوط بها إزاء الفراغ التشريعي لمكافحة هذه الظاهرة. فما كان منها سوى الاسراع إلى احتواء هذا النوع الجديد من الاجرام بسد الفراغ التشريعي المذكور، وذلك بتفعيل قوانينها العقابية الموضوعية الاجرائية القائمة بالرغم عما تتضمنه من نقائص وجعلها تسري على الاجرام الالكتروني، ثم تدعيمها بنصوص أخرى جديدة تكون أكثر تلاءم مع طبيعة هذه الجرائم. ثم القيام بعدها بمراجعة تشريعاتها الجنائية الوطنية بما يكفل التنسيق

المبحث الأول الجهود القانونية المقترحة لتدارك عقبات التحقيق في الجرائم الإلكترونية

المتأمل جيدا في المشاكل الاجرائية التي تصادفها سلطات التحقيق والبحث في الجرائم الالكترونية يجد أن معظمها مرتبط بطبيعة القوانين الاجرائية المتعارف

عليها، وما تتسم به من قصور في استيعاب أهم التحديات التي تفرضها مواجهة هذا النمط المستحدث من الجريمة، والأساليب و الاجراءات التي يتم التعامل بها معها، وكذا المناخ المناسب الذي يسمح بتنفيذ هذه الإجراءات، والسرعة والدقة والمهارة الفائقة المطلوبة لاتخاذها. لذلك يتعين لعلاج هذا القصور الذي تعاني منه عديد الدول، وضمان مواجهة فعالة للجريمة الالكترونية الاسراع من جهة إلى ترشيد تشريعاتها الوطنية الاجرائية بجعل أحكامها التقليدية تسري وتطبق على الجرائم الحديثة حتى لا يفلت من يقدم علىراتكاب هذه الجرائم من العقاب

من جهة أخرى الاسراع في مراجعة هذه التشريعات حتى تتلاءم وطبيعة هذه الجرائم الحديثة وتتواكب مع التطورات الهائلة والمتلاحقة في مجال تقنية المعلومات وما تفرزه من جرائم معلوماتية جديدة (المطلب الأول

(.أما عن المشكلات الأخرى التي لها علاقة بالبعد الدولي للفضاء الالكتروني الذي ترتكب فيه الجرائم الالكترونية، وبعدم كفاية التعاون الدولي وفقا للنصوص التقليدية في مكافحة هذه الجرائم بسبب انعدام نموذج موحد للنشاط الإجرامي المكون للجريمة الالكترونية،ّها يتطلب تبني بالإضافة إلى تنوع واختلاف النظم القانونية الاجرائية للدول، فان حل تشريعات مشتركة وموحدة لمكافحة الجرائم الالكترونية عبر الوطنية، أو على الأقل خلق نوع من التقارب والاتساق بين الأحكام الاجرائية الوطنية للدول التي يتم وفقها ملاحقة مرتكبي هذه الجرائم ومحاكمتهم.

وتوقيع العقاب عليهم وتسليمهم، وهو الأمر الذي لا يتأتى إلا عن طريق إبرام اتفاقيات تعاون دولي في مجال التشريع (المطلب الثاني

المطلب الأول : حوكمة المنظومة التشريعية الوطنية لمواجهة الجريمة الالكترونية

آلية التحقيق في الجريمة الإلكترونية

قد يصل إلى علم المحققين وقوع الجرائم من جراء الدوريات التي تقوم بها الضبطية القضائية و إلا فإنها تصل إلى علمهم إما بتلقي البلاغات من طرف عامة الناس أو الشكاوى من الأطراف المضرورة ، ويثار تساؤل حول ما إذا كانت هناك جهات مختصة لتلقي البلاغات والشكاوى بشأن الجريمة الإلكترونية، أم أنها تقدم أمام الجهات المختصة بتلقي البلاغات والشكاوى في الجرائم العادي

تلقي البلاغات والشكاوى حول الجريمة الإلكترونية تظل الجريمة مستمرة ما لم يتم التبليغ عنها إلى الجهات المختصة بالتحقيق وبمجرد وصول نبأ وقوعها إلى تلك الجهات، فإنها تتخذ عدة إجراءات للتأكد من وقوعها وكشف مرتكبيها،و معرفة المحققين لوقوع جريمة ما يتم وفق طريقتين.

أولا/ البلاغات في الجريمة الإلكترونية والبلاغ هو إخبار السلطات المختصة عن وقوع جريمة، أو أنها على وشك الوقوع ، أو أن هناك اتفاقا جنائيا أو أدلة أو قرائن، أو عزما على ارتكابها أو وجود شك أو خوفا من أنها ارتكبت[1] .

كيفية التبليغ في الجريمة الالكترونية:

قد يكون البلاغ واجب في جميع الجرائم كما في قانون الإجراءات الجناية المصري وقد يكون اختياري في بعض الجرائم وواجب في جرائم أخرى كما هو منصوص عليه في القانون الجزائري في المادتين "32 من ق.ع و 91 من ق ا ج " ويتم التبليغ بمختلف الوسائل التي توصل المعلومات إلى الجهات المختصة بالتحقيق فقد يكون التبليغ كتابيا، أو شفويا ومن أي شخص سواء كان متضررا أو غير متضرر وهذا يطلق عليه مصطلح البلاغ المادي وقد يقدم بواسطة البريد أو التلفون أو

[1] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنيت،دار الفكر الجامعي الإسكندرية، 1 ،2007ط1 ص177

الصحف وهذا ما يصطلح عليه البلاغ المعنوي، وقد يتم عن طريق الانترنيت وهذا ما يسمى بالبلاغ الرقمي [1]

.كما يتم الإبلاغ عن الجريمة الإلكترونية عن طريق الانترنيت أو ما يسمى بالبلاغ الرقمي، وذلك إما عن طريق إرسال رسالة الكترونية إلى عنوان البريد الالكتروني للجهات المختصة بالتحقيق كإبلاغها عن وجود صفحات أو مواقع غير مشروعة بإرسال رسالة الكترونية مثلا، تتضمن التبليغ عن وجود موقع منشور فيه صور الاستغلال الجنسي للأطفال [2].

والمعلومات التي يجب معرفتها من المبلغ والتي ينبغي أن يدونها المحقق عند تلقي البلاغ يمكن الحصول عليها من خلال طرح أسئلة عن: تاريخ ووقت تلقي البلاغ، المعلومات الخاصة بالمبلغ، طبيعة ونوع الجريمة الإلكترونية، محل البلاغ، إلى غيرها من الأسئلة المتعلقة بالجريمة .ب. الجهة المختصة بتلقي البلاغات في الجريمة الإلكترونية: الجهة المختصة بتلقي 3البلاغات في فرنسا في مثل هذه الجرائم هي البريد الإلكتروني للدرك الوطني الفرنسي باعتبارها الجهة المختصة بالتحقيق والتحري عن الجرائم الجنسية المتعلقة بالأطفال، والجهة المختصة بتلقي بلاغات في جمهورية مصر العربية موقع شرطة إدارة مكافحة جرائم

الحاسبات وشبكات المعلومات[3] ، ويوجد موقع خص للتضامن مع حملة الحكومة الفرنسية في مكافحتها للإجرام عبر شبكة الانترنيت، وهناك موقع أخر يختص بتلقي ومتابعة البلاغات التي تقدم إليه لدى الجهات المختصة عبر الانترنيت حول الجرائم التي ترتكب عبرها .ص وهناك موقع أخر 3يخت بتلقي ومتابعة البلاغات

[1] نغس المرجع ص178
[2] نغس المرجع ص 182
[3] http.//www.ccd.gov.eg

التي تقدم إليه لدى الجهات المختصة عبر الانترنيت حول الجرائم التي ترتكب عبرها [1].

ثانيا/ الشكوى في الجريمة الالكترونية قد يترتب على الجريمة ضرر خاص قد يصيب احد الأفراد ماديا أو معنويا فينشأ له حق في تحريك الدعوى العمومية بتقديم شكوى أمام الجهة المختصة بالتحقيق حيث نص 5المشرع الجزائري في المادة72 من ق ا ج على " يجوز لكل شخص متضرر من جناية أو جنحة أن يدعي مدنيا بأن يتقدم بشكواه أمام قاضي التحقيق المختص" وقد عرفت الشكوى بأنها البلاغ أو الإخطار الذي يقدمه المجني عليه أو وكيله الخاص إلى السلطات المختصة طالبا تحريك الدعوى العمومية بشأن جرائم معينة، حظر المشرع تحريكها بصددها قبل 6 تقديمه ، ولا يوجب القانون للشكوى شكلا معينا وإنما يقتصر فيها المعني بالأمر على ذكر سمه وسنه عنوانه وموجز الوقائع، والمواد القانونية التي تعاقب الفعل المرتكب، وإعطاء 1كافة المعلومات الخاصة بمرتكب الجريمة إذا كان معلوما . وقد خصصت العديد من المراكز لمعالجة تلك الشكاوى من بينها :مركز تلقي الشكاوى عن جرائم الاحتيال عبر الانترنيت" IFCC " الذي تم تأسيسه في فرجينيا الغربية بالولايات المتحدة الأمريكية من طرف مكتب التحقيقات الفدرالي "FBI" والمركز الوطني لجرائم الياقات البيضاء" NW3C"من أجل مكافحة ظاهرة الاحتيال عبر الانترنيت المتصاعدة والموقع المخصص لتلقي الشكاوى من الضحايا تحت : http://www.ifccfbi.gov عنوان 2 .

وتوقيع العقاب عليهم وتسليمهم، وهو الأمر الذي لا يتأتى إلا عن طريق إبرام اتفاقيات تعاون دولي في مجال التشريع (المطلب الثاني

حوكمة المنظومة التشريعية الوطنية لمواجهة الجريمة الالكترونية

[1] 2 http://www.pointdecontact.net

إذا كان التطور المتجدد والمستمر للمعلوماتية يمنع القوانين الجزائية الحالية من مواكبة ما يطرا من صور وسلوكيات إجرامية مستحدثة في مجال المعلوماتية، فان تطبيق القواعد القانونية الموجودة التي تنظم الحماية الجنائية بما لها من نقص أفضل بكثير من ترك ما يستجد على الساحة الجنائية دون حماية.

انطلاقا مما تقدم يرى البعض أن المواجهة الفعالة للتحديات الاجرائية التي تثيرها الجرائم الالكترونية يقتضي التصرف بحكمة و بدون تسرع أو طيش معها وذلك بداية بترشيد النصوص الجنائية التقليدية بالشكل الذي يجعلها تسر[1]

تطبق على الجرائم الالكترونية، لا سيما تلك الجرائم التقليدية التي ترتكب عبر شبكة الانترنت، والتي لا تعدو هذه الشبكة أن تكون سوى مجرد وسيلة حديثة لارتكابها. على أن يتم ذلك في حدود ما يفرضه مبدأ الشرعية الجزائية من الالتزام بالتفسير الضيق للنصوص الجزائية وحظر القياس (الفرع الاول)،

وهذا الخيار يعد ضرورة لا مناص منها بالنسبة للدول التي لم تسن بعد تشريعات جنائية خاصة لمواجهة هذا النوع الجديد من الإجرام .ويرى البعض الأخر أنه لا ينبغي التعويل كثيرا على القواعد التقليدية لمواجهة هذه التحديات، إنما لابد من التوجه إلى مراجعة هذه النصوص بصفة دورية و مستمرة بما يضمن مواكبة متغيرات وتطورات الجريمة الالكترونية. ولىء اراساء قواعد قانونية جديدة خاصة تواجه المشكلات المعاصرة التي أسفرت عن هذه الجريمة المستحدثة

وتطوراتها اللامتناهية (الفرع الثاني

(.**الفرع الأول: تطبيق النصوص الجنائية التقليدية على الجرائم الإلكترونية :**

[1] -FALQUE Pierrotin, la gouvernance du monde en réseau, in gouvernance de la société de l’information, cahier du C.R.I.D. n 22, Bruxelles, Bruylant, 2002, P 109

يمثل تطبيق النصوص الجنائية التقليدية الاجرائية منها والموضوعية على الجرائم الالكترونية إحدى الحلول الناجعة التي يمكن الاستعانة بها للتصدي لهذا النمط الإجرامي الجديد ومنع إفلات المجرمين من المسؤولية الجزائية ويتأسس هذا الخيار على أنه في ظل عدم تدخل المشرع الجنائي بإصدار تشريعات جنائية جديدة خاصة ب الاجرام الالكتروني، أو مراجعة النصوص الجنائية الموجودة حتى تصبح كفيلة بمواجهة هذا الإجرام، فانه لا مناص من استعانة القضاء بالنصوص الجنائية التقليدية في القواعد العامة أو أية قوانين جنائية خاصة أخرى، حتى لا تترك الأفعال التي تقع بها هذه الجرائم دون متابعة أو عقاب[1]

يتجسد هذا الحل من خلال الاجتهاد في تفسير النصوص العقابية التقليدية التي تعاقب على مختلف صور الاعتداءات، حتى يمكن تطبيقها على الجرائم المستحدثة التي أوجدتها ثورة الاتصالات عن بعد، فلا محالة أن التطور قد يوسع من دائرة المجالات التي تحميها نصوص التجريم والعقاب بحيث يمكن أن ندخل في إطارها عناصر أخرى طالما أمكن اعتبارها من جنسها وأن المشرع يحميها بذات النصوص[2]

