



وزارة التعليم العالي والبحث العلمي
جامعة 20 أوت 1955 سكيكدة
كلية الحقوق والعلوم السياسية
قسم الحقوق



البحث والتحري عن الجريمة الالكترونية

مذكرة مكملة لنيل شهادة الماستر في القانون الخاص
تخصص قانون جنائي

إشراف الأستاذة:

بوغاغة ياسمينة

إعداد الطالب:

رفعي سمير

لجنة المناقشة:

رئيسا	الدكتور: يونس بدر الدين
مشرفا ومقررا	الأستاذة: بوغاغة ياسمينة
مناقشا	الأستاذة: بوعزيز شهرزاد

دورة جوان 2017

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

إهداء:

إلى من كانت دعواها دوما تنير لي عقلي و دربي
إلى من أفاضت علي برعايتها الوالدة الدافئة التي أتاحت لي
فرصة

الدراسة و البحث

إلى التي تعجز الكلمات عن وصفها مهما سال من سواد الحبر

على بياض الورق

إلى حبيبتي أمي

إلى أبي الكريم

إلى أختي و أخي

إلى الأزهار النرجسية التي تزين حقل العائلة هديل و أنيس و زكريا

إلى كل أقاربي

إلى كل أصدقائي و صديقاتي

إلى أساتذتي الكرام على طول مساري الدراسي

إلى كل هؤلاء أهديهم ثمرة هذا الجهد الطيب المبارك الذي أحسبته

عند الله عز وجل في صحيفة حسناتي و أتمنى أن يكون من العلم

الذي ينتفع به و نرجو من الله القبول.





قال تعالى: " لئن شكرتم لأزيدنكم " .

(إبراهيم_7)

عن أبي هريرة رضي الله عنه أن النبي صلى الله عليه وسلم قال:

" لا يشكر الله من لا يشكر الناس "

(صححه الألباني)

إن من فضل الله علينا ومنته وكرمه أن هدانا إلى سبيل الخير والرشاد وأن يسر لنا طرق لاكتساب من العلم، فله الحمد والشكر. كما أنه من الواجب أن أتقدم بخالص عبارات الشكر والتقدير وعظيم والعرفان للأستاذة الفاضلة/ ياسمينه بوغاغة، التي تكرمت وتفضلت مشكورة بالإشراف على هذه الرسالة، وأعطتني من وقتها وعلمها ما لا يقيم ولا يحصى.

كما أتقدم بالشكر الجزيل لكل من الأستاذة الكرام: الأستاذ يونس بدر الدين والأستاذة بوعزيز شهرزاد أعضاء لجنة المناقشة على وقتهم الثمين في تصويت هذه العمل.

كما لا يفوتني الثناء على إدارة جامعة 20 أوت 1955 وعلى رأسهم أساتذة القانون الجنائي، فجزاهم الله عنا خير الجزاء في الدنيا والآخرة.

مقدمة

أولاً: التعريف بالموضوع:

إن الحديث عن تطور تكنولوجي بالمفهوم التقليدي أصبح من الأمور التي عفى عنها الزمن فنحن اليوم في عصر أصبحت التكنولوجيا تتفوق حتى على طموحات الانسان العادي فسبقا مثلا كان كل الناس يحملون في الطيران او الاتصال بالصوت والصورة مع أشخاص في أقاصي الأرض وهذا ما تحقق لكن نشهد الان فترة تسبق فيها الاختراعات والابتكارات التكنولوجية حتى طموحات الأفراد فأصبح من الضروري البحث في مجال الفضاء الإلكتروني بوصفه بعدا جديدا للصراع وللجرائم، هذا من جهة ومن جهة اخرى فان تقنيات المعلوماتية استوطنت الدائرة والمؤسسة الحكومية حيث جميعها على اتصال بهذه التقنية على مستوى جميع الأعمال والخدمات حتى امتد ذلك وشمل الأفراد في أغلب شئون حياتهم، فشكلت ما يعرف بالمجتمع الافتراضي أو المجتمع الرقمي.

إن مسابرة النصوص القانونية للواقع فرض عليهم تغيير مفاهيم النظرية التقليدية للجريمة، فقد أدخلت الجريمة الالكترونية على هذه الأخيرة صورا جديدة للجريمة بركانها الشرعي وأساليب وطرق حديثة لم تكن معروفة من قبل مست الجريمة من خلال ركنها المادي فالجرائم المعلوماتية جرائم ناعمة، لا تستوجب لتحقيقها وسائلاً وجهداً ماديا كبيرا.

هذا ما يسمح للمجرمين بالتحكم في آثار وأدلة جرائمهم من خلال تدميرها ومحوها وهو ما يجعل من امر أغلب الجرائم الالكترونية خفية لا يمكن اكتشافها أو تتبع آثارها بالنظر إلى الطبيعة الخاصة للأدلة الناتجة عن هذا النوع من الجرائم، والتي أصبحت تشكل التحدي الأكبر الذي يواجه النصوص الجزائية الإجرائية.

فالجريمة الالكترونية تشكل نقطة تعارض بين التكنولوجيا الحديثة وجملة النصوص القانونية الإجرائية، فهذه الأخيرة وضعت لمجابهة الجرائم التقليدية ذات الطابع المادي والتي تخلف ورائها أثارا مادية محسوسة، ولم تتناول في صلب نصوصها الجرائم المستحدث وعلى رأسها التكنولوجية، هذه الأخيرة التي لا ينفك معدل انتشارها عن الارتفاع و تتزايد يوما بعد يوم وذلك بفعل عجز السلطات المختصة بتنفيذ القانون عن

مجابتها بسبب عدم ملائمة النصوص الإجرائية لطبيعتها الخاصة فالنصوص الخاصة بالبحث و التحري في مجال الجرائم التقليدية لا يصلح للتطبيق في مجال الجرائم الالكترونية.

وقد سعينا في هذه الدراسة إلى تلمس طبيعة الجرائم الإلكترونية التي لا تبدو في كثير من الحالات غامضة ومعقدة فحسب، بل تمثل تحدياً هائلاً يستدعي سرعة التأهب نحو نقلة علمية وتقنية دائبة تحققها بالذات مجالات الشرطة والقضاء والنيابة، مع إبراز طبيعة هذه الجرائم التي تشكل أهم جرائم هذا العصر وأعقدها خاصة في المجالات الأمنية لحماية المواقع الالكترونية والبيانات الشخصية مع إبراز بعض الجهود الوقائية الوطنية و الدولية.

ثانياً: أهمية البحث وأسباب إختياره:

ويعد موضوع البحث من الموضوعات الجديدة والمهمة في إطار القسم الإجرائي من القانون الجزائي وهو من الموضوعات التي لا تزال حديثة و لم تتل حظها من البحث على مستوى الفقه خاصة الجزائري منه، وحتى المتوفر منها لم يتعدى التعريفات والإشارة لهذه النوع من الجرائم كأحد أنواع الجرائم المستحدثة وفق قانون العقوبات.

وإذا كانت الجرائم الإلكترونية تعد من الأنماط الإجرامية التي جاءت بها ثورة تقنية المعلومات، حيث تعتبر من المستجدات التي لم تكن معروفة للقانون الجزائي، فمن دون شك أن أي محاولة للتعامل إجرائياً مع هذا النمط الإجرامي في إطار عملية البحث سوف يخلق إشكالات إجرائية للأجهزة المكلفة المتعلقة بهذه العملية.

ومن هنا تأتي أهمية موضوع البحث الذي حاولت من خلاله مناقشة المفاهيم القانونية المتعلقة بالجرائم الالكترونية، وربطها بالمفاهيم القانونية المتعلقة بإجراءات البحث والتحري في الجريمة على العموم، ووضع التصورات المتعلقة بالجوانب الإجرائية في إطار التعامل مع الجريمة المعلوماتية في ظل النصوص التشريعية الحالية في القانون الجزائري .

يستمد موضوع البحث أهميته من عدة جوانب تبرر أسباب اختياره تظهر من خلال:

1- التزايد المستمر و الرهيب لهذا النوع من الجرائم وتزايد درجة خطورة هذا النشاط وارتفاع مستوى التهديدات التي يشكلها على الأمن العام، في ظل الاعتماد المطلق على تكنولوجيا المعلومات في المجتمعات المعاصرة، يقابله عجز سلطات البحث و التحري عن رسم نموذج موحد لهذه الجرائم والاستقرار على جملة من الإجراءات الخاصة بمتابعتها نظرا لتطورها الدائم والمستمر، مما ينتج عنه أحيانا غياب أو جمود النص الإجرائي و عجزه عن تفعيل الإجراءات بسبب عدم ملاءمته للجريمة محل البحث والتحقيق.

2- المكانة التي يحصى بها موضوع إجراءات البحث و التحري بشأن الجرائم الإلكترونية من بين اهم المواضيع المطروحة للنقاش على النطاق الدولي والوطني، فهي تشغل باستمرار حيزا مهما من جهود الباحثين وكذلك الفقه والتشريع لأجل وضع إستراتيجيات قانونية وعملية آنية ومستقبلية، تضمن عدم فقدان السيطرة على تقنية المعلوماتية.

3- الرغبة في معرفة مدى تطور الاليات القانونية التي سنتها الدولة لمجابهة هذا الخطر الداهم، و على رأسها التشريع الخاص الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

4- تحديد القواعد الإجرائية الخاصة التي تسمح بمتابعة هذا النوع من الجرائم ومرتكبيها بشكل يضمن شرعية الإجراءات المتخذة، بهدف ردع هذه الفئة من المجرمين التي دأبت على تبني منطق الإفلات من العقاب.

5- قد تتوفر ترسانة قانونية مناسبة لكن غياب الوسائل المادية الضرورية للبحث والتحري، وقد يحدث أن يتوفرا معا ولكن تغيب المهارة والمعرفة الفنية لدى المحققين المكلفين بهذه العملية هذا كله يثير اشكالا في مدى دقة وسرعة هذه العملية مع الأخذ في عين الاعتبار ميزات هذا النوع من الجرائم.

ثالثا : صعوبات البحث:

إن مثل هذه المواضيع ذات الطابع العملي الدقيق تثير دائما مجموعة من اشكالات الدراسة ويأتي على رأسها تمكن الكتاب في المجال القانوني من استيعاب جزء من علم آخر هو بعيد عليهم في الأصل فنجد أن أغلب الدراسات الموجودة تركز على الشق الموضوعي من باب السلوكيات والعقوبات مع اغفال الجانب الاجرائي تهربا من الطابع الفني للموضوع.

كما تجدر الاشارة إلى أن هذا الموضوع ورغم توفر عدد معتبر من مراجعه إلا أن أغلبها قادمة لنا من الشرق الأوسط مثل مصر في نهاية التسعينات والإمارات العربية المتحدة منذ بداية الالفية الجديدة الى اليوم مع وجود فراغ هائل بالنسبة للمؤلفات الجزائرية التي تعنتي بهذا الموضوع ويرجع هذا في رأينا إلى تأخر المشرع كذلك في سن قوانين واضحة في هذا الشأن.

صعوبة التواصل مع الجهات الأمنية والقضائية التي تختص بمتابعة أعمال البحث والتحقيق في الجرائم الإلكترونية، والتعقيدات الاجرائية المتبعة من أجل مد الباحثين بمعلومات حول موضوع معين مما تسبب في خلو العديد من الدراسات من الإحصائيات الضرورية الخاصة بواقع الحال على المستوى الوطني، إلا أنه و في هذا البحث حاولنا الاستعانة بالإحصائيات المتوفرة عبر المواقع الرسمية للسلطات الأمنية أو عن طريق المداخلات والندوات التي تقدمها هذه السلطات.

رابعاً: إشكالية الموضوع:

ان تطور تقنيات المعلومات الذي سهل للكثير من ذوي الحيلة عملية استغلاله ابشع استغلال عن طريق ارتكاب مجموعة من الجرائم التي تمس بخصوصية وأسرار الغير فنمو هذا النوع الاجرامي المتميز واكبه تطورفي الشق القانوني، فظهرت آليات وإجراءات قانونية جديدة في مجال البحث والتحقيق عن هذا النوع من الجرائم، غير أن تطور كلا المجالين لا يسري بنفس الوتيرة، فالجرائم الإلكترونية تتطور بشكل سريع ومذهل يمكن القول انها تتطور بوتيرة مرتفعة يوميا، فيما تعرف النصوص القانونية وتيرة بطيئة من

حيث مواكبتها للجريمة الإلكترونية، مما يخلق دوما فجوة بين الجريمة والنص القانوني مما يتسبب في تعطيل تعطيل مرفق العدالة في هذا الشأن.

فواقع الحال يظهر نمو متزايد في عدد هذه النوع الجرائم مما يدل على عجز في مجال معين هذا ما دفعنا في سبيل التعرف على حيثيات الموضوع أن نضع إشكالية متناسبة وموضوع البحث وهي الإشكالية التي يمكن صياغتها في الشكل التالي:

ما مدى فعالية الآليات والأساليب المنتهجة في تطوير عملية البحث والتحري في مجال الجرائم الإلكترونية؟

وتتدرج تحت هذه الإشكالية الرئيسية تساؤلات فرعية :

1. ما المقصود بالجريمة الالكترونية والعوامل المتحكمة فيها؟
2. ما هي الخطط والوسائل المادية والقانونية المسخرة للقضاء على هذه الجريمة ومعوقاتها؟

خامساً: مناهج البحث وخطة الدراسة:

وقد تطلب منا هذا البحث اعتماد المنهج الوصفي بالإضافة إلى المنهج التحليلي نلجأ إليه كلما استوجب منا البحث ذلك.

فالمنهج الوصفي يظهر من خلال وصف ظاهرة الجريمة الإلكترونية وتحديد بعض المفاهيم التي تقوم عليها، وكذلك وصف المفاهيم الخاصة بالإجراءات المستعملة في استخلاص الدليل والصعوبات التي تواجهها هذه العملية.

في حين المنهج التحليلي يظهر في هذا البحث من خلال تحليل بعض المفاهيم والغوص في جزئياتها وطرحها بشكل من التفصيل والتشريح لما بدا لنا من أهميتها، مثلما كان الحال لإجراء التفتيش في مجال الجرائم الالكترونية بالإضافة الى تحليل نصوص مواد قانونية أو أرقام إحصائية.

بالاعتماد على المناهج المذكورة و بإتباع خطة ثنائية سنحاول الإجابة من خلال أطوار البحث على كل التساؤلات المطروحة مسبقا و على هذا الاساس:

الفصل الأول: الإطار العام للجريمة الالكترونية

المبحث الأول مفهوم الجرائم الالكترونية

المبحث الثاني: تجريم الأفعال الماسة بالمعالجة الالية للمعطيات

الفصل الثاني: الجوانب القانونية للبحث والتحري عن الجريمة الالكترونية

المبحث الاول: آليات البحث و التحري عن الجرائم الالكترونية

المبحث الثاني: القواعد الاجرائية في البحث والتحري عن الجرائم الالكترونية

الفصل الأول:
الإطار العام للجريمة
الالكترونية

تعد التكنولوجيات الحديثة أهم وأبرز وسائل التواصل الحديثة كما تعمل كذلك بغرض حفظ المعلومات وتخزينها وتسهيل أمر إسترجاعها، حيث وفرت التكنولوجيا وتقنية المعلوماتية مجال واسع في التعامل مع المعلومة، سواء من حيث نقلها أو تخزينها أو استرجاعها بل حتى استعمالها للتنبؤ بما قد يحدث مستقبلاً، و ذلك من خلال انتشار الحواسيب على أعلى نطاق، و ظهور تقنيات حديثة لتبادل المعلومات و للاتصال في شكل شبكة المعلومات الدولية وشبكة الأنترنت، وهذا ما يعد جانباً إيجابياً للتكنولوجيا إلا أننا نعرف انه لكل الاشياء تقريبا كم من السلبيات قد يوازي في بعض الاحيان ايجابياته أو يفوقها فنتج عن هذا التطورات التكنولوجية وعن سوء تسخيرها جملة من الاعتداء على مصالح الغير .

مع اختلاف اسباب ذلك سوى أنهم يحملون ويعبرون عن ميول إجرامي لا يقل خطورة عن باقي المجرمين التقليديين، و يرتكبون أفعالاً مجرمة قانوناً و معاقب عليها بعقوبات بهدف تحصيل مكتسبات ذات طابع معنوي في شكل معلومات وبيانات.

ومن أجل ذلك فقد خصصنا (المبحث الاول) لمفهوم الجرائم الالكترونية و(المبحث الثاني) تجريم الأفعال الماسة بالمعالجة الآلية للمعطيات للتعلم أكثر في مفهوم هذه وما يؤثر بها.

المبحث الأول: مفهوم الجرائم الالكترونية

ان الدور الكبير الذي لعبته الوسائل التكنولوجية والتطور الهائل لسرعة تدفق المعلومات من محركات البحث والبرامج المعلوماتية الحديثة وسهولة الوصول لها واستغلالها جعل أرقام التجاوزات التي تمس هذا المجال هائلة مما شكل ظاهرة الجرائم الالكترونية او السيبرية وفي هذا الصدد وجب التطرق لتعريفها وخصائصها (المطلب الأول) وكذلك لأهم أشخاصها وهو المجرم الالكتروني او المعلوماتي وأهدافه أو دوافعه (المطلب الثاني):

المطلب الاول: تعريف وخصائص الجرائم الالكترونية

في صدد بلورة فكرة أولية أساسية على موضوع رأينا أنه من الواجب في هذا المطلب الذي يعد ركيزة هذا الفصل والمتمثل في الاطار العام لهذه الجريمة أن نقدم تعريفات لأبرز المصطلحات التي ستكون محورية في هذا البحث منها الجريمة الالكترونية والبحث والتحري وهذا ما سنتطرق له في (الفرع الأول) ثم نتجه لتحديد خصائص ومميزات هذه الجرائم في (الفرع الثاني):

الفرع الأول: تعريف الجريمة الالكترونية والمصطلحات المتعلقة بالموضوع.

في هذا الفرع سنعطي فكرة على بعض أشهر التعريفات للجريمة الالكترونية والبحث والتحري كمصلح لغوي وقانوني مع محاولة الجمع بين مختلف هذه الافكار للوصول للفكرة المبتغاة والتي ستكون محور الدراسة وهي البحث والتحري عن الجرائم الالكترونية.

أولاً: تعريف الجريمة الالكترونية:

يتراوح تعريف الجريمة الإلكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى الجرائم التي ترتكب بأي نوع من الوسائل الرقمية التي تسمح بذلك وتعريف الجرائم

الإلكترونية باختصار على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال وآلات الصرافة وبطاقات الائتمان...إلخ.

و يتكون هذا المصطلح الجريمة الإلكترونية أو الافتراضية من جزأين هما الجريمة والإلكترونية وهو ما سنأتي على تعريفه.

فمفهوم الجريمة يختلف مع اختلاف الفئة الدارسة لها او مجال الدراسة من اجتماعي ونفسي وسياسي وغيرها ولهذا سنركز في هذا المجال على الجريمة في الشق القانوني فتعرف على اساس انها هي كل عمل أو امتناع عن عمل معاقب عليه بموجب قانون جنائي معين أو بتعريف آخر هي كل فعل نص القانون على تجريمه ووضع جزاء لمخالفته.

اما فيما يخص الشق الثاني والمتمثل في مصطلح الالكترونية او المعلوماتية وعند التغلغل في تعريف الجريمة الالكترونية يتبين لنا الفرق الجلي بينها وبين الجرائم في القانون التقليدية فمن عالم واقعي إلى عالم افتراضي أوجدته الثورة التكنولوجية حيث برزت الجريمة الإلكترونية أو المعلوماتية وهذا ما سوف نتناوله في مجموعة من التعريفات التي حاول من خلالها الدارسين وفقهاء القانون الوصول الى تعريف شامل لهذا المصطلح فلغويا تعرف المعلوماتية على اساس المعالجة الالية للمعطيات، وهي ترجمة للمصطلح الفرنسي *informatique*، وتعني تكنولوجيا تجميع ومعالجة وإرسال المعلومات بواسطة الكمبيوتر^[1].

اما اصطلاحيا فمن الظاهر عدم اتفاق الفقه على تعريف معين ومانع وشامل لهذه الجريمة فتتضارب بين المعلوماتية والالكترونية وجرائم الحاسوب او الغش المعلوماتي وغيرها من المصطلحات فظهر تعريف موسع وآخر اضيق لهذه الظاهرة سنأتي على ذكرهم فيما يلي:

[1] : يوسف ضغير ، الجريمة المرتكبة عبر الأنترنت، مرجع سابق، ص 14.

التعريف الموسع:

جرائم الالكترونية مصطلح شامل يقصد به كل الجرائم التي يستخدم فيها الكمبيوتر بالدرجة الاولى او وسائل اخرى فتصبح ادت للجريمة او هدف منها ويدخل تحتها الجرائم المعلوماتية وجرائم الانترنت حيث ان الهدف منها هو اخافة الاخرين عن طريق استخدام تكنولوجيا معينة^[1].

و عرفها مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية في عام 1983 الجريمة الالكترونية على انها: "كل أسلوب غير مشروع، أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو بنقله"^[2].

فقيل أنها " نشاط اجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامي " ^[3].

و يعرفها الخبير الامريكي باركر على انها: " كل فعل اجرامي متعمد أي كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق المجني عليه، أو كسب يحققه الفاعل"^[4].

تعرضت هذه التعريفات الى مجموعة من الانتقادات كونها تعتمد على وصف الجريمة لا تحديد مفهومها، حيث أن وصف الجريمة لا يعد من المعايير الدقيقة الكافية لاعتمادها أساسا لتحديد ماهية الفعل الاجرامي.

كما تبني مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاينة المجرمين الذي عقد في فيينا في الفترة ما بين 17/10 أبريل سنة 2000 التعريف التالي: " أنها أية جريمة

[1] : يوسف ضغير ، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير في القانون، تخصص قانون دولي للأعمال، كلية الحقوق و العلوم السياسية، جامعة مولود معمري تيزي وزو، 2013، ص14.

[2] : يونس عرب، صور الجرائم الالكترونية و اتجاهات تبويبها: ورشة تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، هيئة تنظيم الاتصالات، عمان، 2006، ص06.

[3] : عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت، دار الكتب القانونية مصر 2002، ص01.

[4] : نهلا عبد القادر المومني، الجريمة المعلوماتية، الطبعة الثانية، 2010، دار الثقافة للنشر و التوزيع، ص46.

يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية والجريمة تلك تشمل من ناحية مبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية" الذي يعتبر الأنجع من الناحية العملية حيث يشمل جوانب الحاسوب المادية والمعنوية^[1].

التعريف المضيق:

تباينت التعريفات لهذه الجريمة واختلفت حتى داخل الحقل القانوني تبعا لموضوع الدراسة القانونية ذاته، وتعددت حسب ما اذا كانت الدراسة متعلقة بالقانون الجنائي أم متصلة بالحياة الخاصة أم متعلقة بحقوق الملكية الفكرية (حق التأليف على البرامج).

وقد خلت الدراسات والمؤلفات التي في هذا الحقل قديما من تناول اتجاهات الفقه في تعريف جريمة الكمبيوتر وهذا ما حاول الكثير تقليصه من محاولة تقديم تعريفات لهذه الظاهرة فنجد:

من عرفها على " انها كل فعل غير مشروع يكون العلم بتكنولوجية الحسابات الآلية بقدر كبير لازماً لارتكابه من ناحية لملاحقته وتحقيقه من ناحية أخرى"^[2].

و عرفها البعض الآخر كما يلي: " جريمة الانترنت هي الجريمة التي يتم ارتكابها اذا قام شخص ما باستخدام معرفته بالحاسب الآلي لعمل غير قانوني"^[3].

أو هي: " كل نشاط غير مشروع موجه للنسخ أو الوصول للمعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها"^[4].

[1] : محمود أحمد عبابنة، جرائم الحاسوب و أبعادها الدولية، دار الثقافة للنشر و التوزيع، الأردن، 2005، ص 19.

[2] : قورة نائلة، جرائم الحاسب الاقتصادي، دار النهضة العربية، القاهرة، 2004، ص 20.

[3] : محمد عادل ريان، جرائم الحاسب الآلي و أمن البيانات، أنظر الموقع التالي : www.anaharonline.com

تاريخ الاطلاع 2017/04/20 على الساعة 18.20.

[4] : محمود أحمد عبابنة، جرائم الحاسوب و أبعادها الدولية، مرجع سابق، ص 17.

أو تم تعريفها بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول الى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه"^[1]

يستند أنصار هذا الاتجاه إلى أن فاعل هذه الجريمة يجب أن تتوفر له التقنية اللازمة لارتكاب الجريمة ومتابعتها والتهرب منها وتعرض هذا الاتجاه الى نقد كبير خاصة عدم امكانية وضع تعريف لجريمة يعتمد على معيار شخصي وهو ما يتوفر عليه المجرم الالكتروني من مميزات وخصائص^[2].

ثانياً: التعريف القانوني للنظام المعلوماتي في التشريع الجزائري وبعض التشريعات المقارنة:

التشريعات في مختلف المجالات دائمة التهرب من وضع تعريفات دقيقة لبعض المصطلحات مخافة التهرب من العقاب عند التفسير أو تطور الاجرام وعليه أغلب التعريفات كانت فقهية إلا ان هذا لا يمنع وجود مجموعة من المحاولات في بعض القوانين ومنها القانون الجزائري فنجد مثلاً:

قانون المعاملات الالكترونية الاردني رقم 85 لسنة 2001 حيث عرف في المادة الثانية منه نظام معالجة المعلومات على أنه " النظام الالكتروني المستخدم لإنشاء رسائل المعلومات وارسالها أو تسلمها أو معالجتها أو تخزينها أو تجهيزها على أية وجه آخر"^[3].

قانون إمارة دبي الخاص بالمعاملات والتجارة الالكترونية رقم 02 لسنة 2002 حيث عرف هو الاخر نظام المعلومات الالكتروني في المادة الثانية منه بالقول " نظام

[1] هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، الطبعة الأولى، مكتبة الآلات الحديثة، اسبوط، 1992، ص 31.

