جامعة زيان عاشور -الجلفة-
Zian Achour University of Djelfa
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

قسم الحقوق

الآليات القانونية لمكافحة الجرائم الماسة بالأمن الالكتروني

مذكرة ضمن متطلبات
نيل شهادة الماستر في الحقوق تخصص القانون الجنائي و العلوم الجنائية

إعداد الطالب :
- بن عزوز فاطمة اخلاص
- سالمي وهيبة

إشراف الأستاذ:
-د. حمزة عباس

لجنة المناقشة

-د/أ. بن صادق أحمد	رئيسا
-د/أ. حمزة عباس	مقررا
-د/أ. بن يحي أبو بكر الصديق	ممتحنا

الموسم الجامعي 2020/2019

2020/M071P/M1539019996/M1539020713

إهـــداء

إلى من عمل بكدّ في سبيلي وعلمني معنى الكفاح وأوصلني إلى ما أنا عليه فأرجو من الله أن يمدّ في عمرك والدي العزيز

إلى التي وهبت حياتها وأصرّت أن تكمل رسالتها في الحياة فأنارت لنا السبيل وكانت لنا المثل الأعلى إلى التي لو أهديتها حياتي لن تكف في حقها أمّي ثمّ أمّي الحبيبة حفظها الله لنا.

إلى من عرفت معهم معني الحياة إخوتي وأخواتي.

أحبكم حبّا لو مرّ على أرض قاحلة لتفجرت منها ينابيع المحبة.

فاطمة إخلاص / وهيبة

شكـر وتقديـر

من لم يشكر الناس لم يشكر الله، الحمد لله الذي تتم بنعمته الصالحات والصلاة والسلام على نبي الرحمة سيدنا محمد وعلى آله وصحبه الكرام، لا يسعني في هذا المقام إلا أن أتقدم بالشكر الجزيل للأستاذ الفاضل "حمزة عباس" على تفضله بالإشراف على إنجاز هذا العمل وتكرمه بتقديم النصح والتوجيه اللذان من شأنهما تذليل الصعاب حتى تسنى لي الوصول إلى هذه المرحلة ليرى بحثي هذا النور.

مقدمـــة :

مع النمو المستمر للثورة المعلوماتية الذي يعيشه عصرنا و يشهده حاضرنا على جميع الأصعدة و في شتى مجالات الحياة المعاصرة، لدرجة حتى أصبحت جميع القطاعات المختلفة تعتمد في أداء عملها بشكل أساسي على استخدام الأنظمة الإلكترونية، لما تتميز به من عنصري السرعة والدقّة في تجميع المعلومات كتخزينها ومعالجتها، ومن ثم نقلها وتبادلها بين الأفراد والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين عدة دول .

لكن وعلى الرغم من المزايا الهائلة التي تحققت، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبية والخطيرة جراء سوء استخدام هذه التقنية، فإن بعض الأشخاص يحاولون استغلال المخترعات العملية وما تقدمه من وسائل متقدمة في ارتكاب العديد من الجرائم التقليدية ، مستغلين الإمكانيات الهائلة لهذه المستحدثات أو استحداث صور أخرى من الإجرام يرتبط بهذه التقنيات التي تصير محال لهذه الجرائم أو وسيلة لارتكابها، وقد تزايدت معدلات هذه الجرائم في العقدين الأخيرين بكثرة وبصورة أدت إلى ظهور ظاهرة إجرامية جديدة تعرف بالإجرام الالكتروني.

على ضوء ذلك، فإن هذه الظاهرة الإجرامية التقنية أثارت العديد من الإشكالات في نطاق قانون الإجراءات الجزائية ، الذي وضعت نصوصه لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المرتبطة بها، وهو ما لا يمكن تصوره في جريمة ترتكب في بيئة افتراضية تقنية لا تخلف أي أثار مادية محسوسة و لا يرتكبها إلا مجرمون يتسمون بالذكاء والدرية في التعامل مع مجال المعالجة الآلية للمعطيات والإلمام بالمهارات كالمعارف التقنية، كما أن هذه الجريمة تتم في الخفاء و يعمد مرتكبوها إلى إخفاء أنشطتهم الإجرامية عن طريق التلاعب بالبيانات، والذي غالبا ما يتحقق في غفلة من المجني عليه، فضال عن سهولة تدمير الدليل ومحوه من مسرح الجريمة ،مما جعل الأدلة في الجريمة الإلكترونية صعبة الإثبات .

أهمية الدراسة :

من هنا تتجلى أهمية دراسة هذا الموضوع من خلال معرفة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ،وإلقاء العبء على الدولة بوضع التشريعات اللازمة لحماية المجتمع منها، بالإضافة إلى أهمية معرفة مدى خطورة جرائم الالكترونية التي تمس حياة الأفراد وتهدد الأمن القومي والسيادة الوطنية، وكذلك تهديد إبداع العقل البشري ولذلك يجب الإلمام بماهية جرائم الالكترونية وطبيعتها وإظهار موضوعها

وخصائصها ومخاطرها وحجم الخسائر الناجمة عنها ودوافع مرتكبيها، وهذا يتخذ أهمية استثنائية لسلامة التعامل مع هذه الظاهرة ونطاق مخاطرها الاقتصادية والأمنية والاجتماعية والثقافية.

أسباب الدراسة :

فمن الأسباب التي دفعتنا إلى تناول هذا الموضوع بالدراسة، راجع لحداثة الموضوع، والتزايد المستمر للجرائم الالكترونية، و كذا الرغبة في التعمق في البحث ومواجهة النشاط الإجرامي الالكتروني.

الهدف من الدراسة :

الهدف من دراستنا هو تعريف بالجريمة الالكترونية وتطورها في وفتنا العاصر وكذا تسليط الضوء على خطورة هاته الجريمة والتي تمس كل من الأفراد والدولة وأيضا تسليط الضوء على آليات مكافحات الجريمة الالكترونية على المستويين الدولي من خلال الاتفاقيات الدولية والتعاون القضائي والوطني من خلال إنشاء قوانين خاصة وأجهزة

طرح الإشكالية :

عليه فالإشكالية الرئيسة لهذه الدراسة هي:

ما هي الجريمة الالكترونية و ما مدى فاعلية الآليات القانونية في الحد منها ؟

منهج الدراسة :

حرصنا منا في هذه الدراسة و نزولا عند موجبات البحث العلمي، و كما هو متعارف عليه فإن طبيعة البحث في المواضيع القانونية التي تفرض علينا نوعية المنهج المتبع فلقد اخترنا منهجا يلم بدراسة الموضوع بكل جوانبه، و هو المنهج الوصفي التحليلي الذي يهدف إلى بيان إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، وذلك من خلال الرجوع إلى المرجع القانوني والتخصصات والرسائل والدراسات والبحوث والاتفاقيات الدولية ذات صلة بالموضوع .

الفصل الأول
الإطار المفاهيمي للجريمة الالكترونية

نظرا للتطورات التكنولوجية التي شهدها العالم، واختراع الحاسوب، أصبح يستخدم في العديد من المجالات العملية والعملية التعليمية كالتحضير لبعض الدروس وتلقي المحاضرات والترفيه مرورا لاستخدامات متنوعة في مجالات أمنية ومالية ، أصبح الحاسوب عرضة للتهديد و الاختراق من أفراد وتنظيمات ودول في استعمالات غير قانونية تهدف للحصول على أموال أو معلومات أمنية حساسة بطرق غير قانونية وعلى قدر عال من الذكاء والتمرس والحنكة ،وهنا ظهر ما يعرف بمفهوم الجرائم الإلكترونية فهي ظاهرة إجرامية مستجدة نسبيا تقرع في جنباتها أجراس الخطر لتنبه العصر الراهن لحجم المخاطر و هول الخسائر الناجمة عنها و التي تستهدف البيانات والمعلومات بطرق غير مشروعة الأمر الذي قد ينجر عنه ارتكاب جرائم لها علاقة بهذا المجال و نظرا لحداثة هذه الجريمة فقد اختلف الفقهاء في وضع تعريف موحد لها فهي تختلف عن الجريمة التقليدية من حيث خصائصها التي تميزها عن نظيرتها و طرق استعمالها و دوافعها كما أن المجرم الإلكتروني يختلف عن المجرم العادي و كذلك أنواعها ، فهي تتعدد وتأخذ أنواعا مختلفة كالجرائم ضد الأفراد والجرائم ضد الملكية بالاعتداء والتدمير لمختلف البرامج إضافة للجرائم ضد الدول و الحكومات والتي تعمل على مهاجمة المواقع الرسمية وأنظمة الشبكات الحكومية والتي تستخدم تلك التطبيقات على المستوى المحلي والدولي كالهجمات الإرهابية على شبكة الانترنت وغالبا ما يكون هدفها سياسي بحت.

ولعل أهم أهداف الجريمة الالكترونية هو ا الوصول إلى المعلومات والحصول على المال بهذه الطرق أسهل ومن دون بذل أي جهد و هذا ما سوف نتطرق إليه في هذا الفصل

المبحث الأول :ماهية الجريمة الإلكترونية .

المبحث الثاني :مظاهر الجريمة الإلكترونية .

المبحث الأول : ماهية الجريمة الالكترونية

عرف العالم الجريمة الالكترونية حديثا, لتحدث تغيرا و نقلة هائلة في سرعة تنفيذها فلقد عرفت تطورا ملحوظا باستخدام أخر ما توصلت إليه العلوم التقنية و التكنولوجية من اختراعات علمية هائلة كظهور الحاسوب الالكتروني ووجود ما يعرف بالانترنت التي صارت الفضاء الأكثر استقطابا لهذا النوع من الجرائم ,ولكن الإحاطة بمفهوم الجريمة الالكترونية الدقيق لا يزال محل خلاف فقهي ,فهي ظاهرة إجرامية مستحدثة عن الجريمة التقليدية و تختلف عنها من حيث المفهوم و الخصائص وعليه سيتم تقسيم هذا المبحث إلى مطلبين :

-المطلب الأول : مدلول الجريمة الالكترونية

- المطلب الثاني :أركان الجريمة الالكترونية

المطلب الأول : مدلول الجريمة الالكترونية

إن مسالة وضع تعريف لأي مفهوم و ضبطه صار من الصعوبة لتعدد المدارس و المناهج و السياقات التي برزت فيها الظاهرة وهو ما يخص الجريمة الالكترونية و التي تحوي مقطعين هما الجريمة و الالكترونية, فإذا كانت الجريمة هي تلك السلوكيات و الأفعال الخارجة عن القانون فان المصطلح الثاني جاء لوصف فكرة إن يتم استعمالها من طرف الحاسب ولكن لم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة الالكترونية فهنالك عدة تسميات لها منها الجريمة المعلوماتية,جرائم إساءة استخدام تكنولوجيا المعلومات و الاتصال, جرائم الكمبيوتر و الانترنت, الجرائم المستحدثة[1] , الغش المعلوماتي , الجرائم السيبرانية فلقد انقسم الفقهاء إلى اتجاهين في تعريف الجريمة الالكترونية الاتجاه الضيق و الاتجاه الواسع كما أن لها أركان فالجريمة لا تقوم إلا بتوفرها وهذا ما سأتناوله في الفرعين الموالين

الفرع الأول : تعريف الجريمة الالكترونية :

[1] عادل يوسف عبد النبي شكري,بحث بعنوان الجريمة المعلوماتية و أزمة الشرعية الجزائية,جامعة الكوفة,2008,ص 112

لم يكن تحديد مفهوم للجريمة الالكترونية في متناول المختصين وهذا للاختلاف في وضع إطار موحد يضبط الظاهرة و يجد لها تفسيرا في ظل اختلاف المدارس و تنوع الخصوصيات, فالبعض من الفقهاء ينظر إليها بمفهوم ضيق و البعض الأخر بنظر إليها بالمفهوم الواسع و سأحاول التطرق لذلك في البندين الموالين

البند الأول: الاتجاه الضيق من تعريف الجريمة الالكترونية :

عرف أنصار الاتجاه الضيق الجريمة الالكترونية بأنها "كل فعل غير مشروع ,يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم لارتكابه من ناحية , لملاحقة تحقيقه من ناحية أخرى"[1] ومن بين التعريفات أيضا تعريف الفقيه MERWE الجريمة المعلوماتية هي "الفعل الغير مشروع الذي يتورط في ارتكابه الحاسب الآلي أو هو الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية "[2]

فيما ذهب الفقيه ROSBLAT على أنها "كل نشاط غير مشروع موجه لنسخ أو تغير أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو تغيرها أو حذفها أو التي تحولت عن طريقه"[3]

كما عرفها كل من A.HARD,TOTT, COSTER بأنها "تلك الجرائم التي يكون قد حدث في مراحل ارتكابها بعض العمليات الفعلية داخل الحاسوب "و بمعنى أخر هي "تلك الجرائم التي يكون للحاسب الآلي فيها دورا ايجابيا أكثر من سلبيته"[4]

إن التعريفات السابقة جاءت قاصرة على الإحاطة بأوجه ظاهرة الإجرام الالكتروني فبعض من فقهاء هذا الاتجاه ركز على معيار موضوع الجريمة و البعض الأخر على وسيلة ارتكابها و آخرون على معيار النتيجة

---

[1] حمزة بن عقون,السلوك الإجرامي للمجرم المعلوماتي,بحث مكمل لنيل شهادة الماجستير في العلوم القانونية ,تخصص علم الإجرام و العقاب,جامعة باتنة,2011_2012, ص 13

[2] طارق إبراهيم الدسوقي عطية , الأمن المعلوماتي النظام القانوني للحماية المعلوماتية ,الإسكندرية مصر, ص 153

[3] طارق إبراهيم الدسوقي عطية,المرجع السابق, ص 154

[4] احمد خليفة الملط ,الجرائم المعلوماتية ,الطبعة الثانية,دار الفكر الجامعي,إسكندرية مصر,ص30

البند الثاني : الاتجاه الموسع من تعريف الجريمة الالكترونية :

على عكس الاتجاه السابق يرى أنصار هذا الاتجاه ضرورة التوسيع من مفهوم الجريمة الالكترونية ,فالبعض يرى إن هذه الجريمة هي كل فعل ضار يستخدم الفاعل الذي يفترض أن لديه معرفة بتقنية الحاسوب ,نظاما حاسوبيا أو أو شبكة حاسوبية للوصول إلى البيانات و البرامج بغية نسخها أو تغيرها أو حذفها أو تزويرها آو تخريبها و جعلها غير صالحة أو حيازتها أو توزيعها بصورة غير مشروعة[1]

أما البعض الأخر يغرفونها بأنها كل نشاط إجرامي تستخدم فيه التقنية الالكترونية (الحاسب الآلي الرقمي و شبكة الانترنت) بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف[2], و في تقرير الجرائم المتعلقة بالحاسوب اقر المجلس الاروبي بقيام الجريمة في كل حالة يتم فيها تغير معطيات أو بيانات أو برامج أو محوها أو كتابتها أو أي تدخل أخر في مجال انجاز البيانات أو معالجتها و تبعا لذلك تسببت في ضرر اقتصادي أو فقد حيازة ملكية شخص أو بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص أخر[3]

ومن خلال هذه التعاريف يتضح صعوبة الأخذ بهذا الاتجاه لان أنصاره يتجهون إلى أن الجرائم الالكترونية هي تلك التي يكون محلها الحاسب الآلي فقد لا يعدو أن يكون محلا تقليديا في بعض الجرائم كسرقة الحاسب الآلي نفسه على سبيل المثال و من ثم لا يمكن إعطاء وصف الجريمة الالكترونية على سلوك الفاعل لمجرد أن الحاسب الآلي أو أي من مكوناته كانوا محلا للجريمة كما انه يمكن أن ترتكب جريمة و يستعمل الحاسب الآلي ولا نكون أمام جريمة الكترونية كمن يقوم بالاتصال بواسطة الحاسب الآلي بشركائه في جريمة السطو على بنك

[1] كامل فريد السالك,الجريمة المعلوماتية,ندوة التنمية ومجتمع المعلوماتية,حلب,21-23 تشرين الأول ,بدون صفحة

[2] صغير يوسف,الجريمة المرتكبة عبر الانترنت,مذكرة لنيل شهادة الماجستير في القانون,تخصص القانون الدولي للأعمال,جامعة مولود معمري تيزي وزو,06-03-2013,ص09 نقلا عن كحلو علي ,جرائم الحاسوب وأساليب مواجهتها ,مجلة صادرة عن مديرية الأمن الوطني,العدد84, 2007,ص51

[3] مليكة عطوي ,,,,

و بخصوص التعريف القانوني للجريمة الالكترونية فقد اصطلح المشرع الجزائري تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و عرفها بموجب أحكام المادة **02** من القانون رقم **09-04** على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية"[1]

أي أن المشرع الجزائري تبنى معيار دور النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات كما بينها في تعديل قانون العقوبات بموجب قانون رقم **15-04** و المتمم للأمر **156-66** من المادة **394 مكرر إلى 394 مكرر 7** و ترك مجال واسع لأي جريمة أخرى ترتكب عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية مما يجعل هذا التعريف يشمل عدد هائل من الجرائم,ومن أمثلة عن الجريمة الالكترونية في الجزائر تسرب أسئلة البكالوريا سنة 2016 , قيام القرصان الجزائري حمزة بن دلاج بقرصنة حسابات بنكية عالمية[2]

الفرع الثاني : خصائص الجريمة المعلوماتية:

إن التقدم الكبير في مجال المعلوماتية يسر حياة الإنسان و وفر عليه جهد كبير و طبع شتى معاملاته بالسرعة الفائقة ولكن بالمقابل فقد ارتبط استعمال هذه الوسائل الحديثة بظهور جرائم جديدة و زيادة حدة بعض الجرائم فهذه التقنية أوجدت ألوانا جديدة من الجرائم و أسبغت عليها خصائص ميزتها عن الجرائم سواء تعلقت هذه الخصائص بالشخص الذي يقدم على هذه الجرائم فميزته عن المجرم التقليدي أو تعلقت بالجريمة ذاتها و صعوبة اكتشافها ا وثباتها أو تعلق الأمر بالنطاق المكاني لهذه الجريمة

أولا : جريمة عابرة للحدود الوطنية

[1] [1] القانون رقم 09-04 الصادر في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها الجريدة الرسمية العدد 47

[2] جازيه سليماني,موقع العربي الجديد ,تاريخ الدخول 2020-08-10 الساعة 55: 15

بعد ظهور شيكات المعلومات لم يعد هناك حدود تقف أمام نقل المعلومات فلقد أصبح من السهل إمكانية ربط عدد هائل لا حصر له من الحواسيب عبر العالم بهذه الشبكة بحيث يغدو أمر نقل كميات كبيرة من المعلومات و تبادلها بين أنظمة يفصل بينها ألاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية إذ غالبا ما يكون الجاني في بلد و المجني عليه في آخر كما قد يكون الضرر المتحصل في بلد أخر ثالث في الوقت نفسه

و عليه تتخذ جرائم الالكترونية شكلا جديدا من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية[1] ونتج عن هذه الخاصية العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي لهذه الجريمة و كذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية[2] و غيرها من النقاط التي تثيرها الجرائم العابرة للحدود الوطنية بشكل عام

ثانيا : صعوبة إثبات و اكتشاف الجريمة الالكترونية

من المفترض إن اكتشاف الجرائم يتم عن طريق الفحص و التدقيق أو عن طريق الشكاوى التي يقدمها المجني عليهم إلا إن إثبات الجريمة الالكترونية يحيط بها الكثير من الصعوبات و التي تتمثل في إن جهات التحقيق لم تصل إلى المعرفة الواسعة و الإحاطة الكاملة بهذه التكنولوجيا الحديثة و صعوبة اكتشاف هذه الجرائم لأنها لا تترك أثرا خارجيا فالجريمة الالكترونية لا عنف فيها كالسرقة مثلا و إنما هي أرقام و بيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسوب وليس لديها أي اثر خارجي مرئي[3] و أيضا الضحية في هذه الجرائم تمتنع في الغالب عن التبليغ عنها

لهذا لا نعجب إذا وجدنا إن أكثر هذه الجرائم لم تكتشف إلا بمحض الصدفة و هناك من يشير إلى أن هذه الجرائم لم يكتشف منها إلا ما نسبته 01% فقط و ما تم الإبلاغ عنه إلى السلطات

[1] أسامة احمد المناعة,جلال محمد ألزعمي,جرائم تقنية نظم المعلومات الالكترونية,الطبعة الثالثة,دار الثقافة للنشر و التوزيع , 2014 ,ص93

[2] د. نائلة عادل محمد فريد قورة,جرائم الحاسب الاقتصادية,دراسة نظرية وتطبيقية,دار النهضة العربية, القاهرة,2003,ص49