. ويكون اتخاذ سبيل التفسير الموسع للنصوص القائمة من أجل تطبيقها على الجرائم الالكترونية، بمنح القاضي الجزائي حرية تفسير هذه النصوص تفسيرا أكثر مرونة يسمح من وضع هذه الجرائم تحت طائلة التجريم و المتابعة الجزائية وذلك في ظل السلطة التقديرية التي يتمتع بها القاضي[3]

فعندما تعرض قضية جزائية على القاضي، فان أول شيء يقوم به هو تكييف الواقعة لمعرفة مدى تطابقها مع النص القانوني الذيّ يجرمها، وللوصول إلى هذه

[1] شام محمد فريد رستم« الجـ ـ ارئم المعلوماتية أصول التحقيق الجنائي الفني و آلية التدريب التخصصي للمحققين » مجـ ـ لة الأمـ ـ ـن و القانون، عدد 02، صادر عن كلية شرطة دبي، 1999

[2] هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، 2012 ،ص 72

[3] وسف حسن يوسف، الج ارئم الدولية للانترنت، مرجع سابق، ص 126 و ما يليه

الغاية يقوم القاضي باستخلاص عناصر هذه الواقعة من النص، وقد يصادفه أثناء ذلك صعوبة أو غموض فيلجأ عندئذ إلى تفسير النص الجنائي [1]

.وفي هذا الصدد نجد القضاء في العديد من الدول، قام بتفسير النصوص الجنائية التي تّ جرم استخدام مال الغير دون وجه حق، مثل القانون البلجيكي المادة 261/2 والدانمركي المادة)293، بشكل يسمح بمد نطاقها لتجريم سرقة وقت وجهد وخدمات الأجهزة والأنظم المعلوماتية في حالة ما استخدمت من قبل الغير بدون الحصول على موافقة حائزها أو مالكها. وذلك نظرا لعدم توفر قوانينها الجنائية لنصّ صريح يجرم هذه الأفعال[2]

كما نجد القضاء الفرنسي قد وسع من تفسير نص المادة (145)من قانون العقوباتّ المتعلقة بجريمة تزوير المحررات التقليدية قبل تعديلها بالمادة)462)من قانون الغش المعلوماتي لعام 1988 ،لتشمل كل أشكال التلاعب في البيانات و الأنظمة المعلوماتية .وكذلك فعل القضاء الياباني، إذ لجأ في ملاحقة جرائم التزوير المعلوماتي، إلى تبني المفهوم الموسع لجريمة التزوير، واعتبر تغيير الحقيقة في الجزء الممغنط من بطاقات البيانات يقع تحت طائلة العقاب على التزوير في المحررات التقليدية [3]

.كذلك هو الشأن بالنسبة للنصوص الجنائية المتعلقة بجريمة السرقة، فقد أصدرت محكمة النقض الفرنسية أكثر من قرار، وضحت فيها بشكل قطعي بأن الأشياء المعنوية والمعلومات على وجه الخصوص، تشملها الحماية التي يكفلها النصوص التقليدية للسرقة .ومن بين هذه القرارات ، قرار إدانة عاملين بورشة التأليف الضوئي بجريمة السرقة، لقيامهما داخل المطبعة وباستخدام معداتها، بنسخ)47

[1] صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، فرع القانون الدولي للأعمال، كلية الحقوق و العلوم السياسية، جامعة مولود معمري بتيزي وزو، .2013 ص 64

[2] غازي عبد الرحمن هيان الرشيد، الحماية القانـ ـ ـ ـونية من ج ارئم المعلوماتية، رسـ ـ ـ ـالة لنيل درجة دكتـ ـ ـو اره في القانون، كلية الحقوق، الجامعة الإسلامية ، بيروت، 2004 ص222

[3] المرجع نفسه، ص.ص 252 -258.

)أسطوانة معلوماتية تحتوي ملفا للعملاء ذات أهمية وقيمة تجارية كبيرة، ونسخ)70)أسطوانة ممغنطة أخرى مسجل عليها عمليات التأليف الضوئي التي باشرتها المطبعة دون علم رب العمل، بهدف تأسيس مشروع منافس للمطبعة التي يعملاني فيها. وقد أسست المحكمة قرارها، على أن واقعة النسخ هنا تتوفر على سائر العناصر المكونة لجريمة السرقة المنصوص عليها في قانون العقوبات وهي ثابتة في حق المتهمين، لذا يتعين إدانتهما و معاقبتها وفقا لأحكام هذا القانون[1]

ولا يختلف الأمر بالنسبة لقابلية بسط نطاق النصوص التقليدية المتعلقة بجريمة الاحتيال، لتسري على الاحتيال الذي يباشر بواسطة التلاعب في الأنظمة المعلوماتية، إذ سمح الفقه والقضاء في العديد من الدول، بالتوسع في تفسير الركن الشرعي المكون لجريمة الاحتيال إلى المدى الذي يتيح إدخال الاحتيال المعلوماتي في نطاقه، منه الفقه الكندي الذي م الاحتيال عبر الوسائل الإلكترونية، فلاّ يرى بأنه في ظل عدم وجود نصوص جديدة تجر مانع من مد نطاق المادتين(387 و 388 (من قانون العقوبات الكندي إلى جرائم الاحتيال الالكتروني [2]

.ويرى الفقه الفرنسي أن خداع الحاسب الآلي بهدف سلب مال الغير تتحققفيه الطرق الاحتيالية بمفهومها المشار إليه في المادة)405)من قانون العقوبات باعتباره كذب تدعمه أفعال مادية أو وقائع خارجية.

وعملا بهذا الراي قضت محكمة النقض الفرنسية، بتطبيق العقوبة المقررة لجريمة النصب على شخص أدخل سيارته إلى موقف للسيارات، وقام بوضع قطعة معدنية في عداد الموقف لدفع مقابل التوقيف بدلا من النقود، ما ترتب عليه تشغيل الماكينة وتحريك العقارب، واعتبرت المحكمة هذا التصرف من قبيل الطرق الاحتيالية[3]

[1] شام محمد فريد رستم، الجـ ـ وانب الإج ارئـية للج ارئم المعلوماتيةـد ارسة مقارنة، مكتبة الآلات الحديثة، القاهرة ، 1994ص246.

[2] BRIAT Martin. La Fraude Informatique: Une approche de droit compare, Revue D.P.C, N04 Paris, Avril 1985, p 191

[3] Ibid., p 192

. وينبغي ألا يقتصر هذا الحل على تمديد سلطان النصوص الجنائية التقليدية الموضوعية إلى الجرائم الالكترونية فقط، بل لابد أن يشمل كذلك النصوص الإجرائية، لا سيما المتعلقة بالتحقيق والإثبات، وهو ما أوصت به اللجنة الأوروبية الخاصة بمشكلات الاجرائية الجزائية المرتبطة بتكنولوجيات الإعلام الدول الأعضاء في المجلس الأوروبي من خلال توصيتها رقم (ر 89 (9 الصادرة في عام 1990 وأكدته في توصيتها رقم (ر95 13)المؤرخة في 11 سبتمبر 1995 بتصريحها أنه " إلى حين وضع نصوص إجرائية جديدة تخص التفتيش و الضبط و اعتراض المراسلات في البيئة الالكترونية، يمكن للسلطات القضائية المختصة في الدول الأعضاء الاستعانة بالنصوص الاجرائية القائمة في هذا الخصوص، حتى لا تبقى الجرائم المتصلة بتكنولوجيات الإعلام بلا متابعة أو عقاب[1]. "

وتجدر الإشارة إلى أن تطبيق النصوص الجنائية التقليدية على الجرائم التي تقع في البيئة الالكترونية، ون ِ ا كان يشكل ضرورة لا مف ّ سن بعد تشريعات ّ ر منها في الدول التي لم ت حديثة مواكب لهذا النوع من الجرائم، إلا أنه لابد من توخي الحذر في ذلك. إذ أن الآلية الوحيدة لإعمال هذا الخيار هو توسع القضاء في تفسير النصوص الجناية التقليدية بما يضمن سريانها على الجرائم الالكترونية، وهو ما قد يشكل إنتهاكا خطيرا لمبدأ الشرعية الجزائية الذي طالما كان درعا حاميا للحقوق والحريات الفردية من تعسف القضاء

. مع هذا تعتمد غالبية الدول العربية على هذا الحل، بحيث لم تفرد تشريعات عقابية خاصة لمواجهة الجرائم الالكترونية مواجهة شاملة، إنما تعتمد في ذلك على نصوص قانونية متفرقة في بعض التشريعات الخاصة، كقوانين حماية الملكية الفكرية، قوانين حماية حقوق المؤلف، قوانين التوقيع الالكتروني، وقوانين المتعلق

[1] voir : la recommandation n R (89) 9 sur la criminalité informatique, comité européen pour les problèmes de droit procédural liés a la criminalité informatique, conseil de l'Europe, Strasbourg, 1990, p 80. Et sa recommandation n R (95) 13, op.cit., p19.

بتكنولوجيا الإعلام والاتصال، أما غالبية الجرائم الالكترونية فتواجهها هذه الدول من خلال تطويع نصوص قوانين العقوبات و الاجراءات الجزائية التقليدية [1]

الفرع الثاني: ضمان مواكبة التشريعات الجزائية الوطنية لمتغيرات الجريمة الالكترونية (التحيين و التحديث

لا يكفي الاعتماد على التشريعات الجنائية القائمة كحل لمواجهة الجريمة الالكترونية، بل لا بد من العمل على مواكبة هذه التشريعات لمتغيرات وتطورات الجريمة الالكترونية، وذلك إما عن طريق تعديل النصوص الجزائية التقليدية بحيث تتواءم مع هذه الصورة الجديدة مـ ـن الإجـ ـرام، أو بخلق نصوص قانـ ـونية جنائية جديـ ـدة يضـ ـاف إليهـ ـا البعد الخـ ـاص بالبيـئة الالكترونية [2]

تأسيسا على ذلك، فقد استدركت اغلب الدول بمختلف أنظمتها القانونية العجز في ملائمة القوانين النافذة للاعتداءات الحاصلة على النظم المعلوماتية، وسوف نأخذ في هذا الصدد عينة من النماذج الناجحة من التشريع المقارن (أولا)، ثم نركز على دور المشرعالجزائري في هذا المجال ثانيا

أولا - التشريعات المقارنة يعد المشرع الفرنسي من أوائل المشرعين الذين تيقنوا بأن التصدي الفعال لل جرائم الالكترونية لن يكون إلاّ من خلال سن نصوص

عقابية اجرائية خاصة بهذه الجرائم. وقد كانت أولى محاولاته لمد سلطان قانون العقوبات ليشمل المجال المعلوماتي في 06 جانفي 1978حينما أصدر قانون "

[1] -لجنة منع الجريمة والعدالة الجنائية، د ارسة شاملة عن مشكلة الجريمة السيب ارنية والتدابير التي تتخذها الدول 525 الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها، مرجع سابق، ص .05

[2] هشام محمد فريد رستم، الج ارئم المعلوماتية أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، مرجع سابق، ص 418.

المعلوماتية والحقوق الشخصية"، وأعقبه بإصدار مرسوم مؤرخ في 23 ديسمبر 1981 حدد فيه بعض المخالفات المرتبطة بالمعلوماتية [1]

ثانيا ــ سياسة المشرع الجزائري في مواكبة تطورات الاجرام الإلكتروني

اعتمد المشرع الجزائري منذ الألفية الثانية على إستراتيجية مزدوجة لمواكبة الجريمة الالكترونية، بحيث قام من جهة بتعديل العديد من القوانين الوطنية بما فيها التشريعات الجزائية (العقوبات و الإجراءات) وجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجي الإعلام والاتصال. وقام من جهة ثانية باستحداث قوانين أخرى خاصة أكثر انسجاما مع الطبيعة المميزة للجريمة الالكترونية .