[2] محمد عبيد كعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، دار النهضة العربية، القاهرة، ص 32.

[3] : قانون رقم 85 لسنة 2001، الجريدة الرسمية للملكة الأردنية الهاشمية رقم 4524، الصادر بتاريخ 2001/12/31.

الالكتروني لإنشاء أو استخراج أو ارسال أو استلام أو تخزين أو عرض أو معالجة المعلومات أو الرسائل الالكترونية"^[1].

أما المشرع الجزائري فواكب هذه التشريعات العربية ووضع هو الآخر تعريفا لنظام المعلومات فعرفه من خلال المادة 02 الفقرة ب من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها مسميا اياه "اي نظام منفصل أو مجموعة من الانظمة المتصلة مع بعضها البعض أو المرتبطة يقوم واحد منها او اكثر بمعالجة الية للمعطيات تنفيذا لبرنامج معين " ^[2].

و يمكن القول أن المشرع الجزائري قد وفق في تعريفه لهذا المصطلح وغيرها من المصطلحات في القانون كالمعطيات المعلوماتية والجرائم المتصلة بتكنولوجيا الاتصال ووفق المشرع الجزائري في تعريفه حيث اشترط ضرورة الترابط بين مكونات او اجهزة النظام او الانظمة فيما بينها ومركز من جهة اخرى على وظيفة المعالجة الالية للمعطيات موسعا بذلك ليشمل كل من المعالجة الالية والمعالجة المعلوماتية للمعطيات.

ثالثا: تعريف البحث والتحري:

عملية البحث والتحري كما هو معلوم في القانون الجزائري يختص بها أساسا ضباط الشرطة القضائية في التحريات الأولية إلا أن هذا لا يعني أنها تقتصر عنهم فقد يقوم بالبحث والتحري عن الحقيقة بمفهومها الموسع كل من قضاة التحقيق وقضاة النيابة وحتى قضاة الحكم.

[1] : قانون إمارة دبي رقم 02 لسنة 2002 المتعلق بالمعاملات و التجارة الإلكترونية الصادر بتاريخ 12 فبراير 2002.

[2] : قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها، الصادر في الجريدة الرسمية رقم 47 الصادرة بتاريخ 16 أوت 2009.

و التحري لغتا: من الفعل أحرأ فيقال تحرى المكان أو الشئ أي عاينه وهو عمل أصيل لضباط الشرطة القضائية يعملون عليه بواسطة حواسم والوسائل التقنية والمعلوماتية الحديثة التي تكون تحت تصرفهم من اجل معاينة ومعرفة ملابسة الاشياء^[1].

مما سبق يمكننا تعريف البحث والتحري عن الجرائم الالكترونية بالقول أنه كل الأعمال التي يقوم بها الأشخاص المؤهلون والتي تهدف إلى استقصاء ومعرفة الحقيقة فيما يخص الجرائم أو الأفعال التي يعاقب عليها القانون وتستخدم بأحد الوسائل التكنولوجية او المعالجة للمعطيات كل هذا في سبيل معرفة الجناة ومتابعتهم.

الفرع الثاني: خصائص الجرائم الالكترونية

في هذا الفرع الثاني سنعدد مجموعة الخصائص والمميزات التي تتسم بها الجريمة الالكترونية وخاصة مقارنة مع جرائم القانون العام الاخرى وسنشملاها فيما يأتي:

أولاً: العولمة في صورتها القائمة:

تعد الجرائم الالكترونية من الجرائم الحديثة مقارنة بالجرائم التقليدية كالقتل والسرقه مثلاً، وقد ظهرت هذه الجرائم كنتيجة حتمية للاستخدام السيئ للتطور المعلوماتي والتكنولوجي الحاصل فمع ظهور التكنولوجيا وتدني قيمة استغلالها نتيجة التنافس التجاري اصبحت التكنولوجيا في يد الجميع وتتدخل في مختلف المجالات فظهر مثلاً التعليم الالكتروني والتجارة الالكترونية هذا كله تجاوز بمراحل أجهزة الدولة الرقابية في هذا المجال هذا ما سمح للعديد من مجرمي هذا النوع من الجرائم م ن التهرب من القانون مما أصبح يهدد أمن واستقرار الدول^[2].

[1] : مصطفى محمد موسى، التحري في جرائم مجتمع المعلومات و المجتمع الافتراضي، الطبعة الاولى، 2011 ص298.

[2] : فتيحة رصاع ، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة أبي بكر بلقايد، كلية الحقوق و العلوم السياسية، تلمسان، السنة الجامعية 2011/2012، ص47.

فيقال أن: "الجريمة الالكترونية هي الابن غير الشرعي الذي جاء نتيجة للتزاوج بين ثورة تكنولوجيا المعلومات... مع العولمة" أو هي: "المارد الذي خرج من القمقم ولا تستطيع العولمة أن تصرفه بعد أن أحضرته الممارسة السيئة لثورة تكنولوجيا المعلومات"^[1].

ثانياً: الجريمة الالكترونية عابرة للحدود:

إن أهم ما جاءت به التكنولوجيا هو تقريب أطراف العالم المتباعدة من شعوب ومناطق وعملت على إزالة الحدود السياسية والجغرافية، فالقدرة التي تتمتع بها الحواسيب والبرامج التكنولوجية الهائلة في نقل وتخزين ومعالجة كم معتبر من المعلومات في وسط انظمة معلوماتية يفصل بينها آلاف الأميال هذا ما يجعل امكانية ارتكاب جرائم في دول معينة وتقع نتائجها او احد عناصرها في دولة أخرى^[2] ، فهي بهذا الشكل لا تعترف بالحدود بين الدول وهي تشكل بذلك شكل جديد من أشكال الجرائم العابرة للحدود^[3]، ان هذا يجعلنا نقول أن العالم الافتراضي يختصر المكان والزمان في نقرة زر .

و لا يقتصر شمول الجرائم التكنولوجية للمكان والزمان فقط بل يتعداه لإمكانية تعدد الأطراف المتضررة الذي قد يكونوا من نفس الدولة او من دول مختلفة، وهو ما يلاحظ في حالات جرائم نشر المواد ذات الخطر الديني والأخلاقي أو الأمني أو السياسي أو التربوي أو الثقافي أو الاقتصادي، وقد تجلت هذه الخطورة لأول مرة في قضية نقص المناعة المكتسبة قضية نقص المناعة المكتسبة "الايذز": حيث انه في عام 1989 قام أحد الأشخاص بتوزيع نسخ خاصة ببرنامج يهدف الى اعطاء نصائح حول المرض إلا أنه في الواقع كان يحمل فيروس الكروني يترتب عليه تعطيل اجهزة الحاسب الآلي ، ثم يقوم المجني بطلب مبالغ مالية من أجل تزويد الضحايا بمضاد للفيروس وقد تمكنت

[1] : مقولة الدكتور محمد صالح العادلي أستاذ القانون الجنائي بكلية الحقوق بمسقط وجامعة الأزهر بمصر محامي بالمحكمة العليا الدستورية بمصر .

[2] : عباس أبو شامة عبد المحمود، عولمة الجريمة الاقتصادية، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2007، ص52.

[3] : خالد ممدوح ابراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، 2009، ص 88.

السلطات الأمريكية من القبض على "جوزيف بوب" في 1990/02/03 بمدينة أوهايو تقدمت بعد ذلك بريطانيا بطلب تسليمه كون البرنامج المرسل للضحايا تم من على أراضيها وهذا ما حدث فعلا وأعدت هذه أول حالة لتسليم مجرم بتهمة جريمة الكترونية متمثلة في اعداد برامج خبيثة كما تم توجيه قرابة احدى عشر قضية لهذا الشخص من اكثر من دولة [1] ، لذلك على الدول إيجاد حلول عن طريق التعاون الدولي لمكافحة هذا النوع من الجرائم عن طريق المعاهدات والاتفاقيات الدولية [2] وهذا ما نادى به الدول من أجل التصدي لهذه الجرائم بأكثر حزم وقوة [3]، يستخلص مما سبق أن هذا النوع من الجرائم يثير اشكالا قانونيا أساسيا يتعلق بتحديد الاختصاص القضائي في متابعة هذه الأفعال.

ثالثاً: صعوبة الاكتشاف:

من مميزات الجرائم الالكترونية وفي نفس الوقت تعد أحد عوائق التحقيق فيها هو صعوبة الكشف عن هذه الأخيرة، كونها تقع في بيئة افتراضية لا تترك آثار ملموسة مادية ظاهرة للعيان هذا من جهة ومن جهة أخرى فالمجرم الالكتروني يعمل على تدمير ومحو الأدلة التي قد تشير له فالأعداد المكتشفة من هذا النوع من الجرائم قليل جدا بالمقارنة مع نسبة اكتشاف الجرائم التقليدية فأغلب القضايا المكتشفة فيكا تكون عن طريق الصدفة [4]، فهي لا تترك آثار خارجية محسوسة قد تساعد على سرعة اكتشافها للعيان فهي لا تحتاج الا لمسات معدودات على جهاز حاسوب حتى تقع وتنتهي [5].

[1] : نهلا عبد القادر المومني، الجريمة المعلوماتية، مرجع سابق، ص 48.

[2] : سينا عبد الله محسن، المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية و الوطنية الدار البيضاء، المملكة المغربية، 2007، ص52.

[3] : مؤتمر الأمم المتحدة الثامن لمنع الجريمة و معاقبة المجرمين المنعقد في هافانا عام 1990.

[4] : أنظر عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية و أزمة الشرعية الاجرائية، جامعة الكوفة كلية القانون، ص116.

[5] : محمد حماد مرهج الهيتي، التكنولوجيا الحديثة في القانون الجنائي، دار الثقافة للنشر و التوزيع، عمان، الأردن 2004، ص165.

رابعاً: جريمة ناعمة (لا عنفية):

على عكس جرائم القانون العام التقليدية تتميز الجرائم الالكترونية في أفعالها كونها من النوع الذي لا يستلزم استعمال القوة البدنية لتنفيذه عكس نظيراتها من الجرائم التقليدية التي تستلزم جلها نوع من المجهود العضلي كأعمال العنف أو الكسر وغيرها^[1].

حيث يتميز هذا النوع من الجرائم بكونها جرائم هادئة بطبيعتها لا تحتاج إلى العنف بل كل من ما تحتاجه هو القدرة على التعامل مع الحاسوب بمستوى تقني يوظفه صاحبه في ارتكاب أفعال ذات طبيعة جرمية، فهذا ما يؤدي الى أن تكون الجرائم الالكترونية جرائم نظيفة بمفهوم غياب أية آثار أو دلائل على العنف الجسدي خاصة.

خامساً: سرعة التنفيذ ومحو الدليل:

الجريمة الالكترونية من الجرائم التي قد تتم وتنتهي في أجزاء من الثانية لكن نتيجتها قد تكون أكبر من جريمة تقليدية يقوم بها عدد أكبر من الاشخاص وبوسائل أكثر فهي تتم بضغطة زر. مع العلم ان الجريمة الالكترونية من الجرائم القليلة التي ورغم معرفتها إلا ان المشرع لم يتمكن ولن يتمكن من ضبطها ضبطاً نهائياً كون هذه الأخيرة أسرع تطورا من التشريعات وهذا يرجع إلى التطور الرهيب لتكنولوجيا الاتصالات والمعلومات^[2].

كما أن للسرعة في التنفيذ فكرة موازية لها وهي سرعة محو الدليل او ما يعادلها في الجرائم التقليدية مرحلتي محو او عدم ترك الدليل والفرار من مسرح الجريمة وهذا ما لا يتوقع في الجرائم الالكترونية فتقتصر العملية على سرعة محو الدليل وهو ما يتمكن منه المجرم الالكتروني حيث غالبا ما يكون قد خطط لهذه المرحلة وجهاز الوسائل اللازمة

[1] : صالح بن محمد المسند، عبد الرحمان بن راشد المهيني، جرائم الحاسب الآلي الخطر الحقيقي في عصر

المعلومات، المجلة العربية للدراسات الأمنية و التدريب، المجلد 15، العدد 29، ص20.

[2] : محمد عبيد كعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، مرجع سابق، ص33.

لذلك وتساعد البيئة الاللكترونية المعقدة المجرم على هذه المهمة وهذا ما يجعل كشف الجريمة وتحديد مرتكبيها أمرا غاية في الصعوبة والتعقيد^[1].

سادساً: تقادم الدعوى العمومية في الجرائم الالكترونية:

لعى من مجموع الاستثناءات التي تتميز بها الجرائم الاللكترونية على نظيراتها من الجرائم العادية الاخرى هو مدى وقوعها تحت الاطار العادي لقواعد التقادم من عدمه فبقراءة لنصوص (المواد 07 فقرة 1، 08، 08 مكرر من قانون العقوبات) اللذين جاء النص فيهم على:

المادة 07: تتقادم الدعوى العمومية في بانقضاء عشر سنوات كاملة تسري من يوم اقتراف الجريمة إذا لم يتخذ في تلك الفترة أي إجراء من إجراءات التحقيق أو المتابعة....

المادة 08: تتقادم الدعوى العمومية في مواد الجرح بمرور ثلاث سنوات كاملة.

و يتبع في شأن التقادم الأحكام الموضحة في المادة 07.

المادة 08 مكرر: لا تنقضي الدعوى العمومية بالتقادم في الجنايات والجرح الموصوفة بأفعال إرهابية وتخريبية وتلك المتعلقة بالجريمة المنظمة العابرة للحدود الوطنية أو الرشوة أو اختلاس الأموال العمومية.

من استقراء كل هذه المواد يمكن القول ان المشرع لم ينص صراحة على عدم التقادم في الجرائم الاللكترونية او المرتبطة بالمعالجة المعلوماتية للمعطيات كما استثنائها في نصوص عديدة اخرى منها نص المادة (16 فقرة 7 من قانون العقوبات) إلا ان هذا لا يمنع بناء على ما سبق وان ذكرناه في خصوص أحد ميزات هذا النوع من الجرائم وهي خاصية عبورها للحدود الدولية فمن الممكن والمتوقع ان تكون هذه الجريمة من الجرائم العابرة للحدود الوطنية وفي شكل منظم جماعات وفي اطار معين هنا فقط يمكن اعتبارها

[1] : صالح بن محمد المسند، عبد الرحمان بن راشد المهيني، جرائم الحاسب الآلي الخطر الحقيقي في عصر

المعلومات، مرجع سابق، ص 20.

عابرة للحدود الوطنية وهنا يمكن ان تخضع للاستثناء في التقدم لتصبح من الجرائم التي لا يقع عليها حساب التقادم.

المطلب الثاني : المجرم الالكتروني

في هذا المطلب سنتحدث على أبرز أشخاص الجريمة المعلوماتية والمتمثل في المجرم الإلكتروني حيث يعد العنصر الاهم فيها خاصة اذا علمنا أن شخص الصحية في غالبية هذا النوع من الجرائم لا يسلط عليه الضوء كثيرا لأنه يمكن أن يكون شخصا طبيعيا بسيط تكنولوجيا وهنا سيكون ضحية سائغة وإما سيكون عالما هو الاخر بالتكنولوجيا وهنا سيصح صراع متساوي في القوى يحول الى الاقوى مما سبق أردت الاشارة إلى أن الضحية دورها ثانوي مقارنة مع الفعل الأصلي لمجرم ولهذا سنتعرف على مميزاته في (الفرع الاول) ثم الاسباب والدوافع التي تجعله يقوم بمثل هذا النوع من الجرائم في (الفرع الثاني):

الفرع الأول: مميزات المجرم الالكتروني

لا شك أن الشخص القادر على مجابهة ترسانة معقدة من البيانات والمعلومات المتدفقة وفي شكال تشفيرات مختلفة بسرعة وقدرة كبيرة على التخفي لن يكون شخصا عاديا على الاقل ليس بدنيا وإنما ذهنيا ولهذا سنتطرق في هذا الفرع إلى أبرز خصائص ومميزات المجرم الالكتروني أو المعلوماتي:

أولاً: ذكي:

الذكاء من الصفات التي يتحلى بها المجرم في هذا النوع من الجرائم كغيرها من المميزات التي سنأتي على تبيانها وهو ما يتطلب منه المعرفة التقنية لكيفية دخول

الحواسيب وبرامجها المختلفة والقدرة على التغيير والتعديل الاجرامي فيها [1]، لذلك يقال أن الإجرام الالكتروني هو إجرام الانكفاء مقارنة بالإجرام التقليدي الذي يتميز بالعنف [2].

ثانياً: ماهر:

وهي ما يتطلبه النشاط الاجرامي من حرفة في التنفيذ وذلك قد يكون عن طريق اما الدراسة المتخصصة او المهارة المكتسبة في هذا المجال او عن طريق العلاقات الخاصة ومستوى مهارة المجرم يحدد خطورة وضخامة الجريمة الالكترونية التي قد يرتكبها [3]. وهو يتميز عن نظيره المجرم العادي في الغالب بالخبرة الواسعة التي تمكنه من انجاز مخططاته دون أن يكتشف امره او ان يتم ذلك بصعوبة كبيرة فيستخدم اساليب التشفير مثلا او كلمات المرور للحيلولة دون الايقاع به [4].

ثالثاً: منظم ومختص:

فقد أثبت أن عدد من المجرمين الالكترونيين لا يرتكبون سوى هذا النوع من الجرائم دون سواها من جرائم القانون العام المختلفة، ومن ناحية أخرى يكون من الصعب على المجرمين العاديين ارتكاب الجرائم التي يقوم بها المجرم الالكتروني الا استثناء في توفر ظروف معينة أو عند الصدفة، فارتكاب هذا النوع من الجرائم ويستلزم نوع من التنظيم والتخطيط المسبق الذي يتميز به المجرم المعلوماتي من تجهيز للأدوات والوسائل

[1] : و يمكن ان نخرج من هذا النطاق التعديل الضروري لتبيان حقيقة الاشياء فمثلا التعديل في تسجيلات معينة بإزالة التشويش منه فهو ضروري لايضاح الصوت أو الصورة لتبيان الحقيقة.

[2] : غنام محمد غنام، مداخلة بعنوان "الحماية الجنائية لبطاقات الائتمان الممغنطة"، مؤتمر الجوانب القانونية و الأمنية للعمليات الإلكترونية، دبي 2003، ص3.

[3] : خالد ممدوح ابراهيم، الجرائم المعلوماتية، مرجع سابق، ص135.

[4] : جميل عبد الباقي الصغير، القانون الجنائي و التكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، 1992، ص115.

والمعرفة الدقيقة للهدف المراد قرصنته بأي طريقة ثم طرق التمويه او التهرب وذلك عن طريق محاولة اخفاء اي دليل قد يوقع به^[1].

رابعاً: شخص عائد للإجرام:

يكون المجرم الالكتروني أكبر عرضتاً للعودة في الجرائم وذلك نتيجة شبه حتمية كونه دائماً يرغب في التهرب من العدالة عن طريق سد الثغرات التي قد يتركها في نظام معلوماتي معين هذا من جهة ومن جهة ثانية فان النشوة التي يشعر بها المجرم الالكتروني تولد لديه الرغبة في تكرارها للحصول على نفس الشعور^[2].

خامساً: شخص اجتماعي:

فهذا النوع من المجرمين يتميز على استغلاله لذكائه ومهارته في ربط علاقات جيدة داخل الوسط الذي يعيش فيه، فكسبه ثقة وود المجتمع الذي يحيط به يجعل من الصعوبة التنبه لشخصيته الاجرامية^[3].

الفرع الثاني: دوافع المجرم الالكتروني

الدافع (الباعث)، الغرض، الغاية، تعبيرات لكل منها دلالتة الاصطلاحية في القانون الجنائي، تتصل بما يعرف بالقصد الخاص في الجريمة، وهي مسألة تثير جدلاً فقهيًا وقضائياً واسعاً، ذلك أن "القاعدة القضائية تقر أن الباعث ليس من عناصر القصد الجرمي" وان الباعث "لا اثر له في وجود القصد الجنائي" وإذا كان الاستخدام العادي

[1] : حمزة بن عقون، السلوك الاجرامي للمجرم المعلوماتي، مذكرو لنيل شهادة الماجستير في العلوم القانونية، تخصص علم العقاب و علم الاجرام، جامعة الحاج لخضر، كلية الحقوق و العلوم السياسية، باتنة، السنة الجامعية 2011/2012، ص33.

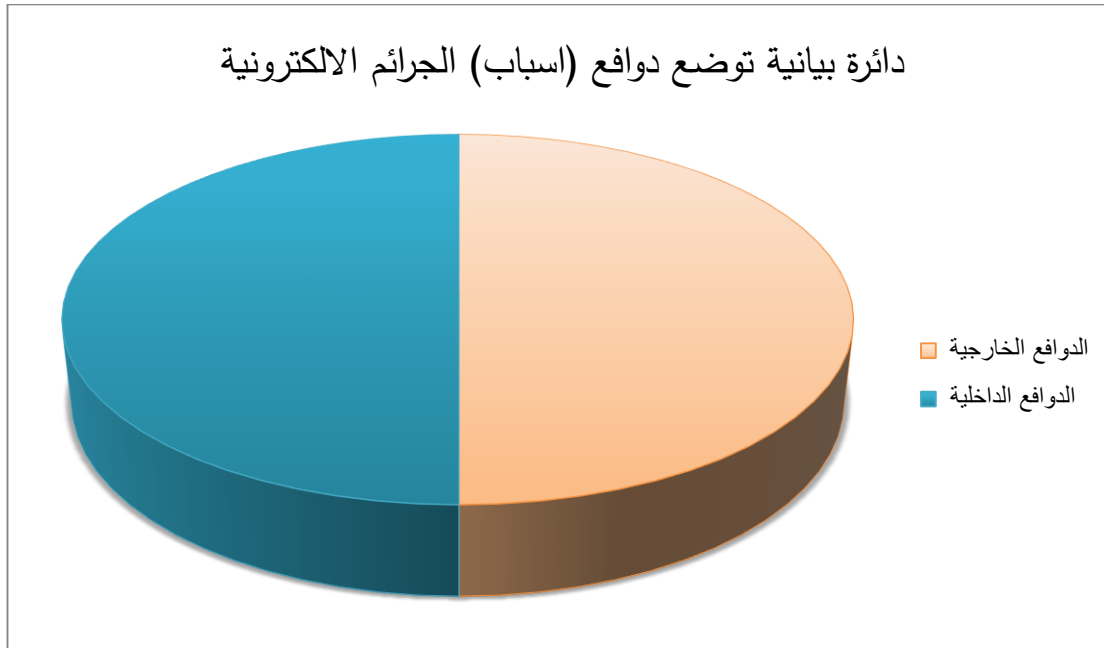
[2] : عادل محمود شرف، عبد الله إسماعيل عبد الله، ضمانات الأمن و التأمين في شبكة الأنترنت، مؤتمر القانون و الكمبيوتر و الأنترنت، كلية الشريعة و القانون بالتعاون مع مركز الامارات للدراسات و البحوث الاستراتيجية، مركز تقنية المعلومات، دولة الامارات العربية المتحدة، أيام من 1 - 3 مارس 2000، المجلد الثاني، ص393.

[3] : عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2010، ص ص80-81.

للتعبيرات المشار اليها يجري على أساس ترادفها في الغالب فإنها من حيث الدلالة تتمايز وينتج عن تمايزها آثار قانونية على درجة كبيرة من الأهمية^[1].

فالباعث (الدافع) هو "العامل المحرك للإرادة الذي يوجه السلوك الاجرامي كالمحبة والشفقة والبغضاء والإنتقام" وهو اذن قوة نفسية تدفع الارادة الى الاتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة وهو "يختلف من جريمة الى أخرى، تبعا لاختلاف الناس من حيث السن ودرجة التعليم وغير ذلك من المؤثرات كما يختلف بالنسبة للجريمة الواحدة من شخص لآخر"^[2].

هناك العديد من أسباب ارتكاب هذا النوع من الجرائم وهو الجرائم الالكترونية والتي نجد منها ما هو شخصي يقع في ذهن الفرد أو لحاجة شخصية له كما قد تكون هذه الأسباب خارجة عن الفرد فيكون المجتمع او افراده من أحد اسبابها وهذا ما يوضح فيما يلي:



[1] : نجيب حسني، دروس في القانون الدولي الجنائي، دار النهضة العربية، القاهرة، ص 1052.

[2] : أحمد فتحي السرور، الوسيط في قانون العقوبات (القسم العام)، دار النهضة العربية، الطبعة السادسة القاهرة،

1991، ص 427.

أولاً: دوافع شخصية:

و هذا النوع من الدوافع هو في الحقيقة ما يتعلق ويدور في الاعماق الداخلية للشخص المجرم في حد ذاته وهي الاخرة تنقسم الى مجموعة من الاسباب نبينها فيما يلي:

أ - دوافع مادية:

الاهداف المادية والتي يسعى من خلالها الشخص الى تحقيق اكبر ربح مالي ممكن ولتحقيق هذا الهدف المالي على المجرم ان يطور نفسه حتى يواكب كل التطورات التي تحدث في مجال التقنية والمعلوماتية ويسعى لتحقيق أعلى قدر من المكاسب وبأقل مجهود ممكن^[1]، وهذا الهدف جاء نتيجة صعوبة تحقيق نفس النتيجة بالطرق القانونية والمقبولة اجتماعيا وذلك بعد تنامي نسب البطالة فالجريمة الالكترونية شأنها شأن الجرائم التقليدية ترتبط بالظروف الاقتصادية فهناك مثل يقول "العقل العاقل عن العمل هو ورشة عمل الشيطان"^[2].

ب - دوافع ذهنية نفسية:

و هي الجزء الثاني وقد نقول انه الاله لان الهدف هنا ذهني بالنسبة للجاني اي انه لا ينتظر منه قيمة مالية بقدر ما يريد الحصول على شعور او قد يكون الشعور هو سبب في ارتكابه هذا النوع من الجرائم فنجد:

[1] : وضاح محمود الحمود و نشأت مفضي المجالي، جرائم الانترنت، دار المنار للنشر، عمان، 2005، ص 30.