[3] سيناء عبد الله محسن,المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية و الوطنية, الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر,الدار البيضاء,المملكة المغربية,2007,ص52

المختصة لم يتعدي 15% من النسبة السابقة و حتى ما طرح أمام القضاء من هذه الجرائم فان الأدلة فيه لم تكن كافية إلا في حدود الخمس[1]

ثالثا : خصوصية مرتكب الجرائم الالكترونية

يتصف المجرم المعلوماتي بخصائص معينة تميزه عن المجرم الذي يرتكب جرائم تقليدية ,فإذا كانت الجرائم التقليدية لا تتطلب مستوى علمي معرفي للمجرم في عملية ارتكابها فان الأمر يختلف بالنسبة للجرائم الالكترونية فهي جرائم فنية تقنية في الغالب و الأشخاص الذين يقومون بارتكابها عادة يكونوا من ذوي الاختصاص في مجال تقنية المعلومات الالكترونية

أو على الأقل شخص لديه حد أدنى من المعرفة ة القدرة على استعمال جهاز الحاسوب و التعامل مع شبكة الانترنت كما إن الباعث إلى ارتكاب المجرم لهذا النوع من الجرائم قد تكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي , فقد يرتبط الدافع بحب التعلم و الاستكشاف, كما قد بالسياسة و الايدولوجيا.... إلى غير ذلك من الدوافع كما يتميز مجرم المعطيات بفئاته و أنماطه المختلفة و هو نوعين رئيسيين :

الأول هم الهواة المولعون بالمعلوماتية,و الثاني محترفو الجرائم الالكترونية و أساس التميز بين النوعين هو الباعث أو الدافع إلى ارتكاب الجريمة ,بينما هو ساذج لدى النوع الأول لا يتعدي الرغبة في الاستطلاع و الاستكشاف, أما النوع الثاني فهو خبيث قد يكون دافع مالي آو سياسي آو غيره[2]

رابعا : الجرائم الالكترونية فادحة الأضرار

إن الاعتماد المتزايد على الحاسب الآلي في إدارة مختلف الأعمال في شتى المجالات ضاعف من الأضرار و الخسائر التي تخلفها الاعتداءات على معطيات هذا الحاسب, لا سيما إذا كانت

[1] د.سعيد عبد الطيف حسن,إثبات جرائم الكمبيوتر و الجرائم المرتكبة عبر الانترنت,الطبعة الأولى, دار النهضة العربية,القاهرة 1999,ص95

[2] د. عبد الله حسين محمود,سرقة المعلومات المخزنة في الحاسب الآلي,دار النهضة العربية,الطبعة الثانية,القاهرة,2002,ص36

تمثل قيما مالية, خاصة مع ازدياد اعتماد البنوك و المؤسسات المالية و مختلف الشركات على الحاسب الآلي في تسيرها

و في هذا الخصوص تشير الدراسات إلى أن الأضرار الناجمة عن الجرائم الالكترونية تفوق بكثير تلك الناجمة عن الجرائم التقليدية [1] ففي الولايات المتحدة الأمريكية و حسب مكتب التحقيقات الفيدرالي (FBI) فالجريمة الالكترونية تكلف خسائر تقدر بمائة و خمسين 150 ضعف ما تكلفه الجريمة العادية , وان الخسائر الناجمة عن 139 عملية غش معلوماتي وقع على البنوك بلغت ثمانمائة ألف دولار ($800000) عام 1981 كما أن الغش المعلوماتي كان السبب في حدوث خمسين 50 حالة إفلاس في ثلاثمائة و أربعة وخمسين 354 بنكا بين شهري جانفي 1985 و جوان 1987

و في دراسة للمركز الوطني لجرائم الكمبيوتر و البيانات قدرت خسائر الجرائم المعلوماتية بين ثلاث (03) و خمس (05) مليارات دولار أمريكي و في المملكة المتحدة آجرت لجنة المراجعة المحاسبية دراسة خلال عدة سنوات تبين منها أن خسائر 64 حالة عام 1984 قدرت ب 1133487 جنيها استراليا

وفي الجزائر فقد سجلت فرق مكافحة الجرائم الالكترونية التابعة للمديرية العامة للأمن الوطني 4210 جريمة الكترونية خلال سنة 2019 فلقد شهدت ارتفاع محسوس و ذلك بالتزامن مع بداية الحراك الشعبي في الجزائر[2]

خامسا : الجريمة الالكترونية جاذبة للمجرمين

إذا كانت بعض الجرائم التقنية تحتاج من مرتكبها إلى قوة عضلية لتنفيذها فان الجرائم الالكترونية لا تحتاج إلى مثل تلك القوة العضلية و إنما تحتاج إلى قوة علمية و قدر من الذكاء و مهارة في توظيف ذلك و الجاني في سبيل تنفيذها لا يحتاج من الوقت سوى ثواني او دقائق و لا

[1] Philip rose , la criminalité informatique edition dahlab imprimerie.alger pp 22-30

[2] منيرة ابتسام طوابلي,تسجيل 4210 جريمة سيبيرانية خلال2019,موقع المحور اليومي , 05-02-2020

يحتاج من القوة العضلية غير تحريك الأنامل من على وسائل الإدخال و قد يتسبب بذلك في حصول خسائر فادحة رغم إن جريمته قد لا ترى بالعين

ونعومة هذه الجريمة وما تدره من أرباح و من إشباع للفضول عند البعض جعلها من الجرائم الجاذبة للمجرمين [1] .

المطلب الثاني : أركان الجريمة الالكترونية

لكي يكمن القول بوجود جريمة ما , فان المشرع يتطلب كأصل عام ضرورة وجود أركان وبغير هذه الأركان لا يمكن القول بوجود جريمة و تتمثل هذه الأركان في الركن الشرعي الذي يتمثل في النصوص القانونية التي تجرم الفعل و الركن المادي و الذي يتمثل في السلوك الإجرامي و العلاقة السببية و كذلك النتيجة أما الركن الثالث فهو الركن المعنوي الذي يتجسد في القصد الجنائي للجريمة الالكترونية

الفرع الأول : الركن الشرعي

يقصد بالركن الشرعي للجريمة وجود نص يجرم الفعل ويوضح العقاب المترتب عليه وقت وقوع الفعل ,يبنى على ذلك عدم جواز ملاحقة الشخص عن فعل ارتكبه قبل صدور نص التجريم وعن فعل ارتكبه بعد إلغاء نص التجريم ,كما لا يجوز قياس أفعال لم ينص المشرع على تجريمها و على القضاة التقيد بمدلول النص و الالتزام بمعاينته[2]

لذا ينتج عن مبدأ الشرعية قاعدة هامة وهي عدم رجعية القانون الجنائي و هذا عملا بما نصت عليه المادة **01** من قانون العقوبات و التي قضت "لا جريمة و لا عقوبة أو تدبير امني بغير قانون"[3] , المشرع الجزائري استحدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل

[1] أسامة احمد المناعسة, جلال محمد الزعبي,صايل فاضل الهواوشة,جرائم الحاسب الآلي و الانترنت , دراسة تحليلية مقارنة,دار وائل لنشر,عمان الأردن ,الطبعة الأولى,2001,ص107

[2] اسامة احمد المناعسة ,حجلال محمد الزعبي,جرائم تقنية نظم المعلومات الالكترونية,الطبعة الثالثة,دار الثقافة للنشر و التوزيع,عمان,2014,ص93

[3] الأمر رقم 66-156المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات ,جريدة الرسمية ,عدد 44

الثالث الخاص بجرائم البيانات و الجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات [1]

الفرع الثاني : الركن المادي

الركن المادي هو ما يعرف بالسلوك الإجرامي الذي يستوجبه القانون كمناط للعقاب على هذه الجريمة على أن يتحقق الضرر للسلوك الإجرامي كشرط لازم لتوقيع العقاب عليه من طرف المشرع و يستوجب وجود علاقة سببية بين هذا السلوك و النتيجة (الضرر)

أولا : السلوك الإجرامي

يتمثل السلوك الإجرامي للجريمة الالكترونية في السلوك الخارجي الذي يقوم به المجرم الالكتروني, وهو كل فعل مادي يسبب ضرر سواء اتجهت نيته إلى حصول هذا الضرر أم لم تكن , و هذا السلوك المادي يجعل هذه الجريمة بواسطة الانترنت ذات ميزة و خاصية موحدة تباشر من حيث النشاط المادي فيها , بحيث طور هذا السلوك عقلية الفاعل الذكية و التي استطاعت أن تخرج من تقليدية السلوك الجرمي إلى مساحات أكثر تعقيدا أوجدت بلا شك صعوبات كثيرة[2]

بالتالي فان ارتكاب الجريمة عبر الانترنت يحتاج بالضرورة إلى منطق تقني بعدمه لا يستطيع الشخص حتى الاتصال بشبكة الانترنت , و تظهر القيمة الموحدة في ضرورة النشاط التقني و إلا فقدت الجريمة أساسياتها

ثانيا : النتيجة الإجرامية

يقصد بالنتيجة الإجرامية الأثر المادي الذي قد يحدث أي التغير الذي يحصل في المحور الخارجي كنتيجة للسلوك الإجرامي الذي يقيم عليه المشرع أحكاما قانونية ,فالنتيجة الضارة لها

[1] عاقلي فضيلة, الجريمة الالكترونية و إجراءات مواجهتها من خلال التشريع الجزائري, مداخلة ألقيت في أشغال المؤتمر الدولي حول الجرائم الالكترونية ,الاتحاد العالمي للمؤسسات العلمية,طرابلس,لبنان,24-25 مارس 2017,ص120

[2] اسامة احمد المناعسة,جلال محمد الزعبي , المرجع السابق ,ص53-55

مفهومان أولهما المفهوم المادي و ثانيهما المفهوم القانوني ,فالمدلول المادي يعني المخلفات التي أحدثتها الجريمة في المحور الخارجي و يوقع القانون على حدوثها عقوبة [1]

و يجب أن يكون للجريمة طبيعة مادية ملموسة في المحيط الخارجي لتتم المعاقبة عليها , و لكن توجد بعض الجرائم التي ليس لها نتيجة و تعرف بالجرائم السلبية

و من هذا المنبر بدت أهمية الاعتراف بالمدلول أو المعنى القانوني للنتيجة دون الاخد بعين الاعتبار حصول الضرر أولا . فمجرد الإخلال بهذه المصلحة ينتج قيام حصول الجريمة من الجهة القانونية

و يطرح موضوع النتيجة الجرمية في جرائم الانترنت مشاكل عديدة , مثلا مكان و زمان تحقق النتيجة , فلو قام احد المجرمين في فرنسا باختراق جهاز خادم Server احد بنوك أمريكا,وهذا الخادم يتواجد في ايطاليا , فكيف يمكن العلم بوقت الجريمة

فهل هو توقيت بلد المجرم أم توقيت جهاز الخادم في ايطاليا , و تطرح أيضا إشكاليات و صعوبات في القانون الواجب التطبيق في هذا الأمر لان هناك أبعاد عالمية في هذا النطاق [2]

ثالثا : العلاقة السببية

تتمثل العلاقة العلاقة السببية في الصلة التي تربط بين الفعل و النتيجة و تثبت إن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة و أهمية الرابطة السببية ترجع إلى إسناد النتيجة إلى الفعل هو شرط أساسي لتقرير مسؤولية مرتكب الفعل عن النتيجة ولا بد من تواجد العلاقة أو الرابط السببية في كافة الجرائم العمدية و لكن يجدر الإشارة انه في بعض الأوضاع قد يحصل النشاط الإجرامي و لكن لا تتحقق النتيجة ,بالتالي نكون إمام حالة من حالات الشروع في السلوك الجرمي فقط لكن يواجهنا أشكال في الجانب السيبيراني عند محاولة وصل النشاط الجرمي بالنتيجة الضارة

[1] حنان ريحان مبارك المضحكي,الجرائم المعلوماتية ,دراسة مقارنة , الطبعى الاولى,منشورات الحلبي الحقوقية ,بيروت, 2014. ص87 88

[2] عماد مجدي عبد المالك,جرائم الكمبيوتر و الانترنت,دار المطبوعات الجامعية.مصر 2001,ص37

التي حدثت بسببه ‘نتيجة لصفة هذه الجرائم و طبيعتها المعقدة و الصعبة , فمن أن تتولد عدة أضرار من نشاط جرمي واحد[1]

الفرع الثالث : الركن المعنوي

لا يقتصر قيام المسؤولية الجنائية من الجهة القانونية أن يصدر من الشخص الجاني نشاط إجرامي ذو طابع مادي فقط وإنما يستلزم زيادة على ذلك توافر الركن المعنوي فهو يعتبر جوهر المسؤولية الجنائية عندما يعتبر الركن المادي مظهرها الخارجي

فيستلزم وجود رابطة أو علاقة سببية بين النشاط الإجرامي و إرادة الجاني المنطلقة إلى جعل النتيجة الغير المشروعة كبصمة للسلوك الإجرامي.و هو الخطأ العمدي فيتطلب أن يدرك المجرم انه يفعل نشاط غير مشروع. و أيضا أن تكون له الحرية المطلقة في الاختيار للقيام بهذا الفعل الإجرامي , أما الإهمال و الرعونة فينتجان الخطأ الغير العمدي فهو لا يشترط من المجرم توافر الإرادة [2]

بالتالي الركن المعنوي هو الاتجاه الذهني آو النفسي للجاني انه يمثل أساس القانون الجنائي ففي حيزة تتوافر كامل أساسيات المسؤولية الجنائية , فالرابطة التي تصل بين شخصية الجاني و ماديات الجريمة هي محل الجرم في مفهوم استحقاق العقاب.

و تجدر الإشارة أن القصد الجنائي في الجرائم العمدية قد يكون قصدا عاما آو خاصا فالأول يقوم باتجاه إرادة المجرم للقيام بالسلوك الإجرامي مع توافر علمه بكامل عناصر الجريمة أما الثاني إلا و هو القصد الجنائي الخاص , فيتحقق بالحالة آو الوضعية النفسية الشخصية المرتبطة بالنتيجة الضارة آو الدافع و ليست متعلقة بالسلوك المادي المكون للمجرم [3]

هذا في الجرائم العمدية ,أما الغير عمدية فهي بغير قصد آو واقعة عن طريق الخطأ,سواء لم يكن في حسبان الفاعل نتيجة سلوكه أو عدم سلوكه ,وكان في مقدوره أو من واجبه حصولها و

[1] حنان ريحان مبارك المضحكي, المرجع السابق ص 90

[2] المرجع نفسه ,ص 91

[3] محمد زكي ابو عامر,الإجراءات الجنائية ,الطبعة السابعة , دار الجامعة الجديدة ,مصر 2002, ص 205

يكون الخطأ أما عاما آو خاصا , و يقوم الأول بواقعة الإخلال بالقواعد العامة التي تكتسب من خبرة الإنسان العامة,أما الخطأ الخاص فهو الذي يحصل نتيجة لمخالفة القواعد المأخوذة من الشرائع و الأنظمة ,فيقوم هذا الخطأ بمخالفة قواعد قانونية ملزمة[1]

و بخصوص الركن المعنوي في الجريمة الالكترونية هو نفسه الركن المعنوي في جميع الجرائم التي تقتضي وجود قصد جنائي عام و خاص فالأول يكون موجودا آو محققا في جميع الجرائم التي الالكترونية ,إلا أن القصد الخاص قد يتحقق في بعض الجرائم دون الأخرى , لكن هذا لا يعني عدم وجوده في الجرائم الالكترونية مثلا في جريمة تشويه السمعة عبر الانترنت , فهذه الأخيرة تقتضي وجود قصد خاص .

أما جريمة الاحتيال الالكتروني التي بدورها جريمة عمدية ,يتطلب المشرع قصدا جنائيا لقيام مسؤولية الجاني, و القصد الجنائي المشترط هو القصد العام و الخاص فالمجرم يعلم انه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير مشروع له آو للغير , آو تجريد شخص أخر من ممتلكاته على نحو غير مشروع [2]

المبحث الثاني : مظاهر الجريمة الالكترونية

تصنف الجريمة التقليدية بحسب خطورتها إلى جناية و هي اخطر الجرائم و إلى جنحة و هي متوسطة الخطورة ثم مخالفة و هي اقل خطورة و تصنف بحسب طبيعتها إلى جريمة عادية و جريمة سياسية ,عسكرية و أخرى إرهابية[3], علا خلاف هذه الجريمة فان الجريمة الالكترونية عرفت اختلاف حول تقسيماتها و أنواعها وذلك بسبب الاختلاف في تسميتها

فالبعض يصفها حسب الأسلوب المتبع في الجريمة و البعض الأخر يستند إلى دوافع ارتكابها , إما بالنسبة للمشرع الجزائري فقد قسمها إلى جرائم مرتكبة بواسطة النظام ألمعلوماتي و نص عليها المشرع و لم يحددها وبالتالي تشمل كل الجرائم المرتكبة بواسطة تكنولوجيا الإعلام و الاتصال إما

[1] حنان ريحان مبارك المضحكي, المرجع السابق ص 93-94-95

[2] احمد خليفة الملط ,مرجع سابق ,ص 120 -121

[3] احسن بوسقيعة ,الوجيز في القانون الجزائي العام,الديوان الوطني للأشغال التربوية,2002,الطبعة الأولى ص24

النوع الثاني من الجرائم يتمثل في الجرائم الواقعة على النظام ألمعلوماتي حددها المشرع بموجب قانون العقوبات و عليه سيتم تقسيم هذا المبحث الى مطلبين :

المطلب الأول: الجرائم الواقعة بواسطة النظام المعلوماتي

المطلب الثاني : الجرائم الواقعة على النظام المعلوماتي

المطلب الأول : الجرائم الواقعة بواسطة النظام ألمعلوماتي

يعد هنا النظام ألمعلوماتي هو أداة و وسيلة تنفيذ الجرائم ,فيعد الحاسب في هذا النوع من الجرائم وسيلة لتسهيل النتيجة الإجرامية ومضاعفة جسامتها و يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية و هي التي سوف نتطرق إليها في هذا المطلب

الجريمة الواقعة على الأشخاص (الفرع الأول) الجريمة الواقعة على الأموال (الفرع الثاني) الجريمة الواقعة على امن الدولة (الفرع الثالث)

الفرع الأول : الجرائم الواقعة على الأشخاص

رغم تطور الحياة اليومية للإفراد و المجتمع بفضل استعمالهم للفضاء الافتراضي, إلا انه أصبح سلاحا فتاكا في يد المجرمين للدخول إلى المعلومات الخاصة للأشخاص وعليه ظهرت عدة أنواع خاصة من الجرائم الالكترونية الواقعة على الأشخاص و من بينها

أولا : الجرائم الالكترونية الواقعة على حرمة الحياة الخاصة للأشخاص

لقد كرس الدستور الجزائري حرصه على حماية الحياة الخاصة للأشخاص و عدم الاعتداء على هده الحرمة, و من بين هذه الجرائم

1) جريمة التهديد : التهديد هو ذلك الفعل الذي يقوم بيه الشخص أو الذي ينذر أخر بخطر يريد إيقاعه بشخصه أو ماله أو هو الإعلان عن شر يراد إلحاقه بشخص معين و من شان ذلك

أن يسبب له ضرر أو قد يكون ذلك بمحرر موقع عليه أو بصور أو رموز أو شعارات و التهديد إما يكون مصحوبا بأمر أو شرط و قد يكون دون ذلك في بعض الأحيان و قد جرمه المشرع الجزائري في قانون العقوبات في المواد من 284 إلى 287 و من بين أنواعه التهديد و الابتزاز الالكتروني و هو السعي من خلال وسائل التواصل الاجتماعي أو عن طريق البريد الالكتروني بإرسال رسالة خاصة لترويع و التهديد[1] أو للحصول على مكاسب مادية أو معنوية وذلك عن طريق تهديده بفضح أسراره أو معلوماته الخاصة مهما كانت وسيلة الحصول على هذه الأسرار و المعلومات ,ومهما كانت وسيلة التهديد و بغض النظر عن اثر التهديد في نفسية الضحية و بغض النظر عن سن الضحية ,ذكر أو أنثى و بغض النظر عن المطلوب من الضحية أكان القيام بعمل أو الامتناع عن عمل أو مال أو تكليف بأمر[2].

