وزارة التعليم العالي والبحث العلمي

جامعة عمار ثليجي بالأغواط

كلية الحقوق والعلوم السياسية

قسم الحقوق

الموضوع:

إجراءات الوقاية والمتابعة في الجرائم الإلكترونية

مذكرة تخرج مقدمة لنيل شهادة الماستر في القانون الجنائي

إعداد الطالب:

♣ جواد العربي دحو بشير .

♣ عز الدين بن بركة

إشراف الأستاذ:

– أ.د خضرون عطاالله

السنة الجامعية: 2019-2020

وزارة التعليم العالي والبحث العلمي

جامعة عمار ثليجي بالأغواط

كلية الحقوق والعلوم السياسية

قسم الحقوق

الموضوع:

إجراءات الوقاية والمتابعة في الجرائم الإلكترونية

مذكرة تخرج مقدمة لنيل شهادة الماستر في القانون الجنائي

إعداد الطالب:

- ♣ جواد العربي دحو بشير .
- ♣ عز الدين بن بركة .

أعضاء لجنة المناقشة:

أ.د بوقرين عبد الحليم.....رئيسا

أ.د خضرون عطاالله ..... مشرفا

أ.د رابحي لخضر..... مناقشا

السنة الجامعية: 2019-2020

كلمة شكر

قال الله تعالى "وإن شكرتم لأزيدنكم "

ومن هذا المنطق نشكر الله تعالى ونحمده حمدا طيبا على توفيقه لي ومده لي بالعون والصبر لإنجاز هذا البحث الذي نتمنى أن يكون فيه فائدة لكل من اطلع عليه فإن أصبنا فمن الله وإن أخطأنا فمن نفسي والله تعالى ولي التوفيق ، كما نتقدم بجزيل الشكر إلى الأستاذ المشرف الدكتور خضرون عطاالله على توجيهاته ونصائحه القيمة كما نشكر لجنة المناقشة الموقرة وإلى جميع أساتذة قسم الحقوق كما لا يفوتنا أن نتقدم بالشكر الخاص إلى كل من ساعدنا من قريب او بعيد .

إهداء

الحمد لله الذي اعاننا على اتمام هذا العمل وانجازه وصل اللهم على عبدك المصطفى ونبيك المجتبى وسلم تسليما كثيرا.

الى التي اضاءت سماء روحي وأنارت درب حياتي وبقلبها الرحيم رعتني وبطيب حنانها غمرتني والتي جعلتني انسانا قويا وشجعتني ولا تزال على مواصلة الدرب فاستحقت ان تكون الجنة تحت اقدامها ادين لها بعمري امي الغالية .

الى من علمني حقيقة الحياة ومعنى الاخلاص والوفاء الى من صنع من شقائه سعادتي ومنحني دون مقابل واعز واغلى ما املك في هذا الوجود ادين له بحياتي ابي الغالي حفظه الله .

إلى كل إخوتي الأعزاء و العائلة الكريمة

وإلى كل من نسيهم قلمي وحفظهم قلبي، إلى من يعرفني من قريب أو بعيد.

"الحمد لله رب العالمين تباركت خالقي وخالق كل شيء "

مقدمة

مقدمة :

مقدمة:

لقد خلق الله سبحانه وتعالى الإنسان وكرمه عن باقي مخلوقاته بالعقل الذي هو مناط التكليف, وباعتباره كائنا عاقلا متميزا ومنفردا عن باقي المخلوقات جعلت منه الضرورة اللجوء للبحث عن سبل أكثر ملائمة لبنيته الفيزيولوجية والبيولوجية بقصد التكيف والتأقلم مع بيئته وظروفه المعيشية ، وبلغ بذلك مراحل متقدمة حيث جعل من العالم قرية صغيرة له واختصر على نفسه آلاف الكيلومترات بمجرد كبسة زر على هاتف أو معاينة ومشاهدة أحداث بالعين المجردة تقع في مشرق الأرض وهو متواجد في مغربها عن طريق فيديو مباشر على حاسوب أو غيره من الوسائل السمعية البصرية الأخرى. وصار من المستحيل تصور الاستغناء على هذه الوسائل التقنية والمعلوماتية و على الحواسب الآلية في الحياة اليومية للبشر كونها أصبحت متجذرة في أدق تفاصيل حياته وخاصة في دول العالم المتقدم .

ورغم كل الامتيازات التي يحصلها الإنسان عن طريق العلم والإبتكار من منفعة إلا أن لها أضرارا وسلبيات إذا ما استعملت بطرق ووسائل غير شرعية تعود بالضرر على النظام العام للمجتمع من انتهاكات على حقوق الشخص الطبيعي والمعنوي على حد سواء.

ونظرا لدراستي السابقة عند الدكتور الفاضل عبد الوهاب ملياني في مقياس الجرائم المعلوماتية كان له الأثر البالغ في وصولي لمعرفة أهم المقتطفات والتعريفات المتعلقة بمنظومة الحاسب الآلي وطريقة استعمالها كأداة للجريمة ، وما جلب انتباهي كطالب باحث عن موضوع للدراسة هو القيمة العلمية لهذا البحث وما يحتويه من معلومات شيقة تدفع بأي باحث كان في هذا مجال الخوض في غماره ومعرفة أسراره والمعوقات التي تعتريه ويعود ذلك لسبب جديته عن باقي الجرائم التقليدية الأخرى ومنه استنتجت أنه مجال مشبع بالإشكاليات المثارة التي تحول بالمشرع الجزائري إلى الوصول لصد وردع هذه الجريمة التي تمثل كابوسا مرعبا لكل التشريعات

مقدمة :

وكانت غايتي من إختيار الموضوع هو محاولة استخلاص الإشكاليات التي تعتري النصوص القانونية في قانون العقوبات الجزائري و القوانين الخاصة المتعلقة بمكافحة الجرائم المعلوماتية ، ومحاولتنا معرفة مدى نجاعة الأساليب المتخذة من قبل المشرع من حيث الإجراءات في سبيل ضبط المجرم الإلكتروني كون أن المجرم العادي يختلف عن المجرم الإلكتروني ، و مقارنتها مع النصوص التقليدية للتوصل بعد ذلك لمدى ملائمتها للنصوص الحديثة بالنسبة للجرائم الإلكترونية ، وبعد فضل الله تعالى علي كان للدراسات السابقة أثر كبيرة في وصولي لهيكلة مضمون هذا البحث من بينها دراسة الدكتورين الفاضلين اللذين تشرفت بالدراسة لديهما هما عبد الوهاب ملياني الذي اعتمد على عنوان أمن المعلومات في بيئة الأعمال الإلكترونية كموضوع تخرج في الدكتوراه والدكتور عبد الحليم بوقرين الذي إعتمدت على مقاله بعنوان المكافحة الإجرائية للجريمة المعلوماتية ومداخلته بعنوان تجربة الجزائر في مكافحة الجريمة الإلكترونية .

و من أكثر الصعوبات التي واجهتها في الدراسة هو كون الموضوع شديد التفرع يحتاج إلى تفصيل وتجد أن أغلب الباحثين يعتمدون عليه كعنوان لمذكرة تخرج في الدكتوراه مما جعلني أقوم بضغط كبير للمعلومات المتحصلة واستنباط أهم الحيثيات المتعلقة بالموضوع مستغنيا بذلك عن المفهوم والخصائص المتعلقة بهذه الجريمة نظرا لإخلالهم بالخطة المعتمدة عند إدراجهم ضمن البحث ، واقتصرت فقد على إجراءات المتابعة والحماية لهذه الجريمة ، والصعوبة الثانية هو الظرف الطارئ الذي تعيشه الأمة وهو فيروس كورونا الذي أدى بي إلى الحيلولة في تحصيل أكبر عدد ممكن من المراجع كون أن جميع مكتبات الوطن و الولاية المقيم بها مغلقة وكنت قد اخترت موضوع البحث متأخرا مما اضطررت إلى الاعتماد بما لدي من مراجع .

ونظرا لأهمية هذا الموضوع ، وما تخلقه الجرائم الإلكترونية من تداعيات على المجتمع في جميع المجالات استلزم على مختلف التشريعات الدولية المسارعة لردع هذه الجرائم الخطيرة وأصبح من الواجب على الباحثين الخوض في غمار وتفاصيل طبيعة الجريمة الإلكترونية والتقصي عن

مقدمة :

مكنوناتها للمساهمة في استخلاص الضوابط الشرعية الازمة في سبيل احتواءها واستخلاصها من طرف التشريع للدفع بعجلة تطور النصوص القانونية المتعلقة بالجرائم الإلكترونية ومواكبتها مختلف التشريعات العالمية ، واعتمادا على الدراسات السابقة المتعلقة بمجال حماية ومتابعة الجرائم الإلكترونية حاولنا نحن كذلك في هذا البحث المتواضع التوصل إلى بعض الإشكالات المتعلقة بهذه الجريمة والصعوبات والمعوقات التي تواجه المشرع الجزائري خاصة والتشريع العالمي عامة معتمدين بذلك المنهج التحليلي الذي يتخلله المنهج المقارن .

.ومنه نتوصل إلى طرح الإشكالية التالية : **إلى أي مدى وفق المشرع الجزائري في ردع الجرائم الإلكترونية ؟**

ومنه قسمنا بحثنا هذا إلى فصلين : فقد تطرقنا في الفصل الأول: إجراءات الحماية القانونية في الجرائم المعلوماتية، وقد قسمناه إلى مبحثين .

بالنسبة للمبحث الأول: فتناولنا من خلاله الحماية القانونية في الجرائم المعلوماتية في ظل قانون العقوبات.

أما المبحث الثاني: فتناولنا من خلاله الحماية القانونية في الجرائم المعلوماتية ضمن القوانين الخاصة

وفي الفصل الثاني فقد تطرقنا إلى إجراءات المتابعة القانونية في مكافحة الجرائم المعلوماتية. فقد قسمناه كذلك إلى مبحثين:

المبحث الأول: إجراءات التحقيق في الجريمة الإلكترونية.

المبحث الثاني: الإجراءات القانونية في متابعة الجرائم المعلوماتية في النطاق الدولي .

خاتمة .

قائمة المصادر والمراجع.

الفصل الأول

إجراءات الوقاية القانونية

في الجرائم الإلكترونية

– المبحث الأول : الوقاية القانونية في الجرائم الإلكترونية في ظل قانون العقوبات.

نظرا لتفشي جرائم الاعتداء على المال المعلوماتي على النطاق الدولي دعت الضرورة لاتفاق الفكر[1] القانوني على استحداث قوانين خاصة لجرائم المعلوماتية وكانت الولايات المتحدة الأمريكية من الدول المسارعة لإصدار قانون خاص بالجريمة المعلوماتية حيث أصدرت قانون فيدرالي سنة 1984 متعلق بالإحتيال وإساءة إستخدام الكمبيوتر، كما أصدرت فرنسا قانون رقم 19/88 بشأن الغش المعلوماتي، والذي أدمج في قانون العقوبات الفرنسي الموافق لـــ 05 /01/ 1988 وأصبح يشكل باب جديد هو الباب الثالث من قانون العقوبات الفرنسي، ثم صدر تعديل جديد لهذا القانون 1994/03/01،وتليها بعد ذلك الكثير من الدول منها كندا وألمانيا وأستراليا.

أما فيما يخص بالمشرع الجزائري فقد استحدث نصوص خاصة في مجال الجرائم المعلوماتية وذلك[2] بموجب تعديل قانون العقوبات الذي تمم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر رقم 156/66 الصادر في 08يوليو 1966باظافة القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الالية للمعطيات من المادة 394 مكرر الى المادة 394 مكرر 7 من قانون العقوبات ، وكذا القانون رقم04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والإتصال ومكافحته.