1ـــ تعديل التشريعات الجزائية : اقتداء بالمشرعين الذين سبقوه، سارع المشرع الجزائري إلى تدارك الفراغ القانوني الحاصل في مجال الاجرام الالكتروني، فقام بتعديل قانون العقوبات بموجب القانون رقم)15-04 544 (مستحدثا فيه جملة من النصوص جرم [2]

من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات، وحدد لكل فعل منها ما يقابله من الجزاء. وقام إلى جانب ذلك بسن قواعد إجرائية جديدة تتعلق بالتحقيق تتماش مع الطبيعة المميزة لل جرائم الالكترونية، وذلك من خلال تعديل قانون الاجراءات الجزائية بموجب قانون (06-22)رقم [3]

.أ-التعديلات المقررة في قانون العقوبات عمد المشرع الجزائري في تعديله لقانون العقوبات بمقتضى القانون رقم (04-15)المؤرخ في 10 نوفمبر 2004 الى

[1] -CHOPIN- Frédérique, Les politiques publiques de lutte contre la cybercriminalité, AJ Pénal, Paris, 2009 p. 102

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

[3] -قانون رقم)22-06)مؤرخ في 20/12/2006 ، يعدل ويتمم الأمر رقم(66-155 ،(يتضمن قانون الإج ارءات 545 الجزائية، ج.ر عدد 84 ،صادر بتاريخ .24/12/2006

استحداث القسم السابع مكرر تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات"، وقد تضمن هذا القسم ثمانية مواد (من 394 مكرر إلى 394 مكرر)7 حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات و ما يقابلها من جزاء أو عقوبة .وباستقراء نصوص هذه المواد يتبين أن المشرع الجزائري حصر هذه الأفعال في ثلاث فئات هي

1- : جرائم الاعتداء على نظام المعالجة الآلية: وهي الجرائم التي تتحقق في صورتين، الصورة البسيطة التي تشمل جريمتي الدخول والبقاء غير المرخص بهما في نظام المعالجة الآلية، وحدد لهما العقوبة نفسها هي الحبس من 03 أشهر الى سنة وغرامة مالية من 50000دج الى 100000دج .والصورة المشددة هي التي تتحقق عندما يقترن فعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية بإحدى ظروف التشديد المنصوص عليها في المادة 394)مكرر)، كمحو أو تعديل بيانات النظام، أو تخريب نظام تشغيل [1] لمنظومة وعاقته عن أداء وظيفته ِ ا .فمتى تحققت هذه الجريمة في صورتها المشددة عوقب الجاني بالحبس من)6)أشهر الى سنتين وبالغرامة من 50000دج إلى 150000دج 2- . 548

جرائم الاعتداء على معطيات نظام المعالجة الآلية : [2]وتشمل الاعتداءات التي تهدف إلى الإضرار بمعلومات الحاسب الآلي أو وظائفه سواء بالمساس بسريتها أو المساس بسلامتها محتوياتها، تكاملها أو بتعطيل قدرة وكفاءة الأنظمة بشكل يمنعها من أداء وظيفتها بصورة سليم. وهي لا تخرج في مجملها عن أحد الشكلين التاليين :

الشكل الأول / الاعتداء على المعطيات الداخلية للنظام: وقد حددت المادة (394مكرر)1 من قانون العقوبات صور هذه الجريمة على سبيل الحصر كالتالي :

[1] أنظر نص المادة 394)مكرر) من القانون رقم(15/04 ،(مرجع سابق

[2] يقصد بالمعطيات محل جريمة الاعتداء بمفهوم هذه المادة 394)مكرر)1 من قانون)15-04 ،)تلك المعطيات 549 والمعلومات التي يحتويها النظام وتشكل جزء منه و التي تمت معالجتها آليا وأصبحت عبارة عن رموز و إشا ارت تمثل تلك المعلومات، وليس المعلومات ذاتها باعتبارها أحد عناصر المعرفة

ـ **الإدخال**: يقصد به إضافة معطيات جديدة غير صحيحة إلى المعطـ ـيات الموجـ ـودة داخل النظام و التي تمت معالجتها أليا.

ـ **المحو** : يعني إزالة من معطيات مسجلة على دعامة موجودة داخل نظام المعالجة الآلية أو تحطيم تلك الدعامة أو نقل جزء من المعطيات من المنطقة الخاصة بالذاكرة .ـ

ـ **التعديل** :يعني تغيير المعطيات الموجودة داخل نظام المعالجة واستبدالها بمعطيات أخرى .ولا تشترط المادة المذكورة اجتماع هذه الصور الثلاثة، بل يكفي أن يصدر عن الجاني -للمزيد من التفاص

إحداها لكي يكتمل الركن المادي لجريمة الاعتداء على معطيات نظام المعالجة[1] .

الشكل الثاني/ الاعتداء على المعطيات الخارجية للنظام: يقصد بالمعطيات الخارجية لنظام المعالجة، تلك المعطيات التي لها دور في تحقيق نتيجة معينة تمثل في المعالجة الآلية للمعطيات، وقد نص عليها المشرع الجزائري في المادة 394)مكرر)2 من قانون العقوبات على النحو التالي:"يعاقب بالحبس من شهرين إلى 3سنوات و بغرامة من 1000000دج الى 5000000دج كل من يقوم عمدا أو عن طريق الغش بـ ـ تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم .

[1] BOUDER Hadjira « protection des systèmes d'informations : aspects juridiques » centre de recherche sur l'information scientifique et technique, Alger, 2012, p 32

ـ حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيـــات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم [1]"

. يتبين لنا من نص هذه المادة أنها جاءت عامة و مطلقة، فهي تقرر الحماية الجنائية لكل من المعطيات الداخلية و الخارجية للنظام معا .فيقصد المشرع بالمعطيات المخزنة إما تلك المفرغة في دعامة مادية خارج النظام كالأقراص الممغنطة أو تلك المخزنة داخل النظام ذاته كذاكرته أو قرصه الصلب[2]

ويقصد بالمعطيات المعالجة، إما تلك التي أصبحت جزءا من النظام بعد أن تحولت إلى إشارات أو رموز تمثل المعطيات المعالجة، وما تلك المعطيات المرسلة عن طريق ا منظومة معلوماتية مثل تبادلراسال المعلومات بين أجهزة المنظـ ـومة المعلومـ ـاتية. فـ ـالأولـى تعتبر معطيات داخلية للنظام والثانية هي معطيات النظام الخارجية [3]

.وعليه فأي تلاعب بالمعطيات المذكورة أعلاه، واستعمالها عمدا أو عن طريق الغش بإحدى الطرق المحددة في المادة 394)مكرر ()2 أي تصميمها أو بحثها أو تجميعها أو توفيرها أو نشرها أو الاتجار بها أو حيازتها أو إفشاءها أو نشرها) يعد جريمة اعتداء على المعطيات الخارجية لنظام المعالجة والتالي يعاقب الجاني بالحبس من شهرين إلى 3سنوات وبغرامة من 1000000دج إلى 5000000دج- .

3 جرائم الاعتداء على سير نظام المعالجة الآلية: لم ينص المشرع الجزائري على هذه الفئة من الجرائم الالكترونية بشكل صريح، إلا انه يمكن استخلاصها من خلال مختلف النصوصّ التي تجرم أفعال الاعتداء على أنظمة المعالجة، اعتبارا أن وقوع هذه الأخيرة تؤثر حتما على سير أو وظيفة نظام المعالجة الآلية .فالاعتداء

[1] أنظر نص المادة 394)مكرر)2 من القانون رقم)15-04 ،)مرجع سابق

[2] فايز محمد ارجح غلاب، الج ارئـ ـ ـم المعلومـ ـاتية في القانون الجزائري و اليمني، رسالة لنيل درجة الدكتـ ـ ـ ـ ـ ـ ـو اره في القانون، فرع القانون الجنائي و العلوم الجنائية، كلية الحقوق، جامعة الجزائر)1. ،)2011ص183

[3] فشار عطاء الله "مواجهة الجريمة المعلوماتية في التشريع الجزائري " بحث مقدم إلى الملتقى المغاربى حول القانون 553 والمعلوماتية المنعقد بأكاديمية الد ارسات العليا، ليبيا، أكتوبر 2009 ،ص 31

على النظام بتخريبه كما نصت عليه المادة 394)مكرر) من شأنه أن يعيب عملية سير النظام، والاعتداء على معطيات الداخلية للنظام باستعمال برامج الفيروسات و برامج القنابل المعلوماتية من شأنه كذالك التأثير في سير أو حسن سير النظام المعلوماتي.

.وعليه يمكن أن تتخذ الأفعال الماسة بسير النظام عدة صور نذكر منه التعطيل: وقد يصيب الأجهزة المادية لنظام المعالجة كتحطيم الاسطوانات أو قطع شبكة الاتصال، أو يصيب كياناته المنطقية كالبرامج أو المعطيات باستخدام برنامج فيروسي أو قنبلة منطقية مما يؤدي إلى عرقلة سير النظام.

ـــ الإفساد: وهو جعل نظام المعالجة الآلية غير صالح للاستعمال بإحداث خلل في نظام سيره و افقاده التوازن في أداء وظائفه، كأن يعطي نتائج غير تلك التي كان من الواجب ِ الحصول عليها، ومثل هذا الفعل إن لم يؤدي إلى تعطيل نظام المعالجة كلية فانه يحول دون تحقيقه لوظائفه بشكل صحيح[1]

.وتجدر الإشارة إلى أن المشرع م كل من الاشتراك و ّ الجزائري جر الشروع فيراتكاب الجرائم الماسة بالأنظمة المعلوماتية المذكورة، وجعل العقوبة عليهما تساوي العقوبة المقررة للجريمة ذاتها

وقد تأخذ هذه العقوبات إما شكل عقوبات أصلية كالحبس والغرامة، أو ِواغلاق المواقع وأماكن عقوبات تكميلية كمصادرة الأجهزة والبرامج والوسائل المستخدمة الاستغلال إذاراتكبت الجريمة بعلم مالكها

.كما أن المشرع ضاعف عقوبة الغرامة المقررة للشخص المعنوي الذي يرتكب إحدى الجرائم الالكترونية المذكورة إلى (05 (مرات الحد الأقصى للغرامة

[1] -فشار عطاء الله، مرجع سابق، ص .28

المحددة للشخص الطبيعي، مع إقراره المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أصليين أو شركاء في الجريمة نفسها التيراتكبها الشخص المعنوي [1]

ب ــ التعديلات المقررة في قانون الاجراءات الجزائية :

:أدرك المشرع الجزائري جيدا بان المواجهة الفعالة للإجرام الالكتروني لا تكون بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية فقط، إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية و تحفظية، وهو ما استدركه بتضمين القانون رقم)22-06)المعدل لقانون الاجراءات الجزائية تدابير إجرائـــية جديـدة تتعلق بالتحقيق في الجـ ـ ـ ـرائم الالكتـ ـرونـ ـ ـ ـية تتمثل فيما يلي:

- اعتراض المراسلات و تسجيل الأصوات و التقاط الصور: بالرجوع إلى المادة (65مكرر)5 من قانون الاجراءات الجزائية،

فان المشرع الجزائري سمح لسلطات التحقيق والاستدلال إذا استدعت ضرورة التحري أو التحقيق في الجريمة الالكترونية، باللجوء إلى اجراء اعتراض المراسلات السلكية واللاسلكية وتسجيل المحادثات والأصوات والتقاط الصور، والاستعانة بكل الترتيبات التقنية اللازمة لذلك من اجل الوصول إلى الكشف عن ملابسات الجريمة و إثباتها دون أن يتقيدوا بقواعد التفتيش و الضبط المألوفة [2]

. نظرا لخطورة هذه الاجراءات على الحقوق والحريات العامة والحياة الخاصة للأفراد، فان المشرع لم يطلق حق اللجوء إليها، إنما قيده بتوفر مجموعة من الشروط القانونية التي تتلخص في، الحصول على الإذن المسبق من السلطات القضائية المختصة للقيام بال اجراء ومراقبتها له، الضرورة الملحة إلى ال اجراء

[1] ارجع العقوبات التكميلية في نص المادة 394)مكرر)6 من قانون العقوبات الجزائري، المرجع نفسه
[2] -أنظر هذه القواعد في المادتين(45 و 47 (من ق إ ج رقم)22-06 ،)مرجع سابق

لإظهار الحقيقة، مراعاة الجرائم التي يجوز فيها الإجراء، مراعاة مدة الاعتراض، مراعاة السر المهني أثناء ال اعتراض [1]

ـ التسرب : بناء على المادة 65)مكرر 11 ق إ ج ج) فقد أجاز المشرع لمتطلبات التحري و التحقيق في الجرائم الالكترونية، اللجوء إلى عملية التسرب للكشف عن الحقيقة، وتقتضي عملية التسرب حسب المادة (65 مكرر)12 من القانون نفسه " قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه فيراتكابهم جناية أو جنحة بإيهامهم انه فاعل معهم أو شريك أو خاف"

.ولضمان إنجاح العملية سمحت المادة 65)مكرر)14 من قانون الاجراءات الجزائية لضابط أو العون المتسرب، استعمال الوسائل المادية كالأموال أو المنتجات أو الوثائق المتحصل عليها منراتكاب الجرائم أو مستعملة فيراتكابها. كما يجوز له تسخير وضع تحت تصرف مرتكبي هذه الجرائم كل الوسائل المادية المتاحة لتنفيذ الجريمة كوسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال، وكذا الوسائل القانونية كتوفير الوثائق الرسمية إن كان هناك ضرورة لذلك كاستخراج بطاقة التعريف الوطنية أو بطاقة رمادية أو جواز السفر و لو استدعى الأمر تزويرها، دون أن يكون الضابط أو العون المتسرب مسئولا جزائيا عن هذه الأعمال .مع هذا واعتبارا أن التسرب اجراء غير مألوف عند سلطات الضبط القضائي، ومن أخطر إجراءات التحقيق انتهاكا لحرمة الحياة الخاصة للمتهم، كان لزاما على المشرع إحاطته بجملة من الضمانات والضوابط التي يتعين مراعاتها عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة اللجوء إليه، وهي

[1] للمزيد من التفاصيل انظر المواد من 65)مكرر 5 الى 65 مكرر) من ق إ ج رقم)22-06)المرجع نفسه

الضمانات المنصوص عليها في المادتين 65)مكرر11 (و (65 مكرر)15 ، والتي لا تختلف كثيرا عن تلك المفروضة على عملية اعتراض المراسلات ـ

ـ تمديد الاختصاص : من أجل تحقيق المواجهة الفعالة لظاهرة الاجرام الالكتروني، فقد قام المشرعالجزائري بموجب المادة (16 الفقرتين 7 و8 (والمادة 16)مكرر)

- الاجراءات الجزائية رقم)22-06)بتمديد الاختصاص المحلي لضباط الشرطة القضائية إلى كامل الإقليم الوطني، فبناء على هذا النص أصبح بمقدور الضبطية القضائية ممارسة جميع إجراءات البحث والتحري التي تدخل ضمن صلاحياتها، عبر كافة الإقليم الوطني إذا تعلق الأمر ب الجرائم الماسة بالمعالجة الآلية للمعطيات. ومثل هذا التدبير لم يكن مسموحا به في السابق إلا في حالات استثنائية ضيقة جدا، وبشروط صارمة [1]

. بالموازاة مع ذلك، فقد تم أيضا توسيع مجال الاختصاص المحلي لنيابة الجمهورية في متابعة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ليشمل نطاق اختصاص مثيلتها في محاكم أخرى دون أن يشكل ذلك حالة تدخل أو تنازع في الاختصاص .وكذلك فعل بالنسبة لقضاة التحقيق بموجب المادة)40/2)من قانون الاجراءات الجزائية التي تنص بأنه "يجوز تمديد الاختصاص المحلي لقاضي التحقيق الى دائرة اختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخذرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.[2]

[1] نظر نص المادة)16)من قانون الإج ارءات الجزائية قبل التعديل الحاصل في .2006.
[2] تنص المادة)37/2)من ق إ ج بأنه " يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في ...الج ارئم الماسة بأنظمة المعالجة الآلية للمعطيات.