2) جريمة انتحال الشخصية

و المقصود بها استخدام شخصية فرد للاستفادة من ماله أو سمعته أو مكانته , ولقد تميزت هذه الجريمة بسرعة الانتشار خاصة في الأوساط التجارية و تتم بجمع قدر كبير من المعلومات الشخصية المراد انتحال شخصيته للاستفادة منها لارتكاب جرائمه عن طريق استدراج الشخص ليدلي بمعلوماته الشخصية الكاملة كالاسم و العنوان الشخصي,رقم بطاقة الائتمان لتتمكن من الوصول لماله أو سمعته عن طريق الغش ,لقد نص قانون العقوبات الجزائري فيما يتعلق بجريمة انتحال صفة الغير و الاحتيال على الأشخاص في المادة 372 من قانون العقوبات

كما يوجد جريمة انتحال شخصية احد المواقع و يتم ذلك عن طريق اختراق احد المواقع للسيطرة عليه ليقوم بتركيب برنامج خاص به هناك باسم الموقع المشهور[3].

3) جرائم السب و القذف :

[1] يوسف صغير, المرجع السابق,ص33

[2] علاء رضوان,الجريمة و العقاب في واقع الابتزاز الالكتروني,موقع اليوم السابع , 10 فبراير 2020

[3] محمد بن عبد الله بن علي المنشاوي,جرائم الانترنت في المجتمع السعودي ,ماجستير في العلوم الشرطية,اكادمية نايف العربية للعلوم الأمنية ,الرياض,2003,ص55

جرائم السب و القذف هي المساس بشرف الغير و سمعتهم و اعتبارهم و يكون ذلك كتابيا أو عن طريق المطبوعات أو الرسوم عبر البريد الالكتروني أو الصوتي , صفحات الويب بعبارات تمس الشرف ,فيقوم المجرم بنشر معلومات تكون مغلوطة عن الضحية و قد يكون شخصا طبيعيا أو معنويا لتصل المعلومات المراد نشرها إلى إعداد كبيرة من مستخدمي شبكة الانترنت حيث جرمها المشرع الجزائري عندما أضاف المادة 144 مكرر في قانون العقوبات التي تجرم القذف و السبب المرتكبة بأية وسيلة معلوماتية أو إعلامية أو بأي وسيلة أخرى.

4) المواقع الإباحية و الدعارة :

رغم الايجابيات التي قدمتها الانترنت للبشرية ,شكلت فرصة ملائمة لذوي النفوس الضعيفة و للمنظمات الإجرامية لتوظيفها في عمليات مختلفة ,ومن أهم الجرائم الالكترونية الواقعة على الأشخاص صناعة و نشر الإباحة و الجنس سواء البالغين أو الأطفال خاصة بحيث إن اكبر صور الاستغلال الجنسي عبر شبكة الانترنت هي الاستغلال الجنسي للأطفال فهم يتعرضون لذلك بإشكال متعددة انطلاقا من الصور إلى التسجيلات المؤدية إلى للجرائم الجنسية العنيفة حيث تستمر معاناتهم ما بعد ارتكاب الجريمة بسبب إمكانية تناقل الصور عبر الانترنت [1],كما أن شبكة الانترنت توفر تسهيلا للدعارة عبر ألاف المواقع الإباحية و تسوق الدعارة و تستثمر لها مبالغ ضخمة مع استخدام احدث التقنيات.

ثانيا : الجريمة الالكترونية الواقعة على حقوق الملكية الفكرية :

يكون النظام ألمعلوماتي وسيلة الاعتداء على حقوق الملكية الفكرية,ومثاله السطو على بنك المعلومات و تخزين و استخدام هذه المعلومات دون إذن صاحبها, لان استخدام معلومة معينة دون إذن صاحبها يعتبر اعتداء على حق معنوي,إضافة إلى كونه اعتداء على قيمتها المالية كون أن للمعلومة قيمة أدبية بجانب قيمتها المادية, ويندرج ضمن الحقوق الفكرية كذلك براءات الاختراع,إذ تمثل فكرة للمخترع تحتوي على حق معنوي و أخر مالي للمخترع

[1] كرستا سكولمان ,عن جرائم الانترنت طبيعتها و خصائصها,الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر,المملكة المغربية,19-20 يونيو 2007,ص40

و قد نص المشرع الجزائري على حقوق الملكية الفكرية من خلال نصوص قانونية و هي الأمر رقم 03-05 الصادر في 2003, المتعلق بحقوق المؤلف و الحقوق المجاورة, و الأمر 03-07 الصادر في 2003 المتعلق براءات الاختراع[1]

الفرع الثاني : الجرائم الواقعة على الأموال :

لقد صاحب تطور شبكة الانترنت تطور وسائل الدفع و الوفاء و أصبحت جزء لا يتجزأ من المعاملات الالكترونية و في خضم هذا التداول المالي عبر الانترنت ظهرت عدة جرائم الكترونية على الأموال كالسطو و السرقة و التحويل الالكتروني غير المشروع للأموال و قرصنة أرقام البطاقات الممغنطة,حيث أصبحت إمكانية خلق مفاتيح البطاقات و الحسابات البنكية بالطريقة الغير مشروعة عبر قنوات شبكة الانترنت [2]

وسوف نتطرق إلى أهم الجرائم الالكترونية الواقعة على الأموال كالأتي:

أولا: السرقة الواقعة على البنوك:

يتم سرقة المال بالطرق المعلوماتية عن طريق اختلاس البيانات و المعلومات الشخصية للمجني عليهم و استخدام شخصية الضحية ليقوم بعملية السرقة المتخفية ما يؤدي بالبنك إلى التحويل البنكي للمال الالكتروني أو المادي إلى الجاني حيث يستخدم الجاني الحاسب الآلي لدخول إلى شبكة الانترنت و الوصول إلى المصارف و البنوك و تحويل الأموال الخاصة بالعملات إلى حسابات أخرى[3]

ثانيا: تجارة المخدرات عبر الانترنت :

[1] سوير سفيان,الجرائم المعلوماتية,رسالة لنيل شهادة الماجستير في العلوم الجنائية و علم الاجرام,كلية الحقوق,جامعة أبو بكر بلقليد,تلمسان الجزائر ,2010,ص39

[2] د.خالد ممدوح إبراهيم,امن الجريمة الالكترونية,الدار الجامعية, الإسكندرية,2001,ص76

[3] عباس أبو شامة ,التعريف بالظواهر الإجرامية المستحدثة حجمها أبعادها و نشاطها قي الدول العربية ,الندوة العلمية للظواهر الإجرامية المستحدثة و سبل مواجهتها ,تونس 29 -30 جوان 1999 ,ص20

من أهم الجرائم الالكترونية على الأموال نذكر جريمة المخدرات عبر الانترنت حيث تتخذ المواقع الالكترونية للترويج للمخدرات و تسويقها للناشئ لاستخدامها,وتعليمه كيفية صناعتها بكافة أصنافها و أنواعها [1], كما يروجون سلعتهم عبر رسوم الغرافيتي المنتشرة على جدران الشوارع كي يلفتوا انتباه الزبائن إلى حساباتهم الالكترونية [2],وظهر نوع أخر من المخدرات فلم يعد استهلاكها يقتصر على ما كان يجري سابقا بحقنها أو مضغها أو تدخينها وإنما تطور الفكر الإنساني ليحول نظم التعاطي إلى تعاطي الكتروني و يتمثل ذلك في جلوس تاجر المواد المخدرة أمام جهاز الحاسب الآلي ليتلقي طلبات شراء للمواد المخدرة عبر موقعه الالكتروني و هنا يكون التسليم عن طريق إجراء المشتري لعملية تحميل المخدر الذي يرغبه في شكل ملفات و هو ما يعرف بالمخدرات الرقمية

و المخدرات الرقمية هي عبارة عن ملفات صوتية تحتوي على نغمات أحادية أو ثنائية يستمع إليها المستخدم تجعل الدماغ يصل إلى حالة من الخدر تشابه تأثير المخدرات الحقيقية[3].

ثالثا: غسيل الأموال :

إن جريمة غسيل الأموال عبر شبكة الانترنت تختلف عن نظيرتها التي تتم عبر الوسائل و الطرق التقليدية , إذ تمم الأولى عبر وسائل و طرق حديثة و جد متطورة عما كان معمول بيه في السابق فلقد استفادوا مجرمو غسيل الأموال عبر الانترنت بتوفير السرعة و تفادي الحدود الجغرافية و القوانين المعيقة لغسيل الأموال و كذلك لتشفير عملياتهم و سهولة نقل الأموال و استثمارها لإعطائها الصيغة الشرعية[4]

[1] محمد صالح الألفي,أنماط جرائم الانترنت ,متوفر على موقع www.eastlaws.com

[2] أنتوني كاثبرتشون ,مجرمو الانترنت الخفي يبيعون المخدرات عبر تطبيقات شائعة وكومبيوترات مسيطرة عليها ,موقع Independent عربية ,16مارس2019

[3] د. أبو سريع احمد عبد الرحمن,بحث حول استخدام الانترنت في تعاطي المخدرات. المخدرات الرقمية , وزارة الداخلية ,قطاع الشؤون الفنية,,الإدارة العامة للمعلومات و التوثيق,ديسمبر 2010,ص05

[4] صالحة العمري,جريمة غسيل الأموال و طرق مكافحتها,مجلة الاجتهاد القضائي,العدد الخامس,مخبر اثر الاجتهاد القضائي على حركة التشريع محمد خيضر ,بسكرة,ص179

ولقد نصت عليها جل التشريعات من بينها التشريع الجزائري كما أعطى من خلال قانون الإجراءات الجزائية المعدل و المتمم بالقانون 17-07 بعض الصلاحيات و المهام للسلطات القضائية و الخاصة للتحري و التحقيق في جرائم غسيل الأموال و الكشف عنها و عن مرتكبيها و ملاحقتهم بتوقيع العقاب طبقا لنصوص قانون العقوبات المعدل و المتمم بأمر رقم 16-02

رابعا : الاستعمال الغير شرعي للبطاقات الائتمانية :

شاع في الآونة الأخيرة استعمال بطاقات الائتمان الالكترونية , باعتبارها وسيلة من وسائل الدفع الحديثة,و أداة مصرفية تقوم مقام النقود في الوفاء بالالتزامات القانونية مقبولة على نطاق واسع لدى الأفراد و التجار وذلك من اجل التيسير على الأفراد في معاملاتهم

و من بين أنواع جرائم تكنولوجيا المعلومات نجد عمليات السطو على بطاقات الائتمان الالكترونية,هذه الأخيرة التي تعد احدث أنماط السلوك الإجرامي باعتبارها نقطة تلاقي بين الجريمة المعلوماتية و بطاقة الائتمان الالكترونية و تكون عن الاستيلاء أو سرقة أرقام البطاقات ثم بيع المعلومات للآخرين ,ومن خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الحاسب الآلي للضحية عن طريق الاحتيال, وذلك بإيهامه بحصول ربح ,فيقدم الضحية معلومات تمكن الجاني من التصرف في ماله[1] أو إساءة استخدام الغير لبطاقات الائتمان,كان يقوم السارق باستعمال البطاقة للحصول على السلع و الخدمات او سحب مبالغ مالية بموجبها من أجهزة التوزيع الآلي أو السحب باستخدام البطاقات المزورة[2]

خامسا : قرصنة البرمجيات :

هي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية على اسطوانات و بيعها للناس بسعر اقل , وجريمة المؤلفات العلمية و الأدبية بالطرق الالكترونية المستحدثة نص عليها المشرع في الدستور المادة 44

[1] صغير يوسف,مرجع سابق,ص45

[2] احمد خليفة الملط,مرجع سابق,ص196

الفرع الثالث : جرائم ضد أمن الدولة :

تعد هذه الجرائم من اخطر الجرائم الالكترونية خاصة الإرهاب ألمعلوماتي و الجريمة المنظمة و جريمة التجسس الالكتروني ,كما تعطي شبكة الانترنت فرصا للتأثير على المعتقدات الدينية و تقاليد المجتمعات مما سهل خلق الفوضى داخل الدولة و المساس بأمنها الداخلي و بنظامها العام[1]

وتقع هذه الجرائم باستعمال النظام ألمعلوماتي سواء لإفشاء الأسرار التي تخص مصالح الدولة و نظام الدفاع الوطني و نصت عليها المادة 394 مكرر02 من الأمر 66-156 "تضاعف العقوبة المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام "

أولا : الإرهاب ألمعلوماتي :

الإرهاب الالكتروني أو ألمعلوماتي هو هجمات غير مشروعة أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة الكترونيا ,توجه من اجل الانتقام أو الابتزاز أو إجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة وبالتالي فلكي ينعت شخصا بأنه إرهابيا عبر الانترنت , وليس فقط مخترقا ,فلا بد و إن تؤدي الهجمات التي يشنها إلى عنف ضد الأشخاص أو الممتلكات ,أو على الأقل تحدث أذى كافيا من اجل نشر الرعب و الخوف

فالإرهاب الالكتروني يعتمد على استعمال الإمكانيات العلمية و التقنية و استغلال وسائل الاتصال و الشبكات المعلوماتية من اجل تخويف و ترويع الآخرين و إلحاق الضرر بهم أو تهديدهم[2]

و لقد أصبحت تستخدم المجموعات الإرهابية حاليا تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية , فهم يستخدمون الوسائل المتقدمة مثل الاتصالات و التنسيق و بث

[1] سامي علي عياد حامد , الجريمة المعلوماتية و إجرام الانترنت ,دار الفكر الجامعي,الإسكندرية,2007,ص77

[2] د.حسين بن سعيد بن سيف ألغافري,الإرهاب الالكتروني,موقع وزارة عمان الرقمية

الأخبار المغلوطة و توظيف بعض صغار السن و تحويل بعض الأموال في سبيل تحقيق أهدافهم ,و يقوم الإرهابيون باستخدام الانترنت لاستغلال المؤيدين لأفكارهم و جمع الأموال لتمويل برامجهم الإرهابية , و الاستيلاء على المواقع الحساسة و سرقة المعلومات و امتلاك القدرة على نشر الفيروسات , وذلك يرجع إلى العدد المتزايد من برامج الكمبيوتر القوية و سهلة الاستخدام[1]

و من اخطر التهديدات و الهجمات التي تمس امن الدولة التسلل الالكتروني إلى الأنظمة الأمنية في دولة ما وشلها لصالح جماعات إرهابية ,وكل ما يحتاجه الإرهابي ذو الخبرة الاحترافية في هذا المجال الحيوي و المعقد هو جهاز حاسب إلي و اتصال بشبكة الانترنت و من ثم القيام بأعمال تخريبية و هو امن في مقره ,بنقرات بسيطة على لوحة المفاتيح , و دون أن يترك أثرا.

ثانيا : التجسس الالكتروني :

التجسس الالكتروني أو ما يعرف بالجاسوسية الرقمية التي ترصد و تراقب أي حاسب إلي عن طريق التسلل إلى أجهزتهم الحاسوبية أو محاولة اعتراض الإشارات و حزم المعلومات التي ترسل من قبل أجهزتهم عبر الانترنت, تعتبر الحواسيب احد أهم وسائل التجسس على الخصوصيات الفردية لقدرة المختصين على تلقي معلومات منها دون علم أصحاب الأجهزة أنفسهم, يتم معظم هذا عن طريق شبكات الحاسب الآلي التي توصل بها معظم الحواسيب باستخدام ثغرات أمنية أو امن الحاسوب Security cracking للحصول على وصول للمعلومات المخزنة على الحاسب

غالبا ما تتم عمليات تجسس دولية للحصول على معلومات سرية رسمية لدى الحكومات من قبل حكومات دول أخرى, أو قد يتم التجسس من قبل حكومة بلد على أفراد معينين من النشطاء السياسيين أو أفراد الجريمة المنضمة و العصابات الضخمة و المافيا ,يعتمد بعض المخترقين أحيانا لإدخال برامج تحول الأجهزة الحاسوبية لمكان مناسب للتجسس[2].

[1] سورية ديش,أنواع الجرائم الالكترونية و إجراءات مكافحتها ,موقع المركز الديمقراطي العربي,22 فبراير 2017

[2] Is the U.S. turning into a surveillance society? American civil liberties union

المطلب الثاني: الجرائم الواقعة على النظام ألمعلوماتي :

إضافة إلى الجرائم المعلوماتية التي تقع باستخدام النظام المعلوماتي هناك نوع آخر من الجرائم المعلوماتية بالاعتماد على التصنيف الذي يقوم على محل الجريمة المعلوماتية و يتمثل في الجرائم الواقعة على النظام المعلوماتي و الواقعة على المعلومات المدرجة بالنظام المعلوماتي و جرائم الاعتداء على البرامج النظام المعلوماتي و هذا ما سأتطرق إليه في الفروع التالية :

الفرع الأول : جرائم الاعتداء على المكونات المادية للنظام المعلوماتي :

يقصد بالمكونات المادية للنظام ألمعلوماتي تلك الأجهزة و المعدات الملحقة به و التي تستخدم في تشغيله كالاسطوانات و الشرائط و الكابلات , و نتيجة للطبيعة المادية لهذه المكونات فالاعتداء عليها يكون عن طريق جرائم عادية و تقليدية[1],كأن تكون محلا للسرقة أو خيانة الأمانة أو الإتلاف ألعمدي كإحراقها أو ضرب الآلات بشيء ثقيل أو حاد و العبث بمفاتيح التشغيل أو خربشة الشريط و إفساد اسطوانات التشغيل المغناطيسي بتعريضها إلى أي مجال مغناطيس متلف و يترتب على هذا الإتلاف خسائر كبيرة [2]

ومن أمثلة على ذلك ما حدث في فرنسا حيث أدى إتلاف معدات مؤسسة كبيرة متخصصة في بيع الأنظمة و توثيق المعلومات الحسابية إلى خسائر مالية معتبرة قدرت ب 5 ملاين فرنك فرنسي [3], و يرى البعض من الفقهاء انه يندرج ضمن هذه الطائفة من الجرائم المعلوماتية سرقة وقت الآلة ,فقد يلجأ العاملين بالنظام ألمعلوماتي إلى استخدامه في أعمال خاصة بهم و عليه تكون واقعة السرقة منصبة على وقت الجهاز الذي يمكن تقويمه ماليا و ليس على الأشياء المادية بمعنى الكلمة[4]

---

[1] د.احمد خليفة الملط ,المرجع السابق,ص176

[2] د.زكي أمين حسونة ,جرائم الكمبيوتر و الجرائم الأخرى التكتيك ألمعلوماتي ,المؤتمر السادس للجمعية المصرية للقانون الجنائي ,القاهرة 25 إلى 28 أكتوبر 1993 , تقرير مصر ,ص471 1993

[3] Rose (Philippe).op-cit.P58-59

[4] André Lucas. le droit de l'informatique. Paris.PUF 1987 p519,521

و تجدر الإشارة أن خطورة واقعة السرقة لا تكمن في الشيء المسروق لضالة قيمته ,بالمقارنة بما تحتويه هذه المكونات المادية من معلومات تقدر خسارتها بأموال طائلة.

الفرع الثاني :جرائم الاعتداء على المكونات المنطقية للنظام المعلوماتي :

تستلزم هذه الطائفة من الجرائم المعلوماتية معرفة فنية عالية في مجال البرمجة , وقد تقع هذه الجرائم إما على البرامج التطبيقية و إما على برامج التشغيل و سنتطرق لهاتين الصورتين فيما يأتي :

أولا: الجرائم المعلوماتية الواقعة على البرامج التطبيقية :

يقوم الجاني في هذه الصورة بتحديد البرامج أولا ثم التلاعب فيه لتحقيق اكبر عدد من الاستفادة المادية

1) تعديل البرنامج :

الهدف الرئيسي من تعديل البرامج يتمثل في اختلاس النقود و تكثر هذه الجرائم في مجال الحسابات [1], و من أمثلة ذلك قيام مبرمج بأحد البنوك الأمريكية بإدارة الحسابات بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات و قام بقيد المصاريف الزائدة في حساب خاص به أطلق عليه اسم Zzwick و حصل على اثر ذلك على مئات الدولارات كل شهر و كان من الممكن إن يستمر هذا العمل الإجرامي لولا أن البنك أراد تأسيس شركة جديدة للدعاية ان يكافئ أول و أخر عميل له ليكتشف عدم وجود ما يدعى Zzwick[2]

و هناك نظام آخر يسمى سلامي salami و يتم الاختلاس بموجب هذا النظام باستقطاع مبالغ زهيدة على فترات زمنية طويلة و متباينة من خلال صفقات عديدة يترتب عليها تحقيق فائدة كبيرة

[1] د.احمد خليفة الملط,مرجع سابق,ص173

[2] Duleroy et rocco (A.M) , l'informatique nouvelle, avril 1976,les escrocs a l'informatique, le nouvel e Économist, octobre 1979 n 202

و قد حقق بموجب هذا البرنامج احد المستخدمين الامركين بإحدى المنشئات التجارية يدعى Royce.E في خلال 6 سنوات ما يقرب من 2 مليون دولار[1]

2) التلاعب في البرنامج :

يأخذ التلاعب في البرنامج عدة أشكال فقد يتم عن طريق استعمال القنبلة المنطقية و هي عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة أو كل فترة زمنية منتظمة و يتم وضعه في شبكة معلوماتية بهدف أو حالة فحوى النظام بغرض تسهيل تنفيذ عمل غير مشروع ,أو عن طريق قيام احد المبرمجين زرع برنامج فرعي غير مسموح به في البرنامج الأصلي يسمح له بالدخول غير المشروع في العناصر الضرورية لأي نظام معلوماتي , و يصعب اكتشاف لصغره و دقته و مثال على ذلك لقد قام مبرمج بأحد البنوك زرع برنامج فرعي بمنشاة بالكيانات المنطقية بادارة الحسابات يتجاهل كل عمليات السحب التي تتم من قبله عن طريق شيكات حسابية إذ يتحمل البنك نتيجة لذلك نتيجة هذه الحسابات في باب ميزانية الإدارة .