أما على المستوى الدولي فنجد مولد أول معاهدة دولية لمواجهة جرائم الكمبيوتر وذلك في[3] سبتمبر2001 في مدينة بودابست بتوقيع 26 دولة من الإتحاد الأوروبي إضافة إلى كندا وجنوب

---

[1] مختارية بوزيدي ، (**ماهية الجريمة الإلكترونية**) ، مداخلة في ملتقى وطني بعنوان : آليات مكافحة الجرائم الإلكتؤونية في التشريع الجزائري ، جامعة الدكتور مولاي الطاهر- سعيدة ، المنعقد يوم 29 مارس 2017. الصفحة 11-12.

[2] **المرجع نفسه**، الصفحة 12.

[3] العاقل فريال ، **الجريمة المعلوماتية في ظل التشريع الجزائري** ، مذكرة لنيل شهادة الماستر ، كلية الحقوق والعلوم السياسية قسم القانون العام ، جامعة أكلي محند اولحاج – البويرة ، الصفحة 43.

إفريقيا والولايات المتحدة الأمريكية، والحقيقة أن تلك المعاهدة وإن كانت أوروبية المنشأ فهي دولية النزعة فهي مفتوحة للدول الأخرى التي تطلب الإنضمام أو الترشح للانضمام لها.

– المطلب الأول : المساس بأنظمة المعالجة الآلية للمعطيات.

يندرج مصطلح نظام المعالجة الآلية للمعطيات من ضمن المصطلحات التقنية المتطورة في مجال[1] الإعلام والإتصال وهذا ما أدّى للمشرع الجزائري بالإمتناع عن تعريفه وترك الأمر للفقه والقضاء مخالفا بذلك المشرع الفرنسي حيث عرّفت المادة الأولى من الإتفاقية الدولية لإجرام المعلوماتي النظام المعلوماتي على النحو التّالي[2] :

"يقصد بمنظومة الكمبيوتر أيّ جهاز أو مجموعة من الأجهزة المّتصلة ببعضها البعض أو ذات صلة بذلك، ويقوم إحداهما أو أكثر من واحد منها، تبعا للبرنامج بعمل معالجة آلية للبيانات ." ويقصد ب" بيانات الكمبيوتر "أيّة عملية عرض للوقائع، أو المعلومات أو المفاهيم في شكل مناسب لعمليّة المعالجة داخل منظومة الكمبيوتر، بما في ذلك البرنامج المناسب لجعل منظومة الكمبيوتر تؤدّي وظائفها."

وقد عّرفه الفقه الفرنسي على أنه : كلٌّ مركّب من وحدة أو مجموعة وحدات للمعالجة، والتي[3] تتكّون كل منها من الّذاكرة والبرامج والمعطيات واجهزة الإدخال والإخراج، وأجهزة الربّط التي تربط بين العناصر المختلفة للنظام، كالشّاشة ولوحة المفاتيح والطّابعة والبطاقات المغناطيسية التي تشكّل وسيلة للدخول، والتي تربط بينها مجموعة من العلاقات التي عن طريقها تتحّقق نتيجة معيّنة، وهي معالجة المعطيات، على أن يكون هذا المركّب خاضع لنظام الحماية الفنية ."

1 لعاقل فريال، المرجع السابق، الصفحة 27 – 28.

2 الاتفاقية الدولية حول الإجرام السيبيري التي أبرمت بتاريخ : 2001/11/08 من طرف المجلس اللأوروبي وتم وضعها للتوقيع منذ تاريخ 2001/11/23.

[3] ا لعاقل فريال، **ال**رجع السابق، الصفحة 27 – 28.

وتعتبر جميع هذه العناصر المادية والمعنوية واردة على سبيل المثال لا الحصر نظرا للتطور السريع الذي يشهده النظام المعلوماتي فإن زيادة أو نقصان أي عنصر وارد طبقا لمقتضيات التي يفرضها التطور التفني في هذا المجال وإن أي إعتداء على أحد هذه العناصر بمعزل عن غيرها لا يرتب وقوع الجريمة.

– الفرع الأول : الدخول أوالبقاء عن طريق الغش في النظام المعلوماتي :

– أولا : الظروف العادية لجريمة الدخول أوالبقاء عن طريق الغش :

أ– الركن الشرعي :حدّث المشرع الجزائري النصوص التجريمية بموجب تعديل قانون العقوبات[1] بالقانون رقم 15/04في المواد من مكرر394 إلى394 مكرر 7 تحت عنوان**" المساس بأنظمة المعالجة الآلية للمعطيات "** ثمّ بعد ذلك بقانون مكافحة جرائم تكنولوجيا الإعلام والاتصال رقم04/09 ومنه نستخلص أنّ الصور التجريمية الأصلية التي عالجها المشرع الجزائري و المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات متغيرة بتغير السلوك المرتكب و النتيجة الواقعة.

وقد نصت المادة394 مكرر من قانون العقوبات بقولها " : يعاقب بالحبس من ثلاثة أشهر إلى سنة[2] بغرامة من 50.000دج إلى100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال

---

[1] عبد الوهاب مليايي ، **أمن المعلومات في بيئة الأعمال الإلكترونية** ، رسالة لنيل شهادة الدكتوراه ، كلية الحقوق والعلوم السياسية قسم الحقوق ، جامعة أبي بكر بلقايد– تلمسان ، الصفحة 177 .

[2] المادة 394 مكرر من الأمر رقم 156/66 المؤرخ في 1966/06/08 المتضمن قانون العقوبات المعدل والمتمم . نصت على : يعاقب بالحبس من ثلاثة أشهر إلى سنة بغرامة[5] من 50.000دج إلى100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج".

المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000دج".

ب- الركن المادي لجريمة الدخول أو البقاء عن طريق الغش:

1- جريمة الدخول عن طريق الغش:

يتمثل فعل الدخول بالولوج إلى النظام المعلوماتي ضد إرادة من له سلطة امتلاكه بحيث يكون[1] دخولا معنويا مخالفا للمفهوم المادي ويكون بأي وسيلة كانت سواء بطريقة مباشرة أو غير مباشرة وترك المشرع الجزائري الباب مفتوحا نظرا للتطور السريع والمستجد لهذه الجريمة ،كما أن هذه الجريمة ليست من الجرائم التي يطلق عليها جرائم ذات صفة إذ يعتبر مجرما كل شخص دخل للنظام المعلوماتي مهما كانت صفته ومكانته أو مهنته.

ويتحقق فعل الدخول عبر صور نذكرها فيما يلي:

1/ الدخول عن طريق تشغيل حاسب آلي مغلق :

يمكن للجاني الدخول الى النظام والحاسب الآلي[2] مغلق إذ أن العبرة ليس في الحاسب الآلي بل في الشروع في الجريمة ويكون الفعل في تشغيل الحاسب الآلي يعاقب عليه القانون لأنه لا يوجد غاية في فعل التشغيل غير الإطلاع على البيانات أما فيما يخص الإطلاع على الشاشة والحاسب الآلي مشتغل بغير إرادة المطلع فقد اتفق بعض الفقهاء على أن الفعل لا يعاقب عليه القانون

2/ الدخول باستعمال حاسب آلي مفتوح:

يتمثل هذا الفعل باستغلال الجاني للحظة التي يكون فيها الحاسب الآلي مفتوح ويقوم بالدخول للمعطيات والبيانات المتعلقة بالجهاز وفي هذه الحالة يكون فعل الدخول غير مشروع ويعاقب عليه القانون.

[1] العاقل فريال، المرجع السابق، الصفحة 33.

[2] مليايي عبد الوهاب، المرجع السابق، الصفحة 180/179

3/ الدخول عن طريق الإختراق:

يتم الدخول عن طريق الإختراق إذا كان الحاسب الآلي موصولا بشبكة أنترنت ويقوم الجاني بالولوج إليه عبر وسائل تقنية متطورة تمكنه من الدخول إلى النظام عن بعد والسيطرة عليه .

4/ الدخول عن طريق خطوط الاتصالات:

يقوم هذا الفعل عن طريق العبث بخطوط الإتصال التي ترتبط بالنظام وإعطائه أوامر بغرض معيّن حيث وقعت مثل هذه الجريمة في فرنسا ممن تمكن من الدخول إلى أجهزة الهواتف الخاصة بإحدى المؤسسات واستطاع من

خلال ذلك إجراء اتصالات تليفونية على حساب تلك المؤسسة.

5/ الدخول إلى نظام الحاسب الآلي باستعمال بطاقة الغير:

يتم هذا الفعل عن طريق إستعمال الجاني لبطاقة الغير بدون إرادة من له حق السلطة عليها وإستعمالها للدخول لنظام الحاسب الآلي لأجل أغراض تخص أصحاب البطاقات .

2 _ جريمة البقاء عن طريق الغش:

أما فعل البقاء فنعني به التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له سلطة[1] السيطرة على النظام ورغم العلاقة المترابطة بين الجريمتين إلاّ أنه قد يتحقق البقاء المعاقب عليه داخل النظام في حين الدخول للنظام مشروعا وقد يجتمعان في عدم المشروعية، وقد يختلفان كذلك في مشروعية البقاء داخل النظام ويكون الدخول إليه غير مشروع وقد يجتمعان كذلك في المشروعية . إذا كانت تلك الجريمة على هذه الصورة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، فإنها تحقق أيضا وبصورة غير مباشرة حماية المعطيات أو المعلومات ذاتها.

1 .العاقل فريال، المرجع السابق، الصفحة33.

وهذا ما يحسب على المشرع الجزائري لفطنته ولسد الباب عن أي ثغرة في هذا الخصوص محاولا حماية النظام المعلوماتي بصفة عامة بغض النظر عن إتلاف أو تعديل أو محو البيانات.

ويتحقق فعل البقاء بمجرد التواجد داخل كل أو جزء من النظام دونما أن يشترط لذلك المحو أو[1] الإتلاف أو التعديل للمعلومات في النظام المعلوماتي ،ويختلف المتهم في جريمة الدخول أو البقاء عن المستعمل التعسفي هو أن المتهم ليس له الحق في الدخول أو البقاء داخل النظام ، في حين أن المستعمل المتعسف له الحق في الدخول والبقاء غير أنه يستعمل الجهاز أو النظام في غير الغرض المخصص له.

ج- الركن المعنوي لجريمة الدخول أو البقاء عن طريق الغش:

تعدّ جريمة الدخول أو البقاء من الجرائم العمدية إذ أن سوء نية الجاني مفترض إلاّ اذا وقع هذا الأخير[2] تحت الإكراه أو التهديد ... الخ ، باستغلال مهاراته التقنية في الدخول لهذه الأنظمة وهذا يكون نافيا للمسؤولية الجنائية ومن هنا يتوفر لدى الجاني القصد الجنائي العام بعنصريه العلم والإرادة بأن الفعل مناقض لإرادة صاحب النظام .

وقد اشترط المشرع الجزائري في المادة 394مكرر[3] أن يتم الدخول أو البقاء بطريقة الغش..." **كل من يدخل أو يبقى عن طريق الغش"**، ويقصد به سوء نية الجاني حيث يعلم بأن دخول النظام أو البقاء فيه ليس من حقه ويقوم بالدخول للنظام المعلوماتي ، ونستنتج سوء نية الجاني من خلال العمليات والتصرفات التي قام بها داخل النظام ، ومع ذلك فإن الغش لا يظهر فقط من خلال عمليات اختراق نظام الحماية وإنما أيضا من خلال الدخول أو البقاء دون وجه حق، وما نظام الحماية إلا وسيلة لإثبات سوء النية أو الغش، وانتفاء نظام الحماية من الجهاز لا ينفي الجريمة، أما

[1] مليايي عبد الوهاب، المرجع السابق، الصفحة 186 .

[2] مليايي عبد الوهاب، المرجع السابق، الصفحة 184 /185.

[3] المادة 394 مكرر ، قانون العقوبات ، مرجع سابق .

بالنسبة للدخول بالصدفة او عن طريق السهو او الخطأ فالفقه اشترط على الشخص في هذه الحالة إلا أن يخرج متى إكتشف أنه دخل دون وجه حق ، فإن بقى و لم يخرج يتوافر في حقه القصد الجنائي ، كما لا يتوفر القصد الجنائي إذا كان دخول الجاني أو بقاؤه مسموح به أصلا أو وقع الجاني في خطأ بشأن حقه في الدخول أو البقاء سواء من حيث النطاق أو الزمان إلا أذا تعسف في الدخول ونكون هنا أمام جريمة أخرى .