إرساء قوانين إجرائية جديدة خاصة بالجرائم الالكترونية :

:يعتبر القانون رقم)04-09 (أهم النصوص الجديدة التي لها سن المشرع الجزائري"[1] لمواجهة الجرائم الناشئة عن الاستخدام غير المشروع لوسائل الإعلام والاتصال الالكترونية وشبكة الانترنيت، والذي" تضمن جملة من تدابير مستحدثة غير مألوفة في القوانين السابقة، وأكثر ملائمة مع خصوصيات هذه الإجرام، تتنوع بين تدابير وقائية، وأخرى إجرائية مكملة لتلك المنصوص عليها في قانون الإجراءات الجزائ

والتي سنفصل فيها بالشكل التالي:

أـــ التدابيـــر الوقائية:

ـ وهي التي يتم اتخاذها مسبقا من طرف مصالح معينة مختصة لتفادي وقوع جرائم معلوماتية أو الكشف عنها و رصد مرتكبيها في وقـت مبكر[2]

، وتتلخص فيمايلي:

مراقبة الاتصالات الالكترونية: لقد نصت المادة)04)من القانون رقم (09-04) علىرابع حالات التي يجوز فيها لسلطات الأمن والتحقيق القيام ب مراقبة المراسلات والاتصالات الالكترونية، وذلك بالنظر إلى خطورة التهديدات المحتملة وأهمية المصلحة المحمية وهي :-

ـ ـ للوقاية من الأفعال التي تحمل وصف جرائم الإرهاب و التخريب و جرائم ضد أمن الدولة

[1] قانون رقم)04-09)مؤرخ في 5/08/2009 ، يتضمن القواعد الخاصة بالوقاية من الج ارئم المتصلة بتكنولوجيات564 الإعلام و الاتصال و مكافحتها، جريدة رسمية عدد 47 ،صادر بتاريخ 16 أوت 2009

[2] تجدر الإشارة إلى أن هذه التدابير هي نفسها المنصوص عليها في المادة(20 الفقرة (ب) و المادة)21)من 565 الاتفاقية الأوروبية لمكافحة الج ارئم المعلوماتية لعام 2001 ،مرجع سابق

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

ـ لضرورة التحقيقات و المعلومات القضائية حينما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى ال مراقبة الالكترونية . في إطار تنفيذ طلبات المساعدات القضائية الدولية المتبادلة.[1]

إقحام مزودي خدمات الاتصالات الالكترونيةفي مسار الوقاية من الجرائم المعلوماتية: وذلك من خلال فرض عليهم مجموعة من الالتزامات المذكورة في المواد 10-11-12[2]

بالشكل التالي

:تسجيل المعطيات المتعلقة بالاتصالات والمراسلات ووضعها تحت تصرفها مع مراعاة سريةالالتزام بالتعاون مع مصالح الأمن المكلف بالتحقيق القضائي عن طريق جمع أو هذه الإجراءات والتحقيق .تساهم في الكشف عن الجرائم ومرتكبيها، وهذين الالتزامين موجهين لكل مقدمي خدماتالالتـ ـزام بحفظ المعطـ ـيات المتعلقـ ـة بحركة السير وكل المعلومات التي من شأنـها أن الاتصالات الالكترونية services de Fournisseurs)دون استثناء

-الالتزام بوضع ترتيبات تقنية للحد من إمكانية الدخول إلى الموزعات التي تحتوي على معلومات متنافية مع النظام العام والآداب العامة مع إخطار المشتركين لديهم

[1] 7أنظر نص المادة)04)من القانون رقم)04-09 ،

[2] -عرفت المادة(2 الفقرة (د) من القانون رقم)04-09)مزودي الخدمات بأنه -1 :أي كيان عام او خاص يقدم لمستعملي خدماته، ضمانة القدرة على الاتصال بواسطة منظومة معلوماتية و/ أو نظام الاتصالات 2 - .أي كيان آخر يقوم بمعالجة أو تخزين معطيان معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليه

بوجودها .ونشير هنا إلى أن هذين الالتزامين يخصان فقط مقدمي الدخول إلى الانترنيت غيرهم دون . Fournisseurs D’accès a l’internet)[1]

- - - التدابير الإجرائية

: إضافة إلى التدابير الوقائية سالفة الذكر، تبنى المشرع في القانون رقم(09-4 (إجراءات تحقيق جديدة" يكمل بها تلك المنصوص عليها في قانون الإجراءات الجزائية بخصوص مكافحة جرائم تكنولوجية الإعلام و الاتصال، و التي نلخصها فيما يلي:

- السماح للجهات القضائية المختصة وضباط الشرطة بالولوج لغرض التفتيش و لو عن بعد إلى منظومة معلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها واستنساخها، مع إمكانية تمديد التفتيش ليشمل المعطيات المخزنة في منظومة معلوماتية أخرى التي يمكن الدخول إليها بواسطة المنظومة الأصلية، بشرط إخطار السلطات المختصة مسبقا.

- إمكانية الاستعانة بالسلطات الأجنبية المختصة للحصول على المعطيات محل البحث المخزنة في منظومة معلوماتية موجودة خارج الإقليم الوطني، وذلك طبقا للاتفاق ـ ـيات الدولية ومبدأ المعاملة بالمثل [2]

بتكنولوجية الإعلام والاتصال المرتكبة من طرف الأجانب خارج الإقليم الوطني، عندما تكونتوسيع دائرة اختصاص الهيئات القضائية الجزائرية لتشمل النظر في الجرائم المتصلة مؤسسات الدولة الجزائرية والدفاع الوطني والمصالح الإستراتيجية للدولة الجزائرية مستهدفة .الأجنبية في مجال التحقيق وجمع الأدلة للكشف عن

[1] بوكر رشيدة، ج ارئم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، منشو ارت الحلبي الحقوقية، بيروت، 2012 ،ص 450

[2] -ارجع المادة)05)من القانون)04-09)المؤرخ في 05-02-2009

الجرائم المتصلة بتكنولوجية الإعلامالسماح للسلطات الجزائرية المختصة اللجوء إلى التعاون المتبادل مع السلطات والاتصال عبر الوطنية ومرتكبيها، وذلك

عن طريق تبادل المعلومات أو اتخاذ تدابير احترازية في إطار الاتفاقيات الدولية ومبدأ المعاملة بالمثل[1]

.وتجدر الإشارة إلى أن أحكام القانون رقم)4-09)جاءت عامة و مطلقة في مجال مكافحة الجرائم المتصلة بتكنولوجية الإعلام والاتصال، إذ تجرم كل الأفعال المخالفة للقانون التي ترتكب عبر وسائل الإعلام والاتصال، وت طبق على كافة التكنولوجيات القديمة والجديدة، بما فيها شبكة الانترنيت وعلى أي تقنية يمكن أن تظهر مستقبلا.

وهو الأمر الذي يجعله قانونا فعالا ويساير حقا التطور التكنولوجي السريع .ومع هذا ينبغي الاعتراف بحقيقة وهي انه رغم الجهود الجبارة التي بذلها المشرع الجزائري في سبيل التصدي لظاهرة الإجرام الالكتروني، إلا أنها تبقى غير كافية لبلوغ الهدف المنشود، نظرا للتطورات السريعة والمستمرة التي تعرفها ظاهرة الإجرام الالكتروني من جهة، ونظرا للطابع العالمي والعابر للحدود الذي تتميز بها هذه الظاهر من جهة أخرى لذلك لابد من التوجه إلى التنسيق التشريعي والقضائي والأمني مع الدول العربية و لما لا مع الدول الغربية الأكثر دراية بالجرائم الالكترونية والاستفادة من خبراتها في مجال مكافحة هذه الجرائم.

[1] ارجع المادتين (16 و 17 (من القانون)04-09 ،)المرجع ن

المطلب الثاني تكثيف التعاون الدولي في مجال التشريع

إن قصور التشريعات الداخلية في مواجهة الجريمة الالكترونية وعجز الدول فرادى التصدي لها بسبب طبيعتها عبر الوطنية، جعل المجتمع الدولي يقتنع بأن توحيد جهوده وحشد قواه هو الحل الأمثل لمكافحة هذا الإجرام[1].

ويعتبر التعاون بين الدول في مجال التشريع أنجع الحلول لمعالجة و تجاوز العقبات التي تعيق عملية مكـافحة الجرائـ م الالكترونية، وأكثرهـا فعالـية في مجـال تعقب مرتكبي هذه الجرائم وملاحقتهم والقبض عليهم ومحاكمتهم وكذا إنزال العقاب عليهم [2].

. وتتجلى أهمية هذا النوع من التعاون الدولي، فيما يحدثه من تقارب وتوافق بين التشريعات الجنائية الوطنية للدول بشقيها الموضوعي والإجرائي، وما يترتب عنه من خلق منظومة قانونية مشتركة لمكافحة ظاهرة الإجرام المعلوماتي ذات الطابع عبر الوطني، تتوحد فيها الرؤية من خلال وضع تعريف موحد للجريمة الالكترونية، تحديد الأفعال وصور النشاط محل التجريم، والتكييف القانوني لكل فعل إجرامي والعقوبات التي تقابله، وكذا توحيد الأحكام الإجرائية التي يتم وفقها ملاحقة مرتكبي هذه الجرائم و معاقبتهم، وهو ما قد يشكل سدا منيعا لاستغلال المجرمين أوجه النقص التي تنطوي عليها تشريعات بعض الدول.

[1] نظر: ق ارر الجمعية الدولية لقانون العقوبات الصادر عن مؤتمرها الدولي الخامس عشر حول القواعد الإج ارئية في بيئة ج ارئم الكمبيوتر، مشار إليه في: زيبحة زيدان، مرجع سابق، ص .144

[2] السبيل الوحيد!، بحث مقدم إلى الندوة الإقليمية حول " الج ارئم المتصلة بالكمبيوتر"، المنعقدة بالرباط في 19 و 20 جويليةإيهاب ماهر السنباطي، الج ارئم الإلكترونية(الج ارئم السيبيرية :) قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو .28ص،7 200

الفرع الأول:الجهود المبذولة على المستوى الدولي

سنركز في هذا العنصر على دراسة تجربتين ناجحتين هما، التنسيق التشريعي في إطار منظمة الأمم المتحدة (أولا)، ومنظمة التعاون والتنمية الاقتصادية(ثانيا) كمايلي

أولا -التنسيق التشريعي في إطار منظمة الأمم المتحدة : [1]**إمانا** منها بأن منع الجريمة الالكترونية و مكافحتها يتطلبان استجابة دولية في ضوء الطابع والأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم التي يخلفها، فقد كانت منظمة الأمم المتحدة من الهيئات الدولية السباقة إلى وضع خريطة طريق للتصدي للجريمة الالكترونية، والحث على تعزيز العمل المشترك والتعاون بين الدول الأعضاء من أجل الحد من انتشارها وتعاظم أثارها[2] وذلك من خلال تنظيمها ورشات عمل دولية خاصة بمنع الجريمة ومعاملة المجرمين، واشرافها على عقد مؤتمرات دولى ا ة في هذا المجال ، أكدت فيها بأن مواجهة هذا النوع الجديد من الإجرام يتطلب من الدول الأعضاء اعتماد عدة تدابير أهمها : [3]

ضرورة تحين وتحديث القوانين الموضوعية والإجرائية التي تتناول هذا النمط الجديد من الإجرام والعمل على تحسين أمن المعلومات والوقاية المتعلقة بالحسابات الآلية وشبكات الانترنت المتصلة بها.

-وضع التدابير الوقائية والأمنية لمنع الجريمة مع مراعاة خصوصية الأفراد واحترام حقوق الإنسان.

ـ -توعية الجماهير بخطورة الجريمة الالكترونية و أهمية مكافحتها.