ثانيا : الجرائم المعلوماتية الواقعة على برامج التشغيل

تعد برامج التشغيل تلك البرامج المسؤولة عن عمل النظام ألمعلوماتي من حيث قيامها بتنظيم و ضبط ترتيب التعليمات الخاصة بالنظام , و تقوم الجريمة المعلوماتية في هذه الصورة عن طريق تزويد البرنامج بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام ألمعلوماتي , و يتحقق هذا النوع من الجرائم المعلوماتية في شكلين:

1) المصيدة : تتمثل هذه الصورة في إعداد المبرمج برنامج به أخطاء و عيوب عمدا لا يكتشف بعضها عند استخدام البرنامج, اذ يترك المبرمج ممرات خيالية و فواصل و تفرعات في البرنامج حتى يستطيع فيما بعد تنفيذ التعديلات الضرورية بإدخال تفرعات إضافية أو إحداث مخارج وسيطة للولوج داخل النظام ألمعلوماتي و الوصول إلى كل المعلومات التي تحويها

[1] د.احمد خليفة الملط،مرجع سابق،ص174

الذاكرة,وهذه التقنية يمكن للمبرمج استخدام البرنامج في اي وقت وفق أهوائه , وبذلك يصبح هو المهيمن على النظام و على صاحب العمل المعتدي عليه[1].

2) تصميم برنامج وهمي : و تقوم هذه الصورة من خلال قيام المبرمج بوضع برنامج يصعب اكتشافه مخصص خصيصا لارتكاب الجريمة و مراقبة تنفيذها و من أمثلة على ذلك قيام إحدى شركات التامين الأمريكية في مدينة لوس انجلوس بواسطة مبرمجيها تصميم برنامج وهمي يقوم بتصنيع وثائق تامين لأشخاص وهمين بلغ عددهم 46000 بهدف تقاضي هذه الشركة من اتحاد شركات التامين عمولات من نظيراتها[2]

الفرع الثالث: جرائم الاعتداء على المعلومات المدرجة بالنظام ألمعلوماتي

للمعلومة المعالجة أليا أهمية كبيرة باعتبارها أساس عمل النظام المعلوماتي و لما لها من قيمة اقتصادية , و بهذا تعد هدفا للجرائم المعلوماتية من خلال التلاعب فيها او عن طريق إتلافها و هذا ما سنتناوله فيما يأتي :

أولا. التلاعب في المعلومات :

يتم التلاعب في المعلومات الموجودة داخل النظام المعلوماتي بطرق مباشرة أو غير مباشرة فاما التلاعب المباشر يتم عن طريق إدخال معلومات بمعرفة المسؤول عن القسم المعلوماتي و ياخد هذا التلاعب عدة صور كضم مستخدمين غير موجودين بالعمل لاسيما في المنشات التي تضم عددا كبيرا من العاملين المؤقتين و دائمي التغير بهدف الحصول على مرتباتهم , (و من أمثلة على ذلك قام احد المسؤولين عن القسم المالي بإحدى الشركات الفرنسية اختلاس أكثر من مليون فرنك فرنسي و وضعه في حسابه الخاص و حساب شركائه باستعمال هذه الطريقة[3]) أو بالإبقاء على ملفات مستخدمين تركوا العمل للحصول على مبالغ مالية شهرية أو عن طريق عمل

[1] د.محمد سامي الشوا,ثورة المعلومات و انعكاساتها على قانون العقوبات ,دار النهضة العربية, 1994, ص67

[2] Equity fuding life insurence. L'informatique nouvelle , mai 1976

[3] Escroquerie aux Assedic de paris, jugement du 2fev 1982 TGI de paris 13éme ch.°39 ,avril 1982

تحويلات لمبالغ وهمية لدى العاملين بالبنوك باستخدام النظام المعلوماتي بالبنك و تسجيلها و إعادة ترحيلها و إرسالها لحساب أخر في بنك بهدف اختلاس تلك النقود

في حين التلاعب غير مباشر يتم عن طريق التدخل الغير المباشر لدى المعلومات المسلحة بالنظام المعلوماتي باستخدام احد وسائط التخزين أو بواسطة التلاعب عن بعد باستخدام أدوات معينة و معرفة أرقام و شفرات الحسابات[1], ويتخذ عدة صور من بينها التلاعب في الشرائط الممغنطة و قد قام في هذا الصدد احد الموظفين بأحد فروع الشركة الفرنسية Isoverst gobain بإرسال شريط ممغنط يحتوي على 139 إذن دفع و عند معالجته بالبنك بالقسم المعلوماتي تم رفض نسخه لعيب في طول الشريط ,و قد قال الخبراء انه لو نجحت هذه العملية لتم النصب على البنك بحوالي 21 مليون فرنك فرنسي[2]

كما قد يتحقق التلاعب غير المباشر في المعلومات عن طريق التلاعب عن بعد باستخدام الجاني كلمة السر أو مفتاح الشفرة أو أداة ربط بالمركز المعلوماتي لأي جهة و تكمن خطورة هذه الصورة في إمكانية تسلل الجاني إلى المعلومات المخزنة بالنظام المعلوماتي و الحصول على المنفعة المالية التي يريدها من مسافات بعيدة .

ثانيا: إتلاف المعلومات :

قد يهدف الجاني من خلال ارتكابه الجريمة المعلوماتية بإتلاف المعلومات المخزنة بالنظام المعلوماتي , و يتخذ الإتلاف عدة صور فقد يتم عن طريق طرق الإتلاف العادية كالحريق أو الضرب أو السرقة أو محو المعلومات , و يشكل استبدال المعلومات نوع من جرائم الغش أو التزوير المعلوماتي و هو على درجة كبيرة بمجرد استبدال رقم بأخر أو إحلال رقم مكان أخر[3]

[1] د.احمد خليفة الملط , المرجع السابق,ص179

[2] Trip de paris. 12éme ch., corr. jugement du 13 janv. 1982,DALLOZ S 1982, p 502

[3] د,احمد خليفة الملط,مرجع سابق,ص179

فمثلا هناك مجموعة من المستخدمين إلادارين استطاعوا خلال سنوات قليلة مضاعفة رواتبهم عن طريق النظام ألمعلوماتي [1]

و قد استعمل شخص يدعى Vladimir loriblitt بإرسال طريقة تدعى ب bluff إذ كان يعمل بوزارة المالية و قام بإدخال فواتير وهمية لا حصر لها و تحويل ما تم سداده من هذه الفواتير لحساب الشركات الوهمية التي اصطنعها

و إما محو المعلومات فهو من أسهل طرق الإتلاف كون انه من خصائص الجرائم المعلوماتية قدرة الجاني على على محو أثار الجريمة في فترة وجيزة جدا لا تتعدى الضغط على زر بسيط في لوحة المفاتيح أو البرنامج عن طريق الفارة , فمثلا قام شخصان باختلاس مبلغ يقدر ب 61.000 دولار مرسلة من شركات التامين إلى إحدى المراكز الجامعية عن طريق محو الحسابات القائمة في سجلات النظام ألمعلوماتي الخاص بالمركز وجعلها غير قابلة للتحصيل [2].

[1] محمد سامي الشوا, المرجع السابق,ص75

[2] Le monde informatique , 21 fev 1983, sous le titre (la délinquance en cal blanc se parte lien)

الفصل الثاني

المكافحة القانونية للجريمة الالكترونية

تعد الجريمة الالكترونية من أخطر الجرائم المستحدثة في عصرنا الحالي حيث تطورت أشكال ارتكابها بتطور تكنولوجيات الإعلام والاتصال من خلال التفنن في طرق ارتكابها من طرف مجرمين في قمة الذكاء والاحترافية الأمر الذي جعل صعب استيعابها بغرض مكافحتها والوقاية منها، ونظرا للخصوصية التي تتسم بها الجريمة الالكترونية كونها ترتكب في بيئة افتراضية غير مرئية عابرة للحدود الجغرافية للدول جعلها لا تخلف أية أثار مادية مقارنة بالجرائم التقليدية المرتكبة في الواقع المحسوس التي يتم الكشف عنها بالأساليب العامة التقليدية على غرار الجرائم الالكترونية التي يكون فيها التحري والتحقيق بواسطة الأساليب الخاصة المستحدثة ,وعلى هذا الأساس تسارعت معظم دول العالم من بينها الجزائر التي وضعت أجهوة وقوانين لمكافحتها والوقاية منها وهذا ما سنتطرق إليه من خلال آليات مكافحة الجريمة الالكترونية على المستوى الوطني في المبحث الأول ، لكن كون العالم الالكتروني عالم افتراضي جعل من هذه الجريمة بعد دولي لا حدود فيه مما أضاف عليها طبيعة ازدواجية دفعت بالمجتمع الدولي إلى توحيد جهوده في سبيل مكافحتها من خلال اتفاقيات وأجهزة دولية وهذا ما سنتطرق إليه من خلال آليات مكافحة الجريمة الالكترونية على المستوى الدولي في المبحث الثاني .

المبحث الأول: آليات مكافحة الجريمة الالكترونية على المستوى الوطني

رغم صعوبة ضبط ومكافحة الجريمة الالكترونية على المستوى الوطني إلا أن المشرع الجزائري قام بجهود معتبرة لمحاربتها وذلك من خلال التدخل بنصوص آمرة لتجريم الظاهرة من جهة وإصدار قوانين خاصة وأجهزة تتلاءم مع طبيعة الجريمة ومستلزمات المكافحة من جهة أخرى والتي تستدعي التعاون بين جهات القانونية والمختصين وعليه سيتم تقسيم هذا المبحث إلى مطلبين:

المطلب الأول: الآليات التشريعية لمكافحة الجريمة الالكترونية

المطلب الثاني: الآليات المؤسساتية لمكافحة الجريمة الالكترونية

المطلب الأول:الآليات التشريعية لمكافحة الجريمة الالكترونية في التشريع الجزائري

إن رغبة المشرع الجزائري في تصدي لظاهرة الإجرام الالكتروني وما يصاحبها من أضرار معتبرة على الأفراد والدولة من جهة، ومحاولة تدارك الفراغ التشريعي من جهة أخرى جعله يقوم بتعديل العديد من القوانين الوطنية على رأسها قانون العقوبات لجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجيا الإعلام والاتصال , كما قام باستحداث قوانين أخرى خاصة لضمان الحماية الجنائية للمعاملات الالكترونية

فرع1:القواعد الموضوعية المعنية لمكافحة الجرائم الالكترونية

لم تكن للجزائر قوانين تطبق على النظم الالكترونية وعلى تكنولوجيا الإعلام والاتصال قبل سنة 2004 لكن أمام تزايد هاته الجرائم كان لابد على المشرع من إيجاد الإطار القانوني المناسب الذي يمنع الاعتداء على هذه النظم أو الاستعمال السيئ لها[1] ، ولسد الفراغ القانوني واقتداء بأغلب دول العالم قام المشرع باستصدار قوانين معدلة متممة لقانون العقوبات واستصدار قوانين خاصة أهمها القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام الاتصال ومكافحتها

[1]-سعيدة بوزنون ،مكافحة الجريمة الالكترونية في التشريع الجزائري ،مجلة العلوم الانسانية ،العدد 52 ، المجلد ب ، 2019 ، ص 49

أولا: تعديل قانون العقوبات

لقد قام المشرع الجزائري باستحداث في القسم السابع مكرر من قانون العقوبات من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات بنص المواد 394 مكرر إلى المادة 394 مكرر 8 ، و باستقراء هذه المواد يتضح لنا أن المشرع قد قسم الجرائم الالكترونية إلى أربعة طوائف تتعدد بحسب المصالح المحمية والتي تتمثل أساسا في سرية هذه المعطيات أو تكاملها وهي :[1]

-الطائفة الأولى: وتتضمن جرائم الولوج إلى المعطيات المعالجة آليا عن طريق الغش والتزوير وكذا جريمة الحذف والتغيير والتخريب في هذه المعطيات.

-الطائفة الثانية: الجرائم الالكترونية بواسطة النظام المعلوماتي و أهمها استعمال أو إفشاء أو نشر معلومات منصوص علىها في قانون العقوبات، وكذا البحث أو التجميع في معطيات مخزنة في نظام معلوماتي.

-الطائفة الثالثة:الجرائم الإلكترونية المتعلقة بأمن الدولة ومؤسساتها كجرائم التجسس و الإرهاب .

-الطائفة الرابعة:الجرائم الالكترونية للشخص المعنوي والتي تعادل عقوبته خمس مرات عقوبة الشخص الطبيعي المادة 394 مكرر 4 من قانون العقوبات[2]

في سنة 2006 قام المشرع بإدخال تعديلات جديدة مست القسم السابع مكرر منها، حيث تم تشديد العقوبة على كل الجرائم الواردة في هذا القسم دون المساس بالجرائم الواردة فيها، ويعود ذلك بالتأكيد إلى إقرار المشرع بأن الجريمة الالكترونية ظاهرة جديدة ومستحدثة متميزة عن الجرائم التقليدية من حيث محلها وأشخاص مرتكبيها، وسعيا منها في ضمان المكافحة لم يميز بين نوعية المعلومات التي تطالها الحماية سواء كانت مادية أو اقتصادية أو مسائل أمنية

[1]-القانون 04-15 المعدل والمتمم للأمر 66-155 المؤرخ في 10 نوفمبر 2004 المتضمن قانون العقوبات ج ر 71

[2] .نمديلي رحيمة، خصوصية الجريمة الالكترونية في القانون الجزائري و القوانين المقارنة، كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان، يومي 24-25|مارس2017 ،ص 105

غرضها في ذلك هو حتما تحقيق الردع العام على اثر التزايد الخطير لنسب الجرائم المرتكبة وتنوعها و خطورتها على الأفراد من جهة وعلى الاقتصاد الوطني من جهة أخرى[1]

وفي سنة 2016 قام المشرع بإضافة تعديل جديد وهو نص المادة 394 مكرر 08 والذي يمس كل شخص يملك صلاحية تقديم خدمات الانترنت حيث أن هذا الأخير تقع عليه مسؤولية جزائية في حالة ارتكابه :

1.عدم التدخل الفوري لسحب تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا

2.عدم وضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها [2]

ثانيا: القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام :

إن التطورات التي عرفتها الجزائر في مجال تطور التقنية و تكنولوجيا جعلت منها محلا للجريمة مما جعل المشرع يباشر بوضع إجراءات جديدة لمواجهتها وتضمنت هذه الإجراءات إصدار قانون 09-04 المؤرخ في 05 أوت2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وهو القانون المنظم للفضاء الالكتروني ومكافحة المجال الإجرامي المتصل به من خلال قواعد تسمح بمتابعة هذا النوع من الجرائم ومرتكبيها بشكل يضمن شرعية الإجراءات المتخذة[3]

ورد في قانون 09-04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام ومكافحتها ستة فصول : تضمن الفصل الأول أحكام عامة تحدد مفهوم المصطلحات المستعملة فيه ومجال تطبيقه من خلال وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل

[1]. عاقلي فضيلة.مرجع سابق ص127

[2]..قانون 16-02 مؤرخ في 19 فيفري 2016 يتمم الامر رقم 66-156 المؤرخ في 08 جوان 1966 المتضمن قانون العقوبات

[3]. ربيعي حسين .آليات البحث والتحقيق في الجرائم المعلوماتية أطروحة لنيل شهادة دكتوراه الحقوق. فرع: قانون العقوبات والعلوم الجنائية .كلية العلوم والحقوق السياسية .جامعة باتنة 2015-2016ص 170

محتواه في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية [1]، وفصلت باقي الفصول هذه الإجراءات كيفية تطبيقها لمحاربة الجريمة الالكترونية والوقاية منها وعليه تكون هاته الفصول كالأتي:

- مراقبة الاتصالات الالكترونية.
- تفتيش المنظومات المعلوماتية.
- حجز المعطيات المعلوماتية.
- حفظ المعطيات المتعلقة بحركة السير.

الفرع الثاني :القواعد الإجرائية المنظمة لمكافحة الجريمة الالكترونية :

تضمنت التعديلات المختلفة لقانون الإجراءات الجزائية عدة قوانين جديدة لمواجهة الجريمة الالكترونية شأنها شأن جريمة منظمة ,حيث خص المشرع الجزائري هذه الجرائم بجملة من الإجراءات الخاصة تمس كل من المراحل الخاصة لمكافحتها وتكمن خصوصية إجراءات المتابعة في الجريمة الالكترونية فيما يلي[2]:

أولا: تمديد الاختصاص المحلي

تمديد الاختصاص المحلي لكل من ضباط الشرطة القضائية وقاضي التحقيق ووكيل الجمهورية المادة 37 من قانون الإجراءات الجزائية إذا تعلق الأمر بالجريمة المنظمة وجرائم المعالجة الآلية للمعطيات، الإرهاب، تبييض الأموال وجرائم الصرف، ولعل اعتماد الاختصاص الإقليمي الموسع هو المواجهة الفعالة لطائفة من الجرائم المنظمة الخطيرة التي تتسم بالتعقيد حتى ولو كان في ذلك خروج عن معايير الاختصاص الأصلية المتمثلة في مكان وقوع الجريمة

[1]. قانون رقم 09- 04 مؤرخ في 05 أوت2009 م، تضمنالقواعدالخاصة للوقاية منالجرائمالمتصلة بتكنولوجّيا الإعلام الاتصال ومكافحتها، ج ر 47.المؤرخة في 16 أوت2009

[2]. أمحمدي بوزينة أمنة ، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية: (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام) .أعمال ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري المنعقد في الجزائر العاصمة يوم 29 مارس 2017 ،ص 57

أو مكان القبض على المتهم أو مكان إقامتها، فهي في الأصل معايير موضوعية تبرر ردة فعل المجتمع اتجاه المجرم الذي أخل بالنظام العام [1]

كذلك نظم المشرع الجزائري في القانون رقم 04/09 المؤرخ في 5 أوت 2009 ، أحكاما جديدة خاصة بالاختصاص في مجال الجريمة الالكترونية تتماشى والتطور الذي لحق الجريمة، من هذه القواعد ما نصت علىها المادة الثالثة التي تضمنت الإجراءات الجديدة التي تتطلبها التحريات والتحقيقات من ترتيبات تقنية، بالإضافة إلى ذلك قررت المادة 15 من القانون 04/09 أنها زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا، و تستهدف مؤسسات الدولة الجزائرية والدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

إضافة إلى ذلك تم سحب نظام الملائمة من النيابة العامة في مجال متابعة بعض الجرائم، إذ يلتزم وكيل الجمهورية بتحريك الدعوى العمومية بقوة القانون، بحيث لا يتمتع بشأنها بسلطة الملائمة بين تحريك الدعوى العمومية وعدم تحريكها مثلما فعل في الجرائم المنصوص عليها في المواد 144 مكرر و144 مكرر1 و144 مكرر2 من قانون العقوبات المعدل والمتمم بالقانون رقم 09/01 المؤرخ في 26 جوان 2000.