والإشكالية المثارة في هذا الخصوص برأيي الشخصي هي المدّة الزمنية التي يجب فيها على الجاني الخروج فيها من النظام إذا توفرت لديه صفة السهو أو الصدفة أو الخطأ.

ولا يشترط أن يتوّقع الضرر الذي سوف يلحق النِّظام أو صاحبه من هذا الدخول، فإذا توّقع[1] الفاعل أّنه بصدد الدخول إلى نظام معين ، ثم ترّتب على فعله الدخول إلى نظام آخر، فإنّ القصد الجنائي يظلُّ متوافراً لديه.

– ثانيا: الظروف المشددة لجريمة الدخول والبقاء عن طريق الغش.

تتمثل الظروف المشددة في النتيجة المادية للفعل الغير مشروع والتي هي وفق ما ندرسه بالأثر الذي[2] يتركه الجاني بعد فعل الدخول ومنه يكون الأثر الناتج عن هذا الفعل هو العلاقة السببية بين الفعل والنتيجة وتتجلى صوره في المحو أو تغيير ويترتب عنهما تخريب نظام إشتغال المنظومة ونستنتج بأن إقتران ظرف التشديد بالجريمة يستوجب العلاقة السببية بين الظرفين وفعل الدخول والبقاء وتقرّر العقوبة على الجاني حتى و لم يهدف إلى توقيع الضرر داخل النظام المعلوماتي.

وهذا ما نصت عليه المادة 394 مكرر[3] فقرة 2+3 من قانون العقوبات على أن " **تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة.**

---

1 العاقل فريال، المرجع السابق، الصفحة34.

[2] المرجع نفسه، الصفحة 34 .

[3] المادة 394 مكرر الفقرة الثانية والثالثة تنص على : أن " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة.

وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150000 دج".

وقد ربط المشرع الجزائري بين فعل الحذف و التغيير وبين فعل التخريب لإمتدادهم من فعل البقاء[1] والدخول مخالفا بذلك المشرع الفرنسي الذي أوردهما في نصين الأول كظرف تشديد والآخر كإعاقة سير النظام المعلوماتي وسنحاول شرح ظرف الشديد في نوع من التفصيل وفق ما نصّ عليه المشرع الجزائري .

أ- الحذف:

يقصد المشرع بالحذف هو نقص في معطيات النظام ولا يشترط أن ينصب الحذف على جميع[2] المعطيات المتعلقة بنظام المعالجة وإنما يكفي حذف جزئي لها، و التساؤل المطروح هنا حول هل يشترط أن يؤدي الحذف إلى تعطيل النظام ؟ وبالرجوع إلى نص المادة المذكور سلفا نجد أن المشرع لم يشترط أن ينتج عن هذا الحذف تعطيل أو ضرر للنظام وبالتالي فمجرد وقوع حذف في معطيات المنظومة كافية لتشديد العقوبة.

ب- **التغيير:**

يختلف التغيير عن الحذف في استبدال معطيات مكان أخرى بحيث يبقى النظام في هذه الحالة[3] سليما لكن بوجود معطيات مغايرة، و لا يشترط تعطيل النظام أو فساده إذ هناك جانب يرى بأن تجريمة فعل الدخول والبقاء هو تجريم إحترازي وما يحدثه بعده من محو أو تغيير فلا يهم ولا يجدر

وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000دج إلى 150000 دج".

[1] مليايي عبد الوهاب، المرجع السابق، ص 186.

[2] مليايي عبد الوهاب، المرجع السابق ، الصفحة 187

[3] المرجع نفسه، الصفحة 187

بالمشرع تشديد هذه الجريمة والجانب الآخر يرى بأن ظرف التشديد لجريمة الدخول و البقاء يتطلب المحو أو التغيير في نظام المعلومات.

– المطلب الثاني: جريمة التلاعب و التعامل غير الشرعي بمعطيات النظام الالكتروني

– الفرع الأول : جريمة التلاعب بالمعطيات داخل النظام المعلوماتي.

أولا :الركن الشرعي :نصت عليها المواد **08،04،03** ، من الإتفاقية الدولية للإجرام المعلوماتي[1] كما نص عليها المشرع الجزائري في المادة **394**[2] **مكرر 1** و **394**[3] **مكرر 2** من قانون العقوبات فجرم في المادة الأولى الاعتداءات العمدية على المعطيات الموجودة داخل النظام المعلوماتي، وجرم في المادة الثانية المساس العمدي بالمعطيات الموجودة خارج النظام، باستقراء المادة **394مكرر 1+2** نجد أن لهذه الجريمة صورتين تتمثل الأولى في التلاعب بالمعطيات داخل النظام أو بالاعتداءات العمدية على المعطيات الموجودة داخل النظام أما الصورة الثانية تتمثل في المساس العمدي بالمعطيات خارج النظام أو التعامل غير الشرعي بالمعطيات ، نجد **الاعتداءات العمدية على المعطيات الموجودة داخل النظام** تتجسد في إحدى الأفعال الثلاثة :**الإدخال** ويقصد بها : **الإدخال، التعديل، المحو.**

---

[1] العاقل فريال، المرجع السابق، الصفحة 36/35

[2] **تنص المادة 394 مكرر1 من قانون العقوبات:** "أنه يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات، و بغرامة من 500.000دج إلى 2.000.000دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

[3] **تنص المادة 394 مكرر 2 من قانون العقوبات:"** يعاقب بالحبس والغرامة كل من يقوم عمدا وعن طريق الغش بما يأتي:

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

– حيازة أو إفشاء أو نشر أو إستعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم".

ثانيا: الركن المادي لجريمة التلاعب بالمعطيات داخل النظام المعلوماتي.

1- الإدخال:

يتم فعل الإدخال من قبل الجاني عن طريق إضافة معلومات لم تكن تتضمنها الدعامة المدخل[1] إليها من قبل بأي غرض كان ولا يتطلب وقوع الضرر أو النتيجة المراد الوصول إليها من قبل الجاني حيث يعاقب المشرع كل من أدخل معطيات في النظام المعلوماتي، فبمجرد إدخال المعلومات تكون الجريمة قد قامت و إنتهت حتى ولو كانت هاته المعلومات الدخيلة خالية من الغلط، فالعبرة من التجريم هو التعدي على المعطيات مخالفة لرغبة من له حق السيطرة في إمتلاكها.

ويتم عادة إستخدام البرامج الخبيثة في جريمة الإدخال بغرض التعديل في البيانات بحيث يؤثر على[2] صحتها أو نسبتها أو قيمتها بحيث يؤثر على المعلومات الأصلية داخل النظام المعلوماتي وذلك بالمساس بسلامتها و قيمتها الحقيقة ، وعملية الإدخال من الأفعال السهلة التي يقوم بها الجاني و بالتالي يكن من السهل تغذية النظام بمعلومات مغلوطة أو زائفة لم تكن موجودة في الدعامة من قبل.

ومن خصائص فعل الإدخال من باب المثال أنه يقع في غالب الأحيان بمعرفة المسؤول عن قسم المعلومات المسند إليه وظائف المحاسباتية و ذلك بالتلاعب غير المشروع بالمعلومات ومن الصور التي يمكن للمسؤول القيام بعملية الإدخال نجد إدخال أسماء وهمية في كشوف المرتبات وذلك لغاية صرف مرتبات لموظفين وهميين ، كذلك التلاعب في معلومات التعاملات المالية كإدخال فواتير وهمية تحت اسم أحد الموردين.

[1] العاقل فريال، المرجع السابق، الصفحة الصفحة 36

[2] مليايي عبد الوهاب، المرجع السابق، الصفحة 193/192

2- الإزالة:

يتمثل قيام هذا الفعل في التلاعب بالمعطيات داخل النظام المعلوماتي إمّا في إزالة بعض المعلومات[1] داخل الدعامة أو تحطيم تلك الدعامة بالكامل أو النقل والتخزين في منطقة خاصة .

و على إثر ذلك تكون الإزالة عملية لاحقة عن عملية الإدخال للمعلومات المغلوطة ، فالمسؤول عن[2] الحفظ يمكنه تدمير أو إتلاف المعلومات المكلف بحفظها داخل النظام.

وهو السلوك الثاني المنصوص عليه في المادة 394 مكرر 1[3] من قانون العقوبات ويقصد بالإزالة المحو الجزئي أو الكلي للمعلومات المتواجدة داخل النظام أو النقل و التخزين لها في منطقة خاصة.

3- التعديل:

يقصد بفعل التعديل تبديل المعطيات مكان معطيات أخرى داخل الدعامة وغالبا ما يتم[4] الإعتماد على برامج خاصة تتكلف بعملية التعديل مثل برنامج الممحاة وبرامج الفيروسات الأخرى التي تقوم بالإزالة الكلية أو الجزئية للمعلومات .

و لم يقم المشرع الجزائري باشتراط وقوع هذه الصور للتجريم دفعة واحدة فبمجرد تحقق صورة واحدة لهذه الأفعال تتحق الجريمة، وفعل النسخ والتقريب ونقل المعطيات لا تعتبر ضمن قائمة جرائم الإدخال والتعديل رغم أنها من الجرائم الإعتداء على نظم المعلومات وإستخدام الجاني هذا السلوك في جريمة التلاعب بالمعلومات نجده بكثرة في جرائم الإحتيال المعلوماتي، كما أنه يدخل في إطاره[5] كذلك التلاعب في البرنامج بإمداده بمعلومات مغايرة تؤدي لنتائج غير تلك التي صمم لأجلها.

---

[1] العاقل فريال، المرجع السابق، الصفحة 36.

[2] مليايي عبد الوهاب، مرجع سابق، الصفحة 194 .

[3] المادة 394 مكرر1 ، قانون العقوبات ، مرجع سابق.

[4] العاقل فريال، المرجع السابق، الصفحة 37/36

[5] مليايي عبد الوهاب، المرجع السابق، الصفحة 195.

ثالثا: الركن المعنوي لجريمة التلاعب بالمعطيات داخل النظام المعلوماتي.

تعتبر جريمة التلاعب بالمعطيات داخل النظم من الجرائم العمدية التي تستوجب القصد العام العلم[1] والإرادة بحيث أن نية الجاني أثناء قيامه بالفعل المجرم تكون موجهة لإلحاق الضرر وتوقيعه على من له حق السلطة على المعطيات.

وهذا ما جعل المشرع يستعمل في صياغته للمادة (عن طريق الغش) ، لأن هذه الجريمة قد تتم بعلم أو رضى صاحبها أو تقع عن طريق الخطأ ، وعليه يجب في هذه الجريمة أن تتوجه إرادة الجاني إلى فعل الإدخال أو الإزالة أو التعديل ثم يعلم أن نشاطه غير مشروع لذلك لا يسأل عنها بل يسأل طبقا للمادة 394 مكرر[2]2 والمادة 394 مكرر3[3] ، وهذا ما يميّز جريمة التلاعب بالمعطيات عن جريمة[4] المحو والتغيير التي تعتبر كظرف تشديد للجريمة الأصلية والتي هي جريمة الدخول والبقاء التي تعدّ من الجرائم الغير عمدية بحيث يسأل الجاني حتى ولو إرتكبها عن طريق الخطأ، ولا يشترط لقيام هذه الجريمة في التشريع الجزائري القصد الجنائي الخاص مخالفا المشرع الفرنسي لذلك بعض التشريعات العربية إستوجبت تواجده كركن معنوي لهذه الجريمة .

– الفرع الثاني : التعامل غير شرعي بمعطيات النظام المعلوماتي:

نصت المادة 394 مكرر2 من قانون العقوبات على حماية المعطيات بشكل عام وشمولي من[5] الإعتداءات أو التلاعبات الواقعة عليها ولم يخصّ المشرع المعطيات المتواجدة داخل النظام فحسب بل شمل أيضا التلاعبات التي تلحق بالمعطيات المتواجدة خارج النظام المعلوماتي .