[2] : ذياب موسى البداينة، ورقة عمل بعنوان الجرائم الالكترونية: المفهوم و الاسباب، مقدمة للملتقى العلمي للجرائم

المستحدثة في ظل المتغيرات و التحولات الاقليمية و الدولية ، عمان ، المملكة الأردنية الهاشمية، خلال الفترة من

2014/09/04-02، ص ص 14-15.

- البحث عن التقدير:

قد يكون شخص الجاني شخصا طائشا وصغير في السن ويتملكه شعور بعدم جدوى وجوده وانه شخص نكرة في المجتمع فيبحث على الظهور في الاعلام وان يجلب لنفسه الاضواء حتى عن طريق ارتكاب مثل هذا النوع من الجرائم^[1].

- المتعة والتحدي:

إن الشغف بالتكنولوجيا والالكترونيات والرغبة في اختراق الوسائل التقنية الحديثة فاخترق الأنظمة وكسر الحواجز الأمنية المحيطة بمثل هذه الأنظمة الالكترونية يشكل متعة وتسلية خاصة لصاحبها، فهو في هذه الحالة ينطلق بدافع التحدي وأثبات الذات اكثر منه التخريب او غيرهاو من مثل هذه الامثلة ما يعرف بمجموعة الجحيم العالمي "Global Hell" وهي قضايا تعامل معها مكتب التحقيقات الفيدرالي وهي عبارة عن مجموعة من الاختراقات التي وقعت على مواقع كل من البيت الابيض والشرطة الفيدرالية الأمريكية والجيش الأمريكي ووزارة الداخلية الأمريكية حيث اثبتت التحقيقات ان الهدف من هذه الاختراقات لا يتجاوز فعل الاختراق ولا يتعداه لا الى التدمير او اخذ بعض المحتويات^[2].

- الانتقام:

يعد دافع الانتقام من اخطر دوافع ارتكاب هذا النوع من الجرائم، لأنه غابنا ما يكون من شخص عالم بخبايا الضحية كان شخصا أو مؤسسة ومن أمثلة أسباب الانتقام الشعور بالظلم او الحرمان والتي قد يكون سببها الطرد او الالهانة او المنع من بعض الحقوق ومثال ذلك فقد دفع الانتقام بحاسب في احدى الشركات للتلاعب بالبرامج المعلوماتية بحيث جعل هذه البرامج تعمل على اخفاء كل البيانات الحساسة الخاصة

[1] : ذياب موسى البداينة، ورقة عمل بعنوان الجرائم الالكترونية: المفهوم و الأسباب، مرجع سابق، ص 11.

[2] : رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية الطبعة الأولى، 2012، ص 95.

بديون الشركة التي يعمل بها بعد رحيله بـ 06 أشهر وقد تحقق هذا الأمر في التاريخ المحدد من قبل هذا المحاسب^[1].

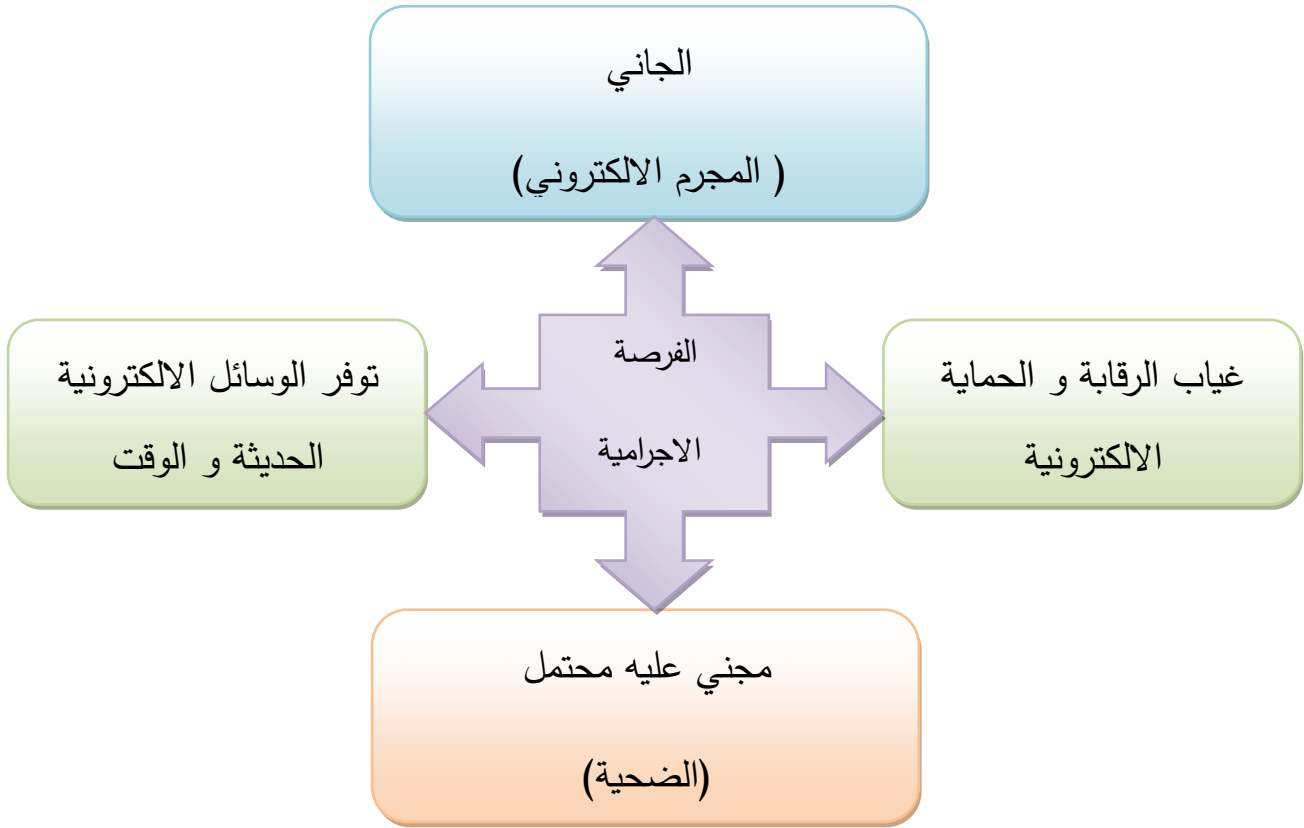
- الفرصة:

لقد وفرت التقنيات الحديثة والحواسيب وتكنولوجيا المعلومات فرصاً غير مسبوقة لانتشار الجريمة الالكترونية، لأن الفرصة تنتج الجريمة وتلعب البيئة وترتيباتها دوراً كبيراً في إنتاج الجريمة، فوقت الانحراف الالكتروني وقت مفتوح ليلاً ونهاراً وفي أي مكان من الاماكن كل هذه العوامل والانفتاح يزيد من فرص وقوع هذا النوع من الجرائم خاصة انها تتم بسرعة وبغموض^[2].

[1] : سامي الشوا، العش المعلوماتي ظاهرة إجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية

للقانون الجنائي، دار النهضة العربية، القاهرة، 1993، ص 525.

[2] : نياح موسى البدانية، ورقة عمل بعنوان الجرائم الالكترونية: المفهوم و الأسباب، مرجع سابق، ص 10.



رسم توضيحي يبين ظروف تكوين الفرصة التي تعد من اسباب ارتكاب الجرائم الالكترونية

ضبط الذات المنخفض:

ان توفر العوامل النفسية المذكورة من توفر فرصة ملائمة للإجرام لا تكفي وحدها لارتكاب الجرائم الالكترونية بل بحفزها على ذلك بعض السمات النفسية التي يتميز بها شخص المجرم ومنها ضبط الذات المنخفض ويعبر عنه البعض بالسلوك الطائش وهو كل فعل يقوم على القوة والخداع لتحقيق رغبات ذاتية ومكبوتات نفسية [1].

[1] : ذياب موسى البداينة، ورقة عمل بعنوان الجرائم الالكترونية: المفهوم و الأسباب، مرجع سابق، ص 16.

ثانياً: دوافع خارجية:

هذا النوع الثاني من الدوافع التي قد تكون احد اسباب أو عوامل جعل الشخص يتجه أو تساعد ففي اتجاهه لارتكاب هذا النوع المميز من الجرائم وهي الاخرة تنقسم الى مجموعة من الاسباب نبين جزء منها فيما يلي:

أ- العولمة :

إن ظهور الفضاء الالكتروني كأحد نتائج البحوث العلمية المتطورة التي جاءت نتيجة عولمة المجتمع جعلت فرص وقوع الجرائم يتزايد ضمن فضاء مميز وخاص وهو الفضاء الالكتروني، فقد يرتكب شخص سلوك معين في فضاء افتراضي لا يكون قادر على ارتكابه في الواقع لمكانته الاجتماعية أو غيرها من الاسباب والعولمة تجلت في مجموعة من الصور منها:

ب- التحول الرقمي

إن من مميزات العولمة القفزة النوعية التي شهدتها عوالم الاتصال وظهرت جليا هذه القفزات في كميات ومقدار المعلومات المتدفقة ونوعيتها فظهر مثلا حاليا ما يعرف بال HD و 4K التي تعتبر اخر ما وصلت لها تكنولوجيا السمي البصري على سبيل المثال، وأصبحت الصور والمقابلات والمعلومات تنتشر في العالم بسرعة رهيبية وظهرت الشبكات وعرف العالم مجموعة فريدة من التطبيقات والبرامج التي كانت للأمس القريب تعد ضربا من الخيال كالبث المباشر الشخصي (Vidéo Live) والمحادثات الصوت والصورة (Appel Vidéo) وغيرها^[1].

ج- التحضر

التحضر في مفهومه الاجتماعي وهو هجرة الأفراد من الريف إلى المدينة والمناطق الحضرية، حيث ان عدد كبيراً من الشباب المهاجر يجد صعوبة في التأقلم مع الوسط

[1] : نياي موسى البداينة، ورقة عمل بعنوان الجرائم الالكترونية: المفهوم و الاسباب، مرجع سابق، ص 14.

الحضاري الجديد الذي وضعوا فيه، هذا الأخير يجبرهم على محاولة الالتحاق بالركب عن طريق الجرائم الالكترونية التي تعد أقل تكلفاً فيقول "ميك" أن التحضر سبب رئيسي للجرائم الالكترونية والتحضر دون جريمة مستحيل [1].

ب - التعاون والتواطئ:

هذا الدافع من الدوافع الاكثر تكرار في مجال الجرائم الالكترونية وغالبا ما يحدث من متخصص في هذا المجال أين يقوم أحد بالجانب الفني في المشروع الاجرامي وبعد اتمامه يقوم هذا المجرم بالتغطية عليه والتلاعب بالمعطيات حتى لا تظهر الفوارق والتجاوزات ويحدث هذا كثيرا في عمليات تحويل الاموال والمكاسب التي تكون اغلبها جراء أنشطة مشبوهة [2].

ت - البطالة:

الجريمة الالكترونية لا تختلف عن الجرائم الاخرى في كون أحد أبرز اسبابها هو العامل الاقتصادي وتشكل ظاهرة البطالة احد روافد هذا السبب فهناك أحد الأمثلة يقول " العقل العاطل عن العمل هو ورشة عمل للشيطان" ولذلك فالشباب الذي يملك جزء من المعرفة ولا يجد الحيز المناسب لاستثماره في العمل أو شيء يعود عليه وعلى المجتمع بالنفع سيتوجه به إلى الاجرام [3].

[1] : نياح موسى البداينة، ورقة عمل بعنوان الجرائم الالكترونية: المفهوم و الأسباب، مرجع سابق، ص 14.

[2] : أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الاسكندرية 2006، ص 90.

[3] : نياح موسى البداينة، المفهوم و الأسباب، مرجع سابق، ص 14-15.

المبحث الثاني: تجريم الأفعال الماسة بالمعالجة الآلية للمعطيات:

إن الانتشار الواسع لتكنولوجيا الاتصالات وتشعبها لكافة المجالات وتزايد ارقم الجرائم او الاعتداءات بهذه الطرق الحديثة أوجب على المشرع الجزائري وغيره المنظمات اتخاذ كافة الاجراءات لمجابهة هذه الظاهرة وهذا ما سنتطرق له في (المطلب الاول) حيث سنتطرق لتجريم الافعال الماسة بأنظمة المعالجة الآلية للمعطيات وفق القوانين الجزائرية وال(المطلي الثاني) نتطرق فيه للجهود الدولية والاقليمية للحد من انتشار هذه الظاهرة أو القضاء عليها:

المطلب الأول: الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في القوانين الجزائرية

يمكن ان نقر بالخطوات الهامة التي جاء بها المشرع الجزائري في باب تجريم هذا النوع من الجرائم من خلال اصداره لمجموعة من القرارات والمراسيم وكان من بينها القانون 04-15 الذي عدل بموجبه قانون العقوبات حيث أدرج قسما كاملا يتضمن العقوبات المقررة للمساس بأنظمة المعالجة للمعطيات في المواد من (394 مكرر - 394 مكرر 8) وغيرها من القوانين الخاصة التي سنتطرق لجزء منها فيما سيأتي بيانه في (الفرع الأول) حديث على القانون الاصل والتمثل في قانون العقوبات و(الفرع الثاني) القوانين المكملة له :

الفرع الأول: الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات الجزائري.

سنتطرق في هذا المجال لأبرز الجرائم والعقوبات التي وقعها المشرع الجزائري على مرتكبي الجرائم الالكترونية بهدف الردع وهي كالاتي:

أولاً: المساس بأنظمة المعالجة الآلية للمعطيات

المساس بالأنظمة الآلية للمعطيات هو مصطلح شامل لعدد معين من الصور الذي جاء بها المشرع الجزائري كما سبق وان اشرنا اول مرة في صدد تعديله لقانون العقوبات بموجب القانون 04-15 من اخلال ادراجه (للمواد من 394 مكرر - 394 مكرر8) والتي من استقرائها نجد:

أ- جريمة دخول معالجة آلية للمعطيات عن طريق الغش

و هو ما نصت على تجريمه نص (المادة 394 مكرر قانون عقوبات) حيث تعاقب بالحبس والغرامة من ثلاثة أشهر إلى سنة وبغرامة مالية من 50.000 دج إلى 100.000 دج كل من يدخل عن طريق الغش في كل او جزء من احد المنظومات المعدة للمعالجة الآلية للمعطيات يلاحظ ان المشرع الجزائري في هذه المادة جرم فعل الدخول بطريقة غير شرعية واعتبر هذا التصرف في حد ذاته يشكل جريمة حتى ولو كان الهدف من هذا الاختراق هو التسلية وحتى ولو لم يمس المنظومة بأي اشكال [1] يمكن القول ان نص المادة يعد باب شامل للتجريم وهي تشابه لفكرة سد الذرائع في التشريع الاسلامي فتجريم الدخول بح ذاته يمنع ارتكاب أشياء اخرى كتغيير أو الحيازة أو إعادة النشر أو غيرها من الافعال.

ب- جريمة إزالة أو تعديل معطيات في نظام المعالجة آلية بطرق تدليسية

بتصور المشرع الجزائري لعدد من السلوكيات التي قد يرتكبها المجرم الالكتروني عدد بعض هذه الصور ف جاء على نكر ذلك في نص المادة (394 مكرر1) من قانون العقوبات الجزائري التي جاء فيها: " يعاقب بالحبس من ستة(6) أشهر إلى ثلاث(3)

[1] : في زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدى، عين مليلة الجزائر، 2011، ص 49 نقلاً عن هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، الطبعة الأولى، دار النهضة العربية، 1992 .

سنوات وبغرامة مالية من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"، سواء كان هذا التعديل أو التغيير جزئيا أو كليا على معلومات وهمية أو حقيقية [1].

تدخل هذه الفقرة كغيرها من فقرات هذه المادة في باب حماية الحياة الخاصة للأفراد وحماية حق الخصوصية كما يمكن أن نلاحظ التدرج المنطقي والموضوعي الذي جاء به المشرع الجزائري في هذه المواد فالنص على هذه الأفعال مثلا لا يتصور تحقيقه دون الولوج البيئية لمعلوماتية التي في هذه الحالة ستكون مسرح للجريمة.

ت - جرائم نشر حيازة أو الاتجار بالمعطيات

و هذه الجريمة نصت عليها (المادة 394 مكرر 2 قانون عقوبات) وهذه الجريمة تعد من الاكثر انتشارا في العالم الالكتروني حيث اعتبر المشرع الجزائري عملية اصطناع برنامج مخصص لارتكاب فعل الغش المعلوماتي او برنامج ناقص عمدا اي يحتوي مجموعة من الثغرات بإمكانه المصنع الاستفادة منها بعد ذلك في الحيازة على معلومات مستعمله ويمكن تعداد هذه الأفعال كما يلي:

- جريمة تصميم أو بحث معطيات مخزنة أو معالجة آليا.
- جريمة تجميع أو توفير لبيانات مخزنة أو معالجة آليا.
- جريمة نشر للمعطيات أو إفشائها.
- جريمة عرقلة سير المعلومات المرسله عن طريق منظومة معلوماتية.
- جريمة حيازة المعطيات المتحصل عليها بواسطة جرائم سابقة.
- جريمة الاتجار في المعطيات.

[1] : الأمر 66- 156 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو 1966 معدل ومتمم بـ قانون رقم 06- 23 مؤرخ في 29 ذي القعدة عام 1427 الموافق لـ 20/12/2006 و القانون 14-01 المؤرخ في فبراير 2014، المتضمن قانون العقوبات.

- جريمة الاحتيال باستعمال بطاقات الائتمان والدفع الالكتروني في قانون العقوبات وقانون الضمان الاجتماعي.^[1]

تتشرك الجرائم الثلاث الواردة سلفا في ركنها المعنوي والذي يتمثل في الغش الذي يقع فيه الضحية والذي يتميز به الجاني في هذه الحالات.

ث- جرائم المعالجة الآلية الماسة بالدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام

تماشيا مع مبادئه قام المشرع الجزائري بتشديد العقوبات في الجرائم الالكترونية التي تستهدف الأمن والدفاع الوطنيين والمؤسسات السيادية في البلاد وذلك لكون كل هذه المؤسسات والادارات تشكل أحد روافد البلاد واي مساس بها هو مساس باستقرار ووجود الدولة في حد ذاتها وهذا ما جاء صراحة في نص المادة (394 مكرر3) من قانون العقوبات الجزائري على أنه: " تضاعف العقوبات المنصوص عليها في هذا القسم ، إذا استهدفت الجريمة الدفاع الوطن أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد"

ج- الجرائم المعلوماتية للشخص المعنوي

إن ترسيخ فكرة تحميل المسؤولية الجزائية للشخص المعنوي والذي اكده المشرع الجزائري في تعديل قانون العقوبات بموجب القانون رقم 06-23 المؤرخ في 2006/12/20^[2] وحدد هذه المسؤولية بدقة في نصوص المواد الواردة في الباب الأول مكرر والمعنون ب:"العقوبات المطبقة على الأشخاص المعنوية" من الكتاب الأول: "العقوبات وتدابير الأمن" من الجزء الأول: " المبادئ العام".

[1] : زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، مرجع سابق، ص 56.

[2] : قانون رقم 06-23 مؤرخ في 29 ذي القعدة عام 1427 الموافق لـ 20 / 12 / 2006 ، يعدل ويتم الامر

66-156 المؤرخ في 18 صفر عام 1386 الموافق لـ 8يونيو 1966 و المتضمن قانون العقوبات.

و على هذا الأساس جاء نص المادة (394 مكرر 4) من قانون العقوبات الجزائري للتأكيد على هذه المسؤولية فيما يخص الشخص المعنوي حين لارتكابه لأحد الجرائم المتعلقة بتكنولوجيا المعلوماتي حيث جاء فيها ما يلي: " يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المحددة للشخص الطبيعي".

ح - جريمة تكوين جمعية أشرار المعلوماتيين لغرض التحضير للجرائم الماسة بأنظمة المعالجة الآلية

نظرا لفوائد التكنولوجيا في تقريب المسافات واختصار الاوقات فقد استفاد منها مجرمو الشبكات المعلوماتية والأنظمة الالكترونية من جانبها الاسود حيث سهل ذلك عليهم الاتفاق وتنسيق الجهود وتوحيدها في شكل جمعيات لارتكاب جرائم من هذا النوع [1]. وقد افرد المشرع الجزائري لهذا التكوين او الاتفاق الاجرامي المتخصص نصا تجريمي خاصا في قانون العقوبات بنصه في المادة (394 مكرر 5) من قانون العقوبات الجزائري على أنه: "كل من شارك في مجموعة أو في تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها".

بقراءة لنص المادة أعلاه يتضح أن المشرع الجزائري كما جرم مختلف الافعال التي سبق ذكرها والتي قد تقع من أشخاص بصفاتهم الفردية لم يتناسى ان ترتكب من طرف جماعات فجرم المشاركة أو الاتفاق الجماعي على التحضير أو الإعداد لارتكاب جريمة أو أكثر من الجرائم الالكترونية.

[1] : زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، مرجع سابق، ص104.

كما أكد على أن العقوبة المقررة للمشاركة والاتفاق المتبوع بأفعال تحضيرية يأخذ عقوبة الجريمة المرتكبة وهو ما جاء في نهاية المادة بنصها على أنه " يعاقب بالعقوبات المقررة للجريمة ذاتها"^[1].

ثانياً: حماية حرمة الحياة الخاصة:

تكريسا لحماية الفرد في الحق في حياة خاصة عدل المشرع الجزائري قانون العقوبات بموجب القانون رقم 06-23 فجاء بنص (المادة 303 مكرر 01 عقوبات) التي جاء فيها: " يعاقب بالحبس من ستة أشهر الى ثلاث سنوات وبغرامة 50.000 دج إلى 300.000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك:

- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه،
- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه.

يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة...."

كما جاء في (المادة 303 مكرر) ونص على الآتي: " يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بان توضع في متناول الجمهور أو الغير أو استخدام لآية وسيلة كانت فالتسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في (303 مكرر)

يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة".

[1] : المادة (394 مكرر 5) من قانون العقوبات الجزائري

من استقراء نص المادتين أعلاه يمكننا عاقب بالعقوبات المنصوص عليها في حالة الافعال المتمثلة في الالتقاط او التسجيل او النقل او وضع في متناول الغير كل ما هو خاص من صور معلومات مكالمات تتميز بالسرية بمفهوم المخالفة يتبين لنا ان نشر او التقاط معلومات او صور او مكالمات غير سرية المحتوى لا يخضع لهذا النص العقابي.

ثالثاً: حماية حرمة رموز الدولة:

في صدد شمول الحماية في النصوص الاولى التي سبق وان اشرنا لها خص المشرع الزائري نص خاص بحماية رئيس الجمهورية وجاء ذلك بالقانون 11-14 المعدل لقانون العقوبات حيث نصت (المادة 144 مكرر عقوبات) على أنه: "يعاقب بغرامة من 100.000 دج إلى 500.000 دج كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأية آلية لبث الصوت والصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى.

تباشر النيابة العامة إجراء المتابعة الجزائية تلقائياً.

و في حالة العود تضاعف الغرامة".

نلاحظ من نص المادة ان المشرع اولى اهمية خاصة لمنصب رئيس الجمهورية لاعتباره أحد رموز الدولة وأعتبر التعدي عليه عن طريق الوسائل التكنولوجية الحديثة معاقب عليه وتضاعف العقوبة في حالة العود وأكد على احقية النيابة العامة في تحريك الدعوى العمومية حتى دون الرجوع للطرف المضرور لان النص يحمي المنصب لا الشخص في حد ذاته.

الفرع الثاني: الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في

القوانين المكملة

من المعروف أن القوانين الجنائية لا تقتصر على قانون العقوبات في الشق الموضوعي للقانون الجنائي بل تتعداه لقوانين أخرى مكملة وهو نفس الشيء بالنسبة لهذا

النوع من الجرائم والمتمثل في الجرائم السيبرية حيث أنه كما تطرق له قانون العقوبات تطرقت له فوانين أخرى تأتي على ذكر أبرزها فيما يلي:

أولاً: الحماية في قانون التأمينات الاجتماعية :

في القانون المتعلق بالتأمينات الاجتماعية رقم 08-01 المؤرخ في 2008/01/23^[1] شدد المشرع في عقوبة المساس الغير مشروع للبطاقة الالكترونية للمؤمن له اجتماعيا، وعاقب كل من يسهل استلام او تسليم هذا النوع من البطاقات وذلك بنص المادة(93 مكرر2) من القانون السالف الذكر.

كما تشمل العقوبة اي اعمال تعديل من حذف او زيادة او تعديل جزئيا كان او كليا للمعلومات الادارية المدرجة في البطاقة او حتى الشروع في ذلك وذلك بنص بالفقرة الثالثة من نص المادة اعلاه.

كما لم يغفل المشرع على تخصيص عقوبة للشخص المعنوي في مثل هذه الحالة وجعل عقوبته ضعف العقوبة المقررة للشخص الطبيعي طبقا لنص المادة (93 مكرر5) من نفس القانون مع امكانية مصادرة الأجهزة والوسائل المستعملة وغلق الاماكن او المحلات التي قد تتم فيها هذه الجريمة.

ثانياً: الحماية في قانون الملكية الادبية والفنية :

قانون الملكية الأدبية والفنية المتعلق بحق المؤلف والحقوق المجاورة الصادر بموجب الأمر رقم 03-05 المؤرخ في 2003/07/23^[2]، حيث وسع هذا القانون قائمة المؤلفات المحمية به بادراج البرامج المعلوماتية ضمن المصنفات الأصلية والتي عبر عنها ب مصنفات قواعد البيانات وبرامج المعلوماتية.