ثانيا: أساليب التحري الخاصة

إن أهمية جهاز الشرطة القضائية في الكشف عن الجريمة الالكترونية والتعرف على المجرم الالكتروني تبعها استحداث المشرع الجزائري أساليب التحري الخاصة المستعملة بما تتناسب ومتطلبات ضبط الوجه الجديد للإجرام حتى يسمح للقضاء والشرطة أن تتكيف بدورها في مهامها

[1] سعيدة بوزنون . مرجع سابق ، ص 51 – 52

مع الإجرام الجديد مستمدة شرعيتها من المواثيق الدولية التي صادقت عليها الجزائر وخاصة المادة 20 من اتفاقية باليرمو لمكافحة الجريمة المنظمة عبر الحدود الوطنية التي أدرجت الجريمة الالكترونية كشكل من أشكال الجريمة المنظمة[1]

ما تجدر الإشارة إليه أن هذه الأساليب لا يرخص بها إلا في بعض الجرائم المعينة من طرف المشرع الجزائري على سبيل الحصر لا المثال بما فيها الجريمة الالكترونية استدركها المشرع بموجب تعديل قانون الإجراءات الجزائية القانون رقم 06-22 والتي تتمثل في[2]:

-اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية

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

- جواز التسرب أو الاختراق للكشف عن الجريمة الالكترونية بمقتضى المادة 65 مكرر 12 من القانون 06-22 المتضمن قانون العقوبات، ولأنها إجراء غير مألوف وخطير في عمل سلطات الضبط القضائي أحاطها المشرع بجملة من الضوابط أهمها: الإذن القضائي بالتسرب من وكيل الجمهورية أو قاضي التحقيق المادة 65 مكرر 11 وأيضا احترام المدة القانونية للتسرب[3]

ثالثا:التفتيش

تتميز الجريمة الالكترونية عن غيرها من الجرائم كونها من الجرائم التي يصعب إثباتها لذلك يجيز المشرع الجزائري التفتيش في المنظومة المعلوماتية ضد كل جريمة يحتمل وقوعها

[1]. سعيدة بوزنون .نفس المرجع السابق ، ص 51

[2]. قانون06-22 المؤرخ في 20 ديسمبر 2006 يتمم الأمر 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية . ج ر 44

[3]. كور طارق، آليات مكافحة جريمة الصرف، دار هومة، الجزائر، الطبعة الثانية 2014 ، ص ص 131-132

وتتقلص معها الضمانات التي يشترطها المشرع عادة في الجرائم الأخرى نظرا لسرعة ارتكابها ومحو آثارها وتخطيها الحدود الوطنية[1]

وإذا كان التفتيش يقصد به البحث عن جسم الجريمة والأداة التي استخدمت في ارتكابها وكل ما له علاقة بها أو بفاعلها، فإن عالم التقنية قد يتميز عن الجرائم العادية بكونه يتكون من شقين هما الكيانات المادية والتي تنطبق عليها القواعد العامة للتفتيش من حيث مكان تواجدها بحسب ما إذا كان مكان عام أو خاص كمسكن المتهم مثلا، و الكيانات المعنوية كالبرامج ونظم التشغيل وقواعد البيانات[2]

وبعيدا عن الآراء الفقهية التي قيلت حولها فقد نص المشرع الجزائري في المادة 47 الفقرة الرابعة من قانون الإجراءات الجزائية الجزائري بإمكانية التفتيش والضبط على المكونات المعنوية للحاسوب، بنصه على أنه: "إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك"

رابعا : التوقيف تحت النظر

وهو إجراء خطير وغير عادي من إجراءات التحري والاستدلال لأنه يمس مباشرة بحرية الفرد المكفولة من طرف كل التشريعات الداخلية والاتفاقيات الدولية ، لذلك فقد أجازه المشرع الجزائري في حالتين اثنتين على سبيل الحصر ومنح الموقوف للنظر حقوقا يجب احترامها أثناء مدة توقيفه[3]:

– الحالة الأولى تكون في الجرائم المتلبس بها طبقا لنص المادة 51 من قانون الإجراءات الجزائية

[1]. المادة 05 من الأمر 09-04

[2].سعيدة بوزنون.مرج سابق .ص 52

[3].بدري فيصل.مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي.أطروحة لنيل ا شهادة لدكتوراه العلوم .قانون عام .كلية الحقوق.جامعة الجزائر.1. سنة 2018/2017 .ص 210

– الحالة الثانية التي يجوز فيها توقيف المشتبه فيه للنظر فتكون اذا ادعت لذلك مقتضيات التحقيق الابتدائي طبقا للمادة 65 من نفس القانون

ولتوقيف النظر شروط هي :

– أن يقوم به ضابط الشرطة القضائية تحت إشراف وكيل الجمهورية .

– إخطار وكيل الجمهورية فورا بالتوقيف للنظر وأسبابه .

– تحرير محضر سماع للموقوف يتضمن مدة استجوابه وفترات الراحة التي تخللت ذلك اليوم والساعة الذي أطلق سراحه فيها أو تم فيها تقديمه للمحاكمة ويجب أن يتضمن المحضر إمضاء الموقوف للنظر أو الاشاره إلى امتناعه عن الإمضاء

وللموقوف حقوق تتمثل في الحق في السلامة الجسدية ، فلا يجوز لضباط الشرطة القضائية تعذيب الموقوف للنظر أو المساس بسلامته الجسدية ، وهذا ما كرسه المشرع الجزائري من خلال إلزام ضبط الشرطة القضائية بعرض الموقوف على طبيب لفحصه وضم شهادة الفحص الطبي لملف الإجراءات بموجب المادة 51 من قانون الإجراءات الجزائية

كما أنه لا يجوز أن تتجاوز مدة التوقيف للنظر ثمان وأربعون ساعة ماعدا بعض الجرائم الخطيرة التي خصها المشرع باستثناءات[1] ، ويمكن تمديدها مرة واحدة حسب المادة 51 من نفس القانون.

المطلب الثاني: الآليات المؤسساتية لمكافحة الجريمة الالكترونية

نظرا لتفاقم الظاهرة الإجرامية الالكترونية من يوم لأخر و بالنظر إلى الطبيعة الخاصة التي تتميز بها كان لزاما تطوير أجهزة الشرطة القضائية لتواكب التطور الحاصل في هاته الجرائم ، وهذا ما عمدت عليه الجزائر حيث قامت بتسخير هيئات ووحدات مختصة معنية بها ، أبرزها

[1] عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري، دار بلقيس، الجزائر بدون طبعة،سنة 2015. ،ص 91.

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال بالإضافة إلى ذلك وحدات قضائية و أخرى تابعة لسلك الأمن و الدرك الوطني

الفرع الأول : الهيئات الغير القضائية المعنية بالجرائم الالكترونية

الهيئات المتخصصة في مجال مكافحة الجريمة المعلوماتية هي وحدات تسند مهام الوقاية ومكافحة الجرائم الالكترونية ، بالنظر إلى تشكيلتها البشرية الخاصة التي تضم محققين من نوع خاص تجمع لدىهم صفة الشرطة القضائية إضافة إلى المعرفة الواسعة بالنظم المعلوماتية و المجرم[1].

أولا:الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

تعرف الهيئة الوطنية حسب أحكام المواد 01 إلى 04 من قانون 09-04 بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى وزير المكلف بالعدل ويقع مقرها بالجزائر .

الهيئة التي تعد سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل، وتضم أساسا أعضاء من الحكومة معنيّين بالموضوع، ومسؤولي مصالح الأمن، وقاضيين اثنين من المحكمة العليا يعيّنهما المجلس الأعلى للقضاء .

تضم الهيئة قضاة وضباطا وأعوانا من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك والأمن الوطنيين، وفقا لأحكام قانون الإجراءات الجزائية تكلف بتجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من اجل استعمالها في الإجراءات القضائية وضمان المراقبة والوقاية للاتصالات الالكترونية قصد الكشف عن الجرائم المنصوص عليها في قانون العقوبات أو الجرائم الأخرى، تحت سلطة القاضي المختص[2]

[1].ربيعي حسين، المرجع السابق، ص171

[2].سعيدة بوزنون .مرجع سابق .ص 53

ولقد تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بموجب نص المادة 13 من القانون 04/09 والتي يتم تحديد تشكيلها وتنظيمها وسيرها عن طريق تنظيم ، وتم إنشائها بهدف مساعدة السلطات القضائية ومصالح الأمن الوطني في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وانجاز الخبرات القضائية [1]، كما أن تحديد تشكيلة الهيئة وتنظيمها و كيفيات سيرها نصت عليهم المادتين 03 و04 من المرسوم الرئاسي 15-261[2]، أما عن تنظيم عملها فقد نص عليها كل من قانون04/09 والمرسوم الرئاسي .

ثانيا:الوحدات التابعة لسلك الأمن الوطني

تعد الجريمة الإلكترونية وجه جديد للجرائم يستلزم استحداث هياكل جديدة وتدعيم الهياكل القديمة المختصة في مكافحة الجرائم على مستوى المديرية العامة للأمن الوطني، وعلى هذا الأساس قررت القيادة العليا للأمن الوطني استحداث مخابر وفصائل وخلايا مختصة في مكافحة الجرائم الإلكترونية، والقيام بعمليات التحسس والتوعية من خلال المشاركة في الملتقيات الوطنية والدولية وجميع التظاهرات التي من شأنها توعية المواطن، بالإضافة إلى تنظيم دروس توعية في مختلف الأطوار الدراسية [3].

1. النيابة المديرية للشرطة العلمية على المستوى المركزي :

قامت المديرية العامة للأمن الوطني بتحديث بنيتها الهيكلية من خلال إنشاء وحدات متخصصة تعمل على مكافحة نوع معين من الجرائم دون سواها، وهذا باستحداث أربعة وحدات نيابية متخصصة تتمثل في :

[1]. حابت أمال .الطابع الخصوصي للاجراءات الجزائية في شأن الجرائم الالكترونية في القانون الجزائري.الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة . بسكرة.16 -17 نوفمبر 2015. ص 11

[2].المرسوم الرئاسي 15-261 المؤرخ في 08 أكتوبر 2015 .يحدد تشكيلة وتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال .ج ر 53 .08 أكتوبر 2015

[3] حملاوي عبد الرحمان، دور المديرية العامة لألمن الوطني في مكافحة الجرائم الإلكترونية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، بسكرة، يومي 16 و17 نوفمبر 2015 ،ص ص 08-09

أ. نيابة الشرطة العلمية والتقنية.

ب. نيابة مديرية الاقتصادية والمالية.

ج.نيابة القضايا الجنائية.

د. مصلحة البحث والتحليل [1].

2: دائرة الأدلة الرقمية والآثار التكنولوجية على المستوى الجهوي :

بالإضافة إلى المخبر المركزي الذي يتواجد بالجزائر العاصمة يوجد أيضا مخبرين جهويين على مستوى كل من قسنطينة ووهران يتوليان أعمال البحث والتحري في الجرائم، بما فيها الجريمة الإلكترونية وهذا تحت تسمية دائرة الأدلة الرقمية والآثار التكنولوجية والتي لم تكن سوى قسم عند استحداثها سنة 2004 ، وبسبب الارتفاع المتزايد لقضايا الجرائم الإلكترونية باستعمال تقنية المعلومات تم ترقيتها إلى دائرة تضم ثلاثة أقسام :

أ.قسم استغلال الأدلة الرقمية الناتجة عن الحاسوب والشبكات .

ب.قسم استغلال الأدلة الناتجة عن الهواتف النقالة.

ج.قسم تحليل الأصوات يتواجد على مستوى المخبر المركزي بالجزائر العاصمة[2].

3. الوحدات التابعة للدرك الوطني :

اهتمت قيادة الدرك الوطني بمكافحة الجريمة الإلكترونية بمختلف أشكالها وأنواعها، وهذا من خلال استحداث هياكل تابعة لها من أجل التصدي للإجرام ألمعلوماتي الذي بات يشكل تهديدا

خطيرا على أمن الدولة و سلامة المجتمع، وعليه تم إنشاء أربعة (04) وحدات تنشط في مجالّ الوقاية من الجريمة الإلكترونية ومكافحتها وهي:

[1].ربيعي حسين .المرجع السابق ص 177

[2]. حملاوي عبد الرحمان، مرجع سابق، ص08.

أ: المعهد الوطني للأدلة الجنائية وعلم الإجرام

تم إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام بموجب المرسوم الرئاسي رقم 04-183 المتضمن إحداث المعهد الوطني للأدلة الجناية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي ، فوفقا لنص مادة 02 من هذا المرسوم يعتبر المعهد مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي، ويوضع تحت وصاية وزارة الدفاع الوطني في بوشاوي بالجزائر العاصمة، فهو يخضع لجميع الأحكام التشريعية والتنظيمية العسكرية، وقد صنف من بين المعاهد الكبرى في العالم[1] .

يشمل المعهد على إحدى عشر 11 دائرة متخصصة في مجالات مختلفة جميعها تضمن إنجاز الخبرة، التكوين والتعليم بالإضافة إلى تقديم المساعدات التقنية والقيام ببحوث ودراسات وتحاليل في علم الجريمة [2]نظرا لاحتوائه على تجهيزات ووسائل تكنولوجية جد متطورة، بالإضافة إلى بنك المعلومات ومخابر للأدلة الرقمية والخبرة الصوتية للوقاية من جرائم الإعلام الآلي والهاتف المحمول [3]، ومن بين دوائره نجد دائرة الإعلام الآلي والالكتروني المكلفة بتحليل البيانات الرقمية وتقديم المساعدة للمحققين في مجال التحري والتحقيق في الجرائم الإلكترونية

ب. مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية :

تم إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية سنة 2008 ويعتبر الجهاز الوحيد المختص بهذا الصدد في الجزائر، يعمل على تأمين منظومة المعلومات لخدمة الأمن العمومي، وأعتبر بمثابة مركز توثيق، و يتواجد مقره ببئر مراد رايس[4] ، ويتجلى هدف

[1]. بهلول مليكة، دور الشرطة العلمية والتقنية في الكشف عن الجريمة، أطروحة لنيل شهادة دكتوراه علوم، فرع: الحقوق، كلية الحقوق، جامعة الجزائر 1 ،2013. ،ص 140

[2]. المعهد الوطني للأدلة الجنائية وعلم الإجرام، مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، يومي 16 و17 نوفمبر 2015 ،ص 03.

[3].بهلول مليكة.مرجع سابق.ص 144

[4]بارة سمير، الدفاع الوطني والسياسات الوطنية الأمن السيبراني في الجزائر ، المجلة الجزائرية للأمن الوطني الانساني ، عدد02 ، جامعة باتنة 1 ،2017 .ص 335

المركز في اكتشاف الجرائم والمخالفات المرتكبة في حق الأفراد والمؤسسات وممتلكاتهم التي تنتشر بواسطة التكنولوجيا الحديثة للإعلام والاتصال عبر الانترنت، ومحاربة كل أنواع الجرائم الالكترونية [1]

يعهد لمركز الوقاية من جرائم الإعلام الآلي و الجرائم المعلوماتية القيام بمجموعة من المهام التي تدخل في مجال اختصاصه لمكافحة الجريمة الإلكترونية بصفة عامة بحيث يكلف بما يلي:

– التعاون بشكل وثيق مع الهيئات الأجنبية على مكافحة الجريمة الإلكترونية .

– إجراء التحقيقات بالتعاون والتنسيق بين مخابر المركز والمعهد الوطني للأدلة الجنائية و علم الإجرام .

– جمع وحفظ الأدلة الرقمية على المستوى المركزي أو على المخابر التقنية.

– البحث عن أسباب حذف وثيقة أو ملف ما أو رسالة معينة و كيفية استخراجها واسترجاعها .

–القيام بإعادة تحليل وتتبع أرشيف البحار عبر الانترنت.

– تتبع مسار البريد الإلكتروني وتحديد مصدر الهجمات بالفيروسات أو الاختراق غير القانوني للوثائق الشخصية.

– توفير الأدلة حو ل سرقة المعطيات والمعلومات و تزوير الوثائق واستعمالها.

–البحث عن أدلة في وثيقة معينة أو رسالة إلكترونية باستخدام برمجيات خاصة ومفاتيح الكلمات[2].

ج. المصلحة المركزية للتحريات الجنائية:

2_ مركز الوقاية من جرائم الاعلام الالي والجرائم المعلوماتية ومكافحتها، مجلة الجيش، عدد 599 ،مؤسسة المنشورات العسكرية، الجزائر، 2013 ، ص 12 –16.

تعد المصلحة المركزية للتحريات الجنائية هيئة ذات اختصاص وطني من بين مهامها مكافحة الجريمة الإلكترونية[1]، وعليه يمكن القول بأنها جهاز تابع لقيادة الدرك الوطني له مهام عديدة في ميدان التحريات الجنائية والمساهمة في إجراء التحقيقات لمكافحة الجرائم بكافة أنواعها ومن بينها الجريمة الإلكترونية بكل أشكالها التي أضحت من جرائم العصر الفتاكة بالمجتمع في العالم الافتراضي.

د. مديرية الأمن العمومي و الاستغلال:

تعتبر بمثابة هيئة تعمل على التنسيق بين مختلف الوحدات الإقليمية والمركز التقني العلمي في مجال أعمال البحث والتحري في الجرائم الإلكترونية[2] ، وقد بلغ عدد القضايا التي عالجتها قيادة الدرك الوطني لسنة 2018 وهذا بداية من شهر جانفي إلى غاية شهر نوفمبر 1140 قضية متعلقة بالجريمة الإلكترونية منها 136 قضية خاصة بالأطفال دون 18 سنة و30 %من مجموع القضايا تتعلق بالابتزاز والتشهير[3] .

الفرع الثاني : الهيئات القضائية الخاصة للبحث في الجرائم الالكترونية

لقد أثمر مسار إصلاح العدالة الذي شرعت فيه الجزائر منذ سنة 2000 والذي انصب على دراسة ثلاث نقاط أساسية: دعم حقوق الإنسان و تسهيل حق اللجوء إلى القضاء وإعادة الاعتبار لنظام التكوين و التأهيل، بإحداث تغييرات جذرية في قطاع العدالة خاصة تعديل واستحداث قوانين تنسجم والالتزامات الدولية للجزائر وكذلك تحسين خدمات قطاع العدالة.

ولعل أهم ما جاءت به توصيات لجنة إصلاح العدالة تعديل القانون الجزائي بشقيه الموضوعي والإجرائي لمواجهة الظواهر الإجرامية الخطيرة وتزايد المنظمات الإجرامية وتزايد

[1]، بارة سمير، مرجع سابق، ص 345 -346

[2]، ربيعي حسين، مرجع سابق، ص 183.

[3]الجريمة الالكترونية :معالجة أزيد من 1100 قضية خلال 2018 على المستوى الوطني. http://www.aps.dz/ar/sante-science-technologie/63173-1100-2018 .11أوت 2020 .15:39

مخاطر التقنية و المعلوماتية على حياة الأشخاص وخصوصياتهم إضافة إلى أن هذا النوع من الجرائم تمتد آثاره خارج حدود الدولة الواحدة مهددة بذلك اقتصاديات الدول وأمنها، حيث شهدت السنوات الأخيرة تزايدا في العمليات الإرهابية و تزايدا في أعمال المنظمات الإجرامية واستعمالها الفضاء الافتراضي للاستفادة من خصائص الجريمة المعلوماتية .

من أجل كل هذا عكف المشرع الجزائري وقبله التشريعات المقارنة خاصة المشرع الفرنسي إلى استحداث الأقطاب الجزائية المتخصصة ، وهي محاكم ذات اختصاص إقليمي موسع بموجب القانون 04 -14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري الذي أجاز توسيع اختصاص بعض المحاكم ووكلاء الجمهورية وقضاة التحقيق في جرائم محددة على سبيل الحصر وتوصف أنها خطيرة وعلى درجة عالية من التعقيد والتنظيم وهي: جرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، تبييض الأموال، الجرائم الإرهابية والتخريبية وجريمة مخالفة التشريع الخاص بالصرف[1]، ولقد تم بالفعل صدور النص التنظيمي الخاص الذي مدد الاختصاص لأربع جهات قضائية[2] والذي تم بموجبه تحديد هذه المحاكم مع تعديل طفيف في المرسوم بحيث شمل التقسيم إضافة بعض المجالس القضائية بمقتضى المادة 3-4-5 المعدلة للمواد 3-4-5 من المرسوم السابق وجاء التقسيم كالتالي:

-محكمة سيدي أمحمد الجزائر العاصمة ويمتد اختصاصها الإقليمي إلى المجالس القضائية التالية:الجزائر، الشلف، الاغواط، البليدة، تيزي وزو، الجلفة، المدية، المسيلة و بومرداس

_محكمة قسنطينة ويمتد اختصاصها للمجالس القضائية: قسنطينة وام البواقي وباتنة وبجاية وتبسة وجيجل وسطيف وسكيكدة وعنابة وقالمة وبرج بوعريريج والطارف وخنشلة وسوق اهراس وميلة.

[1]. كريمة علة، الجهات القضائية الجزائية ذات الاختصاص الموسع، المجلة الأكاديمية للبحث القانوني، المجلد 11 عدد 2015.01،ص 1

[2]. المرسوم التنفيذي رقم 06-348 المؤرخ في 05-10-2006 المعدل والمتمم بالمرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016

–محكمة ورقلة ويمتد اختصاصها للمجالس القضائية التالية: ورقلة وأدرار وتامنغست وايليزي وبسكرة والوادي وغرداية– .