[1] -إيهاب ماهر السنباطي، مرجع سابق، ص 29
[2] -إيهاب ماهر السنباطي، مرجع سابق، ص 29
[3] محمد الأمني البشري و محسن عبد الحميد محسن، معايير الأمم المتحدة في مجال العدالة الجنائية و منع الجريمة، أكاديمية نايف للعلوم الأمنية، رياض، 1998 ،ص 19.

ـ تنظيم دورات تدريب مكثفة لرجال القضاة و الأمن حول تقنيات و فنيات التصدي لمثل هذه الجرائم.

ثانيا: التنسيق التشريعي في إطار منظمة التعاون و التنمية الاقتصادية

(OCDE) تعود أولى اهتمامات المنظمة بالجرائم الالكترونية إلى عام 1980 ،حينما وضعت دليل تشريعي يتضمن مجموعة من قواعدراشادية لحماية الخصوصية و نقل البيانات عبر وسائل الاتصال الالكترونية وأوصت الدول الأعضاء إدراجها ضمن تشريعاتها الداخلية والالتزام بها، ومن بين هذه القواعد :ـ ـ

ـ الحق في الخصوصية مضمون، ولا يجوز الاطلاع على المعلومات الخاصة للأفراد أو إفشائها إلا في إطار القانون بعد علمهم و موافقتهم على ذلك .

ـ ـ لا يجوز استعمال المعلومات الخاصة للأفراد لأغراض أخرى غير تلك التي تم الحصول عليها من اجلها.

الفرع الثاني:الجهود المبذولة على المستوى الجهوي

سنركز هنا على ابراز الجهود المبذولة أوروبيا فيراساء سبل التعاون التشريعي بين الدول(أولا)، ثم على مستوى الدول العربية(ثانيا)، بعدها نتوقف عند جهود مجموعة الدول الثمانية (ثالثا .)

-**أولا:على المستوى الأوروبي:** أدى المجلس الأوروبي دورا مهما في تحقيق الانسجام بين التشريعات الوطنية للدول الأطراف في مجال مكافحة جرائم تقنية المعلوماتية، وقد تجسدت أولى جهوده في توقيع دول الاتحاد في 28-01-1981 اتفاقية رقم)108 (تتعلق بحماية الأشخاص في مواجهة المعالجة الالكترونية للبيانات ذات الصبغة الشخصية، والتي شكّلت الإطار القانوني المشترك

لضمـان حرية تنقل البيـانـات الشخصية المعـالــجة إلكترونا و حمايتها من أي شكل من أشكال التعدي [1]

.حث فيها الدول الأعضاء بمراجعة قوانين الإجراءات الجنائية الوطنية لتتلاءم مع التطور الحاصل في هذا المجال، آخذتا بعين الاعتبار النقاط التالية :ـ

توضيح إجراءات تفتيش أجهزة الحاسب الآلي وضبط المعلومات التي تحتويها و مراقبة انتقال المعلومات عبر وسائل الاتصال الالكترونية، والسماح بممارستها وفقا لذات الشروط و الضمانات الخاصة بإجراءات التفتيش العادية .ـ

ـ ـ الاعتراف للجهات المختصة بالتفتيش إذا دعت الضرورة، بمد عملية التفتيش إلىّ أنظمة الحــاسب الآلــ ـي الأخرى المتصلــ ـة بالنظـلم محـ ـل التفتيش داخل دائـ ـرة اختصـلصهم، وضبط ما بها من معلومات و بيانات.

الموازنة بين المعلــومـات والبيانـ ـات الالكترونية الـ ـواردة علـ ــى أجهزة الحـ ـاسب الآلـ ــي والوثائق التقليدية من حيث إجراءات التحقيق المطبق عليها

.ـ ـ ــ السماح بتطبيق إجراءات ال مراقبة والتسجيل لأغراض التحقيق الجنائي على تقنية المعلومات كلما دعت الضرورة لذلك. وفي حالة جمع المعلومات بطريق ال مراقبة والتسجيل، يجب مراعاة معايير احترام الخصوصية و سرية المعلومات، والحصانات المقررة لذلك .ـ

ــ إعطاء جهات التحقيق سلطة توجيه أوامر، لكل من يحوز أشياء أو معلومات تخص نظام أجهزة الحاسب الآلي(دخول، تشغيل برامج أو قواعد بيانات) تفيد الكشف عن الحقيقة بتسليمها لها .ـ

[1] صغير يوسف، مرجع سابق، ص .97

ـ ـ إلزام متعاملين خدمات الاتصال الحكومية و الخاصة بالتعاون مع سلطات التحقيق ّ وتقديم لهم يد المساعدة بخصوص التحقيق .ـ ـ

ـ تطبيق النصوص الإجرائية الخاصة بالأدلة التقليدية(جمع الأدلة، المحافظة عليها، تقديمها، حجيتها) على الأدلة الالكترونية، والسعي إلى تطوير وتوحيد أنظمة التعامل مع الأدلة الالكترونية حتى يتم الاعتراف بها بين كل دول الأعضاء

ـ على مستوى مجموعة دول الثمانية (G8(تعتبر هذه المجموعة حيزا خصبا للدراسات العلمية والتطبيقية الناجحة في شتى الموضوعات التي تهم الدول الأطراف، فهي تقوم على فكرة تبادل قادة هذه الدول وجهات النظر والمعارف في المسائل ذات الاهتمام المشترك لبلورة إستراتيجية أو خطة عملية موحدة لمواجهة كل ما من شانه التهديد أو التأثير بالمصلحة الخاصة أو المشتركة لدول المجموعة . وفي موضوع مكافحة الجرائم الالكترونية، أجرى وزراء العدل و الداخلية التابعين لدول مجموعة الثمانية عدة دراسات متخصصة في الموضوع انتهت كلها إلى وضع خطط عمل مشتركة تعتمد عليها الدول الأطراف للتصدي لظاهرة الإجرام الالكتروني، نذكر منها خطة العمل بشأن الجريمة ذات التكنولوجيا العالية وجرائم الحاسب الآلي لعام 1997 ،والتي تضمنت المبادئ التي يمكن على أساسها إنشاء شبكة نقاط اتصال وتبادل معلومات وطنية تعمل على مدار 24)سا 24 /سا)، وآليات إنشاء شبكة متابعة لتقديم تقارير دورية حول مدى

فقد صدرت مجموعة دول الثمانية عدة توصيات بخصوص الجريمة الالكترونية 629تح ّث في مجملها الدول الأعضاء على مايلي :

- السهر على توحيد تشريعاتها العقابية والإجرائية الوطنية فيما يتعلق بجرائم التكنولوجيا الحديثة والجرائم ذات الصلة بالحاسب الآلي.

- ـ ـ ـ ـ تكثيف سبل التعاون الدولي لمكافحة الجرائم الالكترونية والتنسيق بين الدول لتجاوز العقبات و معالجة المشاكل المتعلقة بالتحقيقات القضائية في هذه الجرائم.
- ـ ـ ـ ـ ـ اتخاذ تدابير وقائية وأخررادعة لمنع الجريمة الالكترونية.
- ـ ـ ـ ـ العمل الدءوب على اقتناء التكنولوجيات الملائمة والتطوير المستمر للخبرات والقدرات الفنية في مجال التحقيق والادعاء العام، وتشجيع البحث العلمي والتطبيقي في هذا المجال من أجل زيادة فعالية تقنيات تطبيق القانون
- ـ ـ ـ ـ ـ تشجيع التعاون في مجال تطوير الاستراتيجيات المناسبة لرفع الوعي العام في هذا الشأن، مع التقييم المستمر ل برامج المكافحة والوسائل القانونية المتبعة.

تجدر الإشارة إلى، أن جهود مجموعة دول الثمانية ون كانت ا لا تشكل في مجملها إطارا تشريعيا ملزما للدول الأعضاء، إلا أنها قد تمثلراضية مناسبة لبعث التعاون والتنسيق بين الدول الأطراف في مجال مكافحة الجريمة الالكترونية، ومساعدة حكوماتها على تطوير نموذج مشترك للتشريع الالكتروني يكون قابلا للتطبيق محليا ودوليا بالتوازي مع التدابير القانونية الوطنية و الدولية المعتمدة.

❖ المبحث الثاني : لحلول القضائية المقترحة لتدارك عقبات التحقيق في الجرائم الإلكترونية

إذا كان للحلول التشريعية أهمية قصوى في رفع العقبات التي يثيرها البحث والتحقيق في الجرائم الالكترونية، بالنظر لما توفره من مشروعية وفعالية للسلطات القائمة على التحري والضبط والمحاكمة في نشاطاتها ذات الصلة بالسلوك الاجرامي الالكتروني، فان الحلول القضائية بدورها لا تقل أهمية، لأنها تهتم بتجسيد الحلول القانونية فيراض الواقع ونقلها من دائرة التجريد القانوني إلى التطبيق العملي ومن حالة السكون إلى حالة الحركة الفعالة .ا ت الحلول التشريعية قدراتبطت بشكل عام بالعقبات التي تثيرها عملية التحقيق،وذا كان في الجريمة الالكترونية الوطنية، التي تكتمل كافة اركانها على إقليم دولة معينة، فان الحلول القضائية التي نقترحها ترتبط أكثر بالمشكلات الإجرائية والعملية التي تطرحها الجريمة الالكترونية عبر الوطنية التي تمتدراكانها وأثارها إلى خارج حدود الإقليم الوطني، ما يجعل هذه الحلول إحدى الضروريات اللازمة لمواجهة هذا النمط من الإجرام .وتتجلى هذه الحلول، في تعزيز التعاون الدولي القضائي بصوره المختلفة، باعتباره أحد التدابير التي تضمن المساعدة المتبادلة والتنسيق المشترك بين سلطات العدالة الجنائية التابعة لدول مختلفة في مواجهة الجريمة الالكترونية(المطلب الاول). وفي الاستعانة بالتدابير الوقاية والحماية الأمنية، باعتبارها إحدى التدابير المانعة منراتكاب الجرائمّ الالكترونية أو التي تحد من الآثار الضارة المترتبة عنها (المطلب الثاني(

.

المطلب الأول تعزيز التعاون القضائي الدولي

من العقبات الشائعة التي تواجه عملية التحقيق في الجرائم الالكترونية، احترام سيادة الدول ومشاكل الحدود والولايات القضائية، وذلكراجع إلى الطابع العابر للحدود الذي تتميز به هذه الجرائم. ولعل من الحلول الناجعة التي وجدتها الدول لتجاوز هذه العقبات وتحقيق التوافق بين حرية كل دولة في ممارسة اختصاصها الجنائي على كافة حدود إقليمها، وبين ضرورة ممارسة حقها في العقاب، تعزيز التعاون والمساعدة القضائية المتبادلة فيما بينها.

فالتعاون القضائي ينبع من الضرورة ذاتها التي ينبع فيها التعاون التشريعي، وفعالية التحقيق والملاحقة القضائية في الجرائم المعلوماتية غالبا ما تقتضي الحاجة إلى مساعدة من سلطات دولة منشأ الجريمة، أو من سلطات الدولة التي عبر من خلالها السلوك الإجرامي للوصول إلى الهدف أو النتيجة، أو حيث توجد أدلة الجريمة. كما أن الأحكام والقرارات التي تصدر من الهيئات القضائية بالنسبة لهذه الجرائم لا تسري على إقليم دولة أخرى ولا ترتب ّ أي أثر قانوني ما لم تعترف بها هذه الأخيرة، وعليه فلا تتأتي هذه الأمور إلا في إطار التعاون القضائي الدولي المتبادل .وقد يأخذ التعاون القضائي الدولي في مجال مكافحة الجرائم الالكترونية مظهرين، الأول يتعلق باتخاذ جملة من التدابير والآليات المشتركة ذات الطبيعة الأمنية والفنية التي تضمن منع الجريمة أو الكشف عنها في مرحلة التنفيذ أو ما يسمي بالمساعدة الأمنية والفنية)الفرع الأول). أما الثاني فيتعلق بإجراءات إنفاذ القانون لملاحقة ومتابعة ومعاقبة المجرمين بعد راتكاب الجريمة وهو يدعى بالمساعدة القضائية الدولية (الفرع الثاني

الفرع الأول: تدعيم المساعدة الأمنية والفنية المتبادلة بين الدول

اثبت الواقع بأن أية دولة مهما بلغت قوتها ودرجة تطورها لا تستطيع بمفردها القضاء على الجرائم المعلوماتية العابرة للحدود، لأن سلطاتها الأمنية عادة ما تصطدم بمبدأ احترام سيادة الدولة و اختصاصها القضائي الذي يقف حجر عثرة أمام اكتشاف هذه الجرائم وتعقب المجرمين وكذا متابعتهم خارج حدود الإقليم الوطني. لذا فالسبيل في ذلك هو خلق فظاءات تعاون وقنوات اتصال أجهزة الشرطة فيما بين الدول و تنسيق العمل الأمني بعضها مع البعض عن طريق إنشاء هيئات أمنية إقليمية ودولية مشتركة (أولا)، وخلق فظاءات أخرى لتبادل الخبرات والمهارات الفنية في هذا المجال عن طريق عقد دورات تدريبية لمواكبة التطور السريع الحاصل في ميدان الجرائم المستحدث ذات البعد الدولي(ثاني.)