[1] : القانون رقم 08-01 المؤرخ في 2008/01/23 المتعلق بالتأمينات الاجتماعية، الصادر في الجريدة الرسمية، عدد 04، الصادرة في 27 يناير 2008.

[2] : الأمر رقم 03-05 المؤرخ في 2003/07/23 المتعلق بحقوق المؤلف و الحقوق المجاورة الصادر في الجريدة الرسمية، عدد 44، الصادرة في 23 جويلية 2003.

و في نفس الصدد شدد المشرع في العقوبات على المساس بحقوق المؤلفين الخاصة بالمصنفات الرقمية والمعلوماتية المتكفل هذا الاخير بحمايتها.

ثالثاً: الحماية في نصوص التوقيع الالكتروني :

في صدد عصرنة قطاع العدالة الذي جاء في برنامج فخامة رئيس الجمهورية ومواكبة وزارة العدل لتنفيذ هذا المشروع أصدر المشرع قانون رقم 03-15^[1] المتعلق بهذا المجال، ف جاء فيه النص على منظومة معلوماتية مركزية لوزارة العدل والاشهاد على صحة الوثائق الالكترونية وحمايتها كما جاء النص فيه على ارسال الوثائق والاجراءات القضائية والاحكام الجزائية المتعلقة بحماية التوقيع والتصديق الإلكترونيين حيث تعاقب على التزوير او الاستعمال المزور لمثل هذه الوثائق.

رابعاً: الحماية المتصلة بالمواصلات السلكية واللاسلكية:

يعد القانون رقم 03-2000 المتعلق بالبريد والمواصلات السلكية واللاسلكية^[2] من اقدم النصوص القانونية التي وجهة الاشارة لهذا النوع من الجرائم والمتمثل في الجرائم الالكترونية ف جاء فيه على عقوبات جزائية متعلقة بالأشخاص المرخص لهم عملية التزويد بخدمات الاتصالات والأنترنات وكذا العمال الذين ينتهكون السر المهني في هذا المجال. **خمساً: الحماية من خلال قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها :**

يعد القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها^[3] اللبنة الأساس والنقطة الجوهرية في باب

[1] : قانون رقم 03-15 المؤرخ في 01 فيفري 2015 المتعلق بعصرنة العدالة، الجريدة الرسمية، عدد 02، الصادرة في 10 فيفري 2015.

[2] : قانون رقم 03-2000 المؤرخ في 05 غشت 2000 الذي يحدد القواعد المتعلقة بالبريد و المواصلات السلكية و اللاسلكية، الجريدة الرسمية، عدد ، المؤرخة في 06 غشت 2000.

[3] : القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها، مرجع سابق.

مكافحة هذا النوع من الجرائم حيث قام بإرساء قواعد إجرائية جديدة تضمن تحكما جيدا في أساليب مكافحة الجرائم الالكترونية وما يتوافق وخصائصها حيث شمل ما يلي:

1- بنصه على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

2- نصه على القواعد المتعلقة بالاختصاص الإقليمي للقانون الجزائري الجزائري حيث تم التوسع في الاختصاص الإقليمي للسلطة القضائية في متابعة جرائم تمس مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني نظرا لما يمكن لهذه التكنولوجيات الحديثة من القيام به في حالة استغلالها ضد مصالح الدولة ولو في أقاليم دول أخرى من طرف جزائريين أو أجانب، أيضا فإن عالمية استغلال تكنولوجيات الإعلام والاتصال وخاصة الانترنت أدت إلى حذف الحدود الإقليمية وأصبحت الجرائم تمتد عبر عدة أقاليم وتكون من اختصاص القانون الجزائري لأكثر من دولة مما قد ينجر عنه تنازع في الاختصاص أو رفض له، مما قد ينشأ للمجرمين أماكن لا قانون فيها فكان التعاون الدولي في هذا النوع من الجرائم مفيدا وفعال جدا ولا يتأتى ذلك إلا باستعمال الطرق الحديثة للتواصل ما بين السلطات القضائية دون المرور بالطرق الدبلوماسية المعقدة وهو ما تم تشريعه فعلا ضمن هذا القانون.

3- الأمر بتنسيق القوانين الجزائرية العالمية سيؤدي بالتأكيد لإحكام قبضة العدالة على المجرمين في أي دولة يكونون فيها.

4- أيضا فإن لطرق التحري في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ميزات والتي تبناها المشرع في القانون 09-04، فالمراقبة الالكترونية للاتصالات وتفتيش نظم المعلوماتية أعطى لها القانون صفة الشرعية القانونية بتقنياتها وادخالها ضمن الترسانة الإجرائية الجزائرية في القانون الجزائري، تسمح للمتحررين عن الجرائم والمحققين فيها فسحة قانونية لتقديم الأدلة اللازمة لإدانة المتهم أو تبرئته.

5- كما يلعب مقدمو الخدمات بما لديهم من تقنيات متماشية مع تطور التكنولوجيات الحديثة للإعلام والاتصال دورا مهما في مكافحة هذا النوع من الإجرام وتقديم المساعدة التقنية للسلطات المكلفة بالبحث والتحري عن الجرائم المرتكبة بواسطة أو

ضد هذه التكنولوجيات، وأيضاً الالتزام بما قرره المشرع بحفظ للمعطيات المعلوماتية يسمح للمتحرين تتبع الجريمة وحركة المجرمين^[1].

إن صدور القانون 04-09 يعد تحدياً فعلياً للسلطات القضائية وأعاونها (سلطات الضبط القضائي، وكذلك المحامين) من أجل تطبيقه نظراً لخصوصية الإجراءات التي جاء بها، فيكون لزاماً عليها أن تسير التقدم التكنولوجي الحاصل على مستوى الإعلام والاتصال من تكوين جيد يسمح بفهم وتطبيق هذه التقنيات حتى تكون عمليات البحث والتحري أكثر فاعلية، وكذلك الحكم والقضاء في الدعاوى الجزائية المتعلقة بهذه الجرائم مبنيان على فهم جيد للوقائع خاصة إذا كانت مرتبطة بجرائم تقنية محضة.

المطلب الثاني: الجهود العالمية في مواجهة الاجرام الالكتروني

كما سبق وان تطرقنا في المطلب الاول الى ترسانة القوانين التي رسخت من خلالها الدولة الجزائرية مفهوم مجابهة هذا النوع من الجرائم سنتطرق فيما سيأتي الى الجهود العالمية لمواجهه هذه الظاهرة فنترق للجهود الاقليمية في (الفرع الاول) والجهود الدولية مركزينا على جهود هيئة الامم المتحدة في (الفرع الثاني).

الفرع الأول: الجهود الاقليمية

تعتبر دائما الجهود الاقليمية هي اللبنة الاساس للجهود الدولية الاممية وعليه سنتطرق لبعض المنظمات والهيئات الاقليمية ودورها في محاولة التصدي للإجرام الالكتروني:

أولاً: جهود المجلس الأوربي:

اعتمد المجلس الأوربي الطابع الدولي للجرائم الالكترونية منذ عام 1976 وفي سنة 1996 أنشأت اللجنة الأوربية لمشاكل الجريمة (CDPC) لجنة من الخبراء للتعامل مع مشكلة الجريمة السيبرانية، عملت اللجنة بين سنة 1997 و 2000 على الاتفاقية التي

[1] : ضغير يوسف، الجريمة المرتكبة عبر الأنترنت، مرجع سابق، ص 112.

اعتمدها البرلمان الاوربي في الجزى الثاني من جلسته العامة في شهر افريل 2001، وتم التصديق على الاتفاقية من قبل 30 دولة بحلول سنة 2010^[1].

و تعتبر اتفاقية جرائم الانترنت هي المعاهدة الدولية الاولى التي تسعى لمعالجة الجرائم الالكترونية عبر التنسيق بين القوانين الوطنية وقوانين الدول الاخرى ومن اهم اهداف الإتفاقية:

- توحيد عناصر القانون الجزائي المحلي مع الاحكام المتعلقة بالجرائم الالكترونية.
- توفير الاجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة الكترونيا.
- جمع معلومات عن حركة البيانات وعن إمكان وجود تدخل في محتواها.
- تتضمن الاتفاقية المبادئ العامة المتعلقة بالتعاون الدولي في : تسليم المجرمين، المساعدة الدولية المتبادلة، إعطاء المعلومات بصورة آلية وآنية، إنشاء الولاية القضائية على اية جريمة من هذا النوع.^[2]

ثانياً: جهود مجموعة الثمانية:

تعتبر مجموعة الثمانية من ابرز التجمعات الاقليمية رغم بنائها على أساس قوة هذه الدول لا على اساس جغرافي كأغلب الهيئات الاقليمية الاخرى فعملت على ترسيخ مجموعة من المبادئ كان من أبرزها:

- عدم اتاحة ملاذ آمن لمرتكبي هذا النوع من الجرائم.
- التنسيق داخل الدول الاعضاء لملاحقة مرتكبي هذه الجرائم .
- التدريب المشترك للكوادر والاطارات التي تعمل في هذا الاختصاص .
- الاتفاق على عقد اتفاقيات وتجمعات مختلفة مخصصة لهذه النقطة.^[3]

[1] : فاروق خلف ، مداخلة بعنوان، الآليات القانونية لمكافحة الجريمة المعلوماتية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة المنعقد بجامعة بسكرة يومي 16 و 17 نوفمبر 2005، ص7.

[2] : علي حسن محمد الطالبة، التفتيش الجنائي في نظم الحاسوب و الإنترنت، مرجع سابق، ص100.

[3] : موقع مجموعة الثمانية: www.Candainternationalgc.ca/G8

ثالثاً: جهود الإتحاد الإفريقي:

الاتحاد الإفريقي وكأغلب تشريعاته يستمد أسسها من القوانين الامية ف جاء المؤتمر الاستثنائي لوزراء الاتحاد الإفريقي المسؤولين عن تكنولوجيا الاتصال والمعلومات المنعقد في جنوب افريقيا من 02 الى 05 فيفري 2009 بطلب الى مفوضية الاتحاد الإفريقي للقيام بالاشتراك في لجنة الامم المتحدة الاقتصادية لإفريقيا بإعداد اتفاقية حول التشريع القضائي على اساس احتياجات القارة، كما اوصت بضرورة الحماية القانونية للأنظمة المعلوماتية ووافق قادة الاتحاد الإفريقي على هذه الطلبات في يونيو 2014^[1].

رابعاً: الجهود العربية:

تعتبر الدول العربية ولعوامل تاريخية تتعلق اساسا بالاستعمار حيث تعد من أغلبها من آخر الدول التي حازت على الاستقلال مما يجعل ترسانتها القانونية دائماً ما تكون الأخيرة زمنياً مقارنة مع التشريعات الاقليمية والأممية الاخرى فنجد رغم هذا:

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: وافق عليها مجلس وزراء الداخلية والعدل العرب في اجتماعهم المشترك المنعقد بمقر الامانة العالمية لجامعة الدول العربية بالقاهرة بتاريخ 21-12-2010 وتحتوي على (43 مادة) حيث تهدف هذه الاتفاقية إلى تعزيز وتدعيم التعاون العربي في مجال مكافحة جرائم تقنية المعلومات حفاظا على الامن العربي وسلامة مجتمعاتها وافرادها والتعاون الأمني والقضائي في باب ملاحقة والقبض على مجرمي هذا النوع من الجرائم^[2].

وسار مجلس الوزراء العرب بموجب القرار رقم (229) لسنة 1996 في نفس الطريق حيث أنه وباستعراض الباب التاسع الخاص بالتعرض للأشخاص نجد ان الاتفاقية احتوت على فصل خاص بالاعتداء على حقوق الاشخاص الناتجة عن معالجة المعلومات وذلك في (المواد من 461 إلى 464) حيث اشارة المواد السالفة الذكر إلى

[1] : موقع القانون الإفريقي: www.africa-union.org

[2] : الشبكة القانونية العربية: www.arabegalnrt.org

وجوب حماية الحياة الخاصة واسرار الافراد من خطر المعالجة الالية للمعطيات وكيفية جمع المعلومات الاسمية وكيفية الاطلاع عليها، والنص على عقاب من يقوم بفعل الدخول عن طريق الغش الى كامل او جزء من نظام معلوماتي وعرقلة او افساد نظام تشغيل عن اداء وظيفته المعتادة وتغيير المعومات داخل مثل هذه الأنظمة^[1].

الفرع الثاني: الجهود الدولية

إن مكافحة الاجرام الالكتروني لا يتحقق إلا بوجود تعاون دولي متين على المستويين الاجرائي والجنائي، ولهذا تسعى مختلف الهيئات والمنظمات الدولية إلى السعي للعب دورا هام في ابرام الاتفاقيات لترسيخ هذه الافكار فنجد:

أولاً: جهود هيئة الأمم المتحدة:

تبذل هذه الأخيرة جهوداً كبيرة في مجال التصدي للجرائم الالكترونية مؤكدة على وجوب تعزيز العمل المشترك بين أعضاء المنظمة من أجل التعاون للحد من انتشارها وتقادم اثرها وهذا ما برز في مختلف مؤتمرات المنظمة الأممية في اخر مؤتمراتها:

- المؤتمر الثاني عشر لمنظمة الأمم المتحدة من 12-19 أبريل 2010 والمقام بريو دي جانيرو بدولة البرازيل الذي جاء من أجل بناء استراتيجيات شاملة للتحديات العالمية حيث تضمن اليات لمنع الجريمة وتطوير العدالة الجنائية لمواكبتها لها العالم المتغير، وتطرق المؤتمران ثمان نقاط أساسية كان من بينها جرائم الأنترنت حيث دعت لجنة منع الجريمة والعدالة الجنائية إلى عقد اجتماع لفريق من خبراء دولي مفتوح العضوية لدراسة شاملة لمشكلة الجريمة المعلوماتية وتدابير التصدي لها^[2].

[1] : فاروق خلف ، الآليات القانونية لمكافحة الجريمة المعلوماتية، مرجع سابق، ص5.

[2] : المرجع نفسه، ص6.

• المؤتمر الثالث عشر لمنع الجريمة والعدالة الجنائية من 12-19 أبريل 2015 والمقام بدولة قطر^[1] حيث كان الموضوع الرئيسي للمؤتمر "ادماج منع الجريمة والعدالة الجنائية في جدول أعمال الأمم المتحدة الأوسع للتصدي للتحديات الاجتماعية والاقتصادية وتعزيز سيادة القانون على الصعيدين الدولي والوطني، ومشاركة الجمهور".

وأقرت الجمعية العامة في هذا المؤتمر بموجب القرار رقم 67-184 النظر في إنشاء حلقات عمل من بينها تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدي للأشكال المتطورة للجريمة، منها الجريمة الالكترونية^[2].

هذا وكانت هيئة الامم المتحدة قبل هذا قد اقرت مجموعة من القرارات والتوصيات بشأن هذه الظاهرة سنذكر البعض منها^[3]:

- القرار (45-121) سنة 1990، وكذلك نشر دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها في عام 1994.

- القرار رقم (55-63) المؤرخ في 4-12-2000 والقرار رقم (56-121) المؤرخ في 19-12-2001 بشأن مكافحة استخدام نظام المعلومات الادارية الجنائية لتقنية المعلومات حيث دعا هذا القرار الدول الاعضاء الى مواكبة تشريعاتهم الداخلية للتشريع الدولي لمكافحة اساءة استعمال تكنولوجيا المعلومات، على ان تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية.

- القرار رقم(57-239) المؤرخ في 31-01-2003 والقرار رقم (58-199) المؤرخ في 30-01-2004 بشأن إنشاء ثقافة عالمية للأمن السيبراني ودعوة الدول الأعضاء الى التعاون وتعزيز ثقافة الامن السيبراني.

[1] : الصفحة الإلكترونية للمؤتمر :

WWW.moi.gov.qa/UNCCPCJDoha/Arabic/Previous_Congresses.html

[2] : المرجع نفسه الصفحة الإلكترونية للمؤتمر :

WWW.moi.gov.qa/UNCCPCJDoha/Arabic/Previous_Congresses.html مرجع سابق.

[3] : موقع لقرارات الأمم المتحدة: WWW.un.org/arabic/documents/instruments/subj_ar.asp

- قرار لجنة مكافحة المخدرات (48-05) حول تعزيز التعاون الدولي من أجل منع استخدام شبكة الأنترنت لارتكاب الجرائم المتصلة بالمخدرات.

ثانياً: جهود الاتحاد الدولي للاتصالات:

لم تكن هيئة الامم المتحدة المنظمة أو الهيئة الوحيدة التي واكبت التطور في هذا النوع من الجرائم وحاولت تقليصه والحد منه عن طريق المراسيم والقرارات التي سبق وان تطرقنا لها ومن الهيئات الدولية الاخرى التي سارت مسار الهيئة الأممية الاتحاد الدولي للاتصالات الذي وضع استراتيجيات لتطوير نموذج التشريعات السيبرانية يكون قابلاً بتطبيق محلياً ودولياً بالتوازي مع تدابير القانون الوطني والدولي المعمول به واستراتيجيات لتهيئة الأرضية الوطنية والاقليمية المناسبة لوضع الهياكل التنظيمية والسياسية المتعلقة بالجرائم الالكترونية^[1].

[1] : موقع الاتحاد الدولي للاتصالات:

WWW.itu.int/osg/csd/cybersecurity/gca/global-report/index.htm

مما سبق يتضح جليا ان اشكالية تعريف جامع مانع للجريمة الالكترونية من الامور الصعب ادراكها نتيجة تميز هذه الظاهرة الاجرامية بسرعة التطور وواسعة النطاق من حيث التأثير والتأثر هذا من جهة ومن جهة أخرى من الأمور التي تزيد في تعقيد اكتشافها بسهولة هو صفة الجاني في هذا النوع من الجرائم حيث يتميز هذا الاخير بمجموعة من المميزات والخصال التي لا نجد الكثير منها لدى المجرم العادي أو المجرم في الجرائم التقليدية كما يتميز كما شاهدنا حتى في اختلاف اهدافه فمثلا هدف فرض الذات يعتبر مميذا لهذه الجريمة حتى وإن وجدناه يتجسد في بعض الجرائم الأخرى لكنه غير مميز لها.

كما تطرقنا في هذا الفصل الى محاولة المشرع الجزائري وكذا السلطات والهيئات الدولية والإقليمية إلى عملية الحد من هذه الظاهر وذلك بسن مجموعة من القوانين الوضعية المتعلقة بمجابهة هذه الظاهرة التي تستشري يوما بعد يوم.

فتجسد عمل المشرع الجزائري في قانون العقوبات وبعض القوانين الأخرى المكملة له وتجسد عمل الهيئات الدولية إما في شكل مؤتمرات أو اتفاقيات دولية وإعلانات.

الفصل الثاني:
الجوانب القانونية للبحث
والتحري عن الجريمة
الالكترونية

في ظل تعدد الصور الكثيرة و المتعدد للظاهرة الاجرامية منها ظاهرة الإجرام الإلكتروني التي أثارت بعض المشكلات فيما يتعلق بالقانون الجنائي الموضوعي من حيث إمكانية تطبيق نصوصه التقليدية على هذا النوع المستحدث من الجرائم واحترام، فقد أثارت من جهة أخرى العديد من المشكلات في نطاق القانون الجنائي الإجرائي، حيث أن الأصل في وضع النصوص قانون الإجرائية جاء ليحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات كبيرة في إثباتها او التحقيق فيها وجميع الأدلة المتعلقة بها مع خضوعها لمبدأ حرية القاضي الجنائي في الاقتناع وصولاً إلى الحقيقة الموضوعية بشأن الجريمة والمجرم.

وتبدأ المشكلات الإجرائية في مجال الجرائم الإلكترونية بالأشخاص أو الهيئات المسؤولة عن بحثها و جمعها و مدى مواكبة الجرائر و ببعض الدول أو الهيئات الأخرى لهذا الوضع و هذا ما سنتطرق له بأكثر تفصيل في(المبحث الاول) و المعنون بآليات البحث والتحري عن الجرائم الالكترونية، كما تتعداها إلى تعلقها في كثير من الأحيان ببيانات معالجة إلكترونية وكيانات منطقية غير مادية، وبالتالي يصعب من ناحية كشف هذه الجرائم ويستحيل من ناحية أخرى في بعض الأحيان جمع الأدلة بشأنها، ومما يزيد من صعوبة الإجراءات في هذه المجال، فسرعة ودقة تنفيذ الجرائم الإلكترونية وإمكانية محو آثارها وإخفاء الأدلة المتحصل عليها عقب التنفيذ مباشرة كما سبق وان بيناه في الفصل الأول يواجه التفتيش وجمع الادلة صعوبات كثيرة في هذا المجال، وقد يتعلقان ببيانات مخزنة في أنظمة او شبكات إلكترونية موجودة بالداخل أو الخارج وفي هذه الحالة يحتاج الامر إلى تعاون دولي في مجالات البحث والتفتيش والتحقيق وجمع الأدلة.

ويشير التفتيش أو الضبط أو المصادرة في مجال أنظمة الاتصال الإلكترونية ضرورة وضع ضوابط إجرائية لها، تعمل على إقامة التوازن بين الحرية الفردية وحرمة الحياة الخاصة للأفراد، وبين تحقيق الفاعلية المطلوبة للأجهزة الأمنية، وسلطات التحقيق في كشف غموض الجريمة وضبط فاعليتها والتحقيق معهم وتقديمهم للمحكمة خاصة وأن الظاهر أن امكانية تطبيق نفس الشروط و الاجراءات لن يجديا نفعا مع هذه الظاهرة وهذا ما سنتطرق له في (المبحث الثاني) و المعنون بالقواعد الاجرائية في البحث والتحري عن الجرائم الإلكترونية.

المبحث الاول: آليات البحث والتحري عن الجرائم الالكترونية

سننظر في هذا المبحث و الذي يعد جوهرى في موضوع الدراسة الى اهم الاجهزة والهيئات واهم الاجراءات المستحدثة في القانون الجزائري بالأساس مع تطرقنا في بعض الحالات لدول أخرى أو لمنظمات و هيئات دولية حيث سيتحدث (المطلب الاول) على الاجهزة المختصة بالبحث والتحري عن الجرائم الالكترونية و (المطلب الثاني) على تمديد الاختصاص بالبحث والتحري عن الجرائم الالكترونية.

المطلب الأول: الاجهزة المختصة بالبحث والتحري عن الجرائم الالكترونية

سننظر في هذا المطلب والمعنون بالأجهزة المختصة بالبحث والتحري عن الجرائم الالكترونية الى اساسيات هذه العملية البحثية والتي تركز على عنصرين وهما الوسائل المادية والعنصر البشري وعليه سنتحدث في (الفرع الأول) على الاجهزة و(الفرع الثاني) على الاعوان وكيفية ترقية دورهم في هذا المجال

الفرع الأول: الاجهزة المكلفة بالبحث والتحري عن الجرائم الالكترونية

سنتحدث في هذا الفرع الاول على الأجهزة والهيئات سواء كان ذلك على الصعيد الوطني أو الدولي المكفول لها الحق في مقاومة هذا النوع من الاجرام و ادوارها في التقليل من حجم هذا الخطر الدايم

أولاً: على المستوى المحلي(الداخلي):

سنتحدث هنا على الأجهزة والمؤسسات التي استحدثتها الدولة مواكبنا منها للتطور الحاصل في هذا النوع من الاجرام في سبيل القضاء عليه او الحد منه بداية مع تقديم أمثلة على دول أخرى سارت في نفس هذا الاتجاه.

1- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني^[1].

المعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي الجزائر العاصمة مؤسسة عمومية ذات طابع اداري تحت الوصاية المباشرة لوزير الدفاع الوطني أنشئ بالمرسوم رقم 04-183 المؤرخ في 26 جوان 2004 في إطار عصرنة قطاع الدرك الوطني وهو مكلفة بالمهام التالية:

- اجراء الخبرات والفحوص العلمية في اطار التحريات الاولية والتحقيقات القضائية وهذا بغرض اقامة الادلة التي تسمح بالتعرف على مرتكبي الجنايات والجرح.
- ضمان المساعدة العلمية اثناء القيام بالتحريات المعقدة باستخدام المناهج العلمية
- المشاركة في الدراسات والتحليل المتعلقة بالوقاية والتقليل من كل أشكال الإجرام.
- تصميم وانجاز بنوك المعطيات.
- المشاركة في تحديد سياسة جنائية مثلى لمكافحة الاجرام.
- المبادرة وإجراء بحوث متعلقة بالإجرام باللجوء الى التكنولوجيات الدقيقة.
- العمل على ترقية البحوث التطبيقية وأساليب التحريات التي اثبتت فعاليتها في ميادين علمي الاجرام والأدلة الجنائية على الصعيدين الوطني والدولي.
- المشاركة في كل الملتقيات والمحاضرات او الندوات على الصعيدين الوطني والدولي الضرورية لتطوير مستوى مستخدمي المعهد.
- المساهمة في تنظيم دورات الاتقان والتكوين ما بعد التدرج في تخصص العلوم الجنائية.
- تصور وضمان متابعة الابحاث الموكلة الى الغير.

[1] : موقع الدرك الوطني الجزائري <http://www.mdn.dz/>

لتأدية مهامه على اكمل وجه فان المعهد الوطني للأدلة الجنائية وعلم الإجرام يحتوي على العديد من الأقسام والمصالح المختصة نذكر منها:

مصلحة البصمات، مصلحة الوثائق، مصلحة البيئة، قسم الباليستيك، قسم التحليل الدقيق وقسم السيارات.

دائرة الإعلام الآلي والالكترونيك^[1]:

وهي الدائرة الأهم في موضوع دراستنا والتي سنتطرق لها بأكثر استفاضة فهذه الدائرة مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي للعدالة كما تعمل في مساعدة المحققين في أعدة مهامهم.