محكمة وهران ويمتد الاختصاص بها إلى المجالس القضائية التالية: وهران وبشار وتلمسان وتيارت وتندوف وسعيدة وسيدي بلعباس ومستغانم ومعسكر والبيض وتيسمسيلت والنعامة وعين تموشنت وغليزان[1].

بحيث يشمل اختصاص كل جهة قضائية مجموعة من المجالس القضائية تقع في منطقة جهوية من الجزائر شمالا جنوبا شرقا وغربا وذلك لدى أربع محاكم تسمى أقطابا جزائية، كما تم تدعيم عمل هذه الأخيرة باستحداث وسائل التحري الخاصة لمواجهة الإجرام المنظم بما فيها الجريمة الالكترونية[2]

المبحث الثاني: آليات مكافحة الجريمة الالكترونية عل المستوى الدولي

اهتم المجتمع الدولي بموضوع التصدي للجريمة الإلكترونية نظرا لما تتميز به من خصوصية ، مقارنة بالجرائم الأخرى مما جعل المجتمع الدولي يسعى إلى تكثيف جهوده من أجل مكافحتها ، وذلك من خلال إبرام اتفاقيات وعقد مؤتمرات و إنشاء منظمات واليات , و إرسائها في قالب تعاوني لوضع حد لهذا من النوع من الجرائم .

وعليه سيتم تقسيم هذا المبحث إلى مطلبين :

المطلب الأول: الإطار القانوني لمكافحة الجريمة الالكترونية

[1].كور طارق، مرجع سابق ، ص154.

[2]المواد 65 مكرر 5 الى 65 مكرر 18 من قانون الإجراءات الجزائية.

المطلب الثاني: آليات التعاون الدولي في مواجهة الجريمة الالكترونية

المطلب الأول : الإطار القانوني لمكافحة الجريمة الالكترونية

يواجه العالم أخطر الجرائم المستحدثة والتي تتمثل في الجرائم الالكترونية ، حيث أصبحت هذه الأخيرة أكثر إلحاحا على حياة ونشاط الإنسان لذا تنبهت دول العالم إليها , و أسفر عن تظافر جهود الدول و المنظمات الدولية إلى عقد العديد من المؤتمرات و إبرام الاتفاقيات والمعاهدات على المستوى الدولي و الإقليمي من اجل مكافحة هذه الجرائم و الحد منها

الفرع الأول : الاتفاقيات الدولية

إن اغلب الدول والمنظمات الدولية اهتمت بموضوع الجريمة الالكترونية اهتماما خاصا ، الأمر الذي أفرز عنه مجموعة من الاتفاقيات الدولية في هذا المجال ,وفي هذا السياق نشير إلى أهم الاتفاقيات التي تتناول هذا النوع من الجرائم وهي :

أولا : اتفاقية برن[1] :

تعتبر اتفاقية برن التي تم التوقيع عليها في عام 1971 في سويسرا هي حجر الأساس في مجال الحماية الدولية لحق المؤلف وقد وقعت على هذه الاتفاقية 120 دولة ، وتعد المادة التاسعة من هاته الاتفاقية هي الأساس لأنها تنص على منح أصحاب حقوق المؤلف حق استئثاري في التصريح بعمل نسخ من هذه المصنفات بأي طريقة وبأي شكل كان وتم تعديل هذه الاتفاقية في سنة 1979 و ازداد عدد الدول فيها إلى 140 دولة في 1999[2].

[1] المرسوم الرئاسي رقم 341/79 المؤرخ في 1997/09/13 المتضمن انضمام الجزائر مع التحفظ الى اتفاقية برن المؤرخة في 1869/09/09 والمتممة في باريس 1909/05/04 والمعدلة في 1997/09/28 ،جريدة الرسمية عدد 01 المؤرخة في 1997/09/14.

[2] بن الأخضر محمد، جرائم الكمبيوتر والانترنت، مذكرة لنيل رتبة ضابط، المدرسة العليا للشرطة، بن عكنون، ص.49، 2008-2007

وفضلا عن ذلك تمنح اتفاقية برن صاحب حق المؤلف الحق في أن يرخص أو يمنح ترجمة أو اقتباس أو بث إذاعي أو توصيل إلى الجمهور لمصنفه وكذلك تلزم الاتفاقية بتوقيع جزاءات سواء كان المؤلف المعتدى عليه وطنيا أو أجنبيا [1].

لقد تميزت اتفاقية برن بأنها منحت بعض الحقوق لدول لعالم الثالث من بينها حق الترجمة المجانية للجامعات والاستفادة العلمية منها ، والهدف الأساسي من إبرام هذه الاتفاقيات هو حماية حقوق المؤلفين على مصنفاتهم الأدبية والفنية [2]

كما تضمنت هذه الاتفاقية أحكاما خاصة بتحديد المصنفات الأدبية والفنية المشمولة بالحماية والشروط الواجب توافرها للاستفادة من الحماية ومبدأ المعاملة بالمثل [3]

ثانيا: معاهدة الويبو [4]

تأسست معاهدة الويبو بموجب اتفاقية ستوكهلوم التي أبرمت عام 1967 ودخلت حيز التنفيذ عام 1970 ، بلغ عدد الدول الأعضاء فيها عام 1999 إلى 177 دولة [5]، وتنقسم إلى ثلاث معاهدات :

1.معاهدة الويبو بشأن حق المؤلف :

تم التوقيع عليها في 20 ديسمبر1996 وتتكون من ثمانية عشر مادة تقوم على عدة أسس و مبادئ [6]

[1] منير محمد الجنبيهي وممدوح محمد الجنبيهي ,جرائم الانترنت والحساب الالي ووسائل مكافحتها,دار الفكر الجامعي,الاسكندرية ,2005. ص 201

[2] شرابشة ليندة ,السياسة الدولية والاقليمية في مجال مكافحة الجريمة الالكتروية ,الملتقى الدولي حول التنظيم القانون للانترنت والجريمة الالكترونية ,زيان عاشور ,الجلفة .27-28 أفريل 2009 ص 07

[3] عبد الله الكريم عبد الله, جرائم المعلوماتية والانترنت ,منشورات الحلبي الحقوقية .بيروت ,2007 , ص 49

[4]. معاهدة المنظمة العالمية للملكية الفكرية) WIPO) بشأن حق المؤلف 1996.

[5] محمودأحمد عبابنة ،جرائمالحاسوب و أبعادهاالدولّية، دارالثقافة للنشر والتوزيع،الاردن،2009،ص 160.

[6] منير محمد الجنبيهي وممدوح محمد الجنبيهي ,مرجع سابق ,ص 202

حيث تبدأ بديباجة ثم تتناول علاقة تلك المعاهدة بمعاهدة برن ثم تتعرض لنطاق تطبيق حماية حق المؤلف كحق التوزيع والتأجير ونقل المصنف إلى الجمهور والالتزامات المتعلقة بالتدابير التكنولوجية و التقييدات على تلك الحقوق وكذلك الحقوق والالتزامات المترتبة على المعاهدة ودخول المعاهدة حيز التنفيذ الفعلي وأخيرا تعرضت المعاهدة للتحفظ عليها ونقضها سواء من أحد أفرادها الموقعين عليها أو من إحدى الدول غير الموقعة عليها [1]

2.معاهدة الويبو بشأن الأداء والتسجيل الصوتي :

تم التوقيع عليها في 20 ديسمبر 1996 وتناولت أربعة فصول ، الفصل الأول منها الأحكام العامة وعلاقة المعاهدة بالاتفاقيات الدولية الأخرى والتعريف والمستفيدون من الحماية بناءا على تلك المعاهدة .

أما الفصل الثاني فيتناول حقوق فناني الأداء معنويا وماليا وحقوق الاستنساخ والتوزيع والتأجير وحق إتاحة الأداء المثبت

أما الفصل الثالث يتناول حقوق المنتجين كحقوق الاستنساخ والتأجير والتوزيع وحق إتاحة التسجيلات الصوتية

ويتناول الفصل الرابع الأحكام المشتركة كالحق في مكافأة مقابل الإذاعة أو النقل إلى الجمهور والاستثناءات على هذا الحق ومدة الحماية والالتزامات المتعلقة بالتدابير التكنولوجية وأخيرا التعرض للإجراءات الشكلية [2]

3.معاهدة الويبو بشأن الحماية الدولية لحق المؤلف والحقوق المجاورة :

تبدأ تلك الاتفاقية بمقدمة تناول الطابع القانوني للمعاهدتين الجديدتين و علاقتهما بالمعاهدات الدولية الأخرى

[1] أمجد عبد الفتاح أحمد حسان، مدى الحماية القانونية لحق المؤلف (دراسة مقارنة)، رسالة دكتوراه، جامعة تلمسان،2008،ص416.

[2] منير محمد الجنبيهي وممدوح محمد الجنبيهي .مرجع سابق. ص204

ثم تتناول الاتفاقية جدول الأعمال الرقمي و المعاهدات الجديدة ثم تتعرض الاتفاقية إلى أحكام أخرى عامة عن المعاهدتين الجديدتين و أخيرا أعمال المتابعة بعد المؤتمر الدبلوماسي,[1] و تهدف المنظمة العالمية للملكية الفكرية "الويبو" إلى :

– تدعيم اتخاذ الإجراءات التي تهدف إلى تسيير الحماية الفاعلة للملكية الفكرية في جميع أنحاء العالم

–تنسيق التشريعات الوطنية للدول الأعضاء في إطار الحماية الفاعلة للملكية الفكرية على الصعيد العالمي .

–تقديم الخدمات الفنية و القانونية و التدريبية في مجال العمل على الحماية الدولية للملكية الفكرية .

– النهوض بأعباء التسجيل في مجال الحماية الدولية للملكية الفكرية ، و ان تنشير البيانات الخاصة بالتسجيلات حيثما كان ذلك ملائما [2]

لهذا نجد المنظمة منذ نشأتها قد كرست جهودها لتنفيذ رسالتها، وتحقيق أهداف نشأتها من خلال النهوض بحماية الملكية الفكرية في جميع أنحاء العالم في ضوء التعاون الدولي والسهر عل حماية حقوق المبتكرين وأصحاب حقوق الملكية الفكرية [3]

ثالثا: اتفاقية تريبس[4]

اتفاقية تريبس هي الأخرى من المعاهدات التي تم انجازها في مجال حماية الملكية الفكرية من السطو مع انتشار عمليات السطو الالكتروني على الأعمال الفنية ، دون إعطاء مالكيها أي من حقوقهم المادية أو المعنوية .

[1] ,مرجع سابق ,ص 205

[2] رشا علي الدين, النظام القانوني لحماية البرمجيات .دار الجامعة الجديدة .الاسكندرية . بدون دار النشر ،2007.ص 241

[3] نفس الرجع السابق ص 264

[4].الاتفاقية حول الجوانب التجارية لحقوق الملكية الفكرية أو اتفاق تريبس المؤرخة في 1994

وتلك الاتفاقية تم التوقيع عليها من قبل الدول الأعضاء بها عام 1994 وقد عالج موقعوا الاتفاقية العامة للتعريفات والتجارة حقوق الملكية الفكرية بتوقيع اتفاق الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية فربطوا بذلك بين المعايير الدولية والمعايير المحلية [1]

تحتوي اتفاقية تريبس على الشروط التي يجب توافرها في قوانين الدول فيما يتعلق بحقوق المؤلف، بما في ذلك حقوق فناني الأداء ومنتجي التسجيلات الصوتية وهيئات الإذاعة؛ المؤشرات الجغرافية، بما في ذلك تسميات المنشأ؛ الرسوم والنماذج الصناعية؛ تصاميم الدوائر المتكاملة؛ براءات الاختراع؛ العلامات التجارية؛ والمعلومات السرية. كما تحدد اتفاقية تريبس أيضا إجراءات التنفيذ وسبل التحكيم وإجراءات تسوية المنازعات. وتهدف حماية وتنفيذ قوانين حقوق الملكية الفكرية إلى المساهمة في تعزيز الابتكار التكنولوجي ونقل وتعميم التكنولوجيا، بما يحقق المنفعة المشتركة لمنتجي ومستخدمي المعرفة التكنولوجية بطريقة تؤدي إلى الرفاهة الاجتماعية والاقتصادية، والتوازن بين الحقوق والواجبات[2].

الفرع الثاني : الاتفاقيات الإقليمية لمكافحة الجريمة الالكترونية

تبرز الجهود الإقليمية في مواجهة الجريمة الالكترونية في المساعي التي قام بها المجلس الأوروبي[3] الذي برز دوره كعنصر فعال في مكافحة هذه الظاهرة خصوصا في الحفاظ على المعطيات الفردية و كل ما يتعلق بالحياة الخاصة ، و لعل السبب في ذلك أن الدول المنتمية لهذا المجلس من الدول المتقدمة علميا و تقنيا الأمر الذي دفعها لوضع التوصيات و عمل الاتفاقيات التي تحتاج لتشريعات داخلية تعالج كل ما هو مستحدث في مجال التقدم العلمي[4] ، بالإضافة إلى الجهود التي تبذلها جامعة الدول العربية من خلال اعتمادها عبر أمانة مجلس وزراء العدل العرب لما سمى بقانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات

---

[1] منير محمد الجنبيهي وممدوح محمد الجنبيهي ,مرجع سابق ص 208

[2] الاتفاقية حول الجوانب التجارية لحقوق الملكية الفكرية . اتفاقية-حول-الجوانب-التجارية-لحقوق-الملكية - الفكرية/https://ar.wikipedia.org/wiki..يوم12 أوت 2020 .(22:03)

[3].مجلس أوروبا يتكون من 41 دولة .تأسس عام 1949 كاتحاد مضاد للأفكار الديكتاتورية سادت أوروبا في النصف الأول من القرن .موقع مجلس أوروبا على الانترنت هو http://www.coe.int

[4].سعيداني نعيم أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. مذكرة ماجستير .جامعة باتنة .2013.ص 44

وما في حكمها نسبة إلى مقدم هذا المقترح وهو دولة الأمارات العربية المتحدة وهو ما سنتعرض له بالتفصيل حسب التقسيم التالي :

1.اتفاقية بودابست

شهدت العاصمة المجرية بودابست في أواخر عام 2001 أولى المعاهدات الدولية التي تكافح جرائم الانترنت وتبلور التعاون والتضامن الدولي في محاربتها ومحاولة الحد منها خاصة بعد أن وصلت تلك الجرائم إلى حد خطير أصبح يهدد الأشخاص والممتلكات [1]

لقد تم صياغة هذه المعاهدة من جانب عدد كبير من الخبراء القانونيين في مجلس أوروبا وبمساعدة دول أخرى لاسيما و.م.أ.و، تم التوقيع عليها من قبل ثلاثين دولة بتاريخ 23 نوفمبر 2001 في العاصمة المجرية بودابست وذلك لمواجهة الاستخدام الغير المشروع للحسابات وشبكات المعلومات فيما يعرف بالإجرام الكوني أو الإجرام المعلوماتي أو الجرائم المعلوماتية[2]

رغم أن هذه الاتفاقية أوروبية الميلاد إلا أنها مفتوحة ذات الطابع الدولي تسمح بانضمام دول أخرى من غير المجموعة الأوروبية (المادة 48) .

تضمنت اتفاقية بودابست 48 مادة مقسمة إلى أربعة (04) فصول وركزت على ثلاثة (03)عناصر تتمثل في:

العنصر الأول: يتمثل في أهمية التدابير التشريعية الموضوعية أي نصوص التجريم الموضوعية

العنصر الثاني : يتمثل في أهمية التدابير التشريعية الإجرائية المتلائمة مع طبيعة الجرائم الالكترونية أي النصوص الإجرائية

[1] مدنير محمد الجنبيهي وممدوح محمد الجنبيهي.مرجع سابق.ص 180

[2] محمد علي العريان.الجرائم المعلوماتية.دار الجمعة الجديدة للطباعة والنشر والتوزيع.جامعة الاسكندرية .2011.ص 25

العنصر الثالث : يتمثل في أهمية تدابير التعاون الدولي والإقليمي في مجال مكافحة الجرائم ,والانطلاق مما أنجز من جهود دولية وإقليمية في هذا المجال [1]

ومن خلال ما سبق عرضه فإن اتفاقية بودابست 2001 تعد بمثابة دليل إرشادي للدول، يهدف إلى تطوير التشريعات الوطنية في مجال مكافحة الجريمة الإلكترونية والتعاون بين الدول الأطراف لتصدي لهذا النوع من الجرائم.

2.القانون العربي النموذجي لمكافحة جرائم تقنية المعلومات [2]:

اعتمدت جامعة الدول العربية عبر الأمانة الفنية لمجلس وزراء العدل العرب ما سمي بقانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها نسبة إلى مقدم هذا المقترح وهو دولة الإمارات العربية المتحدة، والذي كان قد اعتمده مجلس وزراء العدل العرب في دورته التاسعة بالقرار رقم 490-د-19-2003/10/8 ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين[3] ، ويعد هذا القانون بمثابة دليل إرشادي تستعين به الدول العربية في تشريع القوانين الموضوعية والإجرائية بخصوص الجرائم الإلكترونية، كما يساعد في الوقت نفسه على تجسيد تقارب بين القوانين الوطنية للدول الأعضاء[4] .

تضمن القانون 27 مادة بحيث نصت المادة الأولى على شرح بعض المصطلحات الواردة في القانون، أما المادة الثانية منه حرصت على توقيع الجزاء المنصوص إما في قانون العقوبات أو قانون آخر على كل شخص ارتكب الأفعال المذكورة في نصوص هذا القانون

و المواد من 03 إلى 22 ذكرت أنواع الأفعال التي تشكل جريمة إلكترونية والتي يمكن أن نلخصها فيما يلي :

---

[1] بن الأخضر محمد.مرجع سابق ص 56

[2]. قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها 19- 2003/10/08.د- 495ق، 2003

[3]عبد الله عبد الكريم عبد الله، مرجع سابق، ص 140.

[4]براهيمي جمال .التحقيق الجنائي في الجرائم الالكترونية .أطروحة لنيل شهادة الدكتوراه العلوم. تخصص :القانون.كلية الحقوق والعلوم السياسية .جامعة تيزي وزو.2018 ص ص 287-288

-جريمة غسل الأموال عبر الوسائط الإلكترونية.

- جريمة التزوير المعلوماتي.

- جريمة اختراق النظم المعلوماتية.

-جريمة السرقة المعلوماتية[1].

بالإضافة إلى جرائم أخرى تتمثل في :

-جرائم صناعة ونشر الإباحة إلكتروني

-جرائم الشرف والاعتبار في الوسط الرقمي

-المتاجرة بالمخدرات في المواقع الإلكترونية

المساس بالأمن الفكري والاقتصادي للدول عبر النظم المعلوماتية.

الإرهاب الإلكتروني

المواد من 23 إلى 25 نصت على المساهمة الجنائية، المعاقبة على الشروع والعقوبات التكميلية بالنسبة لغير حسني النية، وبخصوص قواعد الاختصاص القضائي تضمنتها كل من المادتين 26 و 27[2]

فمن خلال عرض ما تناوله هذا القانون نجد بأنه جاء خال من أي قواعد إجرائية في مجال مكافحة الجريمة الإلكترونية بحيث أنه اكتفى بالشق الموضوعي وهذا بإبرازه ألأنواع الجرائم الإلكترونية.

3.الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:

[1].بدري فيصل .مرجع سابق ص ص 35-38

[2]قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها. .