---

[1] المرجع نفسه، الصفحة 196/195.

2 394 مكرر2 ، قانون العقوبات ، مرجع سابق.

3 تنص المادة 394 مكرر 3 من قانون العقوبات: تضاعف العقوبات المنصوص عليها في هذا القسم إذا إستهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد.

[4] العاقل فريال، المرجع السابق، الصفحة 41 .

[5] مليايي عبد الوهاب، المرجع السابق، الصفحة 196.

وتتمثل هذه المعطيات في أشكال عدّة حدّدها المشرع في نص المادة المذكورة أعلاه في فقرتها[1] الأولى كمحل للجريمة:

المعطيات المخزنة أو المعالجة أو مراسلة عن طريق منظومة معلوماتية ، و في الفقرة الثانية الأفعال التي تقع على المعطيات والتي قد يكون الهدف منها المنافسة غير المشروعة، الجوسسة، الإرهاب، أو التحريض على الفسق... الخ.

وسنعرض في دراستنا هذه الأفعال في نوع من التفصيل .

أولا: الركن المادي لجريمة التعامل غير الشرعي في معطيات النظام المعلوماتي.

ينقسم الركن المادي لجريمة التعامل غير الشرعي في معطيات النظام المعلوماتي إلى قسمين وفق ما نصّ عليه المشرع الجزائري في نص المادّة 394 مكرر2 فقرة الأولى والثانية[2] .

حيث ورد في الفقرة الأولى من المادة محل الدراسة على المعطيات الخارجة عن النظام المعلوماتي محل الجريمة والتي سنعنونها ب: **التعامل في معطيات صالحة لارتكاب جريمة ماسة بنظام المعلومات،** أما في الفقرة الثانية فقد نصّ المشرع على الأفعال الواقعة على المعطيات خارج النظام والمعنونة وفق دراستنا ب: **التعامل في معطيات متحصلة من جريمة ماسة بنظام المعلومات.**

أ – التعامل في معطيات صالحة لارتكاب جريمة ماسة بنظام المعلومات:

– التصميم:

يتميز الأشخاص المرتكبين لهذا الفعل بمهارات فنية وتقنية عالية في مجال نظم الحاسب الآلي ونظم[3] المعلوماتية وهذا ما جعل هذه الجريمة تتميز عن باقي الجرائم الأخرى العادية ، ممّا صعب هذا الأمر على القضاء من ناحية الإجراءات المتبعة ضد هذه الجرائم .

[1] العاقل فريال، المرجع السابق، الصفحة 37.

[2] 394 مكرر الفقرة الأولى والثانية ، قانون العقوبات ، مرجع سابق.

[3] مليابي عبد الوهاب، المرجع السابق، الصفحة197-201

ويتمثل فعل التصميم في إنتقاء معلومات التي توجه في إرتكاب الجريمة ، ومن ذلك تصميم برامج لأهداف تخريبية أو فيروسات لضرب المنظومة المعلوماتية .

2- البحث:

لم تحدد **المادة 394 مكرر 2**[1] عنصر البحث وسبب دراستنا له هو دوره الكبير في عملية إنتقاء المعلومات المراد توجيها لعملية إرتكاب الجريمة ، ونقصد بالبحث هنا هو البحث في المعلومات التي تمكن من إرتكاب الجريمة وعادة ما يتوجه الجاني في عملية بحثه للمعلومات إلى الوصول لمحركات البحث في الشبكة العنكبوتية (الإنترنت) لما تحمله من كم هائل وغزارة في المعلومات وهذا يجعلها لقمة سائغة من طرف الجاني لما لها من سهول في الوصول للمعلومة ومن محركات البحث نجد **Google**و **Yahoo** فالباحث لديه هدف محدد من خلال بحثه وبالتالي فمحرك البحث يساعده لبلوغ هدفه المنشود في عملية التصميم لهذه المعلومات ومنه نعتبر عملية البحث هو إمتداد لعملية التصميم المشار إليها في العنصر السابق.

3- التجميع:

لقد إختلفت التشريعات في مصطلح التجميع ومن بينهم المشرع الفرنسي الذي إصطلح عليها بالحيازة وكذلك الإتفاقية الخاصة بالإجرام المعلوماتي التي إصطلحت عليها بالحصول من أجل الإستخدام ، ونجد أن المشرع الجزائي قد وفقّ في صياغته لمصطلح التجميع لأن تجميع المعلومات يتطلب فيه الحيازة أما الحيازة فلا تتطلب فيه الوفرة أو التجميع وكذلك الحصول لا يتطلب التجميع .

والمقصود بالتجميع هو عملية الحصول على معلومات متنوعة وجمعها لأجل القيام بالجريمة في النظام المعلوماتي ولا تشترط وجود النية لدلى الجاني لقيام بالجريمة فبمجرد توفرها لديه تقوم الجريمة وفقا لنص المادة 394 مكرر2.

[1] 394 مكرر2 ، قانون العقوبات، مرجع سابق.

– التوفير:

يكمن وجه الشّبه بين الجريمة السابقة التي هي التجميع مع جريمة التوفير كون أنّ الأولى يكون المستفيد من المعلومات هو صاحب المعلومة نفسه ، أمّا التوفير فهو إتاحة المعلومة المتحصّل عليها لأشخاص آخرين لإرتكاب جرائم داخل النظام المعلوماتي والقيام بعملية تسهيل للغير للقيام بجرائمهم ممّا يجعل جريمة التوفير أكثر خطورة من الجريمة الأولى.

قد إختلف المشرع الفرنسي عن المشرع الجزائري باستعماله مصطلح الوضع تحت التصرف والذي يشير إلى عرض المعلومات وإتاحتها للغير بينما في الإتفاقية الدولية للجريمة المعلوماتية إصطلاحات عليه بأشكال أخرى للوضع تحت التصرف، ويتمثل هذا الفعل في توفير كلمة المرور أو الأكواد أو الشيفرة أو البيانات التي تسمح بالولوج داخل أو جزء من النظام .

5– النشر:

يتمثل هذا الفعل في إذاعة المعلومات للغير مهما كان نوعها أو طبيعتها وبأي نشاط كان لتصل أكبر عدد ممكن من الأشخاص وإتساع دائرة المعلومة ، وبهذا تكمن خطورة الفعل المرتكب لزيادة إحتمالية إنتهاز هاته المعلومات وإستعمالها في الأمور الغير المشروعة وبهذا يكون المشرع الجزائري قد أحسن في تجريمه لهذا الفعل الذي لم يجرمه المشرع الفرنسي .

6– الإتجار:

نصت المادّة 394 مكرر[1]2 كذلك على جريمة الإتجار بالمعلومات لما لها من خطورة على أمن المعلومات حيث تمتد جريمة التوفير إلى جريمة الإتجار كون أن الأولى تقع بدون مقابل أما جريمة الإتجار تشترط مقابل للمعلومات المتحصل عليها ، ويشمل فعل الإتجار كافة التصرفات سواءا كانت عينية أو نقدية ، و نجد أن المشرع الفرنسي استعمل مصطلحا آخر و هو الإستيراد ، ويعتبر تقديم المعلومات سلوكا مجرما سواء كان بمقابل او بدونه، في حين إتفاقية الاجرام المعلوماتي

[1] 394 مكرر2 ، قانون العقوبات ،المرجع سابق.

تضمن البيع و الإستيراد ، بينما الإتجار يتصور وقوعه بالبيع و الإستيراد و الشراء لهذا وهذا ما يحسب على المشرع الجزائري لتوسيعه نطاق العقاب وردع المجرم من الإفلات ساعيا بذلك في الوقاية المسبقة او القبلية للحد من هذه الجرائم وتوقيع العقاب.

ب –التعامل في معطيات متحصلة من جريمة ماسة بنظام المعلومات:

وهي الصور الثانية لجريمة التعامل غير الشرعي في معطيات النظام المعلوماتي ، الواردة في نص المادة 394 مكرر[1] 2 الفقرة الثانية منها ، وتتم هذه الجريمة عن طريق الحيازة ، الإفشاء ، النشر الإستعمال ، و تلك السلوكات تعتبر فريدة من حيث النص لأن المشرع الفرنسي و حتى اتفاقية الإجرام المعلوماتي لم ينصا عليها وسنحاول شرحها وفق ما يلي:

1– الحيازة:

تعتبر الحيازة هي وضع اليد على الشيء بنية تملكه والإنتفاع به ويمّكن فعل الحيازة على الحائز للمعلومات بإتلافها أو تعديلها أو الإنتفاع بها أو إستعمالها أو توجيهها ، كما أنها قد تكون سيطرة محدودة تمكنه فقط من الانتفاع بالمعلومات او استغلالها في نشاط معين.

2– الإفشاء:

يمتدّ فعل الحيازة إلى نشر المعلومات إلى الغير بحث تنتقل المعلومة من شخص إلى آخر وبذلك يقوما الجاني بتوسيع نطاق الجريمة إلى أشخاص آخرين ولا يهم أن يكون هؤلاء الأشخاص ذو صفة معينة ، وتعّد هذه الجريمة أكثر خطورة من سابقتها وذلك لإمتدادها لعلم أطراف أخرى..

[1] 394 مكرر2 ، قانون العقوبات ، المرجع السابق.

3- النشر:

لم تحدد المادة 394 مكرر2 للصور التي يمثلها فعل النشر ، وعليه تقع هذه الجريمة بأي وسيلة تسمح بأطراف أخرى للإطلاع عليها سواءا عن طريق الأقراص المضغوطة أو عن طريق الكتابة أو بوسائل تقنية حديثة خاصة مع التطور في مجال التكنولوجيا التي تسهل بنشر المعلومات بشكل رهيب

4- الإستعمال:

لم يحصر المشرع الجزائري نشاط معين ومخصص يقوم فيه الجاني بإستعمال المعلومات وهذا ما يحسب على المشرع الجزائري لغلقه الفراغ القانوني الذي قد يمّكن الجاني من الإفلات من العقاب لصعوبة حصر الإستعمالات التي تمكن الجاني القيام بها مهما كان الهدف منها ، و مهما كان نوع الإستعمال ، وبأية وسيلة كان ذلك الإستعمال ، و لو لمرة واحدة فقط.

ثانيا : الركن المعنوي لجريمة التعامل غير الشرعي في معطيات النظام المعلوماتي.

لقد إختلف المشرع مع الإتفاقية الدولية للجرائم المعلوماتية بخصوص القصد الجنائي ، حيث[1] إكتفى المشرع الجزائري بتوفر القصد الجنائي العام فقد بنوعيه العام والخاص وأن يعلم الجاني بأنه يقوم بإرتكاب جريمة تتعلق بالمساس بمعطيات النظام المعلوماتي وما يقوم به يعاقب عليه القانون ، وإثبات ذلك هو إستعماله لمصطلح لأي غرض كان وإعتماده على مصطلح الغش ما هو إلاّ تأكيدا منه للعمد وليس للقصد الخاص لدى الجاني ، أما في ما يخص بالإتفاقية المتعلقة بجرائم المعلومات فقد إشترطت على الجاني توفر القصد الجنائي الخاص لديه ألا وهي النية في إرتكاب هذه الجرائم الماسة بالمعطيات .

[1] مليايي عبد الوهاب، المرجع السابق، الصفحة 202/201

– المبحث الثاني : الحماية القانونية في الجرائم المعلوماتية ضمن القوانين الخاصة

بعد دراستنا للطبيعة القانونية للجرائم المعلوماتية من حيث قانون العقوبات سنتطرق الآن إلى الحماية القانونية للجرائم المعلوماتية ضمن القوانين الخاصة ونحاول توضيح أهم النقاط التي عالجها المشرع خاصة في ما يتعلق بالجانب الردعي لهذه الجريمة ومنه قسمنا هذا المبحث إلى مطلبين إثنين ، تطرقنا في المطلب الأول إلى الحماية الحماية القانونية للجرائم المعلوماتية في ظل قوانين الحماية الفكرية والصناعية وحماية المعطيات ذات الطابع الشخصي ، وفي المطلب الثاني إلى الحماية القانونية للجرائم المعلوماتية في ظل قوانين الإعلام والإتصال والتجارة والتوقيع الإلكترونيين.