تسهر أجهزة ومصالح الامن الوطني من قيادة وإطارات على تحسين وتحيين معارفهم حتى تواكب التطورات التكنولوجية الحاصلة لانجاز المهام المنوطة بها في أكمل وجه وتقسم دائرة الاعلام الآلي والالكترونية الى ثلاثة مخابر هم:

أ- مخبر الاعلام الآلي:

حيث يتعهد هذا المخبر بتحليل ومعالجة حوامل المعطيات الرقمية (هواتف، شرائح أقراص...) والعمل على حماية وتحديد للبطاقات الذكية سواء كانت بنكية او متعلقة بالضمان الاجتماعي او بطاقات مهنية اخرى.

يحتوي هذا المخبر على سبع قاعات هي:

- مكتب التوجيه.

- فصيلة الأنظمة المشحونة.

- فصيلة تحليل المعطيات.

- فصيلة الهواتف.

[1]: عز الدين عز الدين، مداخلة بعنوان " الإطار القانوني للوقاية من الجرائم المعلوماتية و مكافحتها" مقدمة للملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافة المنعقد بجامعة بسكرة يومي 16 و 17 نوفمبر 2005.

- فصيلة اقتناء المعطيات.

- قاعة توزيع

- قاعة تخزين

تعمل كل هذه القاعات بقيادة اعوان اكفاء وبتجهيزات عالية من محطات لإجراء الخبرات الاعلامية واجهزة اقتناء الهواتف والحواسيب ومحطات للترميم والصيانة.

ب- مخبر الفيديو:

حيث يتعهد هذا المخبر بإعادة بناء مسرح الجريمة بالشكل ثلاثي الأبعاد (3D) وكذا تحسبن مستوى الصور والفيديوهات بمختلف التقنيات ومقارنة الصور والفيديوهات ومعرفة الحقيقي منها من المزيف او المعدل.

يحتوي هذا المخبر على أربع قاعات هي:

- قاعتان للتحليل.

- قاعة توزيع.

- قاعة تخزين.

تعمل هذه القاعات كغيرها بتجهيزات عالية وحديثة لقراءة الفيديوهات الرقمية والممغنطة وعلى كافة الحوامل وأجهزة لحفظ الفيديوهات والصور عالية الحماية.

ت- مخبر الصوت:

حيث يتعهد هذا المخبر بتحسين نوعية الصوت وذلك عن طريق نزع التشويش وتعديل السرعات ومعرفة ومقارنة الاصوات لتحديد هوية المتكلم كما تعمل على تحديد شرعية هذه التسجيلات ومدى اعتبارها دليلا صحيح من عدمه.

يحتوي هذا المخبر على خمس قاعات، ثلاث منها للتحليل وقاعة توزيع وقاعة للتخزين.

إضافة الى هذه الاقسام والمصالح هناك قسم الحرائق والانفجارات، قسم الطب الشرعي قسم علم الانسان وعلم الاسنان الشرعيين، قسم علم البواعث المؤدية للموت، قسم الادارة مصلحة البيولوجية الشرعية، مصلحة علم الادمان، مصلحة بصمة الاصبع، مصلحة الاشارة.

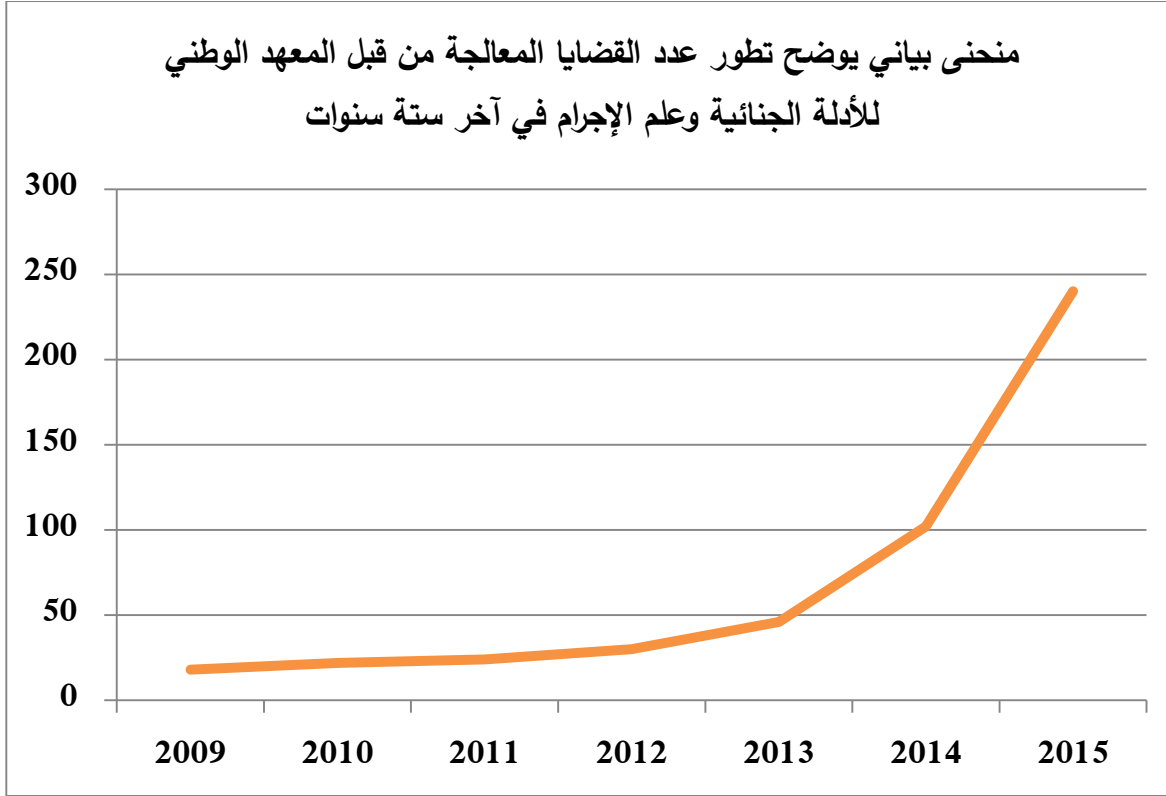
وهكذا وبجمعه للكفاءات والمعدات والوسائل التكنولوجية المتطورة وفي محيط متكيف يعتبر المعهد الوطني للأدلة الجنائية وعلم الإجرام اهم قلاع مكافحة الجريمة وتتبعها على مستوى الجزائر.

التقنية عامل يفرض نفسه اليوم اذا اصبحت وحدات الدرك الوطني مجهزة بوسائل وتقنيات حديثة تساعد على انجاز التحقيقات والتحريات ففي مجال التحقيق في الجرائم الالكترونية مثلا عالجت هذه المصلحة عدد من القضايا في السنوات الاخيرة جاءت كالآتي^[1]:

السنة	القضايا المعالجة
2009	18
2010	22
2011	24
2012	30
2013	46
2014	102
2015	240

جدول يبين تطور عدد القضايا المعالجة من قبل المعهد الوطني للأدلة الجنائية وعلم الإجرام في آخر ستة سنوات.

[1] : عز الدين عز الدين، مداخلة بعنوان " الإطار القانوني للوقاية من الجرائم المعلوماتية و مكافحتها"، مرجع سابق.

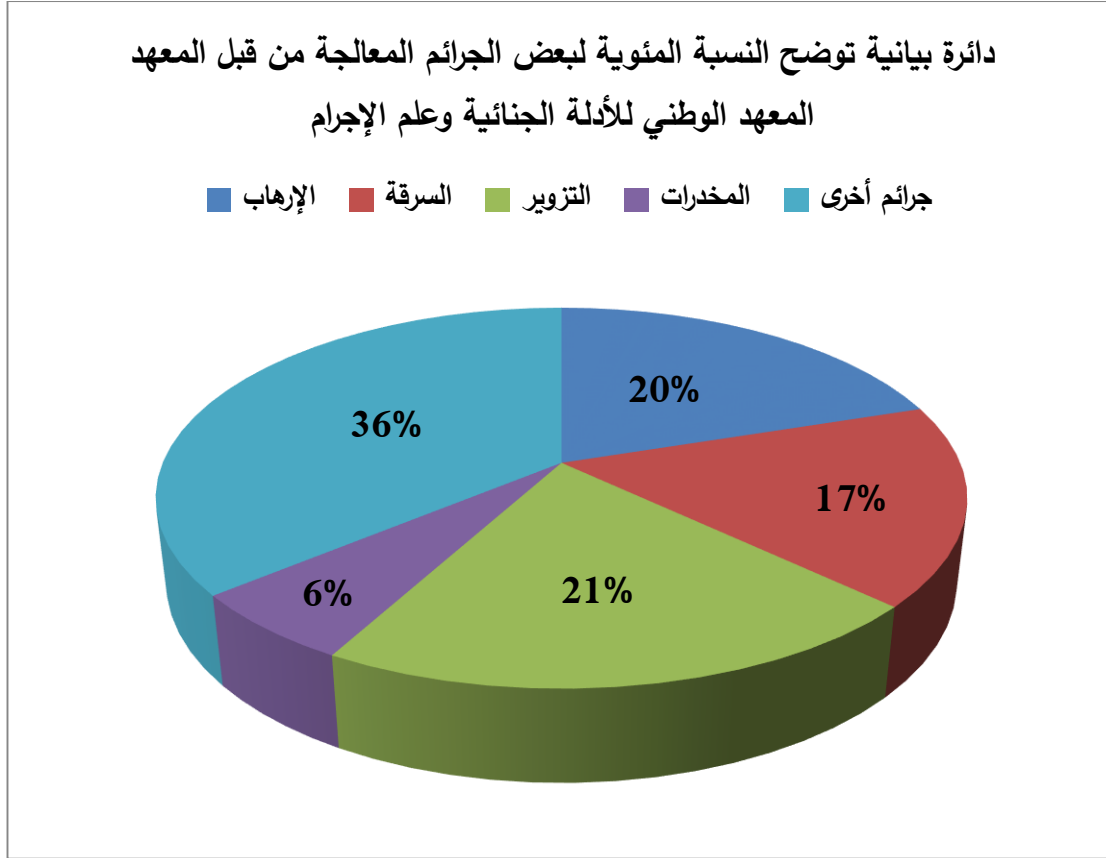


تنوعت واختلقت مجالات الجرائم الالكترونية فبعيدا على الالكترونية المحضة هناك التقليدية والمرتبكة بالتكنولوجيا كالشتم او التهديد بواسطة الوسائل التكنولوجيات الحديثة وجاءت الارقام كالاتي^[1]:

النسبة المئوية %	نوع القضايا
20 %	الإرهاب
17 %	السرقه
21 %	التزوير
6 %	المخدرات
36 %	جرائم أخرى (الإهانة، التحريض على الفسق والدعارة...)

جدول يوضح النسبة المئوية لبعض الجرائم المعالجة من قبل المعهد الوطني للأدلة الجنائية وعلم الإجرام.

[1] : عز الدين عز الدين، مداخلة بعنوان " الإطار القانوني للوقاية من الجرائم المعلوماتية و مكافحتها" ، مرجع سابق.



2- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية

الأمن الوطني.

جاء إنشاء المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني في صدد تدعيم هذه الأخيرة لمصالحها الذي فرضتها عليها عوالم الجريمة فقرر استحداث هذه المصلحة على المستوى المركزي والولائي لمساعدة المخابر الخاصة بالشرطة العلمية المستحدثة هي الاخرة في 2007 بكل من وهران العاصمة وقسنطينة والتي تعمل في مختلف المجالات وبالتحديد في المجال الالكتروني فهي تساهم في :

- تخزين المعلومات والبيانات الرقمية.
- انشاء قواعد للبيانات.
- التعامل السريع والعملي مع الوسائل الالكترونية الحديثة.

و عليه بعد انشاء المصلحة المركزية في 2010 تدعيما للمخابر العلمية وزعت عبر الوطن خلايا لها على النحو التالي:

- 8 خلايا على مستوى ولايات الشرق.
- 8 خلايا على مستوى ولايات الوسط.
- 6 خلايا على مستوى ولايات الغرب.
- واحدة على مستوى ولايات الجنوب.^[1]

تجدر الاشارة ان مصالح المديرية العامة للأمن الوطني ممثلة في شرطة مكافحة الجرائم الالكترونية شهدت ارتفاعا ملحوظ في عدد وتنوع الجرائم الالكترونية التي تعالجها وفيما يلي مقارنة بين ارقام 2014 كاملة والثماني أشهر الأولى من سنة 2016^[2]:

فيما يخص سنة 2014

عدد القضايا	نوع القضايا
75	تمس بأنظمة المعالجة الآلية للمعطيات
59	القذف والمساس بحرمة الحياة الخاصة
28	التهديد والتشهير بالوسائل الالكترونية
26	انتحال هوية الغير
09	نشر صور مخلة بالحياء
03	النصب والاحتيال عن طريق الانترنت
06	الاهانة والسب عن طريق الانترنت
02	الاستعمال غير الشرعي للبطاقات الالكترونية

[1] : حملاوي عبد الرحمان، مداخلة بعنوان " دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية " الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة المنعقد بجامعة بسكرة يومي 16 و 17 نوفمبر 2005، ص 8.

[2] : موقع المديرية العامة للأمن الوطني <http://www.dgsn.dz/>

فيما يخص المتورطين في هذا العدد من القضايا والذي قارب الـ 210 قضية قدمت المصالح ازيد من دليل مادي لتؤكد تورط حوالي 205 مشتبه فيه كان من بينهم 28 امرأة.

فيما يخص الثماني أشهر الأولى لسنة 2016^[1]

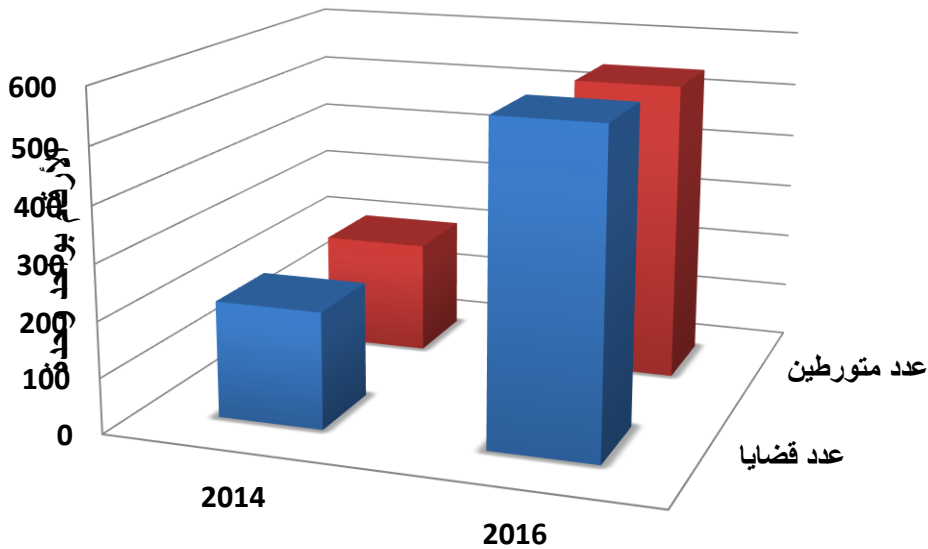
نوع الجريمة	القضايا المسجلة	القضايا المعالجة	عدد المتورطين	النسبة المئوية للقضايا المعالجة
المساس بالأشخاص عبر الأنترنات	430	289	365	68 %
الاعتداء على سلامة الأنظمة المعلوماتية	57	31	39	55 %
جرائم الاحتيال عبر الأنترنات	25	17	32	68 %
التحريض والتطرف عبر الأنترنات	14	14	31	100 %
الجرائم المخلة بالحياء	12	08	22	67 %
جرائم بيع السلع المحضورة عبر الأنترنات	06	05	15	84 %
جرائم مختلفة (نسخ برامج دون حق، قرصنة ...)	23	21	39	92 %
المجموع	567	385	543	68 %

[1] : موقع المديرية العامة للأمن الوطني <http://www.dgsn.dz/>

فيما يلي رسوم بيانية توضح الفرق والتزايد الرهيب لعدد هذه الجرائم والمتورطين

فيها:

مقارنة بين عدد القضايا و المتورطين سنتي 2014 و 2016



	2014	2016
عدد قضايا	210	567
عدد متورطين	205	543

نلاحظ ارتفاع يقارب النصف في كلتي الحالتين في فترة زمنية قصيرة نسبية لم تتعدى سنتين قد تعود هذه الارقام لدخول متدخلات جديدة في هذه الفترة منها دخول تقنيتي الـ (3G و 4G) للسوق الجزائرية والزيادة المعتمدة لعدد مستخدمي هذا النوع من الانترنت بالإضافة الى الانترنت الكلاسيكية، هذا الشيء الذي يزيد العبء على هذه المؤسسات لمكافحة هذا النوع من الجرائم.

وفي تبيان منا لدور الخلايا الولائية المتواجدة على مستوى مديريات الأمن نعطي المثال بخلية مكافحة الجرائم المعلوماتية و الالكترونية على مستوى أمن ولاية الطارف

حيث شهدت هذه الولاية لوحدها في الفترة ما بين شهر جانفي وأكتوبر سنة 2016 أزيد من 60 قضية خاصة بالجرائم الالكترونية تمكنت السلطات المعنية بجل 21 من أصل 61 أي بمعدل يقارب الـ 30 % تم من خلال هذه القضايا تسجيل تورط 20 شخصاً منعم 8 إناث^[1].

3- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

هذه الهيئة المشكلّة والمنظمة بالمرسوم الرئاسي 15-261 لسنة 2015^[2] هذي الهيئة التي جاءت استجابة لما جاء في القانون 09-04 حيث اعتبرها سلطة ادارية مستقلة تتمتع بالشخصية المعنوية تخضع للسيد وزير العدل وتقع بالجزائر العاصمة(المواد^[3]2 و^[4]3).

تشكل الهيئة من:

- لجنة مديرة .
- مديرية عامة.
- مديرية للمراقبة الوقائية واليقظة الالكترونية.
- مديرية التنسيق التقني.
- مركز العمليات التقنية.

[1] : نشرت في جريدة المساء و للتأكد من صحة الأرقام اتصلنا بمحرر الخبر الذي أكد أن الأرقام من خلية الإعلام بالمديرية المذكورة للإطلاع على العدد قم بزيارة موقع الجريدة www.el-massa.com .

[2] : المرسوم الرئاسي رقم 15-261 المؤرخ في 14 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015 يحدد تشكيل و تنظيم و كفاءات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها الصادر في الجريدة الرسمية عدد 53، المؤرخة في 24 ذو الحجة 1436 الموافق 8 أكتوبر لسنة 2015، ص ص 16-21.

[3] : المادة 2: "الهيئة سلطة ادارية مستقلة تتمتع بالشخصية المعنوية و الاستقلال المادي، توضع لدى الوزير المكلف بالعدل".

[4] : المادة 3: " يحدد مقر الهيئة بمدينة الجزائر".

- ملحقات جهوية (المادة 6)

عمل على مساعدة كل الجهات المكلفة بي مكافحة هذا النوع من الاجرام وهي المخولة حصرا بمراقبة الاتصالات الالكترونية بموجب (المادة 41)^[1].

كما تقوم هذه الهيئة بما يلي:

- اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال .

- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحته.

- مساعدة السلطات القضائية و مصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدها بالمعلومات و الخبرات القضائية.

- ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية و التخريبية و الماسة بأمن الدولة و ذلك تحت سلطة قاضي مختص و ذلك كاختصاص حصري.

- تطوير التعاون مع المؤسسات و الهيئات الوطنية المعنية بالجرائم المعلوماتية.

- تجميع و تسجيل و حفظ المعطيات الرقمية و تحديد مسارها من أجل استعمالها في الإجراءات القضائية.

- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا المعلومات

- تنفيذ الطلبات الصادرة عن الدول الأجنبية و تطوير سبل التعاون والتبادل معها.

- المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

و في هذا الصدد تجدر بنا التطرق لما قامه به دول أخرى في قارات العالم الخمسة لمعرفة مدى مواكبة التعديلات التي قامه بها السلطات الجزائرية في هذا المجال فنجد

[1] : المادة 41: " تمارس الهيئة الحصرية في مجال مراقبة الاتصالات الالكترونية تحت مراقبة قض مختص، باستثناء الحالات المنصوص عليها في قانون الاجراءات الجزائية...."

مجموعة من الأمثلة التي تعطي تصورا كاملا لدور مثل هذه الأجهزة في هذا المجال الحساس حيث نجد من الدول والمنظمات التي سبقتنا في تقنين ومجابهة هذا النوع من الاجرام:

4-الولايات المتحدة الامريكية

عملت الولايات المتحدة الأمريكية وبكونها من الدول الرائدة في مجال تكنولوجيا المعلومات الاتصال وكذلك كل ما ينتج عنها من سلبيات والمتمثلة أساسا في الجرائم الالكترونية على انشاء مراكز وأقسام خاصة بهذا النوع من الجرائم نأتي على ذكرها:

-مركز تلقي شكاوى جرائم الانترنت **internrt Crime complaint center**.

-شرطة الواب **wep Police**

-نيابة جرائم الحاسوب والاتصالات **coordinattor Computer and**

Télécommunication [1].

و توجد اجهزة تابعة لقم العدالة تضم في طياتها مجموعة من الخبراء في عالم الانظمة الرقمية[2].

5-في فرنسا

قامت فرنسا كغيرها من الدول الكبرى بمواكبة التطورات التكنولوجية ومحاولة منها للتصدي لهذي الظواهر أنشأت ما يلي:

-القسم الوطني لقمع جرائم المساس بالأموال والأشخاص في 1997.

[1] : نعيم سعيداني ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة

الماجستير في العلوم الجنائية، جامعة الحاج لخضر، باتنة،2013، ص ص 104-105.

[2] : نبيلة هبة محمد هروال، الجوانب الاجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، الطبعة الاولى، دار

الفكر الجامعي، الاسكندرية، 2007، ص 108.

-المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعطيات والاتصالات في
15-05-2000^[1].

6: في مصر

مصر من الدول العربية التي كانت سباقة رفقة الامارات العربية المتحدة لمعالجة هذه الظاهرة فأنشأت مجموعة من الأجهزة والإدارات لمجابهة الجريمة الإلكترونية فكانت من بينها:

- ادارة مكافحة جرائم الحسابات وشبكات المعلومات سنة 2002.
- قسم مكافحة جرائم الحاسوب وشبكات المعلومات^[2].

ثانيا: على المستوى الدولي:

1-الأنتربول:

يعد جهاز الانتربول من أهم الأجهزة على المستوى الدولي لمكافحة الإجرام بصفة عامة وا الجرائم الإلكترونية بصفة خاصة، وتهدف هذه المنظمة الدولية إلى تشجيع التعاون بين أجهزة الشرطة في مختلف الدول على نحو فعال من أجل مكافحة الجريمة ذات الطابع العالمي بما في ذلك الإجرام المرتبط بالتكنولوجيا المعلومات والاتصالات.

حيث تباشر هذه الأخيرة وظيفتين رئيسيتين في مجال مكافحة الجرائم فتتمثل اعمالها في تجميع كافة البيانات و المعلومات المتعلقة بالجريمة و المجرم من خلال عمل المكاتب المركزية الوطنية للشرطة الجنائية الدولية المتواجدة على إقليم الدول الأعضاء والتعاون في ملاحقة المجرمين وتسليمهم إلى الدول التي تطلبهم، وهي بذلك متخصصة

[1] : نعيم سعيداني ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سابق، ص 105.

[2] : المرجع نفسه، ص 106.

بمكافحة الجرائم ذات الطابع الدولي وخصوصا جرائم الاستغلال الجنسي للأطفال عبر شبكة الانترنت^[1].

وفي سبيل تجسيد ذلك نظمت الأنتربول شهر فيفري من سنة 2005 المؤتمر الثاني للتنسيق بشأن جرائم الاحتيال المعلوماتي، و التي دعى إليها بعد وقوع 2000 شخص ضحية من مجموع 60 دولة مختلفة قدرت خسائرهم بحوالي 166 مليون أورو، وقد ألقى القبض على المتهمين بشأنها في ديسمبر 2004 في اسبانيا بعد تقدم النائب العام الألماني بطلب المساعدة الدولية من قبل الأنتربول، وفي سبيل مواصلة الجهود بشأن ذلك وتأكيدا لما دعى إليه مؤتمر القاهرة نظم الأنتربول شهر سبتمبر 2005 بمدينة ليون الفرنسية المؤتمر الدولي الأول لتكوين المحققين في الجرائم المعلوماتية و الذي عرف^[2]. و يمكننا هنا الحديث بالمقارنة مع ما حدث هذا شهر - شهر ماي 2017- على الهجمات الالكترونية الاخيرة التي ضربت العالم حيث شن قراصنة حاسوب هجوما واسعا على مستوى العالم استهدف عددا من المؤسسات والقطاعات وتسبب في تعطيل أنظمتها. وقالت وسائل إعلام روسية وبريطانية إن القراصنة تسببوا في الإطاحة بالنظام الصحي الوطني في بريطانيا واختراق شركة الاتصالات الإسبانية تليفونيكا وشركة الهاتف الخليوي في روسيا "ميجان فون" وغيرها من المؤسسات حول العالم^[3].

2- الأوروبول:

قدم الطرح المتعلق بإنشاء الأوروبول أول مرة أمام المجلس الأوربي من قبل ألمانيا سنة 1991، بمناسبة انعقاد مؤتمر لوكسمبورج، غير أنه تجسد فعليا سنة 1995، وذلك

[1] : حسين ربيعين مرجع سابق، ص 149.

[2] : Mohamed Chawki, Combattre la cybercriminalité, Edition de saint Amans, Paris

France, Mai 2009, p 343.

[3] : الصحافة العربية و العالمية تحدثة مطولا عن هذه الاحداث منها لتفاصيل أكثر عن الاحداث زر موقع

http://arabi21.com/ أو <http://www.almanar.com.lb/2054028> .

بعد مصادقة دول المجلس الأوروبي على اتفاقية ماستريخت في 1995/07/29 ليتخذ من لاهاي (هولندا) مقرا له^[1].