قامت الدول العربية الأعضاء في جامعة الدول العربية بإبرام اتفاقية متعلقة بالجريمة الإلكترونية بالقاهرة سنة 2010 سميت بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات، تضمنت ديباجة و43 مادة، إذ أنها ألزمت في مادتها الأولى على ضرورة تبني اتفاقية إقليمية ملزمة بين الدول العربية الأعضاء تهدف إلى وضع سياسة جنائية في مجال مكافحة جرائم تقنية المعلومات وتعزيز التعاون بين الدول العربية الأعضاء لمواجهة أخطار الجرائم الإلكترونية للحفاظ على أمن الدول وسلامة مجتمعاتها[1] ، وكانت الجزائر من بين الدول الأعضاء فيها والموقعة على هذه الاتفاقية والتي صادقت عليها فيما بعد بموجب المرسوم الرئاسي رقم 14-252 .[2]

المطلب الثاني:آليات التعاون الدولي في مواجهة الجريمة الالكترونية

التعاون الدولي يعد من أهم سبل مكافحة الجرائم الالكترونية ، وملاحقة مرتكبيها فبغير التعاون الدولي يزداد معدل ارتكاب تلك الجرائم ويطمئن مرتكبيها لعدم إمكانية ملاحقتهم إذ يكون من السهل عليهم التنقل من دولة إلى أخرى تبيح القوانين السارية بها ما ارتكبوه من جرائم , وعليه الوضع يفرض وضع آليات ضبط تتناسب مع خصوصية الجريمة الالكترونية في إطار التعاون الدولي

الفرع الأول التعاون القضائي :

إن التعاون القضائي يعد الآلية الرئيسية للكفاح ضد الجريمة العابرة للوطنية بأبعادها المختلفة[3] وفيما يتعلق بالجريمة الالكترونية فان فعالية التحقيق والملاحقة القضائية غالبا ما تقتضي الحاجة إلى مساعدة من السلطات في البلد الذي كان منشأ للجريمة، أو من السلطات في البلد الذي عبر من خلاله النشاط المجرم وهو في طريقه إلى الهدف أو حيث قد توجد أدلة الجريمة ، فقد يكون

[1].براهيمي جمال، مرجع سابق، ص 289

[2] مرسوم رقم 14-252 المؤرخ في 08 سبتمبر 2014 ،يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، جريدة رسمية عدد 57 ،2014 ،ص ص 04 -14

[3].أبو المعالي محمد عيسى ،الحاجة الى تحديث اليات التعاون الدولي في مجالة مكافحة الجرائم ،ورقة مقدمة في المؤتمر المغاربي الأول حول المعلوماتية ، والقانون المنعقد في 28-2009/10/29 ، طرابس –ليبيا ، ص 03

مرتكب الجريمة الالكترونية من جنسية دولة ما مستعملا في جريمته حواسيب موجودة في دولة أخرى وتقع آثار جريمته في دولة ثالثة.

فمن البديهي أن يقف مبدأ السيادة ومشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها ،لذا فان التحقيقات في الجرائم المعلوماتية ومتابعة مرتكبيها قضائيا تؤكد على أهمية المساعدة القضائية المتبادلة بين الدول .

وتعرف المساعدة القضائية الدولية بأنها كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دول أخرى بصدد جريمة من الجرائم[1] .

ولقد نص المشرع الجزائري في القانون 09/04 على مبدأ المساعدة القضائية الدولية المتبادلة في المادة 16 منه، معتبرا أنه في إطار التحريات والتحقيقات القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني ، وتتخذ المساعدة القضائية الدولية عدة صور منها :

أولا تبادل المعلومات

يولي المجتمع الدولي لتبادل المعلومات أهمية قصوى بوصفه وسيلة لمكافحة الإجرام عموما والجريمة الالكترونية خصوصا لما توفره المعلومات الصحيحة و الموثوقة من مساندة لأجهزة تنفيذ القانون ،ويشمل مبدأ تبادل المعلومات تقديم البيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة أجنبية وهي بصدد النظر في جريمة الكترونية .

تميز الجريمة الالكترونية بالعالمية وبكونها عابرة للحدود ، فان مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي ، بحيث يسمح بالاتصال المباشر بين الأجهزة القضائية والأمنية في الدول المختلفة من أجل تبادل المعلومات المتعلقة بالجريمة والمجرمين .

[1].سالم محمد سليمان الأوجلي ، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية ، أطروحة ماجستير ، كلية الحقوق ، جامعة عين الشمس ،القاهرة، 1997، ص 425

ولهذه الصورة من صور المساعدة القضائية صدى كبير في الكثير من الاتفاقيات ، أهمها ما ورد في الفقرة الثانية من المادة الأولى لمعاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية[1] ،وكذا ما ورد في البند الثالث والرابع والخامس من المادة الثامنة لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية ،إذ أوجبت علو الدول الأطراف تيسير تبادل المعلومات المتعلقة بكافة جوانب النشاط الإجرامي .

ويصدق الأمر أيضا على ما قضت به المادة الأولى من اتفاقية الرياض للتعاون القضائي العربي بشأن ضرورة تبادل المعلومات بين الدول الأطراف والتنسيق بين الأنظمة القضائية ، وفي هذا الإطار أيضا صاغ اتفاق شجن للاتحاد الأوروبي نظاما متكاملا لتبادل المعلومات[2] .

وعلى المستوى التشريعي الوطني فقد نصت المادة 17 من القانون 09/04 عل أن الدولة الجزائرية تستجيب لطلبات المساعدة القضائية الدولية الرامية لتبادل المعلومات وذلك في إطار الاتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل .

ثانيا : نقل الإجراءات

ويقصد بهذه الصورة قيام دولة ما بمقتضى اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد التحقيق

في جريمة الكترونية ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توفرت مجموعة من الشروط ، أهمها التجريم المزدوج والذي يقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب نقل الإجراءات إليها بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها[3] .

---

[1].صدرت هذه المعاهدة في 1990/12/14 في الجلسة العامة 68 للجمعية العامة لأمم المتحدة وتقضي باتفاق أطرافها على أن يقدم كل منهم للأخر أكبر قدر ممكن من المساعدة المتبادلة في التحقيقات أو إجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخلا في اختصاص السلطة القضائية للدولة الطالبة المساعدة

[2] MICHEL QUELLIE :strategies en France par la police la criminalité organisée , 1996 p 199

[3].سالم محمد الأوجلي ، مرجع سابق ، ص 02

بمعنى أن تكون مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة وأن تكون هذه الإجراءات ذات أهمية من شأنها أن تؤدي دورا مهما في الوصول إلى الحقيقة .

ولقد أقرت العديد من الاتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية ، منها معاهدة الأمم النموذجية بشأن نقل الإجراءات في المسائل الجنائية[1] ، وكذا اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية[2]

ثالث: الإنابة القضائية الدولية :

يقصد بهذه الصورة طلب اتخاذ إجراء قضائي من إجراءات الدعوى العمومية تتقدم به الدولة الطالبة إلى الدولة الطالبة لتعذر القيام بهذا الإجراء بنفسها[3] .

وهدف هذه الصورة تسهيل الإجراءات الجزائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الاقليمية ،التي تمنع الدول الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى لسماع شهود أو إجراء التفتيش أو غيرها.

ويحدث بدرجة متزايدة أن تشترط المعاهدات والاتفاقيات الخاصة بتبادل المساعدة القضائية الدولية على الدول الأطراف أن تعين سلطة مركزية عادة ما تكون وزارة العدل ترسل إليها الطلبات مباشرة بدلا من المرور عبر القنوات الدبلوماسية ،وذلك بغرض التسريع في الإجراءات .

الفرع الثاني : تسليم المجرمين

[1]. معاهدة نموذجية بشأن نقل الإجراءات في المسائل الجنائية اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة رقم 45/118 المؤرخ في 14 ديسمبر 1990

[2].اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية ، اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة رقم 25 الدورة الخامسة والخمسون المؤرخ 15 نوفمبر 2000، ولقد صادقت عليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم 02-55 المؤرخ في 05 فبراير 2002،ج ر رقم 09 بتاريخ 10 فبراير 2002

[3].جميل عبد الباقي الصغير ،الجوانب الإجرائية للجرائم المتعلقة بالانترنت ،دار النهضة العربية ،القاهرة-مصر ،2001، ص 83

استقر فقه القانون الدولي على اعتبار تسليم المجرمين شكل من أشكال التعاون الدولي في مكافحة الجريمة والمجرمين وحماية المجتمعات من المخلين بأمنها واستقرارها وحتى لا يبقى أولئك العابثين بمنأى عن العقاب يعيثون في الأرض فسادا[1] ، تم تعريف إجراء تسليم المجرمين بأنه عمل بمقتضاه الدولة التي لجأ إلى أرضها شخص متهم أو محكوم عليه في الجريمة تسلمه إلى الدولة

المختصة لمحاكمته أو تنفيذ العقوبة عليه[2] ويتم تسليم المجرمين بموجب توقيع اتفاقية بين دولتين وبناءا على شروط و إجراءات تحددها هذه الاتفاقية.

يكون تطبيق مبدأ تسليم المجرمين في الجرائم التي لم تعد الحدود الجغرافية تشكل حاجزا أمام مرتكبيها ومن ضمنها الجرائم الإلكترونية التي أصبحت آثارها تمتد إلى أقاليم الدول الأخرى[3] ، فقد نصت اتفاقية بودابست 2001 في م 24 على شروط تسليم المجرمين وهذا باتفاق كلا الدولتين على أوسع نطاق للتعاون بهدف إجراء التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية للشبكات والبيانات المعلوماتية وجمع الأدلة في الشكل الإلكتروني لهذه الجرائم [4] .

نصت م 31 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على مبدأ تسليم المجرمين الإلكترونيين بين الدول الأطراف في الاتفاقية وهذا بالنسبة للجرائم المنصوص عليها في الفصل الثاني من الاتفاقية

كما أكد المشرع الجزائري على مبدأ تسليم المجرمين وفقا لنص م 82 من الدستور المتضمنة « لا يسلم أحد خارج التراب وطنيا إلا بناءا على قانون تسليم المجرمين وتطبيقا له. » وعليه فإن

[1].براهيمي جمال، مرجع سابق، ص 319.

[2].مرجع سابق ص.321

[3] ،أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، مكتبة الوفاء القانونية، الإسكندرية، مصر، 2011 ،ص 428.

[4].محمد أحمد سليمان عيسى، "التعاون الدولي لمواجهة الجرائم الإلكترونية"، المجلة الأكاديمية للبحث القانوني، العدد 02 ،كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2016 ،ص ص 58-59.

المشرع الجزائري اعترف بهذا المبدأ دستوريا كما أقره ضمن قانون الإجراءات الجزائية في المواد 694 وما يليها

رغم أن المجتمع الدولي تبنى فكرة التعاون لوضع حد للجريمة الالكترونية من خلال تكاثف جهوده لمكافحتها ،إلا أن هذه الأخيرة باتت إجراء صعب المنال لوجود معوقات وعراقيل متعلقة باكتشاف هذا النوع من الجرائم بهدف مواجهتها وإثباتها وتتمثل هذه العراقيل في :

1.صعبة الاكتشاف : هذا يمكن أن يكون لعدة أسباب تقف وراءها والمتمثلة في صعوبة مسايرة التطور التكنولوجي الذي عرف تقدما هائلا ،عدم نشر الفكر التوعوي، وعدم الإبلاغ عن الجريمة

2. عراقيل متعلقة بالأنظمة التشريعية : إلى جانب صعوبات اكتشاف الجريمة نجد مجموعة من العراقيل المتعلقة بعدم تشريع نصوص خاصة موحدة للجريمة الإلكترونية المتمثلة في عدم وجود نموذج موحد للنشاط الإجرامي ، و اختلاف النظم القانونية الإجرائية ، انعدام وجود قنوات اتصال والتجريم المزدوج[1]

3. العراقيل التي تواجه إثبات الجريمة الإلكترونية: نظرا للطبيعة الخاصة التي تتسم بها الجريمة الإلكترونية عن باقي الجرائم الأخرى فإن القائمين بعملية التحري والتحقيق فيها يواجهون صعوبات في إثباتها من حيث الوصول للدليل، نقص خبرة القائمين على التحقيق ، تشعب البيانات الرقمية الإلكترونية ، وصعوبة تحديد عنوان المجرم الإلكتروني[2]

[1]. وعلي لامية .سعودي كاهنة، اجراءات مكافحة الجريمة الالكترونية ، مذكرة لنيل شهادة الماستر في القانون، القسم الخاص،كلية الحقوق والعلوم السياسية ،جامعة عبد الرحمان ميرة ، 2018-2019 ص 62

[2]. نفس المرجع ،ص 65

خاتمـــة

و في الأخير نخلص إلى القول أن دراسة موضوع المكافحة القانونية للجرائم الماسة بالأمن الإلكتروني تكتسي أهمية بالغة كونها تساهم في التعريف بظاهرة إجرامية جديدة بدأت في الظهور و الانتشار في معظم المجتمعات ، و نظرا لارتباطها بتكنولوجيا متطورة أدى إلى تميزها عن الجرائم التقليدية بدءا بتسميتها وصولا إلى الأفعال التي تدخل ضمن دائرتها بحيث تناولنا في الفصل الأول الجرائم الالكترونية بصفة عامة ، أين بينا مختلف الآراء الفقهية في تعريف هاته الجريمة وانتهينا إلى كونها كل اعتداء على النظام المعلوماتي أو يتم باستخدام النظام المعلوماتي الذي كان له دور رئيسي في السلوك المجرم ، و بهذا المفهوم نرى بأن الجريمة الالكترونية تتميز بعدة خصائص تميزها عن باقي الجرائم الأخرى أهمها طبيعتها المتعدية الحدود و طابعها التقني الذي يعقد من مسألة إثباتها، الشيء الذي يميز مرتكبيها و يجعل دوافع ارتكابهم للجرائم المعلوماتية بمختلف أنواعها تختلف عن المجرمين العاديين .

كما أن للنظام المعلوماتي أهمية كبيرة باعتباره تقنية حديثة في عالم تكنولوجيا المعلومات ، إلا أنه غالبا ما يكون مصدر خصب للجرائم التي تقع عليه و بواسطته، و بذلك تعد الجرائم الالكترونية جرائم خطيرة و سريعة و متطورة و في تزايد مستمر تبعا لازدياد استخدام تلك التقنية و هذا ما دفع بالعديد من الدول إلى مواكبة هذا التطور التكنولوجي بوضع النصوص الملائمة لمختلف استعمالات الإعلام الآلي .

و لمكافحة الجرائم الإلكترونية تم وضع قوانين خاصة داخلية و دولية للحد منها وهذا ما تطرقنا إليه في الفصل الثاني ،حيث أن تنظيم مجال المعلوماتية وسن تشريعات بهذا الخصوص يساعد في زرع الثقة في ثقافة المجتمع عامة، وهذا بدوره يشجع على زيادة استخدام وسائل تقنية المعلومات بدون هضم لحقوق وبدون خوف من العواقب السلبية، حيث صار من الضروري وضع القواعد العامة لاستخدام التقنية في مختلف التعاملات وتسهيل استخدامها على الصعيدين المحلي و الدولي .

إن مكافحة الجرائم الإلكترونية تسعى إلى تحقيق التوازن الضروري بين مصلحة المجتمع في الاستعانة بالتقنية الحديثة و مصلحة الإنسان في حماية حياته الخاصة كالحفاظ على أسراره

خاتمـــــة

، ان المساعدة على تحقيق الأمن المعلوماتي و تطويره بات أمرا حتميا أمام قيام إمبراطورية المعلوماتية وإنشاء ما يسمى بالمحكمات الإلكترونية ، و التي أضحت بحاجة ماسة إلى حماية قانونية.

أما في مجال الجهود الدولية المبذولة لمجابهة ظاهرة الجريمة الإلكترونية يمكن القول بأن بعض الاتفاقيات الدولية لا تزال تتخذ كمرجع لصياغة النصوص المتعلقة بوضع الإطار القانوني لحماية النظام المعلوماتي بشكل عام ومنها اتفاقية تريبس، بالإضافة إلى اتفاقية برن، و اللتان تظلان من أهم الأطر القانونية القائمة كآليات الدولية لفرض الحماية القانونية المطلوبة، والتي ظلت تدفع في اتجاه خلق ضوابط أخرى ، واتفاقية المنظمة العالمية للملكية الفكرية (الويبو) .

أما على المستوى الإقليمي فقد أصدر مجلس الاتحاد الأوروبي في 23 نوفمبر 2001 اتفاقية بودابست المشار إليها والمتعلقة بمكافحة الجرائم الإلكترونية والتي تعتبر مرجعا لا يستهان به في ميدان محاربة الإجرام الالكتروني سواء بالنسبة لبعض الاتفاقيات اللاحقة ذات الصلة أو بالنسبة لتشريعات الداخلية لبعض الدول .

أما على الصعيد العربي فقد صدر القانون العربي النموذجي الاسترشادي بخصوص مكافحة جرائم الكمبيوتر والانترنت كثمرة عمل مشترك بين مجلس وزراء الداخلية العرب ومجلس وزراء العدل العرب في نطاق الأمانة العامة لجامعة الدول العربية بعد أن قدم كلا المجلسين مشروعا بخصوص مكافحة الجريمة الإلكترونية .

وفي الجزائر يبدو أن هناك محاولات لتطوير المنظومة القانونية و تكييفيها مع المعطيات الدولية من خلال إصدار تشريعات تواكب التطور الحاصل في المجال المعلوماتي، ومن أبرز تلك التعديلات ما أورده في 03-05 الصادر في 2003/07/19 والمتعلق بحقوق المؤلف والحقوق المجاورة والتي أدرجت برنامج الحاسوب ضمن المؤلفات مضمونة الحماية، بالإضافة إلى النصوص الخاصة التي تبناها المشرع في تعديله الأخير لقانون (04_15) المؤرخ في 10/11/2004 المعدل و المتمم لأمر(66_156) المؤرخ في 08/06/1966 المتضمن قانون العقوبات، ويشمل المواد من 394 إلى 394 مكرر 08 ، فتعتبر مكافحة فعالة نظرا لما تمتاز به من شمولية، بحيث جاءت لتشمل أغلب الجرائم التي قد تمس نظام المعالجة

الآلية للمعطيات ، و تضمنت أيضا أغلب الجرائم التي قد تمس البيانات والمعطيات المكونة لهذا النظام

وعلى ضوء الإشكاليات التي أظهرتها الدراسة خلصت في الإجابة عنها إلى جملة من النتائج :

1) إن مفهوم الجرائم المعلوماتية ينصرف إلى الأفعال التي تشكل اعتداء على نظم المعالجة الآلية للمعطيات، والتي تستهدف بشكل خاص المعلومات المختلفة في البيئة الرقمية، بالإضافة إلى كل جريمة ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية، وهذه الأخيرة في الغالب ما تكون جرائم تقليدية

2) إن من أهم مميزات جرائم الاعتداء على نظم المعالجة الآلية للمعطيات،أنها تنصب على محل و نوع خاص يختلف تماما على محل الجرائم التقليدية

3) إن جرائم تكنولوجيا الإعلام والاتصال تختلف تماما عن الجرائم التقليدية فهي غير مرئية إذ يمكن إخفاؤها بكل سهولة.

4) صعوبة التحقيق في الجرائم الإلكترونية نظرا لصعوبة مسايرة التطور التكنولوجي الذي يتم استغلاله في هذا النوع من الجرائم.

5) إن إجراءات مكافحة الجريمة الالكترونية هي إجراءات من نوع خاص يشترط لمباشرتها التقييد بمجموعة من الشروط أهمها شرط التقييد بالنص الإجرائي الملائم، لما قد تنطوي عليه هذه الإجراءات من مساس بالحريات الفردية و إطلاع على مستودع سر الأفراد، كالتصنت الإلكتروني و اعتراض البريد الإلكتروني، و حجز للمعطيات و البيانات الشخصية، كل ذلك حفاظا على سالمة الإجراءات من طائلة البطلان و كذلك حفاظا على حريات الأفراد و كرامتهم

6) يقترن نجاح الحد من الجرائم الإلكترونية بنجاح إجراءات البحث و التحقيق في الجرائم الالكترونية بمدى براعة و فعالية جاهزة الجهات المختصة بمباشرة الإجراءات لتتبع الأدلة الإلكترونية، و تحصيلها و حفظها بغرض عرضها على الجهات المختصة بتقديرها

7) على المستوى القانوني و التشريعي فإننا لاحظنا مدى الاهتمام الذي توليه الدول و الحكومات لهذا المجال من خلال التحديثات المستمرة و المتوالية للنصوص العقابية والإجرائية،

خاتمـــــة

بشكل متناسق مع تطور الأساليب الإجرامية، و هي الجهود التي لاحظنا قلتها في التشريع الجزائري الذي أصبح يميزه الجمود و القدم مقارنة بما آلت إليه الجريمة الالكترونية، و كل ذلك بدعوى عدم تأثر المجتمع الجزائري بالظاهرة الإجرام الالكتروني بالشكل الذي يستوجب سن و تعديل النصوص على وجه الاستعجال، و هي المعطيات و الحجج التي من شانها تشجيع المجرمين على التصعيد من نشاطهم و تهديد المصالح العامة و الخاصة، خصوصا و أن هذه التقنية الالكترونية أصبحت من التقنيات الأكثر شيوعا في الجزائر

8) يستحيل القضاء على ظاهرة الإجرام الالكتروني بشكل نهائي، و ذلك لاتصالها المباشر بالتقنية الالكترونية، ففكرة التخلي عن هذه التقنية هي الحل الوحيد لمشروع القضاء على الجريمة الالكترونية، و ذلك بالرغم من درجة التطور التي آلت إليها المنظومة القانونية العقابية منها و الجزائية في مجال مكافحة الجريمة الالكترونية

من خلال الملاحظات السابقة الذكر ارتأينا ، وبناء على كل ما استعرضناه جاز لنا وضع تنويه مجموعة من التوصيات التي تساهم في حل الإشكاليات و العوائق التي صادفتنا في مجال البحث و لتكون إسهاما علميا واضح، و التي تتمثل فيما يلي:

1) العمل على التحسس بخطورة الجريمة الالكترونية على الأمن العام، و أمن الأفراد من خلال إدراج مفهوم الجريمة الالكترونية ضمن المقررات الدراسية

2) ضرورة العمل على تحسس ضحايا الجرائم الالكترونية بضرورة التبليغ عن أي جريمة الكترونية قد يقعون ضحايا لها

3) على المستوى الدولي :استحداث تشريعات نموذجية لمكافحة الجريمة الإلكترونية يمكن تطبيقها عالميا وقابلة للاستخدام مع مراعاة التدابير التشريعية القائمة عمى الصعيدين الدولي و الإقليمي

4) .ضرورة تعزيز الجهود الدولية الرامية إلى مكافحة الجريمة المعلوماتية بغرض صوغ صم شامل متعدد الأطراف ، يضع معالم نهج دولي في مجالات التجريم،و الصلاحيات الإجرائية، و الولاية القضائية، والتعاون الدولي.