– المطلب الأول: الحماية القانونية للجرائم الإلكترونية في ظل قوانين الحماية الفكرية والصناعية وحماية المعطيات ذات الطابع الشخصي .

– الفرع الأول: الحماية القانونية لبرامج الحاسوب من خلال نصوص قانون الملكية الفكرية.

سنتطرق في دراستنا في هذا المبحث إلى الحماية القانونية للجرائم المعلوماتية في ظل القوانين الخاصة وهو القانون 05/03[1] المتعلق بحق المؤلف .

ويعتبر الإعتداء على الحقوق الفكرية لبرامج الحاسوب هو إعتداء على الحقوق المالية و على[2] الحقوق الأدبية وتتميز حماية هذه الحقوق عن نظيراتها كونها تستوجب الحماية لبرامج الحاسوب وفقط كما تتمثل هذه الإعتداءات في التملك غير المشروع لهذه البرامج .

وتظهر العلاقة بين حماية المعلوماتية عن طريق قوانين حقوق المؤلف ، في كون النظام المعلوماتي ما[3] هو إلا ابتكار جديد لأحد تطبيقات برامج الحاسب الآلي ومعطياته وبياناته واعتباره من قبيل المصنفات الفكرية .

---

[1] أمر رقم 05/03 المؤرخ في 19/ 2003/07 المتعلق بحقوق المؤلف والحقوق المجاورة ، الجريدة الرسمية عدد 44.بتاريخ 2003/07/23.

[2] أمير فرج يوسف ، **الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر و الإنترنت** ، مكتبة الوفاء القانونية ، الطبعة الأولى ، مصر، 2011، الصفحة 96 .

[3] مليايي عبد الوهاب، المرجع السابق، الصفحة 105 .

ومن حق كل مؤلف إستعمال حقه في إبتكاره مهما كان نوعه أو الهدف منه من خلال ملكيته له[1] بصفة مستقلة ولا يجوز لأي شخص إستغلال هذا الحق مخالفا لرغبة من له حق السلطة عليه بإلزام الغير بإحترام حقه ولهذا إتجه المشرع الجزائري لإصدار نصوص تكفل الحماية لهذا الحق ، ومن بين هاته الحقوق الملزمة بالحماية نجد برامج الحاسوب والتي هي محل دراستنا لما لها من طبيعة فكرية وتقنية في ذات الوقت ، وهذا ما أدّى بالمشرع الجزائري لإعتماده لقانون حقوق المؤلف في حمايته لبرامج الحاسوب.

وقد أدرج المشرع الجزائري الإعلام الآلي من ضمن المصنفات المحمية وذلك بالأمر 10/97 المؤرخ في 1997/03/06[2] المتعلق بحق المؤلف والحقوق المجاورة في نص المادة الرابعة منه.

وقد صدرت عدّة إتفاقيات على المستوى الدولي لحماية حقوق المؤلف والتي فرظتها الظروف الملحّة[3] لردع الإنتهاكات الواردة عليهم لحقهم في الملكية الفكرية ومن أهمها إتفاقية برن لسنة 1979 التي تطرقت إلى الجانب الجزائي وتركت الأفعال الواقعة على حقوق المؤلف للتشريعات الداخلية ، وكذلك إتفاقية تريبس لحقوق المؤلف ، وسايرها المشرع الجزائري بعد ذلك في إصداره لقوانين حقوق المؤلف من أحدثها الأمر 05/03الموافق ل 19 يوليو / 2003[4] ، ومن أهم المصنفات المعنية بالحماية نجد برامج الحاسوب وذلك بنصه في المادة الرابعة منه على إعتبارها كمصنفات ملزمة بالحماية .

---

[1] المرجع نفسه، الصفحة 108.

[2] نص المادة 04 من الأمر 10/97 من الأمر المتعلق بحق المؤلف والحقوق المجاورة المؤرخ في 1997/03/06 على أنه ":
تعتبر على الخصوص كمؤلفات فيه أو فنية محمية ما يأتي ، المصنفات الأدبية المكتوبة مثل المحاولات الأدبية والبحوث العلمية التقنية والروايات والقصص والقصائد الشعرية
ومصنفات و قواعد بيانات. "

[3] العاقل فريال، المرجع السابق، الصفحة 49- 51.

[4] أمر رقم 05/03 ، المتعلق بحقوق المؤلف والحقوق المجاورة ، المرجع السابق.

ونظرا لهاذه لإنتهاكات الخطيرة على حقوق المؤلف سعت العديد من الدول على حتمية إصدار[1] نصوص جزائية ردعية بما تفرضه المقتضيات العامة وذلك لنقص فاعلية النصوص المدنية ونجاعتها على مثل هذه الإعتداءات، وهذا ما سار عليه المشرع الجزائري من خلال الأمر رقم 05/03 من الماد 151إلى 159 بنصّه على جرائم وعقوبات حقوق المؤلف .

وسنحاول من خلال دراستنا تحديد هاته الجرائم الواقعة على البرامج المعلوماتية من ثمّ نتطرق إلى الجزاءات الواردة عليها .

♣ جريمة التقليد :

عرّف الفقهاء جريمة التقليد على أنها : إعتداء مباشر أو غير مباشر على حقوق المؤلف الأدبية أو[2] المالية المحمية لقانون حق المؤلف، أما فيما يخص بالتشريعات الوطنية فلم يقم المشرع بتحديد تعريف خاص بجرائم التقليد واكتفى بتبيّان الأفعال المتمثل لهذه الجريمة فقط.

ولقد نص المشرع الجزائري في المادة 151 من الأمر05/03[3] على أنه يعد مرتكب لجنحة التقليد كل من يقوم بالكشف غير المشروع للمصنف أو يمس بسلامته، أو يقوم باستنساخ مصنف أو يقوم باستيراد أو تصدير أو نسخ مقلدة من مصنف أو يقوم بتأجير أو وضع رهن التداول لنسخ مقلدة لمصنف، أما المادة 154[4] منه فقد نصت على أنه يعد مرتكب لجنحة التقليد كل من يشارك بعمله أو بالوسائل التي يحوزها للمساس بحقوق المؤلف، ونصت المادة 155[5] منه على أنه يعد مرتكب لجنحة التقليد كل من يرفض عمدا دفع المكافئة المستحقة للمؤلف.

[1] العاقل فريال، المرجع السابق، الصفحة 50.

[2] العاقل فريال، المرجع السابق، الصفحة 51.

3 المادة 151 من أمر رقم 05/03 ، المتعلق بحقوق المؤلف والحقوق المجاورة ، المرجع السابق.

4 المادة 154 من أمر رقم 05/03 ، المتعلق بحقوق المؤلف والحقوق المجاورة ، المرجع السابق.

5 المادة 155 من أمر رقم 05/03 ، المتعلق بحقوق المؤلف والحقوق المجاورة ، المرجع السابق.

وما يعاب على هذه المواد أنها شملت أفعال لا ينطبق عليها وصف التقليد بل هي من الجرائم اللاحقة لجريمة التقليد .

– أولا : الجزاءات المقررة لجرائم الاعتداء على برامج الحاسوب.

تصنّف جرائم الإعتداء على برامج الكمبيوتر على أنها جنحة ، لهذا لا يجرّم من قام بالشروع في[1] هذه الجريمة نظرا لعدم وجود نص خاص وكما تعلمون أن عملية الشروع بالنسبة للجنح لا تجرّم إلاّ بنص خاص .

وقد نص المشرع الجزائري في المواد :159/158/157/156/153 من الأمر 05/03[2]المتعلق بحقوق المؤلف والحقوق المجاورة الجزاءات الرادعة والواقعة على حقوق المؤلف ، وسنتطرق إلى توضيح هذه العقوبات من ذكر العقوبات الأصلية والتكميلية لهذه الجريمة .

1– العقوبات الأصلية.

حدد المشرع الجزائري في المادة 153 من الأمر05/03 عقوبة تتمثل في الحبس من 3أشهر إلى[3]3 سنوات وغرامة من 500.000 دج الى 1.000.000 دج سواء كان النشر قد حصل في الجزائر أو خارجها.وقال عصام الكردي الخبير القانوني في مجال حماية الملكية الفكرية إن القانون لا يجب أن يتضمن الحد الأقصى وأن يتم تحديد حد أدنى للغرامة ويترك للقاضي تحديد الحد الأقصى للغرامة.

أما في حالة العود فقد قرر المشرع الجزائري في نص المادة 156 من الأمر 05/03 على تشديد العقوبة إذا ما قام الجاني بإعادة إرتكابه للجرائم المذكورة في المواد 155/154/151 من هذا الأمر.

1 العاقل فريال، المرجع السابق، الصفحة51.

[2] المواد 159/158/157/156/153 من أمر رقم 05/03 ، المتعلق بحقوق المؤلف والحقوق المجاورة ، المرجع السابق.

[3] العاقل فريال، المرجع السابق، الصفحة 52- 54.

2- العقوبات التكميلية.

نصت المواد 159/158/157/ على العقوبات التكميلية لهذه الجرائم والتي تتمثل في المصادرة ونشر الحكم أما في ما يخص بالمصادرة فقد نصّت عليها المادة 157 من الأمر 05/03 التي نصت على انه تقرر الجهة المصادرة القضائية المختصة مصادرة المبالغ التي تساوي مبلغ الإيرادات أو أقساط الإيرادات الناتجة عن الاستغلال غير الشرعي للمصنف ومصادرة العتاد المخصص لمباشرة النشاط أو المشروع والنسخ.

العتاد أو النسخ المقلدة أو قيمة ذلك كله وكذلك الإيرادات موضوع المصادرة للمؤلف أو لأي مالك حقوق أخرى أو ذي حقوقهما لتكون عند الحاجة بمثابة تعويض عن الضرر اللاحق بهم ، ولم يلزم المشرع الجزائري على الجهات المختصة المصادرة بل جعلها جوازية وليست في جميع الأحوال.

وفي نص المادة 158 من الأمر 05/03 نص المشرع على العقوبة التكميلية الثانية وهي نشر الحكم والتي تقضي أنه يمكن للجهة القاضية المختصة بطلب من الطرف المدني، أن تأمر بنشر أحكام الإدانة كاملة أو مجزئة في الصحف التي تعينها وتعليق هذه الأحكام في الأماكن التي تحددها ومن ضمن ذلك على باب المسكن الخاص بالمحكوم عليه وكل مؤسسة أو قاعة حفلات يملكها على أن يكون ذلك على نفقة هذا الأخير شريطة أن لا تتعدى هذه المصاريف الغرامة المحكوم بها.

وهذا للتشهير بالمجرم والمساس بشخصيته وهي عقوبة معنوية ماسة بشرفه .

وفي الأخير تجد الإشارة إلى ظرورة الجدّة والإبتكار لبرامج الحاسوب من طرف المؤلف وعلى تحقق إحدى النماذج من هاته الجرائم المذكورة أعلاه لكي تتوفر شروط حماية حق المؤلف وإذا تخلف أحد هذه الجرائم أو إنتفى عنصر الإبتكار لبرامج الحاسوب فسيفقد البرنامج حقّه في حمايته كمصنف محمي قانونا وبذلك لا يترتب وقوع الجريمة .

3- مدى نجاعة الجزاءات لحماية البرامج الحاسوب.

رغم كل الجزاءات التي كرّسها المشرع الجزائري لردع الجرائم الواقعة على برامج الحاسوب إلاّ انّه لم[1] يسلم من النقد، إذ كان للفقه رأي آخر حول مدى ملاءمة أو نجاعة هذه النصوص بخصوص جرائم الحاسوب ، إذ أنّ الطبيعة الخاصة للمؤلف تختلف حول طبيعة النظام المعلوماتي وكل في فلكه ، وهذا ما يخلق إشكال عند المشرع الجزائري من ناحية ضبط العقوبة الملائمة ووضع أسس للتفرق بينهما ، هذا من جهة ومن جهة أخرى فإن الإعتداءات الواقعة على حق المؤلف لا تتماثل مع الإعتداءات الواقعة على النظام المعلوماتي من ناحية الخسائر المترتبة عليهما بحيث أن الأولى أقل بكثير من حيث الأضرار الناجمة عليه مقارنة بالنظام المعلوماتي.