يختص الأوروبيون وفي مجال مكافحة الجرائم المعلوماتية، بكل أشكال الإجرام التي ترتكب بواسطة التكنولوجيا الرقمية، تكون إحدى المنظمات الإجرامية الناشطة على الإقليم الأوروبي طرفا فيها ولذلك يرصد الأوروبيون هيكلا بشريا يضم أكثر من 600 شخص بلاهاي يضمون التنسيق و الدعم للمحققين الميدانيين سواء تعلق الأمر بدعمهم بالبيانات اللازمة أو التقنيات في مجال التحقيق^[2].

الأوروبيون هيئة مختصة بالبحث و التحقيق في الجرائم المعلوماتية خصوصا تلك المتعلقة بالاستغلال الجنسي للأطفال و الإرهاب الإلكتروني، وهو يهدف من خلال نشاطه إلى تسهيل الإجراءات أمام رجال الشرطة لأجل التحري بشأن الجرائم المتعلقة ببلدانهم، من خلال مدهم بمختلف النشرات الأمنية و التقارير حول هوية المتهمين و الأدلة المحصلة خارج الحدود الإقليمية لمجال اختصاصهم^[3].

الفرع الثاني: الاشخاص المختصين بالبحث والتحري عن الجرائم الالكترونية ومميزاتهم

من المعروف أن سلطات التحقيق الابتدائي في الجزائر والمخول لها سلطات البحث والتحري عن الجرائم وتحرير محاضر عنها هي الضبطية القضائية ممثلا في مختلف فروعها وأشكالها كأصحاب اختصاص اصيل وقد يحقق قاض التحقيق اذا راء واجب لذلك او حتى قاضي الحكم بطرقه الخاصة والمشكلة الأساسية التي تواجه المحققين في جرائم نظم المعلومات هي خلفية المحقق نفسه فمخصص الحاسب الآلي قد تكون لديه

[1] : Céline Renard Castétes, Cours de Droit de l'internet, Edition 2010, Edition Lex tenso, Paris, France, 2010, P564.

[2] : Myriam Quéméner, Yves Charpenel, La Cybercriminalité, Edition Economica, Paris France, 2010, p209.

[3]: Myriam Quéméner, Joël Ferry, Cybercriminalité Défi mondial, Op.cit P 237.

المعرفة التقنية اللازمة ولكنه ليس مدرب على تفهم دوافع الجريمة وجمع الأدلة لتقديم المتهم للمحاكمة.

عليه أن يكون المحقق ملم بجميع جوانب التحقيق والجريمة امر ضروري لحسن سير الاجراءات والتطبيق الامثل لنصوص القانون وهذا بدوره ما سيرسخ العدالة

ففي كثير من الحالات نجد أن متخصص الحاسب يعتقد أن لديه الدليل الحاسم حول جريمة الكترونية ما ولكن من الناحية القانونية يتبين 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 المجرمين الالكترونيين في هذا النوع من الجرائم^[1].

أولاً: الخصائص الفنية

ان من اشكاليات الحصول على الدليل الرقمي هو افتقار ضابط الشرطة القضائية للتأهيل الكافي في الميدان التقني قد يفضي إلى إتلاف وتدمير الدليل، على اعتبار أن جهله بأساليب ارتكاب الجريمة المعلوماتية يجعله يقع في كثير من الأحيان في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية أو تدميرها مثل إتلاف محتويات الأقراص الممغنطة وأوعية المعلومات التي تحزن فيها البيانات، وبالتالي فإن الكشف عن هذه الجرائم يقتضي أن تكون الأجهزة المعنية على دراية كافية بأساسيات التعامل مع هذه الجرائم وكيفية تقصيها وعليه يجب ان تتوفر مجموعة من الشروط في الضابط او المحقق الالكتروني وهو ما سنتحدث عنه فيما سيأتي:

[1] : جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجية الحديثة، دار النهضة العربية، القاهرة 2002 ،

- الدراية الفنية:

إن الصراع في ايجاد الدليل الرقمي لا يقوم بين المحقق والاجهزة او المعطيات بل هو صراع بين عقل المحقق وعقل الجاني وعليه يتوجب على المحقق معرفة آلية عمل تشكيلات الحاسوب والأنترنت وطرق حفظ وتخزين البيانات [1] وتبرز أهمية فهم المحقق لهذه المبادئ في كونها ضرورية لتصور كيفية ارتكاب الفعل الإجرامي في العالم الافتراضي من اختراق للشبكات واعتراض حزم البيانات أثناء انتقالها عبر الشبكة والتجسس عليها وتحويلها عن مسارها، كما أنها تعطي للمحقق تصور جيدا عن مدى إمكانية متابعة مصدر الاعتداء على الشبكة والمعوقات التي تحول دون ذلك هذا كله لن يتمكن منه المحقق إذا لم يكن شخص ذو خبرة فنية في هذا المجال.

- إتباع الإجراءات الصحيحة والمشروعة :

إن صحة الاجراءات كما هي عامل أساسي على المحققين الدراية به فهو اكثر اهمية بالنسبة للجريمة الالكترونية من أجل سرعة المحافظة على الأدلة الإلكترونية التي تدل على وقوع الجريمة من عدمه، ونسبتها لشخص الجاني وتخزينها في الأقراص المعدة لذلك ومنع حذفها والحرص على عدم تعريض سائط التخزين كالأقراص المرنة أو المدمجة لأية مؤثرات خارجية كالقوى حتى لا تتلف محتوياته.

ثانياً: التأهيل والتدريب

إن طبيعة الجرائم الالكترونية وصلتها بالحاسب الآلي تقتضي معرفة متميزة بنظم الحواسيب، وكيفية تشغيلها ووسائل إساءة استعمالها من قبل مستخدميها، ولن تتحقق هذه المعرفة التقنية إلا بتدريب القائمين على أعمال التحري، والمباشرين للتحقيق في مجال

[1] : تم حفظ البيانات الرقمية داخل الحاسوب على شكل مجموعات أو كتل من البيانات تمثل وحدة واحدة تسمى الملفات ويتميز كل ملف ببينة وصيغة خاصة تميزه عن غيره، وغالبا ما ترتبط صيغة بنوع محدد من المحتوى كأن يحتوي الملف على بيانات تمثل صورا أو أصواتا أو مستندا خطيا منسق أو غير منسق.

الجرائم الإلكترونية إلى الحد الذي دعا البعض إلى القول بضرورة وجود شرطة متخصصة ونيابة متخصصة في هذا المجال.

ويجب أن يشمل التدريب على كيفية تشغيل الحواسيب، بعد التعرف على أنواعها ونظمها المختلفة، لاكتساب مهارات ومعارف تتعلق ببرمجيتها، والمعالجة الإلكترونية للبيانات والجرائم التي تقع عليها، فضلا عن أمن الحواسيب، ووسائل إختراقها، مع دراسة حالات تطبيقه لجرائم وقعت سلفا، وكيف تم مواجهتها.

وفي كثير من بلدان العالم تعقد الدورات التدريبية المتخصصة لرجال الشرطة وأعضاء النيابة العامة، سواء في داخل الوطن أو خارجه أو في مراكز تابعة لوزارة الداخلية أو في المراكز المتخصصة التابعة لوزارة العدل، كما هو الحال في امريكا وانجلترا، وكندا وهو ما يُعمل به حاليا في الجزائر على مستوى مختلف الأجهزة المختصة في هذا النوع من القضايا ومن امثلتها ما تقوم به المديرية العامة للأمن الوطني في هذا الباب حيث سطرت برنامج لتكوين الملازمين الأوائل للشرطة يتطرق إلى موضوع الجرائم الإلكترونية منذ 2003 على النحو الموضح في الجدول^[1] أدناه:

[1] : عبد الرحمان حملاوي ، مداخلة بعنوان " دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية " مرجع سابق، ص7.

التكوين بالداخل بمشاركة كفاءات وطنية		التكوين بالخارج		التكوين بالداخل بمشاركة خبراء أجانب		السنوات
الضباط المستفيدين	عدد الدورات	الضباط المستفيدين	عدد الدورات	الضباط المستفيدين	عدد الدورات	
/	/	/	/	22	01	2003
/	/	03	01	/	/	2004
/	04	02	/	/	/	2005
/	/	/	/	/	/	2006
/	/	/	/	66	03	2007
/	/	/	/	20	01	2008
/	/	02	01	20	01	2009
39	01	/	/	/	/	2010
39	01	09	04	128	06	المجموع

قراءة في الجدول أعلاه:

-من حيث عدد الدورات: يلاحظ أنه وخلال السبعة (7) سنوات التي تقع حيز الدراسة نجد أن عدد الدورات بمختلف الصيغ لم يتجاوز 11 دورة أي بمعدل 1.5 في السنة الواحدة وهذا العدد يعد منخفضا جدا مقارنة بالاتساع الجغرافي للجزائر وانشار اعوان الامن الوطني على كامل هذه المساحة.

-من حيث عدد الضباط المستفيدين من التكوين: وبتابع نفس الطريقة نجد أن عدد الضباط المستفيدين من التكوين في مدة خلال السبعة (7) سنوات هو أقل من 180 ضابط أي ما يعادل حوالي 25 ضابط في السنة الواحدة وهذا الرقم يظهر رقم معقول للوهلة الأولى إلا انه حقيقتا يعد قليلا مع تقشي ظاهرة هذا النوع من الجرائم وتطورها السريع والملحوظ مع سهولة استخدام التكنولوجيا وبساطتها.

-من حيث تنوع التكوين: نلاحظ تركيز التكوين في الجزائر على التكوين بالداخل بمشاركة خبراء أجانب بمعدل 06 دورات وبمشاركة قرابة ال 130 ضابط في حين تقل

هذه الاعداد في الأنماط الأخرى للتكوين حيث نجد أنه بين كل من نمط التكوين بالخارج ونمط التكوين بالداخل بمشاركة كفاءات وطنية الاعداد تصل إلى 05 دورات وحوالي 50 ضابط مستفيد من هذه الانماط .

-من حيث الاستمرارية والثبات: حيث نلاحظ عدم الثبات في برامج التكوين في الانماط الثلاثة من سنة الى اخرى وغيابها كليا سنة 2006.

و بالتطرق لأحد هذه الدورات وتحديدًا الدورة المتعلقة بسنة 2010 والتي واكبتها انشاء المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني حيث كانت الدورة في مكافحة الجرائم المعلوماتية بمعهد الأدلة الجنائية بسحاولة غرب العاصمة حيث كانت هذه الدورة تهدف إلى تعزيز قدرات ومعارف محققي الشرطة في مجال مكافحة الجريمة بأشكالها ومواكبة تطورها وتحسين المحققين علميا في مجال معالجة الجرائم المعلوماتية [1].

المطلب الثاني : تمديد الاختصاص بالبحث والتحري عن الجرائم الالكترونية

يتميز كل من وكلاء الجمهورية بصفتهم ممثلين للنيابة العامة وضباط الشرطة القضائية بعملهم المشترك في مجال التصدي للجرائم بمختلف أنواعها وفي كامل الأوقات والظروف إلى أن هذا الاختصاص الموكل لهم مقيد بشروط مكانية ووظيفية معينة حيث يثار التساؤل هنا حوا لذا كانت تلك الشروط نفسها التي تحكم عملهم في صدد مجابتهم لهذا النوع المستحدث من الجرائم التي لا تعرف مكان وزمان ثابت وللإجابة على هذه النقطة سنتطرق في (الفرع الأول) لى تمديد الاختصاص الاقليمي لوكيل الجمهورية وفي (الفرع الثاني) سنتطرق لتمديد الاختصاص الاقليمي لضباط الشرطة القضائية

[1] : جريدة النهار، ليوم 23-01-2010 .

الفرع الأول: تمديد الاختصاص الاقليمي لوكيل الجمهورية

إن الحديث على اختصاص النيابة العامة وعلى قضاة التحقيق في ما يخص الجرائم الإلكترونية يلزمنا حتما بالمرور على اختصاصاتها الاصلية في باقي الجرائم حيث انه كأصل عام يختص وكيل الجمهورية اقليميا في الحالات الآتية:

- مكان وقوع الجريمة .
- محل اقامة احد الاشخاص المشتبه بهم في وقوع الجريمة.
- المكان الذي تم في دائرته القبض على أحد الأشخاص المساهمين في الجريمة أو لسبب آخر .

هذا ما نصت عليه المادة 37 من قانون الاجراءات الجزائية في فقرتها الاولى.

غير أنه جاء في فقرتها الثانية إمكانية تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم اخرى في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلى جانب جرائم المخدرات والجرائم العابرة للحدود الوطنية وجرائم تبييض الاموال والجرائم الإرهابية والجرائم المتعلقة بالتشريع الخاص بالصرف.

وتأكد هذا بعد صدور المرسوم التنفيذي 06-348 المؤرخ في 05 أكتوبر 2006 [1] المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق و المعدل و المتمم بالمرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016 و الصادر في الجريدة الرسمية رقم 62 إلى النطاق المحدد بما يلي :

[1] : المرسوم التنفيذي 06-348 المؤرخ في 12 رمضان الموافق 05 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية وقضاة التحقيق، صادر في الجريدة الرسمية رقم 63 المؤرخة في 15 رمضان الموافق 8 أكتوبر 2006، المعدل و المتمم بالمرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016 والصادر في الجريدة الرسمية رقم 62.

المادة 2:

محكمة سيدي محمد بالجزائر العاصمة تشمل جميع محاكم المجالس القضائية الآتية		
الأغواط	الشلف	الجزائر
تيزي وزو	البويرة	البليدة
المسيلة	المدية	الجلفة
عين الدفلى	تيارة	بومرداس

المادة 3:

محكمة قسنطينة تشمل جميع محاكم المجالس القضائية الآتية		
سكيكدة	الطارف	قسنطينة
تبسة	ميلة	بجاية
باتنة	سطيف	جيجل
برج بوعريرج	قالمة	عنابة
خنشلة	أم البواقي	سوق اهراس

المادة 4:

محكمة ورقلة تشمل جميع محاكم المجالس القضائية الآتية		
تامنغاست	أدرار	ورقلة
غرداية و بسكرة	الوادي	إليزي

المادة 5:

محكمة وهران تشمل جميع محاكم المجالس القضائية الآتية		
وهران	بشار	تلمسان
تيارت	سعيدة	سيدي بالعباس
مستغانم	معسكر	البيض
تيسيمسيلات	النعامة	عين تيموشنت
غليزان	تندوف	/

ويعود الاختصاص للبت في أحقية الاختصاص إلى رئيس مجلس القضاء الذي تقع في دائرة اختصاصه المحكمة التي تمتد اختصاصها أي رئيس مجلس قضاء الجزائر ورقلة، قسنطينة، وهران وهي التي يصطلح عليها بالأقطاب القضائية. وتخول للنيابة العامة في مجال البحث والتحري عن الجريمة الإلكترونية مجموعة من الصلاحيات منها :

- مباشرة اجراءات المتابعة الجزائية فيما يخص (المواد 144 مكرر، 144 مكرر2 عقوبات) المتعلقةن بالإساءة إلى رئيس الجمهورية والرسول الأعظم صلى الله عليه وسلم وبقية الانبياء أو الاستهزاء بالمعلوم من الدين بالضرورة أو بأي شعيرة من شعائر المسلمين.

- كما تمنح النيابة العامة الاذن بالتفتيش او القيام بالمراسلات وتسجيل الاصوات او التقاط الصور كما هو منصوص عليه(المادة 65 مكرر 5 من قانون الاجراءات الجزائية)

الفرع الثاني: تمديد الاختصاص الاقليمي لضباط الشرطة القضائية

تجدر الاشارة في بادى الأمر أن المشرع الجزائري وبموجب الامر 15-02 المعدل والمتمم لقانون الاجراءات الجزائية نص على استحداث فئة جديد في الضبطية القضائية وهم الموظفون التابعون للأسلاك الخاصة للمراقبة ومن بينهم الجرائم الالكترونية.

و هذا ما تأكد عن طريق المرسوم الرئاسي رقم 15-261^[1] الذي نص في (المادة 11) منه على أنه: " تكلف مديرية المراقبة والوقاية واليقظة الإلكترونية على الخصوص بما يأتي:...

-إرسال المعلومات المحصل عليها من خلال المراقبة الوقائية إلى السلطات القضائية ومصالح الشرطة القضائية المختصة....
-تزويد السلطات القضائية ومصالح الشرطة القضائية تلقائيا أو بناء على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال."

الأصل العام أن الضبطية القضائية ممثلتا في رجال الضبط القضائي توكل بعملية البحث والتحري عن الجرائم ومرتكبها بشرط احترام النطاق الاقليمي والمحدد بدائرة الاختصاص الوظيفي، مع مراعاة صفة الضابط ونوع الجريمة واحترام إجراءات التمديد في حالة وجوده، وقد يكون هذا التمديد إما إلى دائرة المجلس وهذا ما جاء النص عليه في (المادة 16 الفقرة 2 قانون اجراءات جزائية) حيث يجب اخطار وكيل الجمهورية في حالة الاستعجال، أو كامل التراب الوطني في حالة توفر وهو ما اشارة لخ نفس المادة في الفقرة الثالثة منها^[2].

ومن الشروط التي يجب توفرها حتى يتمتع ضباط الشرطة بالاختصاص الوطني ما يلي:

[1] : المرسوم الرئاسي رقم 15-261 لسنة 2015 المتعلق بتشكيل و تنظيم و كفاءات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها، مرجع سابق، ص18.

[2] : المادة 16 فقرة 3 : " و يجوز لهم أيضا في حالة الاستعجال، ان يباشروا مهمتهم في كافة الاقليم الوطني إذا طلب منهم اداء ذلك من القاضي المختص قانونا، و يجب أن يساعدهم ضابط الشرطة القضائية الذي يمارس وظائفه في المجموعة السكنية المعنية "

-كون الجرائم واحد من الجرائم التي تنص عليها (المادة 16 فقرة 7 اجراءات جزائية)^[1].

-العمل تحت إشراف النائب العام لدى المجلس المختص.

-إعلام وكيل الجمهورية المختص.

وفي العديد من الحالات يمتد اختصاصهم إلى مراقبة الاشخاص متى توفرت ضدهم مبررات مقبولة في الجرائم المذكورة في المادة 16 الفقرة 7 سالفه الذكر ومن بين هذه الحالات ما يتعلق بالمجرمين الإلكترونيين، باعتبار ان الشكل الجديد للجرائم المنظمة تجد مجالا خصبا لإجرامهم في الفضاء الالكتروني^[2].

[1] : المادة 16 فقرة 7 : " غير أنه فيما يتعلف ببحث ومعيانة جرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم تبيض الأموال و الإرهاب و جرائم المتعلقة بالتشريع الخاص بالصرف يمتد إختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني".

[2] : حاتم عبد الرحمان منصور الشحات، الحماية الجنائية للثقة في المستند الإلكتروني، مجلة الحقوق، العدد الاول، الكويت، 2006، ص 141.

المبحث الثاني: القواعد الاجرائية في البحث والتحري عن الجرائم الالكترونية

في هذا المبحث سنتطرق الى أهم الطرق و الأساليب الإجرائية ومدى تطابقها مع الجرائم الالكترونية و عوائقها التي قد تعرقل دور الحصول على الدليل الالكتروني الصحيح من طرف الهيئات والأشخاص المسؤولين على ذلك حيث سنتحدث في (المطلب الأول) على اساليب البحث والتحري الخاصة بالجرائم الالكترونية و في (المطلب الثاني) على معوقات البحث والتحري عن الجريمة الالكترونية.

المطلب الأول: اساليب البحث والتحري الخاصة بالجرائم الالكترونية

لقد سن المشرع الجزائري مجموعة من أساليب التحري الخاصة كما أن هناك أساليب بحث تقليدية تبلورت في اشكال جديدة لإمكانية التأقلم مع ظواهر اجرامية حديثة كالجريمة الالكترونية وعليه سنتطرق في (الفرع الاول) الى التفتيش في مجال الجرائم الالكترونية وفي (الفرع الثاني) سنتطرق الى تجميع واعتراض المراسلات الالكترونية

الفرع الأول: التفتيش في مجال الجرائم الالكترونية

يثور التساؤل في صدد تحدثنا على التفتيش في مجال الجرائم الالكترونية على امكانية تطبيق امكانية تطبيق القواعد العامة والأساسية للتفتيش على هذا النوع من الجرائم.

أولاً: تعريف التفتيش

لم يورد المشرع الجزائري تعريفا خاصا ودقيقا للتفتيش بقدر ما أعتبره إجراء من إجراءات التحقيق يهدف الى الكشف عن الحقيقة وقد ورد النص عليه بموجب الدستور

الجزائري في نص (المادة 47)^[1] بقولها: فلا تفتيش إلا بمقتضى القانون وفي اطار احترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة". وجاء في قانون الاجراءات الجزائية على النص عليه وقسم نظريا الى تفتيش اشخاص وتفتيش مساكن مع تبيان حدوده وشروطه وطرق الاستدلال به مع حماية حقوق وحرريات الأفراد^[2].

و يعرف في الفقه المقارن بـ: "البحث عن الأشياء المتعلقة بالجريمة لضبطها وكل ما يفيد في كشف حقيقتها، ويجب أن يكون للتفتيش سند قانوني^[3]".

و يعرف أيضا: "البحث في مستودع سر المتهم عن أشياء تفيد في كشف الحقيقة ونسبتها إليه، أو هو الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه يستوي في ذلك أن يكون المحل سكنا أو ما هو في حكمه أو أن يكون شخصا"^[4].

ثانياً: محل التفتيش في البيئة الرقمية

يتكون النظام الالكتروني والمعلوماتي من تزاوج بين مكونات مادية ومكونات منطقية وتشكل هذه المكونات اشكالات اجرائية وتفتيشية بالتحديد.

أ-تفتيش المكونات المادية للحاسوب

ان تفتيش المكونات المادية للحاسوب على اساس انه العنصر الرئيس في أغلب الجرائم الالكترونية لا يشكل مشكلة اجرائية كبيرة كالشق الثاني والمتمثل في المكونات المعنوية، مع وجوب الحذر في طرق التعامل مع مثل هذه المكونات لحساسيتها وإمكانية

[1] : قانون رقم 16-01 مؤرخ في 26 جمادي الأول عام 1473 الموافق لـ 6 مارس لسنة 2016، يتضمن التعديل الدستوري، الصادر في الجريدة الرسمية رقم 14 ، المؤرخة في 27 جمادي الأول عام 1437 الموافق 7 مارس لسنة 2006، ص 11.

[2] : زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، مرجع سابق، ص ص 130-1301.

[3] : خالد ممدوح إبراهيم، فن التحقيق في الجرائم الالكترونية، مرجع سابق، ص 7.

[4] : ابراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، الاسكندرية، 2009، ص 371.

اتلافها بسهولة، وهذه الاشياء المادية تخضع للتفتيش وفقا للحالات العادية في قانون الاجراءات الجزائية^[1].

فقد جاء في نصوص (المواد 44^[2] و 64^[3] من قانون الاجراءات الجزائية الجزائري) ان التفتيش يقع على الأشياء ويمكن ضبطها فيما بعد ذلك وهذا ما يعني انه لا اشكال في ان ينصب التفتيش على المكونات المادية للحاسوب وملحقاته، مع مراعاة طبيعة الاماكن المتواجد فيها مثل هذه الوسائل كمنزل المتهم او مكان عمله فتفتيش هذه المكونات يخضع لشروط تفتيش المنازل او المكاتب هذا كأصل عام فيما يخص تفتيش الاشياء والمسكن.

لكن المشرع الجزائري استثنى الجرائم الالكترونية والمتعلقة بالمعالجة المعلوماتية للمعطيات من كل هذه الشروط حيث جاء التأكيد لى استثناء هذا النوع من الجرائم في نصوص المواد:

(المادة 45 من قانون الاجراءات الجزائية) حيث جاء فيها "...لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ..."

و (المادة 47 الفقرة الثالثة من قانون الاجراءات الجزائية) التي جاء فيها "وعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات... فإنه يجوز إجراء التفتيش والمعaine والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص".

[1] : خالد ممدوح إبراهيم، فن التحقيق في الجرائم الالكترونية، مرجع سابق، ص 7.

[2] : المادة 44: "لا يجوز لضباط الشرطة القضائية...يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية...".

[3] : المادة 64: "لا يجوز تفتيش المساكن و معاينتها و ضبط الأشياء المثبتة للتهمة...".

و (المادة 47 الفقرة الرابعة من قانون الاجراءات الجزائية) التي جاء فيها " عندما يتعلق الأمر بالجرائم المذكورة في الفقرة الثالثة أعلاه، يمكن قاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهاراً وفي أس مكان على امتداد التراب الوطني ويأمر ضباط الشرطة القضائية المختصين للقيام بذلك".

و (المادة 64 الفقرة الثالثة منها من قانون الاجراءات الجزائية) التي جاء فيها " غير أنه عندما يتعلق الأمر بتحقيق في إحدى الجرائم المذكورة في المادة 47(الفقرة الثالثة)من هذا القانون، تطبق الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر.

من استقراء مجموعة هذه المواد يمكننا ملاحظة أن المشرع من مجموعة هذه الاستثناءات لا يشترط حضور الشخص الذي يشته في كونه الفاعل عند تفتيش مسكنه أو ضبط محرزاته، أنه يجوز تفتيشه في مختلف الاوقات دون الحاجة لأخذ رأيه او الاستعانة به.

و كبقية الجرائم المستثناة قدم المشرع الجزائري المصلحة العامة للدولة على حساب المصلحة الفردية للأفراد، وذلك لاعتبارين أساسيين هما:

- خصائص الجريمة المعلوماتية من سرعة تنفيذ وسرعة اخفاء عناصرها.
- إفتراض أن الدليل الالكتروني او الرقمي هو الدليل الوحيد في هذا النوع من الجرائم ولهذا يركز البحث عليه بكل الوسائل المتاحة^[1].