أولا ـــ تفعيل التعاون الأمني أو الشرطي الدولي: يعتبر التعاون الشرطي مظهر من مظاهر التعاون الدولي الذي تسعى من خلاله الدول إلى تجاوز الصعوبات التي تطرحها عملية البحث والتحري وجمع الأدلة خارج الإقليم الوطني بخصوص الجرائم الالكترونية العابرة للحدود، ويتجسد هذا التعاون في إنشاء هيئات أمنية دولية وقليمية ا مشتركة تضمن الاتصال المباشر بين سلطات الأمن في الدول والتبادل السريع للمعلومات بخصوص الجرائم المرتكبة والمجرمين، وتوفر المساعدة و التنسيق فيما بينها من اجل تحقيق أهداف لا قبل للشرطة الإقليمية بتحقيقها . 630ومن أبرز هذه الهيئات على هذا الصعيد نذكر مايلي:

دور المنظمة الدولية للشرطة الجنائية(INTERPOL)في دعم التعاون الأمني تعتبر المنظمة الدولية للشرطة الجنائية أحسن نموذج للتعاون الشرطي [1]، فهي تمثل 6 أكبر شبكة اتصالات لتبادل المعلومات الأمنية على المستوى العالمي، الهدف منها تعزيز وتشجيع المساعدة المتبادلة بين أجهزة الشرطة الجنائية في الدول الأطراف

[1] http://www.interpol.int/public/icpo/default.asp

من أجل التصدي الفعال للجرائم ذات الطابع العالمي بما في ذالك الجرائم المرتبطة بالمعلوماتية، وتجاوز العقبات التي يثيرها الطابع العالمي و الخاص لهذا النوع من الجرائم. بالإضافة إلى إنشاء وتطوير كل النظم القادرة على المساهمة بفعالية في الوقاية من هذه الجرائم و مكافحتها، وتعتمد المنظمة لتحقيق أهدافها على طريقتين

: الطريقة الأولى: تتمثل في تجميع كافة البيانات و المعلومات المتعلقة بالجريمة والمجرمين عن طريق المكاتب المركزية للمنظمة الموجودة على أقاليم الدول الأطراف، وتخزينها على شكلراشيف يتم الرجوع إليها و تبادلها بشكل سريع فيما بين هذه المكاتب كلما دعت ضرورة التحقيق و البحث إلى ذلك

الطريقة الثانية: تتجسد في التنسيق والتعاون بين الدول الأعضاء في ملاحقة المجرمين الفارين والقبض عليهم وتسليمهم للدولة طالبة التسليم، عن طريق المكاتب المركزية المتواجدة على أقاليمها. ومن خلال إذاعة مذكرات التوقيف دوليا ومنحها قوة نفاذ عالمية

2-ـــــ مساهمة شرطة (الانترنت) الويب الدولية IWP في تكريس المساعدة الأمنية :هي منظمة دولية أنشئت في الولايات المتحدة الأمريكية عام 1986 ،لتلقي بلاغات وشكاوي مستخدمـ ـي شبكة الانترنـت وملاحقة الجـ ـناة الكترونـ ـيا والبحث والتحـ ـري عن الأدلـ ـة ضـدهـ ـم وتقديمهم للمحاكمة [1]

وتضم هذه الهيئة متخصصين من سلطات إنفاذ القانون والمؤسسات الحكومية وضباط شرطة وخبراء فنيين من 61 دولة حول العالم، كما أنها تمارس اختصاصها في تتبع الأنشطة الإجرامية التي ترتكب عبر شبكة الانترنت على المستوى العالمي، وبالتعاون والمشاركة مع سلطات إنفاذ القانون التابعة للدول الأعضاء، أو أية دولة أخرى معنية بالجريمة .وتعتمد منظمة شرطة الانترنت في عملها على قاعدة بيانات

[1] - http://www.web-police.org.

مركزية عملاقة يتم من خلالها تسجيل كافة الحوادث والأنشطة الإجرامية التي استخدم فيها الانترنت والتي تم الإبلاغ عنها[1]

. ونظرا للمهارات الفنية العالية والقدرات المعرفية والعلمية الخارقة التي يتمتع بها القائمين على هذه المنظمة في مجال التكنولوجيات الحديثة، أضحت مقصدا لطلبات المساعدة الأمنية والقضائية من مختلف دول العالم، وفضاء واسعا للتنسيق وتبادل المعلومات والإجراءات وأدلة الإثبات بخصوص جرائم الانترنت مع مختلف أجهزة المكافحة و الضبط في دول المعمورة، ومختلف المنظمات والوكالات الدولية المتخصصة المنخرطة في محاربة هذا النمط الإجرامي. كما أصبحت مصدرا مهما لتقديم المشورة الفنية في ذات المجال

دور الشرطة الأوروبية (EUROPOL) في توفير التنسيق الأمني في أوروبا

:يمثل الأوروبول جهاز للشرطة الجنائية على مستوى الاتحاد الأوروبي، انشأ في لكسمبورغ بموجب الاتفاقية 26 جويلية 1995 ودخل حيز الخدمة في عام 1999 بعد أن اتخذ 0 مقره في مدينة لاهاي بهولندا، ليكون همزة وصل بين أجهزة الشرطة الوطنية للدول الأعضاء في مجال ملاحقة الجرائم العابرة للحدود بما فيها جرائم الإرهاب والمخدرات، الجريمة المنظمة، وكذا الجرائم الالكترونية[2]

ثبتت الشرطة الأوروبية نجاعتها في التصدي للإجرام الالكتروني العابر للحدود ّلت من خلال عديد العمليات نفذتها بالتنسيق مع سلطات أمن تابعة للدول الأعضاء وكل بالنجاح، نذكر منها العملية الشهيرة بمحطم الجليد icebreaker( ) التي قامت بموجبها الاوروبول في 14 يونيو 2005 بمداهمة وتفتيش أماكن في ثلاث عشرة دولة أوروبية هي،)النمسا، بلجيكا، فرنسا، ألمانيا المجر، أيسلندا، إيطاليا، هولندا،

[1] سليمان احمد فيصل، مرجع سابق، ص .417

[2] -أنظر مبادئ و أهداف الأوروبول في المادة)9(K1.من اتفاقية مستر يخت منشور في الموقع الالكتروني : http//:fr.wikipedia.org/wiki/Trait%C3%A9 de Maastricht

بولونيا، البرتغال، سلوفاكيا لسويد، وبريطانيا العظمى) وتوجت بتوقيف عدد من المجرمين في كل من فرنسا، بلجيكا، المجر، وأيسلندا والسويد [1]

انظمة الشرطة الجنائية الإفريقية) : AFRIPOL) وهي أكبر منظمة شرطة في القارة الإفريقية مكونة من قوات الشرطة لـ 41 دولة، أنشئت بمبادرة من الدولة الجزائرية يوم .و[2]تم الإعلان رسميا عن بداية 8 13 ديسمبر 2015 ، ومقرها الرئيسي بالجزائر العاصمة نشاطها يوم الأحد 06/07/2017 بمناسبة اجتماع مسئولي أجهزة الشرطة للدول الإفريقية الأعضاء في الإتحاد الإفريقي المنعقد بالجزائر، وترتكز مهام الافريبول كما أعلن عنها المدير العام للأمن الوطني الجزائري في، مضاعفة رصيد التعاون الشرطي الإقليمي والدولي، تحديد عادة تأهيل مختلف أجهزة الشرطةِ السياسة العامة للشرطة الجنائية وتوفير التكوين وا الإفريقية التي تشهد تأخرا أو ضعفا على مستوى الأداء، تعزيز قيم السلم والأمن والاستقرار يجاد الحلول الجادِ في القارة الإفريقية، رفع التحديات والفعالة للجرائم العديدة التي تواجهها بعض الدول الإفريقية، مثل تنامي الجرائم الإرهابي والمتاجرة بالمخدرات والقرصنة البحرية وتبييض الأموال والجرائم المعلوماتية، السماح بالتحدث بصوت واحد على الصعيد الدولي وتطور الموقف الإفريقي المشترك في سبيل تفضيل الحلول الإفريقية وتفادي الوصفات المفروضة عليها، وكذا السعي إلى تعميق تبادل وجهات النظر حول ترقية العلاقات الثنائية بين المؤسسات الشرطية للبلدان الإفريقية

ثانيا ـــــ تكثيف التعاون الفني الدولي: لا تكفي المساعدة الأمنية الدولية وحدها لتجاوز العقبات التي يفرضها التحقيق الجنائي في الجرائم الالكترونية، بل لا بد منّ

[1]

[2] طرحت الجزائر لأول مرة فكرة إنشاء منظمة الأفريبول بمناسبة الندوة الجهوية الإفريقية ال22 للأنتربول التي احتضنتها في شهر سبتمبر 2013 ،و تم دعم الفكرة على هامش الجمعية العامة ال 82 للمنظمة الدولية للشرطة الجنائية "الأنتربول" التي انعقدت في أكتوبر 2013 علانِ في كولومبيا، قبل أن يتم اعتماد الفكرة من خلال تبني الوثيقة المبدئية وا الجزائر خلال الندوة الإفريقية للمديرين والمفتشين العامين الأفارقة للشرطة المنعقدة في فب ارير 2014 بالجزائر العاصمة ثم تبنيها رسميا خلال القمة الـ 23 للاتحاد الإفريقي في غينيا الاستوائية في جوان .2014

مصاحبتها بالمساعدة الفنية وتبادل الخبرات والمعارف بين الدول. لان سلطات الأمن وأجهزة العدالة الجنائية ليست بذات الجاهزية والكفاءة لمواجهة الجريمة الالكترونية في جميع الدول، إنما تختلف من دولة إلى أخرى بحسب درجة تقدمها و رقيها.

الفرع الثاني: تشجيع المساعدة القضائية الدولية

يقصد بالمساعدة القضائية الدولية، كل إجراء قضائي تقوم به دولة من شأنه تسهيل عملية المتابعة والمحاكمة الجزائية في دولة أخرى بخصوص جريمة من الجرائم . انطلاقا من هذا التعريف تظهر الحاجة الملحة إلى المساعدة القضائية الدولية في عملية مكافحة[1]

لإجرام العابر للحدود بصفة عامة والجريمة الالكترونية على وجه الخصوص، بسبب ما تثيره هذه الأخيرة من صعوبات في تحديد هوية المجرم الالكتروني، صعوبات إثباتها وملاحقة مرتكبها، في ظل عالميتها و تشتت عناصرها بين الدول، وكذا المشكلات المتعلقة بكيفية استيراد البيانات التي تم تخزينها عن بعد في حالة اعتبارها دليل إثبات، حيث لا توجد قاعدة عامة لحل هذه المشكلات دون تعاون أو مساعدة قضائية

: تثمين الإجراءات التقليدية للتعاون القضائي الدولي: وتتضمن مختلف صور حد سواء، وقد كرستها الاتفاقية الأوروبية في المادة 23 حينما أوصت الدول الأطراف على تطبيق الاتفاقات الدولية حول التعاون الدولي في المسائل الجريمة ذات الصلة، ويمكن تلخيص هذه الإجراءات فيما يلي

تبادل المعلومات: يعتبر هذا الاجراء من وسائل التعاون الدولي على المستوى الإجرائي الجنائي، التي تسمح بالاتصال المباشر بين الأجهزة القضائية والأمنية في

[1] -يوسف حسن يوسف، مرجع سابق، ص .150

الدول المختلفة من أجل تبادل المعلومات المتعلقة بالجريمة والمجرمين. وعادة ما يتحقق هذا الاجراء بتقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية، بمناسبة نظرها في جريمة ما، عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات المتخذة ضدهم والسوابق القضائية الخاصة

نقل الإجراءات : يقصد بهذا الإجراء، قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية على إقليمها بخصوص جريمةتراتكبت في إقليم دولة أخرى ولمصلحة هذه الأخيرة متى ما توافرت شروط معينة، أهمها التجريم المزدوج، وشرعية الإجراءات المطلوب اتخاذها بمنظور قانون دولة المطلوب منها، وأن تكون هذه الإجراءات ضرورية ومهمة لكشف الحقيقة

ـ تبادل الإنابة القضائية الدولية: وهو طلب تتقدم به دولة ما إلى أخرى يتضمن اتخاذ إجراء قضائي من إجراءات الدعوى الجزائية في إقليمها نيابة عنها، ويكون هذا الاجراء ضروري للفصل في قضية معروضة على السلطة القضائية في الدول الطالبة [1]

طلب الحفظ العاجل للمعطيات المخزنة de rapide conservation stockées (données (:

يعتبر هذا الاجراء آلية جديدة للتعاون القضائي الدولي في مجال مكافحة الجرائم المرتكبة عبر وسائل الإعلام والاتصال الالكترونية، والتي استحدثت بموجب المادة 29 من الاتفاقية الأوروبية لعام 2001 لتمكين أي دولة طرف في الاتفاقية المخّز في أجهزة الحاسب الموجودة في أراضي الدولة من المطالبة بحفظ البيانات نة المطلوب منها على وجه السرعة، خلال الفترة اللازمة لتقديم طلب المساعدة المتبادلة بشأنها بغرض القيام بالتفتيش، أو الدخول بأي طريقة مماثلة، وضبط، أو الحصول، أو الكشف عن هذه البيانات

[1] حازم الحارون، الإنابة القضائية الدولية، المجلة الجنائية القومية، العدد الثاني، القاهرة، 1988 ،ص 20.