وتجدر الإشارة أن الحماية التي وضعها المشرع الجزائري في الأمر05/03[2] لم تصنّف برامج الحاسب أو البرامج المعلوماتية على أنها مصنفات إلّا من ناحية الإعتداءات الواقعة على حق المؤلف دون الإعتداءات الأخرى ، إذ أنّ الخوارزميات لم يصنّفها قانون حق المؤلف على أنها من المصنفات لافتراضه على أنهاّ ملكية عامة تستعمل في الوسائل المعلوماتية من دون أي ترخيص من مؤلفها ، ولكن في رأيي الشخصي والمتواضع أعتقد أن ترخيص صاحب الحق لهذه الخوارزميات هو ترخيص ضمني وهذا لنشره إيّاها وهذا ما يعني أنه غير معارض لإستعمالها من طرف أشخاص مجهولين ، ومثالي على ذلك هو قيام أشخاص بإبتكار "مودات" خاصة بألعاب الفيديو ونشرها على الأنترنت ويتم إستعمال هذه المودات من طرف أشخاص آخرين ونشرها على موقع التواصل الإجتماعي "اليوتيب".

[1] مليايي عبد الوهاب، المرجع السابق، الصفحة 109

[2] أمر رقم 05/03 ، المتعلق بحقوق المؤلف والحقوق المجاورة ، المرجع السابق.

– الفرع الثاني: الحماية الجزائية للجرائم الإلكترونية في ظل نصوص قانون الملكية الصناعية.

لقد تمّ النص على حماية براءة الإختراع من طرف المشرع الجزائري من خلال[1] الأمر رقم07/03 المتعلق ببراءة الإختراع الصادر ب:2003/07/19 [2]، والذي عرّف براءة الإختراع في المادة الثانية منه ب: "الإختراع: فكرة لمخترع ، تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية."

وذلك بشرط أن يكون الإخترع محل الحماية جديدا إذا لم يكن مدرجا في مجال التقنية بحسب نص المادة الرابعة من نفس هذا القانون ، وعليه سنحاول التطرق في موضوع دراستنا إلى الأساليب المعتمدة من قبل المشرع الجزائري في تأطير الحماية القانونية لبرامج الحاسوب عن طريق براءة الإختراع من خلال العناوين التالية.

– أولا:الشروط الواجب توفرها في براءة الإختراع.

لكي تتوفر الشروط الواجبة على الإختراع يجب أن تتوفر فيه شروط المادة الثالثة من هذا الأمر[3] والتي تنص على ما يلي : " يمكن أن تحمى بواسطة الإختراع، الإختراعات الجديدة و الناتجة عن نشاط إختراعي والقابلة للتطبيق الصناعي" ، وعليه يتجلى لنا من خلال نص هذه المادة تأكيد المشرع على ظرورة توفر شرط أساسي وهو شرط الجدّية في الإختراع ليحظى هذا الأخير بالحماية القانونية، وسنحاول ذكر الشروط الواجب توفرها من خلال العناوين التالية .

– الإبتكار.

– الجدية.

---

[1] العاقل فريال، المرجع السابق، الصفحة 55.

[2] أمر رقم 07/03 المؤرخ في 19/ 2003/07 المتعلق ببراءة الإختراع ، الجريدة الرسمية عدد 44.بتاريخ 2003/07/23. عرّف براءة الإختراع في المادة الثانية ب: "الإختراع: فكرة لمخترع ، تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية."

[3] العاقل فريال، المرجع السابق، الصفحة 56.

- القابلية للتطبيق الصناعي

- المشروعية .

وقد فرّق الفقه التجاري بين براءة الإختراع و المصنفات الأدبية على كون الإختراع يجب أن يكون ماديا ولا تنطبق النصوص القانونية لبراءة الإختراع إلاّ على الأشياء المادية والملموسة سواءا كان منتجا أو وسيلة خاصة وعليه فإن النصوص الواردة الأمر 07/03 [1]المتعلق ببراءة الإختراع يمكن أن تطبق على المكونات المادية للكمبيوتر وفقط مع ظرورة توافر الشروط التي يتطلبها هذا القانون أما مكونات الكمبيوتر غير مادية فلا يمكن أن نطبق عليها النصوص الخاصة بقانون براءة الاختراع وذلك لانتفاء الطابع المادي لها. إذ لاحظنا أن كل ذلك في إطار شرط القابلية للاستغلال الصناعي، وعلى هذا يمكن القول بأن الفقه التجاري وإن كان قد اختلف في ترتيب شروط الاختراع التي تؤهله للحصول على البراءة، فإنه متفق على الطابع المادي لهذا الاختراع أو الابتكار الجديد القابل للاستغلال الصناعي.

ثانيا: مدى تطبيق نصوص براءة الاختراع على برامج الكمبيوتر.

على الرغم من إتفاق الفقه التجاري مع ما نصّ عليه المشرع الجزائري من خلال نصوصه على براءة الإختراع وعلى الشروط الواجب توفرها في الإختراع لكي يحظى بالحماية الازمة قانونا من حيث وجوب أن يكون الإختراع ماديا إلاّ أن هناك من يخالف هاذ الرأي .

من ضمن المنتقدين لهذا الرأي نجد الدكتور محمد حسينين الذي يرى بأن برامج الكمبيوتر تعدّ جزءا[2] من منظومة الكمبيوتر بحيث أنها تستعمل للتعامل مع آلات الكمبيوتر وإدارتها وأنها أيضا

[1] أمر رقم 07/03 المؤرخ في 19/ 2003/07 المتعلق ببراءة الإختراع ، الجريدة الرسمية عدد 44.بتاريخ 2003/07/23.

[2] العاقل فريال، المرجع السابق، الصفحة 57/56.

من ظمن براءة الإختراع لأنها تتضمن إستخدامات جديدة لأفكار أو مبادئ علمية لتشغيل الكمبيوتر.

وكذلك هناك من يرى من المنتقدين أن قوانين براءة الإختراع حتى وإن كانت تعمل على حماية براءة الإختراع إلاّ أن هناك حيلولة لحماية المكونات الغير المادية للحاسوب والتي قد تكون جزء رئيسي له ، وكذلك رأى بعض المختصين أن شرط توفر الجديّة والإستغلال الصناعي أدّى إلى صعوبة في توفير حماية كاملة وشاملة للبرمجيات من خلال الملكية الصناعية إن وافقت التشريعات المقارنة بخصوص الشرطين السابقين مع أن يكون الإختراع نشاطا خلاقا.

1- شرط الجدية.

الإشكالية المثارة بالنسبة لهذا الشرط في نظر الفقهاء هو صعوبة التحقق منه في مجال البرمجيات[1] وغالبا ما يكون تقرير الجدة جزافيا لما يتميز به من طابع ذهني بحت ، ويتطلب هذا الأمر أن تكون الجهة التي تقوم بفحص طلبات البراءة تتميز بدرجة عالية من الكفاءة والتمييز في المجال الذي تتولى بحثه لكي تقرر ما إذا قد سبق وأن قدم إختراع ممثال لإختراع محل التحقق منه أم لا وخصوصا عند القضاة إذ يعتبر صعبا حتى على المبرمجين أنفسهم فكيف يكون بالنسبة والسبب للقضاة لا يعود لإعتبارات قانونية بل في الكيانات التي تبحث في موضوع الجدّة والإبتكار من عدمه في ما يخص بالإختراعات الغير المادية التي ينقصها الكفاءة والخبرة الازمتين في التحقق من الجدة في الإبتكار.

ومنه أيضا نصطدم بإشكال آخر وهو إعتماد القاضي على تقرير الخبرة في مجال التحقق من شرط الجدية ويعتمد عليه إعتمادا مطلقا ، وهذا ما يستدعي في نظري الشخصي على القضاة الخضوع لتكوين خاص في مجال الحاسب الآلي والنظم المعلوماتية حتى يكون هناك موازنة بين

[1] العاقل فريال، المرجع السابق، الصفحة 58/57.

رأي القاضي الشخصي و إقتناعه وبين تقرير الخبرة كون أن القاضي الجنائي قاضي أمير يحتكم على قناعته الشخصية .

2- صعوبة الإستغلال الصناعي بالنسبة للكيان المعنوي .

من بين الإشكاليات التي وقع فيها المشرع الجزائري في مجال الحماية الصناعية لبرامج الحاسوب هو[1] إستخدام هذا الأخير في الإستعمال أو الإستغلال الصناعي ، وصعوبة تحقق هذا الشرط أحدث خللا في إعتبار ما إذا كانت البرامج تحظى بالحماية القانونية كون أن نسبة كبيرة من برامج الحاسب الآلي لا تستغل في المجال الصناعي .

و هذا ما إتّجهت إليه أغلب التشريعات المعاصرة في عدم توفيرها للحماية لبرامج الحاسوب في نصوص الملكية الصناعية وذلك لتجردها لأي طابع صناعي وكذلك لصعوبة التحقق من أمر الجدّية في برامج الحاسب الآلي مثل ما ذكرنا سابقا ، و استثناءات لكل ما سبق يعتبر البرنامج إختراعا إذا ما كان جزءا من ذاكرة الحاسوب أو إذا كان طلب براءة الإختراع ينصبّ على وسيلة صناعية يكون البرنامج يحقق إحدى مراحلها .

ونعيد الذكر بمدى صعوبة تحقق هذا الأخير وذلك وفق ما أجرته المنظمة العالمية للملكية الفكرية عام 1978 التي جاء فيها أن 1% فقط من البرامج يستوفي شرط قابلية الاستغلال الصناعي.

وهذا بسبب أن الإختراع ذا صفة مادية، ويجب أن يؤدي استغلاله إلى منتج صناعي، أو يمكن الوصول إلى نتيجة صناعية، وكل هذه الأمور تتناقض مع الكيان المعنوي ، وفي المقابل نجد أغلب التشريعات لم تشترط أن يكون الإختراع ماديا ليحظى ببراءة الإختراع كون أن النظريات العلمية مجرد أفكار .

[1] العاقل فريال، المرجع السابق، ص58/57.الصفحة 59/58

أمّا المشرع الجزائري فقد إستبعد البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءة الاختراع وذلك طبقا للمادة 07 من الأمر 07/03 [1] " لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب "

وقرر توفر الحماية بالنسبة لحقوق المؤلف والحقوق المجاورة .

– الفرع الثالث: حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي:

من بين الأمور التي يجب على الإنسان إحترامها في معاملته للغير هو عدم المساس بكرامته بأي[2] شكل كان ولأهمية هذا الأمر أصدر المشرع الجزائري في مجال مكافحة الجرائم المعلوماتية قانون يكفل به حماية الأفراد من الإعتداءات الواقعة عليهم وهو القانون رقم 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي بإعتبار البيئة الإلكترونية بؤرة من بؤر الجرائم الواقعة في هذا المجال .

وقد حدد المشرع مجموعة من التعريفات المتعلق بمجال حماية المعطيات ذات الطابع الشخصي في نص المادة 03 من هذا القانون حيث جاء تعريف المعطيات ذات الطابع الشخصي كالتالي :

(كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه،'' الشخص المعني ''بصفة مباشرة أو غير مباشرة ، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الإجتماعية).

وعرف معالجة المعطيات ذات الطابع الشخصي على النحو التالي : (المشار إليها أدناه "معالجة" كل عميلة أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات

1 تنص المادة 07 من الأمر رقم 07/03 اعلى : " لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب "

[2] قانون07/18 المؤرخ في 10/06/2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، الجريدة الرسمية عدد 34.

ذات طابع شخصي، مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملاءمة أو التغيير أو الاستخراج أو الإطلاع أو الإستعمال أو الإيصال عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال الإتاحة أو التقريب أو الربط البيني وكذا الإغلاق أو التشفير أو المسح أو الإتلاف).