ب - تفتيش المكونات المعنوية للحاسوب

المكونات المعنوية للحاسوب وهي ما تميزه عن بقية الاشياء وتجعل منه وسيلة حية تؤثر وتتأثر لكن هذا النوع من المكونات أثار جملة من الاشكالات الاجرائية والفنية والقانونية في مدى صحة الأخذ به كأحد وسائل الاثبات في المادة الجزائية وقد ذهب الفقه في هذا المجال الى مذهبين اساسيان وهما:

[1] : نعيم سعيداني، مرجع سابق، ص 145.

1- المذهب الأول:

ويذهب أصحاب هذا المذهب إلى عدم امكانية معاملة هذا النوع من المكونات الداخلية اللامادية للحاسوب بنفس معاملة المكونات المادية فهناك من يذهب إلى حماية هذا النوع من المكونات اللامادية عن طريق قوانين خاصة على رأسها قوانين الملكية الفكرية^[1] خاصة وأن إبتعد هذه البرامج على الدعامه المادية لها تجردها من أي قيمة لها^[2].

2- المذهب الثاني:

يرى اصحاب هذه الفكرة ان مختلف برامج الحاسوب قد تنطبق عليها سمة المادة وبالتالي يمكن ان تخضع للتفتيش مثلها مثل المكونات المادية دون النظر الى نوعية البرنامج سواء كانت برامج تشغيل اي برامج نظام معين او برامج تطبيقات خاصة معينة اخره.

و يقوي هذا المذهب حجته في هذا بقولهم أم المادة هي كل ما يشغل حيزا ماديا في فراغ معين، وهذا الحيز يمكن قياسه والتحكم فيه وتقاس هذه الفراغات بالبايت (byte) والكيلوبايت (KB) والميغابايت (MB)^[3]

و بهذه الطريقة تقاس الذاكرة الداخلية للحاسوب والتي تشغل فيها البرامج حيزا معين وبالرجوع للمواد السابقة في ما يخص التفتيش الذي يقع على الاشياء دون تحديدا فاعتبروا البرامج من الاشياء وبالتالي تعد مادة او موضوع للتفتيش.

[1] : يرى أنصار هذا المذهب وجوب اعادة صياغة النص التشريعي و تعميم فكرة الاشياء حتى تصبح تشمل الاشياء الغير مادية بكافة انماطها.

[2] : عفيفي كامل عفيفي، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون، دراسة مقارنة، منشأة المعارف المصرية، الاسكندرية، ص358.

[3] : تقاس سعة الحواسيب او الانظمة و البرامج الالكترونية بأحد هذه السعات او ما يعادلها:

- الكيلوبايت يساوي 1024 بايت.
- الميغابايت تساوي 1024 كيلوبايت .
- الجيغابايت يساوي 1024 ميغابايت.
- التتيرابايت يساوي 1024 جيغابايت.

و فيما يخص المشرع الجزائري ومن خلال القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، حينما أجاز صراحة التفتيش في المنظومات المعلوماتية بموجب نص المادة الخامسة منه بقولها " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الاجراءات الجزائية وفي الحالات المنصوص عليها في المادة الرابعة، الدخول بغرض التفتيش، ولو عن بعد، إلى:

- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
- منظمة تخزين معلوماتية"

3- تفتيش الشبكات المعلوماتية المتصلة بالحاسوب

تعرف الشبكة المعلوماتية على أنها" مجموعة مكونة من اثنين أو اكثر من اجهزة الحاسوب والمتصلة ببعضها بعضا اتصالا سلكيا أو لا سلكيا"^[1]، وقد تكون هذه الأجهزة موجودة في مكان واحد او أماكن متعددة. خاصة بعد ظهور الأنترنت فلم يصبح هناك مجال للحديث على الحدود التقليدية للدول حيث يدخل في تركيبها ملايين الاجهزة الحاسوبية الموزعة عبر مختلف أرجاء المعمورة.

في هذه الحالة اجاز المشرع الجزائري في نص (المادة 05 من القانون 09-04) السالف الذكر اجاز صراحة الانتقال الى منظومة معلوماتية أخرى إذا كان لذلك سببا وبتابع الاجراءات القانونية المعمولة لذلك فقال في نصها: " في الحالة المنصوص عليها في النقطة الاولى من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك"^[2]، وهو ماذهب له المشرع

[1] : علي حسن محمد الطوالة، التفتيش الجنائي في نظم الحاسوب و الإنترنت، عالم الكتب الحديثة، الأردن، 2004 ص07.

[2] : المادة 5 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال و مكافحتها، مرجع سابق.

البلجيكي كذلك في نص (المادة 88) من قانون تحقيق الجنايات البلجيكي التي نصت على: "إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي أو جزء منه فإن البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي". [1]

و نتيجة لإمكانية التضارب بين القوانين الواجبة التطبيق في حالة تعدد الدول يذهب مجموع من الفقه الى ان التفتيش العابر للحدود يجب ان يتم في اطار اتفاقيات تعاون ثنائية او دولية تجيز تمديد الاختصاص تجنباً لتضاربه [2].

ثالثاً: شروط التفتيش

التفتيش في البيئة الرقمية او في مجال الجرائم الالكترونية لا يختلف على غيره في الجرائم الاخرى من حيث احاطة المشتبه به من شروط شكلية وموضوعية لحماية جزء من حقوقه وعدم التعدي على حرّيته او حرّمته [3] ونأتي فيما يلي للتطرق لأبرزها:

1 - شروط شكلية

إن الشروط الشكلية كما هو معروف لا تهدف الى الوصول الى الحقيقة بصورة اولى بقدر ما تهدف إلى تنظيم وحسن سير مرفق العدالة وما يتبعه وتحمي حقوق الافراد من امكانية تسلط الاشخاص الذين يخول لهم القانون القيام ببعض الاعمال الاجرائية التي قد تمس بحرية الشخص ولهذا سنتطرق لبعض الشروط الشكلية التي يتعين على القائم بالتفتيش احترامها حال قيامه بمهمته.

[1] : خالد ممدوح إبراهيم، فن التحقيق في الجرائم الالكترونية، الطبعة الاولى، دار الفكر الجامعي، الاسكندرية، 2009 ص203.

[2] : محمد أبو العلا عقيدة، التحقيق و جمع الأدلة في مجال الجرائم الالكترونية، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية، اكااديمية الشرطة، مركز البحوث و الدراسات، دبي، خلال الفترة من 26-28 أبريل 2003، ص 10.

[3] : علي حسن محمد الطوالبة، التفتيش الجنائي في نظم الحاسوب و الإنترنت، مرجع سابق، ص 47.

أ- إجراء التفتيش بحضور صاحب الشيء :

كما سبق الإشارة لهذه النقطة في باب تفتيش المكونات المادية للحاسوب فإن المشرع يشترط كأصل عام في تفتيش المنازل والأشياء حضور صاحبها أو من يمثله إلا أنه تنازل عن هذا الشرط في مجال هذا النوع من الجرائم وهو ما تؤكد نص (المادة 45 من قانون الاجراءات الجزائية).

ب- توقيت إجراء التفتيش:

هنا كذلك سلك المشرع الجزائري نفس السلوك بالنسبة للتفتيش بحضور صاحب المنزل أو الشيء حيث أن الاصل ان هناك توقيت العمل الإدارية التي يجب أن تحترم والتي تنحصر من الساعة الخامسة صباحاً إلى الساعة الثامنة مساءً، وأخرج منها كذلك مجموعة من الجرائم لما لها من الخطورة والخصائص المميزة وكان من ضمنها الجرائم الالكترونية حيث أجاز بنص (المادة 47 من قانون الاجراءات الجزائية) التي سبق الإشارة لها الى امكانية التفتيش كل اوقات النهار والليل في مثل هذا النوع من الجرائم بناء على اذن مسبق من قبل وكيل الجمهورية المختص.

2- شروط موضوعية

تأتي الشروط الموضوعية لإكمال ميزان العدالة في جانبه الموضوعي فيتأتي القانون والقضاء ليؤكد على مجموعة من الشروط والمبادئ التي يجب احترامها اثناء التفتيش وتتلخص فيما يلي:

أ- وجود سبب للتفتيش:

وفي هذه الحالة فغالبا ما يكون سبب التفتيش عموما هو وقوع جريمة ما يبحث لها عن اسبابها وملابسات وقوعها واتهام احد الاشخاص بها أو ضلوعه فيها أو وجود دلائل قوية على نسبتها له وبإسقاط هذا الشرط على موضوع الدراسة يتبين ان سبب التفتيش هو ارتكاب جريمة من الجرائم الالكترونية التي سبق الإشارة لها في الفصل الأول حيث لا يتصور تحقيق دون وقوع الجريمة إلا ان المشرع استثناء بنص (المادة الرابعة الفقرة ب

من القانون 09-04) منها حيث انه في حالات معينة يمكن تجاوز هذه النقطة رغم ان نص المادة الرابعة قد ورد في الفصل الثاني والمتعلق بمراقبة الاتصالات السلكية وأسيرا لها في نص المادة الخامسة المتعلقة بالتفتيش.

ب - الإذن بالتفتيش: غالبا ما يصدر الاذن بالتفتيش فيما يخص المساكن دون غيرها من الأشياء دون ان نص المشرع على اذن خاص باللجوء إلى المنظومات المعلوماتية وطبقا لمعيار الخصوصية التي يحميها المشرع فانه من المفترض أنه في الغالب يحتاج ضباط الشرطة القضائية إلى إذن للتفتيش^[1]، إلا أنه ومن وجهة نظر شخصية أرى أنه ولخطورة هذا النوع من الجرائم وتقديمها للمصلحة العامة وتقديراً لتهرب المجرمين من العقاب أرى أن الاذن الواحد بإمكانه ومن الاحسن ان يتعدى المنزل الى المنظومات المعلوماتية.

ت - تحديد مجال الإذن بالتفتيش: يتعين في الاصل ان يتضمن الأمر بالتفتيش كل البيانات المتعلقة بالمجرم والجريمة ومحل ومجال التفتيش والهدف منه وتبين أهمية هذه النقاط في مجال البيئة الالكترونية لان هذه الاخيرة بإمكانها احتواء الالف والملايين من المعلومات والملفات قد يفقد صاحبها طابع الخصوصية في حالة اطلاع ضباط الشرطة القائية عليها وهي لا تتعلق لا من قريب ولا من بعيد بالجريمة المفتش عنها^[2].

الفرع الثاني: مراقبة واعتراض المراسلات الالكترونية

يعد كل من اجراء تجميع ومراقبة الاتصالات الالكترونية واعتراض المراسلات السلكية واللاسلكية من أبرز الإجراءات التي جاء بها المشرع في باب مواكبته للتطور التكنولوجي الهائل في مجال الجريمة من جهة وفي مجال مكافحتها من جهة أخرى وهذا ما أوجب علينا التطرق لهم في هذا الفرع :

[1] : نعيم سعيداني ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري،مرجع سابق ص157.

[2] : خالد ممدوح إبراهيم، فن التحقيق في الجرائم الالكترونية، مرجع سابق، ص 221.

أولاً: مراقبة الاتصالات الالكترونية:

جاء قانون 04-09 زيادة على اجراء اعتراض المراسلات امكانية مراقبة الاتصالات الالكترونية^[1]، هذا الاجراء مسموح بشروط هي:

-أن تكون من الحالات التالية:

• الوقاية من الافعال الموصوفة بجرائم ارهابية او التخريب او الجرائم الماسة بأمن الدولة.

• توفر معلومات عن احتمال اعتداء على منضومة معلوماتية على نحو يهدد على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

• قضايات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

• في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

-أن يكون بإذن مكتوب من السلطة القضائية المختصة وعندما يتعلق الأمر بالوقاية من الأفعال الموصوفة بالجرائم ارهابية او التخريب او الجرائم الماسة بأمن الدولة يختص النائب العام لدى مجلس قضاء الجزائر.

-الضباط المختصين بهذا الاجراء في شأن جرائم الارهاب او التخريب او الجرائم الماسة بأمن الدولة هم المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ويسلم الاذن

[1] : حيث تنص المادة 3 من القانون 04-09 : " مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

بمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها أما الجرائم الأخرى تخضع للأحكام المنصوص عليها في قانون الاجراءات الجزائية.

ثانياً: اعتراض المراسلات السلكية واللاسلكية:

استحدث المشرع الجزائري بموجب القانون 06-22 المؤرخ في 20-12-2006 المعدل والمتمم لقانون الاجراءات الجزائية من خلال الفصل الرابع من الباب الثاني من الكتاب الاول تحت عنوان اعتراض المراسلات وتسجيل الاصوات والتقاط الصور وقد ضمنه 6 مواد من (المادة 65 مكرر الى المادة 65 مكرر 10) وتناول من خلالها المقصود بهذا الاجراء وضمانات استخدامه.

1- مفهومه :

ورد في اجتماع لجنة الخبراء للبرلمان الأوروبي بستراسبورغ القائم في 20-06-2006 حول اساليب التحري التقنية وعلاقتها بالأفعال الارهابية تعريفا لإجراء اعتراض المراسلات بأنها عملية مراقبة سرية للمراسلات السلكية واللاسلكية، ذلك في إطار البحث والتحري عن الجريمة وجمع الادلة والمعلومات حول الأشخاص المشتبه فيهم أو في مشاركتهم في ارتكاب الجرائم^[1].

و باستقراء نص (المادة 65 مكرر 5 من قانون الاجراءات الجزائية) نجد ان المشرع الجزائري يقصد باعتراض المراسلات، اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات او وسائل الاتصال السلكية او اللاسلكية، وهذه المراسلات هي عبارة عن بيانات قابلة للإنتاج والتوزيع والتخزين والاستقبال والعرض.

[1] : نور الدين لورجاني أساليب البحث و التحري الخاصة و إجراءاتها و فقا للقانون 06-22، مداخلة في يوم دراسي حول علاقة النيابة العامة بالشرطة القضائية، وزارة الداخلية، المديرية العامة للأمن الوطني، منعقد يوم 12-12-2007 باليزي، ص8 مشار له عند نعيم سعيداني ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سابق، ص177.

بالرجوع لنص وباستقراء نص (المادة 39 من الدستور) التي نصت على سرية المراسلات والاتصالات الخاصة بكل اشكالها مضمونة ، وكذا نص(المادة 303 من قانون العقوبات)^[1] التي تعاقب كل من يفض او يتلف رسائل او مراسلات موجهة للغير فانتهاه يمكن التوصل للقول ان المراسلات الخاصة تعني كل رسالة مكتوبة باس شكل من الاشكال سواء ماديا او إلكترونياً سواء كانت على دعامة ورقية او رقمية مرسله بأي وسلة لعدد معين من المرسل اليهم باستثناء الكتب والمجلات والجرائد والحوليات التي لا تعتبر مراسلات خاصة^[2].

و هذا ما يؤكد القانون 09-04 في المادة 2 الفقرة ومنه في تعريفه للاتصالات الالكترونية حيث جاء فيها " الاتصالات الالكترونية: أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية" .

2- شروطه:

ترخيص السلطة القضائية ومراقبتها للتنفيذ: طبقا لنص (المادة 65 مكرر 5)^[3] من قانون الاجراءات الجزائية فانه لا يمكن لضابط الشرطة القضائية اللجوء الى اجراء اعتراض المراسلات إلا بعد ان يحصل على اذن مكتوب ومسبب من طرف وكيل

[1] : المادة 303: " كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير وذلك بسوء نية و في غير الحالات المنصوص عليها في الادة 137، يعاقب بالحبس من شهر الى سنة و بغرامة من 25.000 دج الى 100.000 دج أو باحدى هاتين العقوبتين فقط.

[2] : نعيم سعيداني ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سابق، ص.ص 178-179.

[3] : المادة 65 مكرر 5 : "... تنفيذ العمليات المأذون بهل على هذا الاساس تحت المراقبة المباشرة لوكيل الجمهورية المختص.

في حالة فتح تحقيق قضائي، تتم العمائيات المذكورة بناء على اذن من قاضي التحقيق و تحت مراقبته المباشرة"

الجمهورية او قاض التحقيق في حالة فتح تحقيق قضائي، فالسلطة القضائية هي وحدها المختصة بإصدار هذا الاذن وهو ما يعد ضمانا لمشروعية هذا الاجراء^[1].

و على وكيل او قاضي التحقيق قبل منح هذا الاذن تقدير فائدة اجرائه وجديته ومسايرته لسير اجراءات الدعوى.

تحديد طبيعة المراسلة ومدة الاعتراض: وهذا ما يفهم صراحة من نص المادة 65 مكرر 7 التي نصت على انه يجب ان يتضمن الاذن باعتراض المراسلات كل العناصر التي تسمح بالتعرف على الاتصال او المراسلة المطلوب اعتراضها كما ان المشرع قد استوجب ان لا تتجاوز مدة هذا الاجراء 4 اشهر قابلة للتجديد حسب تقدير نفس السلطة مصدره الاذن وفق لمقتضيات التحري والتحقيق^[2].

المطلب الثاني: معوقات البحث والتحري عن الجريمة الالكترونية

مرحلة جمع الدليل كما لها من قوة تأثير على الحكم النهائي الذي سيصدره الحكم فان لها دور أهم في ترسيخ مجموعة من المبادئ القانونية، إلا ان هذه المرحلة التي يقوم بها رجال على قدر من الكفاءات النسبية في اختصاصهم تصطدم بمجموعة من العراقيل التي قد تؤثر اما على سرعة ضبط الدليل او عدم ضبطه من اساسه حيث سنتطرق هنا في الفرع الاول الى العراقيل المتصلة بشخص الضحية و في الفرع الثاني الى العراقيل المتصلة بالجهات المسؤولة على ضبط هذا الدليل.

الفرع الأول: معوقات تتصل بشخص الضحية

قد يكون لشخص الضحية في الجريمة الإلكترونية دور في إعاقة التحقيق والوصول إلى الدليل لإثبات الجريمة، فالتقنية المستخدمة في نظم المعلومات تعد مجال استثمار وتسابق بين الشركات مما يدفعها في مقابل تحقيق الربح إلى تبسيط الإجراءات وتسهيل

[1] : نعيم سعيداني ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سابق، ص.ص 180-181.

[2] : المرجع نفسه، ص 181.

استخدام البرامج وملحقاتها وزيادة المنتجات واقتصار تركيزها على تقديم الخدمة في مقابل إهمال الجانب الأمني، وقد وصل الحد ببعض مستخدمي شبكات الأنترنت عبر مزودي الخدمة في خضم التنافس التجاري إلى درجة عدم مطالبة المشتركين بتحديد هوياتهم عند الاشتراك في خدمة الأنترنت^[1] فهذا ما قد يعتبره الزبون تسهيلا له هو في نفس الوقت سلاح في يد الجاني المتمكن والمتأهب لمثل هذه الفرص هذا وبالإضافة الى اخطاء أخرى يقوم بها الضحية نذكر منها :

أولاً: عدم العلم والدراية بوقوع الجريمة

أن الاختلاف بين الجريمة الالكترونية والجريمة العادية ففي الاخيرة عادة يترك السارق المختلس أو القاتل آثار مادية يمكن ان تستدل بها سلطات التحقيق من أجل إدانة المجرم أو تعلم الشخص وتنبهه لما قد وقع له.

وبما أن الجريمة الالكترونية هي جريمة متخصصة فحتى المجرم المعلوماتي أو الالكتروني له طبيعة خاصة ففي الكثير من الأحيان يمكنه محو ما قام به أو مسح آثار الجريمة سواء عند نشر الفيروس أو الاختلاس أو الخرق الآلي أو التسلل الى الموقع وهذا ما سبق الإشارة له في خصائص هذه الجريمة.

مثلا عند نشر الفيروس فآثاره مدمرة بينها تعطيل الأجهزة وعند تشويه المعلومات على الموقع فلذلك آثاره ولكن ليست هي الآثار المقصودة بل المقصود هو الدليل الذي يقودنا الى المجرم، وتعزى صعوبة ترك الأثر في هذه الجرائم إلى ما يلي:

ثانياً: عدم التبليغ

إن عدم الإبلاغ من طرف الأشخاص الذين شاهدوا المجرم عند قيامه بالجريمة أو الذين وقعت عليهم الجريمة هو ما زاد في صعوبة اكتشاف الجريمة ومن أسبابه نجد:

[1] : نعيم سعيداني ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مرجع سابق، ص 191.

- عدم ابلاغ الشركات وخصوصا التجارية منها بعمليات الخرق التي يقوم بها المجرم الإلكتروني وهذا خوفا على سمعتها التجارية، وهروب الزبائن من التعامل معها.
- إن هذا الإبلاغ يتسرب الى المجرم الإلكتروني وبالتالي تكشف الثغرات الأمنية في النظام المعلوماتي .
-نقص الغطاء تشريعي لهذه السلوكيات^[1].

وقد يحدث أن يبلغ عن سلوكيات مشبوهة للمجرمين الإلكترونيين ولكن في الكثير من الأحيان لا يمكن اكتشاف الشخص الذي قام بالسلوك الإجرامي، فمثلا جريمة نشر فيروس في الكثير من الأحيان لا يمكن اكتشاف الشخص الذي قام بنشره ومما يزيد من مشكل عدم الابلاغ ما يلي:

- المعرفة المتأخر من أن الجهاز أصيب بفيروس عن طريق الشبكة.
- ضخامة الأضرار حيث أن الفيروس ليس مقيد برقعة جغرافية معينة.
- تحويل الشبكة لساحة من المعارك بين الدول مما أصبحت المعاملات التجارية غنيمة سهلة للاختراق.

ثالثا: عدم الوقاية:

حيث أن أغلب الأشخاص الذين يقومون بفتح صفحات او مواقع او غيرها لا يقومون بعملية تحصين هذه المواقع بمضادات للفيروسات و الاختراقات مما يسهل عمل الجناة في التغلغل لمثل هذه الأنظمة.

الفرع الثاني: معوقات تتصل بجهات البحث والتحري

إن نقص معرفة الضحية او عدم تبليغة لا يعدا الاسباب الوحيد التي تعيق تحقيق النتيجة الفعالة والرادعة في مجال البحث وإيجاد الدليل الإلكتروني المناسب بل تتعداه هذه

[1] : جودة حسين جهاد، بحث بعنوان: "المواجهة التشريعية للجريمة المنظمة بالأساليب التقنية"، مؤتمر القانون والكمبيوتر و الأنترنت ، الامارات العربية المتحدة، 2000، ص 23.

المعوقات حتى تشمل الجهات والأجهزة والأشخاص المسؤولين على متابعة هذا النوع من القضايا وهذا ما سنوضحه فيما يأتي:

أولاً: نقص الخبرة أجهزة التحقيق

إن صعوبة اكتشاف الجريمة بالدرجة الأولى مرده الى نقص خبرة المحققين مما يضعنا أمام معادلة غير متكافئة طرفها أجهزة التحقيق بنقص خبرتها في مجال الكمبيوتر والأنترنات والطرف الآخر قرصنة محتالون ومنحلون أخلاقياً يتمتعون بمهارات عالية يواكبون كل جديد في عالم المعلوماتية.

و قد وصل بعض المجرمون الإلكترونيين الإطلاق على أنفسهم اسم النخبة أما رجال الشرطة فقد أطلقوا عليهم اسم الضعفاء ونلاحظ أن عملية سن التشريعات أبطأ من عملية الإجرام وهذا في العالم كله دون استثناء ومن العوامل المساعدة في نقص الخبرة في الجرائم الالكترونية هي :

- عدم تخصيص أموال من أجل التأهيل الجيد للمحققين.
- حداثة الجريمة وخصوصيتها التي لم يعتد عليها رجال الشرطة، مما جعلهم قاصرين في مواجهتها.
- ضخامة المعلومات الموجودة على الشبكة وانتشار أجهزة الكمبيوتر مما يصعب عملية التحقيق.
- الأنترنات بيئة خصبة للسلوك الإجرامي.
- التطور السريع للتقنية الحديثة.
- عدم وجود هيئات قضائية مختصة.
- وجود مواقع على الشبكة تسهل عملية إرسال البريد الإلكتروني دون الحاجة الى ذكر البيانات اللازمة مثل معرفة المرسل.

ويميل الفقه الجنائي الى القول بضرورة تنمية الخبرة والمهارات للأشخاص المتخصصين لوضع مناهج مدروسة للتدريب على التحقيق إثباتها مراعين في ذلك خصوصية التطور التقني السريع دون إهمال التعاون الدولي في مثل هذه الحالات^[1].

ثانيا: نقص التعاون الدولي :

في ظل الصراعات التي أصبحت سما من سمات هذا العالم، يعصب إيجاد تعاون دولي حقيقي من أجل مكافحة الجريمة الإلكترونية أو حتي التعاون من أجل كشف الجريمة.

فكما بينا سابقا قد يتم السلوك الإجرامي في بلد معين ولكن النتيجة تحدث في بلد آخر، كأن تقوم مجموعة من المجرمين بتشويه معلومات معينة وليس بالضرورة أن ينتج هذا السلوك آثاره في بلد المجرمين بل قد يتعداه لبلد آخر ومن اشكاليات نقص هذا التعاون ما يلي:

- فتضارب الصالح.
- اختلاف النظم القانونية.
- عدم الاتفاق على تعريف جامع مانع لهذه الجريمة، فما هو محظور في الجزائر من الناحية الأخلاقية مباح في غيرها من الدول.
- التطور السريع للجريمة والمعالجة البطيئة للحالات، ساعد المجرم الإلكتروني على تصوير صورة القاهر لمجموعة من الدول والانظمة.
- التعاون الدولي مهم عند التعامل مع هذه الجرائم، لأنه سوف يطور أساليب متماثلة للتحقيق ويوجد قانون جنائي وإجرامي لحماية شبكة المعلومات الدولية.

[1] : عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت، منشأة المعارف الاسكندرية، 2009، ص69.