2ـــــ طلب الكشف العاجل عن البيانات المحفوظة (de rapide divulgations conservées données (:

يعتبر هذا الاجراء مكمل للإجراء الأول (الحفظ السريع للبيانات) نصت عليه المادة 30 من الاتفاقية الأوروبية أعلاه، بحيث تلتزم بموجبه الدولة المطلوب منها حفظ بيانات المرور المتعلقة بأي بث أو اتصال عبر أجهزة الحاسب التابعة لها، والتي تبين لها أن هذا البث أو د خدمات ّ الاتصال انتقل من مور موجود في دولة ثالثة، بان تفصح وتكشف على وجه السرعة إلى الدولة مقدمة الطلب أكبر نسبة ممكن من البيانات المـ ـارة حتى يتسنـ ـى الكشف عن هوية مورد الخدمـ ـ ـات هذا، ومصدر الاتصـ ـال، وكذا المسار الذي تم من خلاله الاتصال

3ـــــ طلب الدخول لغرض التفتيش والضبط والكشف عن البيانات المخزنة ( ): pour pérquisitionner, saisir, divulguer les données تمaccès’L stockersالنص على هذا الاجراء في المادة)31)من الاتفاقية الأوروبية حول الجريمة الالكترونية، التي أجازت لأية دولة طرف أن تطلب من دولة طرف أخرى السماح لها بإجراء التفتيش .

4- - ـ تبادل المساعدة لجمع البيانات في الوقت الحقيقي (la dans entraide ن :(collecte en temps réel de données relative au trafic ّ بى ا فيما سبق أنه عادة ما يستغرق المحققون وقتا كثيرا في تعقب اتصال الكتروني ما قبل الوصول إلى مصدره، وقد يحدث أثناء هذه الفترة إقدام مورد الخدمات على محو بيانات المرور المتعلقة بهذا الاتصال قبل التمكن من حفظها. الأمر الذي يحول دون إمكانية الحصول على هذه البيانات في وقتها الحقيقي [1]

المطلب الثاني الاستعانة بالتدابير الوقاية والحماية الفنية

أثبتت العديد من الدراسات المتخصصة بأن إتباع أسلوب الردع و العقاب الجنائي وحده لا يشكل حلا كافيا لمكافحة الجرائم الالكترونية، فحتى تكون هناك الفعالية في الحركة ّ والأداء لابد أن يعزز هذا الأسلوب بوسائل الوقاية والحماية الفنية التي تعمل على الحيلولة دون وقوع هذه الجرائم، أو الإنذار بها بمجرد وقوعها .وما يهمنا أكثر في هذه التدابير ليس الدور الوقائي الذي تلعبه في منع حدوث الجريمة الالكترونية، إنما كونها وسيلة فعالة تستعين بها سلطات التحقيق للكشف عن هوية المجرم الالكتروني من خلال الاطلاع على المعلومات و البيانات التي يخلفها فيها عن محاولاته لارتكاب الجريمة.

وهو ما يجعلها مخرجا مهما لمعضلتي سهولة اختفاء وتعديل الدليل الالكتروني و صعوبة اقتفاء آثار المجرم الالكتروني ويمكن تقسيم هذه التدابير حسب غرضها المذكور إلى أنظمة الحماية الفنية الكترونية)الفرع الأول)، و وسائل الوقائية الأخرى (الفرع الثاني

[1] -أنظر نص المادتين(33 و 34 (من الاتفاقية الأوروبية حول الجريمة الالكترونية لعام 2001 ،مرجع سابق

الفرع الأول: تقنيات الحماية الفنية مصدرا موثوقا لإثبات الجريمة الإلكترونية

تتحقق هذه العملية بتزويد وسائل الاتصالات الالكترونية منها الحواسيب الآلية ببرمجيات وتطبيقات تكفل الحماية الكافية للمعلومات الالكترونية من خلال التعريف بالمستخدم وموثوقية الاستخدام ومشروعيته، وكذا ضمان سرية المعلومات، تكاملها واستمرارها وسلامة محتواها. وهو ما يرشحها لان تكون مصدر غنيا وموثوقا للأدلة الالكترونية. وتتعدد تقنيات الحماية الفنية المتعين استخدامها في بيئة المعالجة الآلية إلى الحماية عن طريق البرامج (أولا)،

والحماية عن طريق الرقابة الوقائية(ثانيا).

أولا ـــــ الحماية الفنية عن طريق البرامج الأمنية: وهي الحماية التي يتم توفيرها اعتمادا على البرامج الأمنية التالية1 :

ـــ برامج التعريف بالشخص المستخدم وموثوقية الاستخدام ومشروعيته:

وتهدف هذه البرامج إلى ضمان استخدام الجهاز أو النظام أو الشبكة من قبل الشخص المرخص له بهذا الاستخدام فق هذه الطائفة كلمات السرّ ط، وتضم بأشكالها المختلفة، رموز المرور، بطاقات التعريف الذكية، ووسائل التعريف البيومترية التي تعتمد على سمات معينة في الشخص المستخدم متصلة ببنائه المرفولوجية، كبصمة اليد أو الأصبع، أو بصمة العين أو الوجه، بصمة الصوت، البصمة الوراثية، أو متصلة بتصرفاته مثل طريقة التوقيع، طريقة استخدام لوحـ ـ ـة المفاتيح، طريـ ـقة التنفس. كمـ ـ ـا تضم أيضـ ـا مفـ ـاتيح التشفير، ومـ ـ ـا يعرف بالأقفـ ـال الالكترونية التي تحدد دخولها لأشخاص بذاتهم[1]

[1] أشرف السعيد احمد، تكنولوجيا المعلومات في المجال الأمني، مطابع الشرطة، القاهرة، 2013 ،ص .69.

برامج التحكم في النفاذ إلى الشبكة: تهتم هذه البرامج أساسا بالحماية ضد الدخول غير المشروع إلى مصادر الأنظمة والاتصالات والمعلومات، وكذا التأكد من أن الشبكة قد استخدمت بطريقة مشروع

3ـــ برامج الحفاظ على سرية المعلومات: الغرض منها ضمان عدم إفشاء المعلومات للجهات غير المصرح لها بذلك، وتشمل تقنيات تشفير المعطيات والملفات، إجراءات حماية نسخ الحفظ الاحتياطية، ومختلف برامج التمحيص و الغربلة4 (filtration.) ـــ

برامج حماية التكاملية وسلامة المحتوى: يكمن دور هذه البرامج في حماية محتوى المعطيات أو البيانات الالكترونية من مخاطر العبث بالتعديل أو الإتلاف أو الإلغاء من قبل جهة غير مخول لها بذلك، بعد الاطلاع عليها أو أثنـاء عملية إدخالها أو نقلها.

5ـــ برامج منع إنكار التصرف: مهمة هذه البرامج هو تأكيد انتساب تصرف ما على الوسائل الالكترونية إلى مصدره الحقيقي، و ضمان عدم قدرة شخص المستخدم من إنكار التصرف الذي صدر عنه، أو إنكار بأنه هو مصدر هذا التصرف. وتكمن هذه البرامج في تقنيات التوقيع الالكتروني، و شهادات التوثيق الصادرة عن الطرف الثالث[1]

برامج مراقبة الاستخدام وتتبع سجلات النفاذ والأداء: وتتمثل في مختلف التقنيات التي تستخدم ل مراقبة العمليات الالكترونية الجارية على نظام حاسب معين، وتحديد مصدرها والوقت والمدة التي استغرقتها، وتسجيل كل ذلك في ملفات خاصة يطلق عليها (Logs). ومن ضمن هذه البرامج نذكر[2]

[1] أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، بدون دار النشر، القاهرة ، 2005، ص.ص152-151

[2] - 728حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، مرجع سابق، ص.ص 1817 -

أ-برنامج : tracer( ) وهو برنامج يتولى تقديم تقارير مفصلة حول المسار الذي سلكه مستخدم شبكة الانترنت من خلال تحديد موقع الولوج و عنوانه الشخصي IP(، (المواقع والصفحات التي اطلع عليها، الوقت والفترة التي قضاها في كل صفحة أو موقع، ومختلف العماليات التي أجراها وتحديد نوعها

ب-برنامج : stat net( ) وهو برنامج مناط به عرض جميع الاتصالات التي أجراها المستخدم، ومنافذ التصنت، وعرض المنافذ والعناوين بصورة رقمية، و تقديم تقرير كامل لجدول التوجه

-برنامج كشف الاختراق) : IDS) يتولى مراقبة العمليات التي يجرى حدوثها على أجهزة الحاسب أو شبكة الانترنت و تحليلها بحثا عن أية إشارة قد تنبئ بوجود خطر قد يهدد أمن الحاسب أو الشبكة. وفي حالة اكتشاف النظام وجود هذا التهديد يقوم برصد كل البيانات المتعلقة به، مصدره، طبيعته، ودرجة خطورته، من ثم إنذار صاحب النظام فورا بهذا التهديد[1]

الفرع الثاني: التوعية و التحسيس

لقد سبق البيان أنه من ضمن العقبات التي تعتري عملية البحث والتحقيق في الجرائم الالكترونية، تقاعس المجني عليه عن الإبلاغ بوقوع الجريمة، ما قد يستغرق اكتشافها من قبل سلطات الضبط القضائي وقتا كبير، قد يحول دون الوصول إلى الأدلة والقرائن في الوقت المناسب أو عدم الوصول إليها إطلاقا، بسبب إمكانية محوها أو التخلص منها بسهولة في الفترة بين حدوث الجريمة واكتشافها.

ن أجل التصدي لهذه العقبة اتخذت عدة مبادرات جريئة منها، إقرار قاعدة تجريم عدم الإبلاغ عن الجريمة، وذلك من خلال وضع نصوص عقابية تعتبر الشخص الذي يعلم بوقوع جريمة الكترونية ويتماطل في تبليغ سلطات الأمن عنها، شريكا

[1] -أشرف السعيد أحمد، مرجع سابق، ص 78.

فيها يستوجب معاقبته .ولكن رغم اشتقاق هذا الحل من المنطق ذاته الذي تقوم عليه جريمة "عدم مساعدة شخص في حالة خطر"، إلا لّ انه لم يفع ، وسرعان ما استبدل بقاعدة أخرى تعرف بالالتزام برفع و(، L'obligation de porter plainte)شكوىّ هذه القاعدة و إن تم فعلا العمل بها في بعض الولايات الأمريكية كجيورجيا و آوتاه، إلا أنها لقيت رفضا كبير من غالبية دول العالم بحجة تناقضها مع منطق التجريم و العقاب،

إذ لا يعقل معاقبة الضحية فقط لمجرد عدم انصياعه للقانون الذي يقضي بواجب التبليغ، في حين يترك المجرم الحقيقي حرا طليق . 735أمام هذا الوضع، لم تجد الدول حلا أخر لمشكلة الإعراض عن التبليغ بالجريمة الالكترونية إلا اللجوء إلى سياسة التحريض على التبليغ dénonciation)(la a incitation'L) ، وذلك عن طريق وضع تحت تصرف مستخدمين الانترنت آليات سهلة ومجانية تشجع المتضررين من جريمة على التبليغ عنها إلى سلطات الأمن، كإنشاء ما يسمى بخطوط اتصال خضراء أو الأرقام الساخنة [1]

، وهي قنوات مرتبطة مباشرة بمصالح الأمن، تسمح لأي شخص الاتصال من أي مكان وفي كل وقت وحين وبدون أن يكشف عن هويته، للإبلاغ عن وقوع جريمة الكترونية ما. أو خلق لدى مراكز الأمن بوابات أو أنظمة الكترونية تعمل 24)سا 24 /سا) مخصص لاستقبال شكاوى أولية عبر الانترنت)plainte (Pré- ، كما فعلت المملكة السعودية بإنشائها نظام استقبال الشكاوي الالكترونية 737 "أبشر"، والجزائر باستحداثها مؤخرا موقع للشكاوى الأولية لدى مصالح الدرك الوطني يسمي (DZ.MDN.PPGN(.ومن أجل تفعيل وتعزيز هذه الآلية قامت بعض شركات التامين

[1] نذكر منها الرقم الساخن في مصر وهو)108 ،)الرقم)1909)في المملكة السعودية، الرقم الأخضر للشرطة 736 (1548(في الجزائر

في بعض الدول بإدراج شرط رفع شكوى ضمن بنود عقد التأمين الالكتروني الذي يؤدي تخلفه إلى فقدان الحق في التعويض

ومع ذلك، فقد كشفت الدراسة الاستقصائية التي أجرها مؤخرا فريق خبراء حول الجريمة السبيرانية والتدابير التي تتخذها الدول والمجتمع الدولي والقطاع الخاص للتصدي لها ، بأن أحسن وسيلة للقضاء على مشكلة العزوف عن التبليغ بالجريمة الالكترونية بل لمنع وتفادي وقوعها هي التوعية والتحسيس، وذلك من خلال تنظيم حملات زيادة الوعي العام تشمل كل شرائح المجتمع، والمؤسسات والإدارات العمومية، بما فيها حملات التوعية بالتهديدات والمخاطر الناشئة عن هذا النمط الإجرامي، وعن سياسات و ّ ممارسات تدبر هذه المخاطر والوقاية منها. وكذا تحسيسهم بأن مهمة الإفصاح عن الجريمة الالكترونية ومكافحتها هي مسؤولية مشتركة وتستلزم تضافر جهود الجميع دون استثناء.