وأتى أيضا بتعريف : - الشخص المعني- موافقة الشخص المعني - المعالجة الآلية - معطيات حساسة - مضمون غير شرعي - حماية معطيات جينية - معطيات في مجال الصحة – ملف - الإتصال الإلكتروني -المسؤول عن المعالجة – معالج من الباطن – الغير – المرسل إليه – تنازل أو إيصال – الربط البيني بين المعطيات – السلطة الوطنية – مقدم الخدمات – الإستكشاف المباشر – غلق المعطيات .[1]

- أولا : الأحكام الجزائية .

حدد المشرع الأحكام الجزائية ضمن الفصل الثالث من الباب السادس المعنون بأحكام إدارية وجزائية من المادة 54إلى المادة 74 وحدد مجموعة من المخالفات نذكرها في ما يلي :

- كل يخالف أحكام المادة 02 من هذا القانون.

- كل من يقوم بمخالفة بمعالجة المعطيات ذات الطابع الشخصي خرقا لأحكام المادة 07من هذا القانون

- القيام بمعالجة معطيات ذات الطابع الشخصي رغم إعتراض الشخص المعني ، عندما تستهدف هذه المعالجة ، لاسيما الاشهار التجاري او عندما يكون الإعتراض على أسباب شرعية.

- الإخلال بالشروط المذكورة في المادة 12 من هذا القانون.

- القيام بتصريحات كاذبة .

- مواصلة نشاط معالجة المعطيات رغم سحب التصريح أو الترخيص الممنوح له.

[1] بتنص المادة 07 من الأمر رقم 07/03 اعلى : " لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب

- القيام بمعالجة معطيات حساسة دون موافقه الشخص المعني.

- القيام بإستعمال أو إنجاز معالجة معطيات أغراض أخرى غير تلك او المرخص بها.

- قيام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير مشروعة .

- السماح لأشخاص غير مؤهلين بالولوج لمعطيات ذات طابع شخصي.

القيام بعرقلة عمل السلطة الوطنية.

إفشاء معلومات محمية من طرف الشخص المشار إليه في المادتين 23/ 27 المنصوص عليها في هذا القانون وإحالة تحديد العقوبة لقانون العقوبات .

- كل من يلج دون أن يكون مؤهلا لذلك إلى السجل الوطني المنصوص عليه في المادة 28 من هذا القانون.

- كل مسؤول عن المعالجة يرفض دون سبب مشروع، حقوق الإعلام أو الولوج أو التصحيح أو الاعتراض المنصوص عليها في المواد 32و34و35و36 من هذا القانون.

- المسؤول عن المعالجة الذي يخرق الإلتزامات المنصوص عليها في المادتين 38 و 39 من هذا القانون [1]

- كل من قام بالاحتفاظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها في التشريع الساري المفعول أو تلك الواردة في التصريح أو الترخيص.

- مقدم الخدمات الذي لا يقوم بإعلام السلطة الوطنية والشخص المعني عن كل إنتهاك للمعطيات الشخصية.

- كل من ينقل معطيات ذات طابع شخصي نحو دولة أجنبية.

[1] .قانون 18/ 17 ، المرجع السابق مادة 22 وما بعدها .

– كل من قام في غير الحالات المنصوص عليها قانونا، بوضع أو حفظ في الذاكرة الآلية، المعطيات ذات الطابع الشخصي بخصوص جرائم أو إدانات أو تدابير أمن.

– كل مسؤول عن معالجة وكل معالج من الباطن وكل شخص

مكلف ، بالنظر إلى مهامه ، بمعالجة معطيات ذات طابع شخصي، يتسبب أو يسهل، ولو عن طريق إهمال ، الإستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة أو يوصلها إلى غير المؤهلين لذلك.

– معاقبة الشخص المعنوي الذي يرتكب الجرائم المنصوص عليها في هذا القانون وفقا للقواعد المنصوص عليها في قانون العقوبات.

–في حالة العود، تضاعف العقوبة المنصوص عليها في هذا الفصل..

ثانيا : السلطة المختصة بالمتابعة:

أحدث المشرع الجزائري سلطة مكلفة خصيصا بمتابعة جرائم الإعتداء على البيانات ذات الطابع[1] الشخصي ، في المواد 22من إلى 31 ضمن الفصل الثالث المعنون بالسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي ، وهي سلطة إدارية تنشأ لدى رئيس الجمهورية وتتمتع بالشخصية المعنوية وبالاستقلال المالي والإداري مقرها بالعاصمة ، وتتشكل من ثلاث شخصيات يعينهم رئيس الجمهورية لعدة مدتها 05 سنوات قابلة للتجديد طبقا لما نصت عليه المادة 03 من هذا القانون : (تتشكل السلطة الوطنية من:

– ثلاث شخصيات من بينهم الرئيس يختارهم رئيس الجمهورية من بين ذوي الاختصاص في مجال عمل السلطة الوطنية،

– ثلاث قضاة يقترحهم المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة.

[1] قانون 18/ 17 ، المرجع السابق مادة 22 وما بعدها .

– عضو عن كل غرفة من البرلمان يتم اختياره من قبل رئيس كل غرفة، بعد التشاور مع رؤساء المجموعات البرلمانية، وممثلين عن الوزارات الوطنية .

ويقوم الأعضاء بأداء اليمين قبل تنصيبهم وحدد المشرع مهاما للسلطة الوطنية في المادة 25 تتمثل في ما يلي :

– منح التراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي.

– اعلام الاشخاص المعنيين والمسؤولين عن المعالجة في حقوقهم وواجباتهم.

– تقديم الاستشارات للأشخاص والكيانات التي تلجا لمعالجه المعطيات ذات الطابع الشخصي.

– تلقي الإحتجاجات والطعون والشكاوى بخصوص تنفيذ شكاوى ذات الطابع الشخصي.

– إعلام الأشخاص المعنيين والمسؤولين عن المعالجة في حقوقهم وواجباتهم .

– تقديم الإستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي .

– تلقي الإحتجاجات والطعون والشكاوى ذات الطابع الشخصي.

– الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا للشروط المنصوص عليها في هذا القانون .[1]

– الأمر بالتغييرات اللازمة لحماية المعطيات ذات الطابع الشخصي المعالجة.

– الأمر بإغلاق المعطيات أو سحبها أو أتلافها.

– تقديم اي اقتراح من شانه تبسيط وتحسين الاطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي. – نشر التاريخ الممنوحة والآراء المدلى بها في السجل الوطني المشار إليه في المادة 28من هذا القانون.

– تطوير علاقات التعاون مع السلطات الأجنبية المماثلة مع مراعاة المعاملة بالمثل.

[1] قانون 18/ 17 ، المرجع السابق مادة 25 وما بعدها .

- إصدار عقوبات إدارية وفقا لأحكام المادة 46 من هذا القانون.[1]

- وضع معايير في مجال حماية المعطيات ذات الطابع الشخصي.

- وضع قواعد السلوك والأخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي.

وفي الأخير تقوم السلطة بإعداد تقرير سنوي حول نشاطها وترفعه إلى رئيس الجمهورية.

- المطلب الثاني : الحماية القانونية للجرائم الإلكترونية في ظل قوانين الإعلام والإتصال والتجارة والتوقيع والتصديق الإلكترونيين.

- الفرع الأول : الحماية القانونية للجرائم الالكترونية في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها :

يعتبر هذا القانون من بين أهم الركائز القانونية التي أصدرها المشرع الجزائري لمكافحة الجرائم[2] الإلكترونية بعد قانون العقوبات كون أن الجرائم المتصلة بتكنولوجيات الإعلام والإتصال من بين أخطر صور الجرائم المعلوماتية .

ومن أهم ما جاء فيه إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته[3] كذلك القواعد المتعلقة بالاختصاص الإقليمي للقانون الجزائي الجزائري حيث تم التوسع في الاختصاص الإقليمي للسلطة القضائية في متابعة جرائم التي تمس بمؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني نظرا لما يمكن لهذه التكنولوجيات الحديثة من القيام به في حالة استغلالها ضد مصالح الدولة ولو في أقاليم دول أخرى من طرف جزائريين أو أجانب، أيضا فإن عالمية استغلال تكنولوجيات الإعلام والاتصال وخاصة

---

[1] قانون 18/ 17 ، المرجع السابق مادة 46وما بعدها .

[2] قانون رقم 04/09 المؤرخ في 2009/07/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ، الجريدة الرسمية عدد 47بتاريخ 2009/07/16 .

[3] أحمد مسعود, مريم قريشي محمد ، 23/04/2013 ، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال القانون رقم 09/ 04 ، تم الإطلاع عليه بتاريخ 19/09/2020م على الساعة 02:04 ، نسخة إلكترونية، رابط الموقع : https://dspace.univ-ouargla.dz/jspui/handle/123456789/1467

الانترنت أدت إلى حذف الحدود الإقليمية وأصبحت الجرائم تمتد عبر عدة أقاليم وتكون من اختصاص القانون الجزائي لأكثر من دولة مما قد ينجر عنه تنازع في الاختصاص أو رفض له، مما قد ينشأ للمجرمين ، وقد حدد المشرع الجزائري المجالات المكفولة بالحماية ومفاهيمها المندرجة ضمن هذا القانون في المادة الثانية منه ونذكرها في ما يلي :

- الجرائم المتصلة بتكنولوجيات الإعلام والإتصال .
- منظمومة معلوماتية .
- معطيات معلوماتية .
- مقدمو الخدمات .
-المعطيات المتعلقة بحركة السير .
- الإتصالات الإلكترونية .

وقد أحال المشرع الجزائري في غالبية النصوص هذا القانون إلى قانون الإجراءات الجزائية كون أن جلها متعلقة بالطابع الإجرائي وهذا ما جاء في نص المادة 03 والتي حددت مجال التطبيق في وضع ترتيبات التقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها فيحينها والقيام بإجراءات التفتيش والحجز داخل منظومة المعلوماتية وقد عنون المشرع الجزائري في الفصل الثاني من هذا القانون مراقبة الإتصالات الإلكترونية وبين حالات التي يتم فيها اللجوء إلى المراقبة في المادة الرابعة ونذكرها في ما يلي : [1]

- للوقاية من الأعمال الموصوفة بجرائم الإرهاب .
- في حالة توفر معلومات عن احتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام.
- لمقتضيات التحريات والتحقيقات القضائية .

[1] قانون 18/ 17 ، المرجع السابق مادة 22 وما بعدها .

- في إطار تنفيذ طلبات المساعدة القضائية .

ولا يجوز إجراء عمليات المراقبة المذكورة أعلاه إلا بإذن مكتوب من السلطات القضائية .

وقد جاء المشرع بتفصيله للقواعد الإجرائية في الفصل الثالث حيث نص في المادة الخامسة على إجراءات التفتيش في الحالات المذكورة أعلاه وحدد الأجهزة المختصة بالتفتيش والتي هي السلطة القضائية المختصة وضباط الشرطة القضائية ويكون التفتيش ولو عن بعد في :

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

ب- منظومة تخزين معلوماتية .

وفصل في إجراءات حجز المعطيات المعلوماتية المتحصلة من التفتيش في المادة 06 و07 و08و09 من هذا القانون و تتمثل هذه الإجراءات في :

- الحجز عن طريق منع الوصول إلى المعطيات .
- المعطيات المحجوزة ذات المحتوى المجرم .
- حدود استعمال المعطيات المتحصل عليها .

وقد أنشأ المشرع الجزائري الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته مندرجة تحت الفصل الخامس من المادة 13 وأحال تشكيل الهيئة وتنظيماتها وكيفيات سيرها إلى التنظيم وحدد مهامها ضمن المادة 14 نذكر منها ما يلي :[1]

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها
- تبادل المعلومات مع نظيراتها من الخارج .

1 .قانون 13/ 14، المرجع السابق مادة 22 وما بعدها .