5) حث الدول العربية على إبرام اتفاقية فيما بينها على غرار الاتفاقيات الأوروبية، بغية تعزيز التعاون القضائي و الشرطي بجميع صوره لمواجهة التحديات الإجرائية الناجمة عن الجرائم الإلكترونية عبر الوطنية.

6) .سد الفراغ التشريعي في مجال البيئة الرقمية بتشعباتها كافة مع إصدار المذكرات التوضيحية لتشريعات، لاسيما في مجال مكافحة الجريمة الإلكترونية ، على أن يكون شاملا للقواعد الموضوعية والإجرائية

7) إنشاء جهاز خاص داخل الشرطة يختص بالبحث والتحري عن هذا النوع من الجرائم ووضع سياسة تكوينية وتدريبية تتماشى والتطورات التكنولوجية الهائلة .

8) ضرورة تكثيف الجهود الوطنية لنشر المعرفة وزيادة الوعي بالجرائم الإلكترونية و مدى خطورتها ووسائل الوقاية منها و سبل مواجهتها

ضرورة العمل على تحسس ضحايا الجرائم الالكترونية بضرورة التبليغ عن أي جريمة الكترونية قد يقعون ضحايا لها.

01/- المراجع باللغة العربية :

أولا : الكتب

أ: الكتب العامة :

1. احسن بوسقيعة ,الوجيز في القانون الجزائي العام,الديوان الوطني للأشغال التربوية,2002,
2. كور طارق، آليات مكافحة جريمة الصرف، دار هومة، الجزائر، الطبعة الثانية 2014
3. عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري، دار بلقيس، الجزائر بدون طبعة،سنة 2015.

ب: الكتب الخاصة :

1. عادل يوسف عبد النبي شكري,بحث بعنوان الجريمة المعلوماتية و ازمة الشرعية الجزائية,جامعة الكوفة,العراق،2008
2. طارق إبراهيم الدسوقي عطية , الأمن المعلوماتي النظام القانوني للحماية المعلوماتية ,الإسكندرية،2010
3. احمد خليفة الملط ,الجرائم المعلوماتية ,الطبعة الثانية,دار الفكر الجامعي,إسكندرية مصر ,2006
4. أسامة احمد المناعة,جلال محمد الزعبي جرائم تقنية نظم المعلومات الالكترونية,دار الثقافة للنشر و التوزيع , 2014
5. نائلة عادل محمد فريد قورة,جرائم الحاسب الاقتصادية,دراسة نظرية وتطبيقية,دار النهضة العربية, القاهرة,2003
6. .سعيد عبد الطيف حسن، إثبات جرائم الكمبيوتر و الجرائم المرتكبة عبر الانترنت,دار النهضة العربية,القاهرة 1999
7. عبد الله حسين محمود,سرقة المعلومات المخزنة في الحاسب الآلي,دار النهضة العربية,القاهرة,2002,

8. أسامة احمد المناعسة, جلال محمد الزعبي ,صايل فاضل الهواوشة,جرائم الحاسب الآلي و الانترنت , دراسة تحليلية مقارنة,دار وائل لنشر ,عمان الأردن.2001

9. حنان ريحان مبارك المضحكي,الجرائم المعلوماتية ,دراسة مقارنة ,منشورات الحلبي الحقوقية ,بيروت, 2014

10. عماد مجدي عبد المالك,جرائم الكمبيوتر و الانترنت,دار المطبوعات الجامعية.مصر 2001

11. محمد زكي ابو عامر,الإجراءات الجنائية , دار الجامعة الجديدة ,مصر 2002

12. خالد ممدوح إبراهيم,امن الجريمة الالكترونية,الدار الجامعية, الإسكندرية,2001

13. سامي علي عياد حامد , الجريمة المعلوماتية و إجرام الانترنت ,دار الفكر الجامعي,الإسكندرية,2007

14. محمد سامي الشوا,ثورة المعلومات و انعكاساتها على قانون العقوبات ,دار النهضة العربية, 1994

15.منير محمد الجنبيهي وممدوح محمد الجنبيهي ,جرائم الانترنت والحساب الالي ووسائل مكافحتها,دار الفكر الجامعي,الاسكندرية ,2005.

16. محمودأحمد عبابنة ،جرائمالحاسوب و أبعادهاالدولّية، دار الثقافة للنشر والتوزيع،الاردن،2009،

17عبد الله الكريم عبد الله, جرائم المعلوماتية والانترنت ,منشورات الحلبي الحقوقية .بيروت ,2007

18. رشا علي الدين, النظام القانوني لحماية البرمجيات .دار الجامعة الجديدة .الاسكندرية ،2007

19. محمد علي العريان.الجرائم المعلوماتية.دار الجمعة الجديدة للطباعة والنشر والتوزيع.جامعة الاسكندرية .2011.

20.أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، مكتبة الوفاء القانونية، الإسكندرية، مصر ،2011

21. جميل عبد الباقي الصغير ،الجوانب الإجرائية للجرائم المتعلقة بالانترنت ،دار النهضة العربية ،القاهرة–مصر ،2001

ثانيا: الأطروحات والمذكرات الجامعية

أ . أطروحات :

1. ربيعي حسين .آليات البحث والتحقيق في الجرائم المعلوماتية أطروحة لنيل شهادة دكتوراه الحقوق. فرع: قانون العقوبات والعلوم الجنائية .كلية العلوم والحقوق السياسية .جامعة باتنة 2016-2015

2. بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم، تخصص: قانون عام، كلية الحقوق، جامعة الجزائر01 ،2018

3. بهلول مليكة، دور الشرطة العلمية والتقنية في الكشف عن الجريمة، أطروحة لنيل شهادة دكتوراه علوم، فرع: الحقوق، كلية الحقوق، جامعة الجزائر 1 ،2013

4. أمجد عبد الفتاح أحمد حسان، مدى الحماية القانونية لحق المؤلف (دراسة مقارنة)، رسالة دكتوراه، جامعة تلمسان،2008

5. براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه في العلوم، تخصص: القانون، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2018

6. بن الأخضر محمد، جرائم الكمبيوتر والانترنت، مذكرة لنيل رتبة ضابط، المدرسة العليا للشرطة، بن عكنون، ، 2008

ب.مذكرات الماجستير:

1. حمزة بن عقون,السلوك الإجرامي للمجرم المعلوماتي,بحث مكمل لنيل شهادة الماجستير في العلوم القانونية ,تخصص علم الإجرام و العقاب,جامعة باتنة,2011_2012

2. محمد بن عبد الله بن علي المنشاوي,جرائم الانترنت في المجتمع السعودي ,ماجستير في العلوم الشرطية,اكادمية نايف العربية للعلوم الأمنية ,الرياض,2003

4. سوير سفيان,الجرائم المعلوماتية,رسالة لنيل شهادة الماجستير في العلوم الجنائية و علم الاجرام,كلية الحقوق,جامعة أبو بكر بلقايد,تلمسان الجزائر,2010

5. سعيداني نعيم آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. مذكرة ماجستير .جامعة باتنة .2013

6. سالم محمد سليمان الأوجلي ، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية ، أطروحة ماجستير ، كلية الحقوق ، جامعة عين الشمس ،القاهرة ، 1997

ثالثا المقالات العلمية:

1. سعيدة بوزنون ،مكافحة الجريمة الالكترونية في التشريع الجزائري ،مجلة العلوم الانسانية ،العدد 52 ، المجلد ب ، 2019 ،

2. كحلو علي ,جرائم الحاسوب وأساليب مواجهتها ,مجلة صادرة عن مديرية الأمن الوطني,العدد84, 2007

3. بارة سمير، الدفاع الوطني والسياسات الوطنية الأمن السيبراني في الجزائر ، المجلة الجزائرية للأمن الوطني الانساني ، عدد02 ، جامعة باتنة 1 ،2017

4. مركز الوقاية من جرائم الاعلام الالي والجرائم المعلوماتية ومكافحتها، مجلة الجيش، عدد 599 ،مؤسسة المنشورات العسكرية، الجزائر، 2013

5. محمد أحمد سليمان عيسى، "التعاون الدولي لمواجهة الجرائم الإلكترونية"، المجلة الأكاديمية للبحث القانوني، ع 02 ،كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2016

6. صالحة العمري,جريمة غسيل الأموال و طرق مكافحتها,مجلة الاجتهاد القضائي,العدد الخامس,مخبر اثر الاجتهاد القضائي على حركة التشريع محمد خيضر ,بسكرة 2018

رابعا المداخلات :

1. سيناء عبد الله محسن,المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية و الوطنية, الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر,الدار البيضاء,المملكة المغربية,2007,

2. عاقلي فضيلة, الجريمة الالكترونية و إجراءات مواجهتها من خلال التشريع الجزائري, مداخلة ألقيت في أشغال المؤتمر الدولي حول الجرائم الالكترونية ,الاتحاد العالمي للمؤسسات العلمية,طرابلس,لبنان,24-25 مارس 2017

3. كرستا سكولمان ,عن جرائم الانترنت طبيعتها و خصائصها,الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر,المملكة المغربية,19-20 يونيو 2007

4. عباس أبو شامة ,التعريف بالظواهر الإجرامية المستحدثة حجمها أبعادها و نشاطها قي الدول العربية ,الندوة العلمية للظواهر الإجرامية المستحدثة و سبل مواجهتها ,تونس 29 -30 جوان 1999

5. زكي أمين حسونة ,جرائم الكمبيوتر و الجرائم الأخرى التكتيك ألمعلوماتي ,المؤتمر السادس للجمعية المصرية للقانون الجنائي ,القاهرة 1993 25 إلى 28 أكتوبر 1993 ,

6. نمديلي رحيمة، خصوصية الجريمة الالكترونية في القانون الجزائري و القوانين المقارنة، كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان، يومي 24-25|مارس2017

7. . أمحمدي بوزينة أمنة ، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية: (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام) .أعمال ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري المنعقد في الجزائر العاصمة يوم 29 مارس 2017

8. حابت أمال .الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الالكترونية في القانون الجزائري.الملتقى الوطني حول الجريمة

9. المعلوماتية بين الوقاية والمكافحة . بسكرة.16 -17 نوفمبر 2015

10. حملاوي عبد الرحمان، دور المديرية العامة لألمن الوطني في مكافحة الجرائم الإلكترونية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، بسكرة، يومي 16 و17 نوفمبر 2015

11. المعهد الوطني للأدلة الجنائية وعلم الإجرام، مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، يومي 16 و17 نوفمبر 2015 .

12. شرابشة ليندة ,السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية ,الملتقى الدولي حول التنظيم القانون للانترنت والجريمة الالكترونية ,زيان عاشور ,الجلفة .27-28 أفريل 2009

13. أبو المعالي محمد عيسى ،الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجرائم ،ورقة مقدمة في المؤتمر المغاربي الأول حول المعلوماتية ، والقانون المنعقد في 28-2009/10/29 ، طرابس –ليبيا

خامسا النصوص القانونية:

أ.النصوص التشريعية:

1. أمر رقم 66-156 ،مؤرخ في 08 يونيو 1966 ،يتضمن قانون العقوبات، معدل ومتمم، جريدة رسمية عدد 49 ،الصادرة في 11 جوان 1966

2. قانون06-22 المؤرخ في 20 ديسمبر 2006 يتمم الأمر 66-155 المؤرخ في 08 جوان 1966 المتضمن قانون الإجراءات الجزائية . جريدة رسمية عدد44

3. القانون 04-15 المعدل والمتمم للأمر 66-155 المؤرخ في 10 نوفمبر 2004 المتضمن قانون العقوبات جريدة رسمية عدد 71

4. قانون رقم 09-04 مؤرخ في 05 غشت 2009 ،المتضمن القو اعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية عدد 47 ،الصادرة في 16أو ت 2009 .

ب. النصوص التنظيمية :

1.المرسوم الرئاسي 15-261 المؤرخ في 08 أكتوبر 2015 .يحدد تشكيلة وتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال .جريدة رسمية 53 .08 أكتوبر

2.المرسوم الرئاسَي رقم 341/79 المؤرخ فًي 1997/09/13 المتضمن انضمام الجزائر مع التحفظ الى اتفاقية برن المؤرخة في 1869/09/09 والمتممة فًي باريس 1909/05/04 والمعدلة فًي 1997/09/28 ،جريدة الرسمية عدد 01 المؤرخة في 1997/09/14.

3.المرسوم الرئاسي رقم 14-252 المؤرخ في 08 سبتمبر 2014 ،يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، جريدة رسمية عدد 57 ،صادرة في 28 سبتمبر 2014

4.المرسوم التنفيذي رقم 06-348 المؤرخ في 05-10-2006 المعدل والمتمم بالمرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016

ج.المعاهدات والاتفاقيات :

1. معاهدة الأمم النموذجية بشأن نقل الإجراءات في المسائل الجنائية اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة رقم 45/118 المؤرخ في 14 ديسمبر 1990

2.اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة رقم 25 الدورة الخامسة والخمسون المؤرخ 15 نوفمبر 2000، ولقد صادقت عليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم 02-55 المؤرخ في 05 فبراير 2002،ج ر رقم 09 بتاريخ 10 فبراير 2002

3. الاتفاقية حول الجوانب التجارية لحقوق الملكية الفكرية أو اتفاق تريبس المؤرخة في 1994

4. معاهدة المنظمة العالمية للملكية الفكر(WIPO)بشأن حق المؤلف 1996.

5. قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها 19- 2003/10/08.د- 495ق، 2003

سادسا: المواقع الإلكترونية

قائمـــــــة المراجـــــــــع

1.علاء رضوان ، الجريمة و العقاب في واقع الابتزاز الالكتروني ، موقع اليوم السابع , 10 فبراير 2020

2.محمد صالح الألفي ، أنماط جرائم الانترنت ، متوفر على موقع www.eastlaws.com

3.أنتوني كاثبرتسون ، مجرمو الانترنت الخفي يبيعون المخدرات عبر تطبيقات شائعة وكومبيوترات مسيطرة عليها ,موقع Independent عربية

4.منيرة ابتسام طوابلي ، تسجيل 4210 جريمة سيبيرانية خلال2019، موقع المحور اليومي ، 2020-02-05

5.سورية ديش,أنواع الجرائم الالكترونية و إجراءات مكافحتها ,موقع المركز الديمقراطي العربي,22 فبراير 2017

6. حسين بن سعيد بن سيف ألغافري,الإرهاب الالكتروني,موقع وزارة عمان الرقمية

7.الاتفاقية حول الجوانب التجارية لحقوق الملكية الفكرية . اتفاقية-حول-الجوانب-التجارية-لحقوق-الملكية -الفكرية/https://ar.wikipedia.org/wiki.

7.مجلس أوروبا يتكون من 41 دولة .تأسس عام 1949 كاتحاد مضاد للأفكار الديكتاتورية سادت أوروبا في النصف الأول من القرن .موقع مجلس أوروبا على الانترنت هو http://www.coe.int

8.الجريمة الالكترونية :معالجة أزيد من 1100 قضية خلال 2018 على المستوى الوطني. http://www.aps.dz/ar/sante-science-technologie/63173-1100-2018

02/- المراجع باللغة الفرنسية:

1- Is the U.S. turning into a surveillance society ? American civil liberties union

2- Rose (Philippe).op-cit.P58-59

3- André Lucas. le droit de l'informatique. Paris.PUF 1987

4- Duleroy et rocco (A.M) , l'informatique nouvelle, avril 1976,les escrocs a l'informatique, le nouvel e Économiste, octobre 1979

5- Equity fuding life insurence. L'informatique nouvelle , mai 1976

6- Escroquerie aux Assedic de paris, jugement du 2fev 1982 TGI de paris 13éme ch.°39 ,avril 1982

7- Escroquerie aux Assedic de paris, jugement du 2fev 1982 TGI de paris 13éme ch.°39 ,avril 1982

8- Trip de paris. 12éme ch., corr. jugement du 13 janv. 1982,DALLOZ S 1982

9-Le monde informatique , 21 fev 1983, sous le titre (la délinquance en cal blanc se parte lien)

10- MICHEL QUELLIE :stratégies en France par la police la criminalité organisée , 1996

الفهرس

الرقم	التحـــــديـــــد	الصفحـــــة من	الصفحـــــة إلى
01	**مقدمـــــة**	01	03
02	**الفصل الأول : الإطار المفاهيمي للجريمة الالكترونية**	04	04
03	المبحث الأول : ماهية الجريمة الالكترونية	05	05
04	المطلب الأول: مدلول الجريمة الالكترونية	05	05
05	الفرع الأول : تعريف الجريمة الالكترونية	05	08
06	الفرع الثاني : خصائص الجريمة المعلوماتية	08	12
07	المطلب الثاني : أركان الجريمة الالكترونية	12	12
08	الفرع الأول : الركن الشرعي	12	13
09	الفرع الثاني : الركن المادي	13	15
10	الفرع الثالث : الركن المعنوي	15	16
11	المبحث الثاني : مظاهر الجريمة الالكترونية	16	17
12	المطلب الأول : الجرائم الواقعة بواسطة النظام ألمعلوماتي	17	17
13	الفرع الأول : الجرائم الواقعة على الأشخاص	17	20
14	الفرع الثاني : الجرائم الواقعة على الأموال	20	22
15	الفرع الثالث : جرائم ضد أمن الدولة	23	24
16	المطلب الثاني: الجرائم الواقعة على النظام ألمعلوماتي	25	25
17	الفرع الأول : جرائم الاعتداء على المكونات المادية للنظام المعلوماتي	25	26
18	الفرع الثاني :جرائم الاعتداء على المكونات المنطقية للنظام المعلوماتي	26	28
19	الفرع الثالث: جرائم الاعتداء على المعلومات المدرجة بالنظام ألمعلوماتي	28	30
20	**الفصل الثاني : المكافحة القانونية للجريمة الالكترونية**	31	31
21	المبحث الأول: آليات مكافحة الجريمة الالكترونية على المستوى الوطني	32	32
22	المطلب الأول:الآليات التشريعية لمكافحة الجريمة الالكترونية في التشريع الجزائري	32	32
23	الفرع الأول :القواعد الموضوعية المعنية لمكافحة الجرائم الالكترونية	32	35
24	الفرع الثاني :القواعد الإجرائية المنظمة لمكافحة الجريمة الالكترونية	35	39
25	المطلب الثاني: الآليات المؤسساتية لمكافحة الجريمة الالكترونية	40	40
26	الفرع الأول : الهيئات الغير القضائية المعنية بالجرائم الالكترونية	40	45
27	الفرع الثاني : الهيئات القضائية الخاصة للبحث في الجرائم الالكترونية	46	47
28	المبحث الثاني: آليات مكافحة الجريمة الالكترونية عل المستوى الدولي	48	48
29	المطلب الأول : الإطار القانوني لمكافحة الجريمة الالكترونية	48	48

الفهرس

الرقم	التحـــــديـــــد	الصفحـــــة	
		مـــن	إلى
30	الفـرع الأول : الاتفاقيات الدولية	48	52
31	الفرع الثاني : الاتفاقيات الإقليمية لمكافحة الجريمة الالكترونية	52	56
32	المطلب الثاني:آليات التعاون الدولي في مواجهة الجريمة الالكترونية	56	56
33	الفـــرع الأول : التعاون القضائي	57	60
34	الفـرع الثاني : تسليم المجرمين	60	62
35	**خـــــــاتمـــة**	63	67