إن الحلول القانونية كطبيعة الاختراعات تكون في أغلب الاحيان مواكبة لانتشار جرائم معينة أي لنقص تشريعي معين في مجال ما و هذا ما م تداركه محليا ودوليا حيث أنه و كما بينا اهمية الدور وجهود الوحدات الخاصة التابعة للهيئة الوطنية للوقاية و مكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال، و كذلك الخلايا الأمنية التابعة للمديرية العامة الوطنية للأمن الوطني و المختصة بمكافحة الجرائم المعلوماتية والتي تنتشر عبر كافة التراب الوطني ، شأنها شأن تلك الوحدات المتخصصة التابعة للقيادة العامة للدرك الوطني الجزائري في مكافحة الجرائم الالكترونية في ظل سياسة مكافحة الجرائم المتعلقة بالمعلومات و المعالجة المعلوماتية لها المتبناة من قبل المشرع الجزائري أملا منه في وضع حد للظاهرة الإجرامية الإلكترونية أو التخفيف منها.

كما لحظنا الطفرة التي شهدتها التشريعات الدولية و الوطنية في سبيل و وضع حلول نهائية لإشكالية تناسب الاجراءات التقليدية مع هذا النوع من الجرائم و هذا ما يعد عائقا حقيقيا في مسار نجاح إجراءات البحث و التحقيق في الجرائم الالكترونية، و كيفية تليين هذه الاجراءات او استحداث الجديدة منها من اجل نجاح مثل هذه العملية في هذا المجال بدليل نجاح هذه الوحدات و الفرق الخاصة بالإطاحة بأكبر الشبكات في مجال الإجرام السيبرني، و القبض على مرتكبيها و تقديمهم امام العدالة، في ظل عدم كفاءة و قدرة الوحدات الأخرى على تحقيق نفس الأهداف بسبب عدم تخصصها بمجال المعلوماتية .

خاتمة

بعد ما سعت إلى محاولة الإحاطة بجوانب البحث ضمن رؤية موضوعية اجرائية لموضوع البحث والتحري عن الجريمة الالكترونية.

فتطرق في الفصل الأول من هذه الى الطبيعة القانونية للجريمة لالكترونية وأبرزت فيه خصائصها وخصائص مرتكبيها و الدوافع الاجرامية التي أدت بهم لارتكاب هذا النوع بالتحديد من الجرائم، وأوجه الحماية الجزائية للنظم المعلوماتية في مواجهتها في قانون العقوبات و قوانين اخرى مكملة له.

حيث ان منطق الأمور و الأشياء يجبرنا للتطرق لهذه المسائل فلا يستقيم منطقاً ولا عقلاً أن نغوص في الاجراءات دون المعرفة الدقيقة لحيثيات الموضوع .

أما الفصل الثاني فكان مخصصا للجوانب القانونية المتعلقة بمسألة البحث والتحري في الجريمة الإلكترونية وتحدثت فيه عن أبرز الهيئات الوطنية المسؤولة عن التحري في هذه الجرائم كما بينت الخصائص التي يتسم بها المحققين في هذا النمط الإجرامي المتميز والعوائق التي تعترضهم في سبيل أداء مميز لوظائفهم.

وعلى ضوء الإشكاليات المطروحة و اجابة عنها نستخرج ما يلي:

أولاً: النتائج

تأسيسا على ما سبق دراسته، خلصنا في الأخير إلى مجموعة من النتائج وهي كالتالي:

- تتميز الجريمة الإلكترونية بمجموعة من الصفات كونها جريمة يصعب الكشف عنها، إضافة إلى أنها جريمة ناعمة وعابرة للحدود ومن ثم اكتسابها طبيعة العالمية.
- صفة مرتكبها - المجرم الالكتروني - وتميزه بالذكاء والفتنة والعلم الكافي بتكنولوجيات الاتصال.
- افتقار هذه الجريمة في الجزائر على الأقل لإحصائيات حقيقية دقيقة، حيث يختلف الفارق بين الحجم الحقيقي للجريمة الإلكترونية وما هو مسجل في الإحصائيات وهذا راجع لعدة عوامل أهمها غياب الدليل المادي الملموس إضافة إلى عدم التبليغ عنها.

- تزايد خطورة الجريمة الإلكترونية بعدما أصبحت تمثل تهديدا مباشرا للأمن والاستقرار والسلام في العالم، وعائقا يحول دون إتمام عمليات التطوير والتنمية.
- محاولات التصدي لهذه الجريمة من قبل الجزائر عن طريق مؤسستي الامن والدرك الوطنيين واستحداث هيئة وطنية خاصة لمجابهة هذه الظاهرة وهو نفس الشيء في بعض الدول الاخرى وحتى المنظمات الاقليمية و الاممية.

ثانياً: التوصيات

وفي التوصيات المقترحة لمواجهة الجرائم الإلكترونية يمكن أن نلخصها في هذه النقاط:

- وجوب تأهيل رجال الشرطة المتخصصة في الجرائم الإلكترونية على الأساليب التقنية الحديثة المستخدمة لمقاومة هذا النوع من الجرائم، وتدريبهم على التدابير الواجب اتخاذها في هذا المجال بصفة دورية سريعة لان هذا النوع من الجرائم يتطور بسرعة تفوق تطور الاجهزة الامنية.
- العمل على تعزيز التعاون والتنسيق الدولي بين الدول مع بعضها البعض وبين الدول والمؤسسات المعنية بهذه المشكلة وخاصة الأنتربول، سواء في مجال المساعدات القضائية المتبادلة أو في مجال تسليم المجرمين أو في مجال التدريب.
- إسراع الدول لانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة الجرائم الإلكترونية خاصة.
- ضرورة إنشاء نيابة عامة وقضاة مختصة بالجرائم الإلكترونية نتيجة عدم قدرة القضاة العاديين على استيعاب الشق العلمي لمثل هذه الجرائم والاهتمام بمنح أعضائها دورات تدريبية تقنية حتى يكونوا على علم بهذه الطبيعة.
- تكثيف الدور التربوي عبر المؤسسات الوطنية كالمدارس و المساجد أو حتى من قبل المنظمات و الجمعيات من أجل توعية الفرد على أهمية التكنولوجيا وخطورتها في آن وقت.
- تطوير الدور الاحصائي للمنظمات و الهيئات الخاصة و الوطنية للتزويد بأرقام اكثر دقة و أقرب للواقع.

- دعوة وسائل الإعلام لإبراز الدور الهام لمكافحة الجرائم الإلكترونية وإبراز دور التشريعات العقابية لتكون جزء من الردع الذي تسعى السلطات لتجسيده وتحسيس المواطن بخطورتها ووجوب التبليغ عنها.

ثانياً: آفاق الموضوع:

إن هذا الموضوع كما سبق وأن ذكرنا لا يزال حديث التداول في شقه الاجرائي خاصة وعليه قد يكون هذا البحث المتواضع نقطة انطلاق للتعمق أكثر في حجية الدليل الالكتروني ومدى تأثيره على القاضي الجزائي كما قد يكون رافداً للبحث في مدى مناقشة الشريعة الاسلامية لموضوع الجرائم الالكترونية الذي لم يناقش بصفة علمية حد الساعة.

وفي الختام:

نسأل الله العلي القدير أن يتقبل منا هذا العمل المتواضع راجيناً منه التوفيق والسداد لنا ولجميع.

ولقد بذلنا في هذا البحث قصارى جهدنا، لكن الكمال لله وحده، فإن كان من صواب وخير وتوفيق فمن الله وحده، وإن ندد بعض النقص والخلل والخطأ فمن أنفسنا ومن الشيطان، نرجوا من الله عز وجل أن يعفو عنا بهذا، وأن يجعل هذا العمل خالصاً لوجهه الكريم، وأنه سميع قريب مجيب.

والحمد لله رب العالمين.

**قائمة
المصادر
والمراجع**

أولاً: النصوص القانونية.

- 1- الأمر 66 - 156 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو 1966 معدل ومتمم بـ قانون رقم 06-23 مؤرخ في 29 ذي القعدة عام 1427 الموافق لـ 20/12/2006 و القانون 01-14 المؤرخ في فبراير 2014، المتضمن قانون العقوبات.
- 2- قانون رقم 03-2000 المؤرخ في 05 غشت 2000 الذي يحدد القواعد المتعلقة بالبريد و المواصلات السلكية و اللاسلكية، الجريدة الرسمية، عدد ، المؤرخة في 06 غشت 2000.
- 3- قانون رقم 85 لسنة 2001، الجريدة الرسمية للملكة الأردنية الهاشمية رقم 4524، الصادر بتاريخ 2001/12/31.
- 4- قانون إمارة دبي رقم 02 لسنة 2002 المتعلق بالمعاملات و التجارة الإلكترونية الصادر بتاريخ 12 فبراير 2002.
- 5- الأمر رقم 03-05 المؤرخ في 23/07/2003 المتعلق بحقوق المؤلف والحقوق المجاورة الصادر في الجريدة الرسمية، عدد 44، الصادرة في 23 جويلية 2003.
- 6- المرسوم التنفيذي 06-348 المؤرخ في 12 رمضان الموافق 05 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية وقضاة التحقيق صادر في الجريدة الرسمية رقم 63 المؤرخة في 15 رمضان الموافق 8 أكتوبر 2006 المعدل و المتمم بالمرسوم التنفيذي رقم 16 / 267 المؤرخ في 17 أكتوبر 2016 الصادر في الجريدة الرسمية رقم 62..
- 7- القانون رقم 08-01 المؤرخ في 23/01/2008 المتعلق بالتأمينات الإجتماعية الصادر في الجريدة الرسمية، عدد 04، الصادرة في 27 يناير 2008.
- 8- قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها، الصادر في الجريدة الرسمية رقم 47 الصادرة بتاريخ 16 أوت 2009.

- 9- قانون رقم 15-03 المؤرخ في 01 فيفري 2015 المتعلق بعصنة العدالة، الجريدة الرسمية، عدد 02، الصادرة في 10 فيفري 2015.
- 10- المرسوم الرئاسي رقم 15-261 المؤرخ في 14 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015 يحدد تشكيل و تنظيم و كفاءات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها الصادر في الجريدة الرسمية عدد 53، المؤرخة في 24 ذو الحجة 1436 الموافق 8 أكتوبر لسنة 2015.
- 11- قانون رقم 16-01 مؤرخ في 26 جمادى الأولى عام 1473 الموافق لـ 6 مارس لسنة 2016، يتضمن التعديل الدستوري، الصادر في الجريدة الرسمية رقم 14 ، المؤرخة في 27 جمادى الأولى عام 1437 الموافق 7 مارس لسنة 2016.

ثانياً: المؤلفات

- 1- ابراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، الاسكندرية، 2009.
- 2- أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الثانية الاسكندرية 2006.
- 3- أحمد فتحي السرور، الوسيط في قانون العقوبات (القسم العام)، دار النهضة العربية، الطبعة السادسة القاهرة، 1991.
- 4- جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجية الحديثة، دار النهضة العربية، القاهرة، 2002.
- 5- جميل عبد الباقي الصغير، القانون الجنائي و التكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، 1992.
- 6- خالد ممدوح ابراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي الاسكندرية، 2009 .
- 7- خالد ممدوح إبراهيم، فن التحقيق في الجرائم الالكترونية، الطبعة الاولى دار الفكر الجامعي الاسكندرية، 2009.

- 8- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، الطبعة الأولى، 2012.
- 9- زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدى، عين مليلة الجزائر، 2011.
- 10- سينا عبد الله محسن، المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية و الوطنية، الدار البيضاء، المملكة المغربية.
- 11- عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية و أزمة الشرعية الاجرائية، جامعة الكوفة كلية القانون.
- 12- عباس أبو شامة، عولمة الجريمة الاقتصادية، جامعة نايف العربية للعلوم الأمنية الرياض، المملكة العربية السعودية.
- 13- عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر والانترنات، منشأة المعارف، الاسكندرية، 2009.
- 14- عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2002.
- 15- عفيفي كامل عفيفي، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون، دراسة مقارنة، منشأة المعارف المصرية، الاسكندرية
- 16- علي حسن محمد الطوالبه، التفتيش الجنائي في نظم الحاسوب والانترنات عالم الكتب الحديثة، الأردن، 2004.
- 17- محمد حماد مرهج الهيتي، التكنولوجيا الحديثة في القانون الجنائي، دار الثقافة للنشر و التوزيع، عمان، الأردن 2004.
- 18- محمد عبيد كعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت دار النهضة العربية، القاهرة.
- 19- مصطفى محمد موسى، التحري في جرائم مجتمع المعلومات و المجتمع الافتراضي، الطبعة الاولى، دون مكان نشر، 2011
- 20- نائلة قورة ، جرائم الحاسب الاقتصادي، دار النهضة العربية، القاهرة.

21- نبيلة هبة محمد هروال، الجوانب الاجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، الطبعة الاولى، دار الفكر الجامعي، الاسكندرية، 2007.

22- نجيب حسني، دروس في القانون الدولي الجنائي، دار النهضة العربية، القاهرة.

23- نهلا عبد القادر المومني، الجريمة المعلوماتية، الطبعة الثانية، دار الثقافة للنشر و التوزيع، 2010.

24- هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، الطبعة الأولى، مكتبة الآلات الحديثة، اسيوط، 1992.

25- وضاح محمود الحمود و نشأت مفضي المجالي، جرائم الانترنت، دار المنار للنشر، عمان، 2005.

ثالثاً: المذكرات و الرسائل

1- حمزة بن عقون، السلوك الاجرامي للمجرم المعلوماتي، مذكو لنيل شهادة الماجستير في العلوم القانونية، تخصص علم العقاب و علم الاجرام، جامعة الحاج لخضر، كلية الحقوق و العلوم السياسية، باتنة، السنة الجامعية 2011/2012.

2- ضغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجستير في القانون تخصص قانون دولي للأعمال، كلية الحقوق و العلوم السياسية، جامعة مولود معمري تيزي وزو، 2013.

3- فتيحة رصاع ، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة أبي بكر بلقايد، كلية الحقوق و العلوم السياسية، تلمسان، السنة الجامعية 2011/2012.

4- نعيم سعيداني ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم الجنائية، جامعة الحاج لخضر باتنة، 2013.

رابعاً: المؤتمرات و المداخلات

- 1- جودة حسين جهاد، بحث بعنوان: " المواشحة التشريعية للجريمة المنظمة بالأساليب التقنية"، مؤتمر القانون و الكمبيوتر و الأنترنت ، الامارات العربية المتحدة، 2000.
- 2- نيا ب موسى البداينة، ورقة عمل بعنوان الجرائم الالكترونية: المفهوم و الأسباب مقدمة للملتقى العلمي الجرائم المستحدثة في ظل المتغيرات و التحولات الاقليمية و الدولية عمان ، المملكة الأردنية الهاشمية، خلال الفترة من 02-04/09/2014
- 3- سامي الشوا، العش المعلوماتي ظاهرة إجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، دار النهضة العربية، القاهرة 1993.
- 4- عادل محمود شرف، عبد الله إسماعيل عبد الله، ضمانات الأمن و التأمين في شبكة الأنترنت، مؤتمر القانون و الكمبيوتر و الأنترنت، كلية الشريعة و القانون بالتعاون مع مركز الامارات للدراسات و البحوث الاستراتيجية، مركز تقنية المعلومات، دولة الامارات العربية المتحدة، أيام من 1- 3 مارس 2000، المجلد الثاني.
- 5- عبد الرحمان حملاوي ، مداخلة بعنوان " دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية " الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة المنعقد بجامعة بسكرة يومي 16 و 17 نوفمبر 2015.
- 6- غنام محمد غنام، مداخلة بعنوان "الحماية الجنائية لبطاقات الائتمان الممغنطة" مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي 2003.
- 7- فاروق خلف ، مداخلة بعنوان، "الآليات القانونية لمكافحة الجريمة المعلوماتية"، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة المنعقد بجامعة بسكرة يومي 16 و 17 نوفمبر 2015.
- 8- محمد أبو العلا عقيدة، التحقيق و جمع الأدلة في مجال الجرائم الالكترونية، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية اكااديمية الشرطة، مركز البحوث و الدراسات، دبي، خلال الفترة من 26-28 أبريل 2003.

قائمة المصادر والمراجع

- 9- المؤتمر الثالث عشر لمنع الجريمة و العدالة الجنائية و المقام بدولة قطر من 12-19 أبريل 2015.
- 10- المؤتمر الثاني عشر لمنظمة الأمم المتحدة و المقام بريو دي جانيرو بدولة البرازيل من 12-19 أبريل 2010.

خامساً: المجالات

- 1- حاتم عبد الرحمان منصور الشحات، الحماية الجنائية للثقة في المستند الالكتروني مجلة الحقوق، العدد الاول، الكويت، 2006.
- 2- صالح بن محمد المسند، عبد الرحمان بن راشد المهيني، جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية والتدريب المجلد 15، العدد 29.

سادساً: المواقع الالكترونية

- 1- محمد عادل ريان، جرائم الحاسب الآلي و أمن البيانات، أنظر الموقع التالي: www.anaharonline.com
- 2- موقع المديرية العامة للأمن الوطني <http://www.dgsn.dz/>
- 3- موقع الدرك الوطني الجزائري <http://www.mdn.dz/>
- 4- موقع مجموعة الثمانية: www.Candainternationalgc.ca/G8
- 5- موقع القانون الافريقي: www.africa-union.org
- 6- الشبكة القانونية العربية: www.arabegalnrt.org
- 7- الصفحة الإلكترونية للمؤتمر المنعقد في قطر: WWW.moi.gov.qa/UNCCPCJDoha/Arabic/Previous_Congresses.html
- 8- موقع لقرارات الأمم المتحدة: WWW.un.org/arabic/documents/instruments/subjar.asp
- 9- موقع الاتحاد الدولي للاتصالات: WWW.itu.int/osg/csd/cybersecurity/gca/global-report/index.htm

-10 موقع: <http://arabi21.com/> عربي 21 للأخبار.

سادساً: الكتب اللغة الفرنسية

- 1- Céline Renard Castétes, Cours de Droit de l'internet, Edition 2010, Edition Lex tenso, Paris, France, 2010.
- 2- Mohamed Chawki, Combattre la cybercriminalité, Edition de saint Amans, Paris France, Mai 2009.
- 3- Myriam Quéméner, Joël Ferry, Cybercriminalité Défi mondial, Edition Economica, Paris, France, 2009.
- 4- Myriam Quéméner, Yves Charpenel, La Cybercriminalité, Edition Economica, Paris, France, 2010.

فهرس المحتويات

فهرس المحتويات

الصفحة	العنوان
	البسمة
	إهداء
	شكر وتقدير
أ- و	مقدمة
02	الفصل الأول : الإطار العام للجريمة الالكترونية
03	المبحث الأول مفهوم الجرائم الالكترونية
03	المطلب الأول تعريف و خصائص الجرائم الالكترونية
03	الفرع الأول: تعريف الجريمة الالكترونية والمصطلحات المتعلقة بالموضوع
03	أولاً: تعريف الجريمة الالكترونية
07	ثانياً: التعريف القانوني للجريمة المعلوماتية في التشريع الجزائري وبعض التشريعات المقارنة
08	ثالثاً: تعريف البحث والتحري
09	الفرع الثاني: خصائص الجرائم الالكترونية
09	أولاً: العولمة في صورتها القائمة
10	ثانياً: الجريمة الالكترونية عابرة للحدود
11	ثالثاً: صعوبة الاكتشاف
12	رابعاً: جريمة ناعمة (لا عنفية)
12	خامساً: سرعة التنفيذ ومحو الدليل
13	سادساً: تقادم الدعوى العمومية في الجرائم الالكترونية
14	المطلب الثاني : المجرم الالكتروني
14	الفرع الأول: مميزات المجرم الالكتروني

14	أولاً: ذكي
15	ثانياً: ماهر
15	ثالثاً: منظم ومختص
16	رابعاً: شخص عائد للإجرام
16	خامساً: شخص اجتماعي
16	الفرع الثاني: دوافع المجرم الإلكتروني
18	أولاً: دوافع شخصية
22	ثانياً: دوافع خارجية
24	المبحث الثاني: تجريم الأفعال الماسة بالمعالجة الآلية للمعطيات
24	المطلب الأول: الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في القوانين الجزائرية
24	الفرع الأول: الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات الجزائري
25	أولاً: المساس بأنظمة المعالجة الآلية للمعطيات
29	ثانياً: حماية حرمة الحياة الخاصة
30	ثالثاً: حماية حرمة رموز الدولة
30	الفرع الثاني: الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في القوانين المكملة
31	أولاً: الحماية في قانون التأمينات الاجتماعية
31	ثانياً: الحماية في قانون الملكية الادبية والفنية
32	ثالثاً: الحماية في نصوص التوقيع الإلكتروني
32	رابعاً: الحماية المتصلة بالمواصلات السلكية واللاسلكية
32	خامساً: الحماية من خلال قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها
34	المطلب الثاني: الجهود العالمية في مواجهة الاجرام الإلكتروني
34	الفرع الأول: الجهود الاقليمية
34	أولاً: جهود المجلس الأوربي
35	ثانياً: جهود مجموعة الثمانية
36	ثالثاً: جهود الإتحاد الإفريقي

36	رابعاً: الجهود العربية
37	الفرع الثاني: الجهود الدولية
37	أولاً: جهود هيئة الأمم المتحدة
39	ثانياً: جهود الاتحاد الدولي للاتصالات
41	الفصل الثاني: الجوانب القانونية للبحث و التحري عن الجريمة الالكترونية
44	المبحث الاول: آليات البحث و التحري عن الجرائم الالكترونية
44	المطلب الاول: الاجهزة المختصة بالبحث و التحري عن الجرائم الالكترونية
44	الفرع الأول: الاجهزة المكلفة بالبحث و التحري عن الجرائم الالكترونية
44	أولاً: على المستوى المحلي(الداخلي)
57	ثانياً: على المستوى الدولي
59	الفرع الثاني: الاشخاص المختصين بالبحث والتحري عن الجرائم الالكترونية ومميزاتهم
60	أولاً: الخصائص الفنية
61	ثانياً: التأهيل والتدريب
64	المطلب الثاني : تمديد الاختصاص بالبحث والتحري عن الجرائم الالكترونية
65	الفرع الأول: تمديد الاختصاص الاقليمي لوكيل الجمهورية
67	الفرع الثاني: تمديد الاختصاص الاقليمي لضباط الشرطة القضائية
70	المبحث الثاني: القواعد الاجرائية في البحث والتحري عن الجرائم الالكترونية
70	المطلب الأول: اساليب البحث والتحري الخاصة بالجرائم الالكترونية
70	الفرع الأول: التفتيش في مجال الجرائم الالكترونية
70	أولاً: تعريف التفتيش
71	ثانياً: محل التفتيش في البيئة الرقمية
76	ثالثاً: شروط التفتيش
78	الفرع الثاني: مراقبة واعتراض المراسلات الالكترونية
79	أولاً: مراقبة الاتصالات الالكترونية
80	ثانياً: اعتراض المراسلات السلكية واللاسلكية

82	المطلب الثاني: معوقات البحث والتحري عن الجريمة الالكترونية
82	الفرع الأول: معوقات تتصل بشخص الضحية
83	أولاً: عدم العلم والدراية بوقوع الجريمة
83	ثانياً: عدم التبليغ
84	ثالثاً: عدم الوقاية
84	الفرع الثاني: معوقات تتصل بجهات البحث والتحري
85	أولاً: نقص الخبرة أجهزة التحقيق
86	ثانياً: نقص التعاون الدولي
89	الخاتمة
92	قائمة الملاحق
105	قائمة المصادر والمراجع
113	فهرس المحتويات
	ملخص

المخلص

الملخص:

إن التطور التكنولوجي الرهيب الذي اوجد هذا النوع من الجرائم والمتمثلة في الجرائم الإلكترونية ذات الميزات المتعددة والتي تنفذ عن طريق أشخاص ذو خصائص عقلية وفكرية مميزة هذا كله يعمل على إعاقة عملية اكتشافها بسرعة ودقة، وعليه سار المشرع الجزائري كغيره من دول العالم على تجريم الأعمال الإلكترونية الضارة وذلك وفق قانون العقوبات وقانون الإجراءات الجزائية والقوانين الخاصة والمتعلقة بها مرسخا ترسانته القانونية بمجموعة من المراسيم و اللوائح، كما أنشأت الدولة أجهزة خاصة لمتابعة ومكافحة هذه الجريمة كمخابر الدرك والأمن الوطنيين والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والاتصال تعمل بأحدث الطرق العلمية المتطورة.

إن الجريمة الإلكترونية مهما كانت الاجراءات التي تتم مكافحتها بها فهي تتطور مستمر بتطور وسائل التكنولوجيا الحديثة.

وقد أثارت وستبقى تثير إشكالات إجرائية بالأساس في عملية متابعتها والقبض على مجرميها كون القانون هو من يلحق بالجريمة وليس العكس فالجريمة سبابة دائما وعلى القانون سد الثغرات المتواجدة فيه.

Résumé :

L'important développement technologique qui a créé ce genre de crimes, en l'occurrence la cyber criminalité aux multiples caractéristiques qui se font exécutés par des personnes aux aptitudes mentales exceptionnelles, tout cela fait qu'il est difficile de les découvrir sur le coup et d'une manière précise, voilà pourquoi le législateur algérien tout comme les autres pays du monde, condamne la cyber criminalité nocive selon le code pénale et les lois spécifiques à ce genre de crimes, tout en renforçant son arsenal législatif par des décrets et des règlements, l'état a aussi créé des institutions spécialisées pour suivre et combattre ces crimes, ces institutions étant les laboratoires de gendarmerie et de sureté nationale ainsi que la commission nationale pour la prévention des crimes liés aux technologies de l'information et de la communication qui utilise la pointe de la technologie.

Pour finir on peut dire que la cyber criminalité aussi déterminé qu'on soit à la combattre évolue selon l'évolution des nouvelles technologies, elle a depuis toujours créé des problèmes procéduraux surtout en ce qui concerne son suivi et l'arrestation de ses criminels et continuera toujours à le faire.