الخاتمة

الخاتمة

مع التطور التكنولوجي والعلمي في عصرنا الحديث، أصبحت حياة الإنسان سهلة بكثير مما سبق وذلك بفضل التقنيات الحديثة كالكمبيوتر والانترنت ، الذين أصبحا ركيزة أساسية تقوم عليها جل المعاملات، سواء الاقتصادية، الاجتماعية، السياسية وغيرها، إلا انه صاحب هذا التطور تطورا في الجريمة، التي اختلفت الآراء حول تسميتها فهناك من أطلق عليها اسم " الجريمة المعلوماتية " وآخرون أطلقوا عليها " جرائم الحاسب الآلي والانترنت " وهناك من اكتفى بتسميتها " جرائم الحاسب الآلي " أو " جرائم الانترنت "، كما أطلق عليها اسم " الجريمة الالكترونية "، وكل هذه التسميات وغيرها تطلق على جريمة واحدة تتحقق عندما يساء استخدام التقنيات الحديثة ، وقد صاحب الاختلاف في التسمية اختلاف في التعريف بالجريمة فهناك من ضيق من مفهوم الجريمة الالكترونية، وهناك من وسع في مفهومها، وهناك من عرف الجريمة الالكترونية بالنظر إلى موضوعها وآخرون ربطوا مفهوم الجريمة الالكترونية بمدى معرفة الجاني لتقنية النظام المعلوماتي والحاسب الآلي، فالجريمة الالكترونية بحسبهم لا يرتكبها إلا شخص له دراية ومعرفة بمجال التقنية الحديثة مما يسمح له بالتلاعب بالنظم المعلوماتية

.وقد تمحورت نتائج البحث في الآتي:

- 1 الجريمة الإلكترونية هي الأفعال المخالفة للقانون التي ترتكب بواسطة الكمبيوتر من خلال شبكة الانترنت .

- 2مرتكب الجريمة الإلكترونية يتميز عن المجرم العادي بمجموعة من الصفات، منها انه اجتماعي وذكي، يتمتع بالخبرة في مجال التقنية الحديثة، بالإضافة إلى انه غير عنيف، فهذا النوع من الإجرام لا يتطلب القوة والعنف.

- 3 تختلف دوافعراتكاب الجريمة الإلكترونية من شخص لأخر، فقد تكون دوافع شخصية هدفها تحقيق مصلحة خاصة، وقد تكون خارجية بهدف الانتقام مثلا .

- 4الجريمة الإلكترونية كغيرها من الجرائم التقليدية تتميز بالخطورة لكونها تمس الإنسان والمؤسسات وتتعدى حتى لان تكون خطر على امن الدولة واستقرارها، وكذلك هي من الجرائم العابرة للحدود لارتباطها بشبكة الانترنت، كما تتميز الجريمة الالكترونية بكونها تعتمد على التقنيات الحديثة، وصعوبة اكتشافها وإثباتها.

- 5 يواجه المحقق للكشف عن الجريمة الإلكترونية والقبض على مرتكبيها ونسبتها إليهم عدة معوقات، أهمها معوقات تشريعية تكمن في عدم حصر لكل صور الجريمة الإلكترونية في القوانين الجنائية.

- 6 الشاهد في الجريمة الإلكترونية شخص فني، صاحب خبرة وتخصص في مجال التقنية الحديثة وعلوم الحاسوب، كمشغلوا الحاسب الآلي وخبراء البرمجة.

7-المعاينة في الجريمة الإلكترونية اقل أهمية منها في الجرائم العادية، لقلة الآثار المادية بينما الخبرة تعتبر من أهم إجراءات التحقيق في الجرائم الالكترونية وهذا ما تستدعيه طبيعة هذه الجريمة، كونها تعتمد بالدرجة الأولى على وسائل مستحدثة

الخاتمة

الإقتراحات

•رغم أن عقوبة الإعدام تم نص عليها من هذا القانون لكن لم نسمع بتنفذيها لذلك .

•يجب أن تنفذ هذه العقوبة لردع المجرمين .

•ندعوا أن مشرع إلى التنسيق بين المواد وتفادي التكرار .

•لسلامة الأطفال في المدارس يجب وضع عند كل مؤسسة رجال شرطة لتفقد المكان عند خروج التلاميذ من المدارس .

•يجب أن يكون هناك رقابة على الطفل في المدرسة وخارجها .

•إعطاء الإهتمام الكافي لدور المجتمع المدني الذي من شأنه تسيير نظام العام فالمجتمع المدني الذي له دور لتسير النظام العام ومجتمع متحضر .

•على الإعلام ان يكون تحت يد ممثلين من السلطة ممتهنين لهذه الحرفة لأن الإعلام يجب أن يكون دوره يخدم المصلحة العامة فقط لا يعرقل التحقيق.

الخاتمة

في ضوء النتائج السابقة التي أظهرتها الدراسة تخلص إلى بعض التوصيات والإقتراحات تتمثل في :

- ضرورة إعطاء تعريف موحد للجريمة الإلكترونية يشمل فيه كل سلوكات المجرمة.
- ضرورة تدريب وتأهيل أفراد الضبطية القضائية وكذا النيابة العامة على كيفية التعامل مع هذا النوع من الجرائم وتحيقي التعاون مع التقنيين من أصحاب الخبرة.
- وضع إجراءات كالتحقيق والمحاكمة للجريمة الإلكترونية تختلف عن الجريمة التقليدية.
- توعية المجتمع وخلق له ثقافة إجتماعية جديدة عن هذه الجرائم بأنها أعمال غير مشروعة ويتعرض صاحبها لعقوبات جزائية.
- تدريس مواد الأنظمة المعلوماتية والجرائم التي قد تنشأ منها المدارس بشكل مبسط في الكليات الحقوق والمعاهد القضائية.

قائمة المصادر و

المراجع

قائمة المصادر و المراجع:

الكتب:

1. أشرف السعيد احمد، تكنولوجيا المعلومات في المجال الأمني، مطابع الشرطة، القاهرة، 2013 .
2. آمال بن صوليح، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني وفي الجزائر، مداخلة الملتقي الدولي حول " الإجرام اليبيرالي المفاهيم والتحديات ، " 12 -11 أفريل 2017.
3. أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الج ارئم المعلوماتية، بدون دار النشر، القاهرة ، 2005.
4. بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، 2014 ،
5. بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، دراسة مقارنة، 2016 .
6. بن سولة نور الدين، الجرائم الالكترونية في ضوء التشريع الجزائري، المجلد التاسع، العدد 1 ،مارس 2018 .
7. بوظياف إسماهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، العدد 11 ،سبتمبر 2018
8. جميل عبد الباقي صغير أدلة الإثبات الجنائي والتكنولوجي الحديثة، دار النهضة العربية، القاهرة، 2002 .
9. حازم الحارون، الإنابة القضائية الدولية، المجلة الجنائية القومية، العدد الثاني، القاهرة، 1988 .
10. حسن الجوخندار، التحقيق الابتدائي في قانون الأصول المحاكمات الجزائية، دار الثقافة عمان، الطبعة الأولى، 2008 .
11. حسين سعيد بن سيف الغافري، الجهود الدولية، في مواجهة جرائم الأنترنت، ورقة مقدمة للاتحاد العربي للتحكيم الإلكتروني، 2007 .
12. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، 2009 .
13. خالد ممدوح، أمن الجريمة الإلكترونية، الدار الجامعية، الإلكترونية، الإسكندرية، 2008.
14. ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، جامعة باتنة، 2015 - 2016
15. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، 2013 .

16. سميرة معاشي، ماهية الجريمة الإلكترونية، مجلة المنتدى القانوني، العدد السابع، جامعة، بسكرة،
17. صغير يوسف، الجريمة الإلكترونية، عبر الانترنت، تيزي وزوو، 2013 .
18. ضياء مصطفى عثمان، السرقة الإلكترونية، دار النفائس، عمان، الطبعة الأولى، 2011.
19. عبد الله حسين محمود، إجراءات جمع الأدلة في الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، 2003 .
20. عبد الفتاح البيومي حجازي، مكافحة جرائم الأنترنت، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2006.
21. محمد الأمني البشري و محسن عبد الحميد محسن، معايير الأمم المتحدة في مجال العدالة الجنائية و منع الجريمة، أكاديمية نايف للعلوم الأمنية، رياض، 1998
22. محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إيليزا للبحوث والدراسات، العدد الثاني، ديسمبر 2017 ،المركز الجامعي إليزي، الجزائر.
23. محمد أمنية الشوايكة جرائم الحاسوب والأنترنت (الجريمة المعلوماتية)، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2009 ، 8.ص
24. محمد طارق عبد الرؤو ف، جريمة الإحتيال عبر الإنترنت الأحكام الموضوعية والأحكام الإجرائية، منشورات الحلبي الحقوقية، الطبعة الأولى، 2011 .
25. محمد مصطفى موسى، التحقيق في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، 2009.
26. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنيت،دار الفكر الجامعي الإسكندرية، 1 .،2007ط1 .
27. نواوي سليمة، دور الدرك الوطني في محاربة الجريمة الالكترونية، جامعة مسيلة، 2019/2018 .
28. هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، 2012 .
29. يوسف جفال، التحقيق في الجريمة الإلكترونية، 2017/2016 .
30. يوسف خليل يوسف العطيفي، الجرائم الإلكترونية في التشريع الفلسطيني، غزة، 2013.

المجلات:

1. بوظياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11 سبتمبر 2018.

2. سعيدة بوزنون، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، المجلد ب، عدد 52 ديسمبر ، 2019.
3. شام محمد فريد رستم« الجـرائم المعلوماتية أصول التحقيق الجنائي الفني و آلية التدريب التخصصي للمحققين » مجـ ـلة الأمـ ــن و القانون، عدد 02، صادر عن كلية شرطة دبي، 1999.
4. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي، دار الكتب القانونية المجلة الكبرى، الطبعة الأولى.
5. كريمة علة، الجهات القضائية الجزائية ذات الاختصاص الموسع، المجلة الأكاديمية للبحث القانوني، المجلد 11 عدد 117 .

المذكرات و الرسائل:

1. بوكر رشيدة، ج ارئم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، منشو ارت الحلبي الحقوقية، بيروت، 2012 .
2. السبيل الوحيد، بحث مقدم إلى الندوة الإقليمية حول " الج ارئم المتصلة بالكمبيوتر"، المنعقدة بالرباط في 19 و 20 جويليةإيهاب ماهر السنباطي، الج ارئم الإلكترونية(الج ارئم السيبيرية :) قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو .28ص،7 200
3. صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانـون، فرع القانون الدولي للأعمال، كلية الحقوق و العلوم السياسية، جامعة مولـود معمري بتيزي وزو، .2013 .
4. عمر بن إبراهيم بن حماد العمر، إجراءات الشهادة في مرحلة الاستدلال والتحقيق الابتدائي في ضوء نظام الإجراءات السعودي، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمينة، 2007 .
5. غازي عبد الرحمن هيان الرشيد، الحماية القانــونية من ج ارئم المعلوماتية، رسـ ـ ـ ـالة لنيل درجة دكتــو اره في القانون، كلية الحقوق، الجامعة الإسلامية ، بيروت، 2004 شام محمد فريد رستم، الجـ ـوانب الإج ارئـية للجرائم المعلوماتية-د ارسة مقارنة، مكتبة الآلات الحديثة، القاهرة ، .1994ص246
6. فايز محمد ارجح غلاب، الجرائـم المعلومــاتية في القانون الجزائري و اليمني، رسالة لنيل درجة الدكتــو اره في القانون، فرع القانون الجنائي و العلوم الجنائية، كلية الحقوق، جامعة الجزائر)1. ،)2011.
7. فشار عطاء الله "مواجهة الجريمة المعلوماتية في التشريع الجزائري " بحث مقدم إلى الملتقى المغاربى حول القانون 553 والمعلوماتية المنعقد بأكاديمية الد ارسات العليا، ليبيا، أكتوبر 2009 .
8. محمد نصير السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

قائمة المصادر و المراجع

مراجع باللغة الأجنبية:

-CHOPIN- Frédérique, Les politiques publiques de lutte contre la cybercriminalité, AJ Pénal, Paris, 2009

1 BOUDER Hadjira « protection des systèmes d'informations : aspects juridiques » centre de recherche sur l'information scientifique et technique, Alger, 2012, p 32

1 BRIAT Martin. La Fraude Informatique: Une approche de droit compare, Revue D.P.C, N04 Paris, Avril 1985, p 191

1 voir : la recommandation n R (89) 9 sur la criminalité informatique, comité européen pour les problèmes de droit procédural liés a la criminalité informatique, conseil de l'Europe, Strasbourg, 1990, p 80. Et sa recommandation n R (95) 13, op.cit.

المواقع الإلكترونية

الموسوعة العربية الالكتونية على الرابط :
http://droit7.blogspot.com/2019/09/blog-post_15.html#

http.//www.ccd.gov.eg

2 http://www.pointdecontact.net

-FALQUE Pierrotin, la gouvernance du monde en réseau, in gouvernance de la société de l'information, cahier du C.R.I.D. n 22, Bruxelles, Bruylant, 2002, P 109

http://www.interpol.int/public/icpo/default.asp

- http://www.web-police.org.

فهرس المحتويات

قائمة المصادر و المراجع