وحدد المشرع مجالات التعاون والمساعدة القضائية الدولية وأورد عليها قيودا وذلك ضمن الفصل السادس في المواد 15 ، 16 ، 17 18، 19.

– الفرع الثاني : الحماية القانونية للجرائم المعلوماتية في ظل قانون التجارة الإلكتروني :

من بين القوانين أيضا التي توجب الحماية القانونية للجرائم المعلوماتية هو قانون التجارة الإلكتروني[1] الذي يطبق في مجال المعاملات التجارية الإلكترونية للسلع والخدمات و قد واشترط المشرع الجزائري لتطبيق هذا القانون أن يكون أحد أطراف العقد الإلكتروني متمتعا بالجنسية الجزائرية أو مقيما إقامة شرعية في الجزائر أو شخصا معنويا خاضعا للقانون الجزائري .

وقد فصل قانون التجارة الالكتروني في بابه الأول الأحكام العامة من المادة الأولى إلى المادة 06 بتوضيح القواعد التي تبيح التعامل في مجال التجارة الإلكترونية وخطر بعض المعاملات التي من شأنها المساس بمصالح الدفاع الوطني والأمن الوطني ومن أهم ما جاء فيه هو:

1- المعاملات التجارية العابرة للحدود .

2- شروط الممارسة التجارة الالكترونية

3- المتطلبات المتعلقة بالمعاملات التجارية عن طريق الإتصال الإلكتروني

4- شروط ممارسه التجارة الالكترونية

5- المتطلبات المتعلقة بالمعاملات التجارية عن طريق الإتصال الالكتروني.

6- إلتزامات المستهلك الالكتروني.

7- واجبات المورد الإلكتروني ومسؤولياته .

8- الدفع في المعاملات الإلكترونية.

[1] قانون رقم 05/18 المؤرخ في 10/05/2018 المتعلق بالتجارة الإلكترونية ، الجريدة الرسمية عدد 28 بتاريخ 16/05/2018.

9- الإشهار الالكتروني.

10- الجرائم والعقوبات.

وقد حدد المشرع الجزائري في المادة 36 من هذا القانون السلطات المختصة بمعاينة مخالفة هذا القانون حيث نصت المادة على ما يلي : (خلافا على الضباط وأعوان الشرطة القضائية يتم مراقبه المخالفات هذا القانون الاعوان المنتمون للأسلاك الخاصة بالرقابة التابعون للإدارات المكلفة بالتجارة).

وسنتطرق في هذا القانون الى الجرائم والعقوبات المنصوص عليها من المادة 35 إلى المادة48 المتعلقة بمراقبة الموردين الإلكترونيين ومعاينة المخالفات. [1]

أدرج المشرع الجزائري الجرائم والعقوبات ضمن الفصل الثاني لهذا القانون وقد نصت المادة 37 على أنه : (دون المساس بتطبيق العقوبات الأشد المنصوص عليها في التشريع المعمول به يعاقب بغرامة من 200.000 إلى 1000.000دج كل من يعرض للبيع أو يبيع عن طريق الإتصال الإلكتروني المنتجات أو الخدمات المذكورة في المادة 3 من هذا القانون).

وبرجوعنا للمادة 03 نجد هذه الخدمات تتمثل في :

- لعب القمار والرهان والمناصيب .
- المشروبات الكحولية والتبغ .
- المنتجات الصيدلانية .
- المنتجات التي تمس بحقوق الملكية الفكرية والصناعية أو التجارية .
- كل سلعه او خدمة محظورة بموجب التشريع المعمول به.
- كل سلعة أو خدمة تستوجب عقد رسمي .

[1] . قانون رقم 05/18 المؤرخ في 10/05/2018 المتعلق بالتجارة الإلكترونية ، الجريدة الرسمية عدد 28 بتاريخ 16/05/2018.

وشدد المشرع الجزائري العقوبة في المادة 38 على من يخالف الأحكام التي جاءت بها المادة 05 من هذا القانون التي نصت على ما يلي (المادة 05) : (تمنع كل معاملة عن طريق الإتصلات الإلكترونية في العتاد والتجهيزات والمنتجات الحساسة المحددة عن طريق التنظيم المعمول به و/أو الخدمات الأخرى التي من شأنها المساس بمصالح الدفاع الوطني والنظام العام والأمن العمومي).

ويغرم بذلك كل من يخالف تص المادة من 500.000 إلى 2.000.000 دج وبإمكان القاضي الأمر بغلق الموقع الإلكتروني والشطب من السجل التجاري طبقا للفقرة الثانية من المادة 38.

وقد فرض المشرع الجزائري غرامة على الموردين إذا ما تم بذلك مخالفة أحكام المادة 11و 12 حيث نصت على ما يلي : (يعاقب بغرامة من دج50.000 دينار جزائري إلى 500.000 دج كل مورد إلكتروني يخالف أحد الإلتزامات المنصوص عليها في المادتين 11 و 12 من هذا القانون كما يجوز للجهة القضائية التي رفعت أمامها الدعوة أن تأمر بتعليق نفاذه إلى جميع منصات الدفع الإلكتروني لمدة لا تتجاوز سته أشهر).

وقد أدرج المشرع إجراء الصلح بين الموردين في نص المادة 45 في فقرتها الثانية وحدد المصالح المخولة بذلك بإحالته لنص المادة 36 و أمام في حالة العود فقد أسقط المشرع هذا الجراء في الفقرة الثالثة من نفس المادة.

– الفرع الثالث: الحماية القانونية للجرائم المعلوماتية في ظل قانون التصديق والتوقيع الإلكتروني.

بتطور التكنولوجية على مستوى العالم وتطور الإتصالات أصبح الحاسوب ظرورة حتمية لا بد منه[1] في شتى المجالات وأصبح مجبرا التعامل به عن طريق طرق ووسائل حديثة مما أدى بظهور

1 غربي خديجة ، **التوقيع الإلكتروني** ، مذكرة لنيل شهادة ماستر ، كلية الحقوق والعلوم السياسية قسم الحقوق ، جامعة قاصدي مرباح–ورقلة ، الصفحة 05.

عقود إلكترونية والتي تحتاج إلى توقيع يتلائم مع طبيعتها بإعتبارها تتم بكتابة إلكترونية ومحررات إلكترونية فظهر ما يعرف بالتوقيع الالكتروني.

وقد عرف المشرع الجزائري في المادة الثانية من الفصل الثاني في هذا القانون التوقيع الإلكتروني بأنه[1] : (بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق).

وقد جاء المشرع أيضا بجملة من التعريفات المتعلقة ببعض المصطلحات الخاصة بمجال التوقيع الإلكتروني والتي تتمثل في : -الموقع - بيانات إنشاء التوقيع الإلكتروني- آلية إنشاء التوقيع الإلكتروني- بيانات التحقق من التوقيع الإلكتروني -آلية التحقق من التوقيع الإلكتروني - شهادة التصديق الإلكتروني- مفتاح التشفير الخاص - مفتاح التشفير العمومي – الترخيص - الطرف الثالث للموثوق - مؤدي خدمات التصديق الإلكتروني – المتدخلون في الفرع الحكومي - صاحب شهادة التصديق الإلكتروني - سياسة التصديق الإلكتروني- التدقيق .

وما سنحاول التطرق إليه هو الجانب العقابي المندرج في الفصل الأول من الباب الرابع المعنون بالعقوبات والفصل الثاني من الباب الثاني المعنون بسلطات التصديق الإلكتروني وسنتطرق لكل سلطة على حدة .

- أولا: العقوبات .

1/- العقوبات المالية والإدارية:

نص المشرع على العقوبات المالية والإدارية في المادتين 64 و 65 حيث جاء في نص المادة 64 في فقرتها الأولى ما يلي :(في حالة عدم إحترام مؤدي خدمات التصديق الإلكتروني أحكام دفتر الأعباء أو سياسة التصديق الإلكتروني الخاصة به والموافق عليها من طرف

[1] قانون رقم 04/18 المؤرخ في 01/02/2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين ، الجريدة الرسمية عدد 06 بتاريخ 10/02/201.

السلطة الاقتصادية تطبق عليه هذه السلطة عقوبة مالية يتراوح مبلغها ب مائتي ألف دين " 200.000دج " وخمسة ملايين دينار " 5.000.000 دج " حسب تصنيف الأخطاء المنصوص عليه في دفتر الأعباء الخاص بمؤدي الخدمات ، وتعذره بالإمتثال لإلتزاماته في مدة تتراوح بين ثمانية أيام و 30 يوما حسب الحالة وتبلغ المآخذ المتخذة ضد مؤدي الخدمات ، حتى يتسنى له تقديم مبرراته الكتابية ضمن الآجال المذكورة سابقا).

والعقوبة الثانية التي تقع على مؤدي خدمات التوقيع الإلكتروني في حالة ما إذا إنتهك لمقتضيات التي يتطلبها الأمن العمومي أو الدفاع الوطني وذلك طبقا لنص المادة 65 في الفقرة الأولى وتقوم السلطة السلطة الاقتصادية التوقيع الإلكتروني بالسحب الفوري للتلخيص.[1]

وجاءت في فقرتها ثانيه تنص على ما يلي: (وتكون تجهيزات مؤدي خدمات التوقيع الإلكتروني محل تدابير تحفظية طبقا للتشريع المعمول به وذلك دون الإخلال بالمتابعات الجزائية).

2/- **الأحكام الجزائية**: أما الأحكام الجزائية فقد أدرجها المشرع ضمن الفصل الثاني من المادة 66 إلى المادة 75 بعقوبات تفصيلية لكل جريمة والتي حصرها المشرع في ما يلي :

- القيام بإقرارات كاذبة لأجل الحصول على شهادة تصديق إلكتروني موصوفة .
- الإخلال بإلتزام إعلام السلطة الإقتصادية بالتوقف عن نشاطه في الآجال المحددة قانونا.
- حيازة أو إفشاء أو إستعمال بيانات إنشاء توقيع إلكتروني موصوف خاص بالغير.
- الإخلال عمدا بإلتزام تحديد طالب هوية شهادة توقيع إلكتروني موصوفة.
- عدم الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الإكتروني الممنوحة.
- جمع البيانات الشخصية للمعني من دون موافقته الصريحة

[1] قانون رقم 04/18 نفس الرجع السابق مادة 64 و ما بعدها.

- تأدية خدمات التوقيع الإلكتروني للجمهور من دون رخصة أو كل مؤدي خدمات التوقيع إلكتروني يستأنف ويواصل نشاطه بالرغم من سحب ترخيصه .

- إفشاء كشف معلومات سرية إطلع عليها أثناء قيامه بالتدقيق.

- إستعمال شهادة التصديق الإلكتروني الموصوفة لغير الأغراض التي منحت لأجلها.

- مضاعفة عقوبة الشخص المعنوي بخمس مرات الحد الأقصى عند إرتكابه الجرائم المذكورة في هذا الفصل مقارنة بالشخص الطبيعي.

ثانيا: سلطات التصديق الإلكتروني .

1/- السلطة الوطنية للتصديق الإلكتروني :

قام المشرع الجزائري بإستحداث السلطة الوطنية للتصديق الإلكتروني ونص عليها في المواد من[1] 16 إلى 25 وتعتبر هذه السلطة كآلية إدارية رقابية ضابطة مستقلة عن النظام الحكومي وتمتاز بالشخصية المعنوية والإستقلال المالي لضمان موثوقية التصديق الإلكتروني وتعمل بمعزل عن الأهداف الحكومية أو خارج السياسة العامة التي تسطرها الدولة وتشرف على تنفيذها ، لذلك قام المشرع بتخصيص نظام خاص بها وسلطات تقديرية واسعة لضرورات مرونة العمل الإداري ، وتختص السلطة القضائية بمراقبتها لعدم مواجهة إحتمال تعسفها في إستعمال امتيازات السلطة العامة.

وتتمثل مهام هذه السلطة في ما يلي :

- إعداد سياساتها للتصديق الإلكتروني وعرضها على السلطة.

- الموافقة على سياسات التصديق الصادرة عن الأطراف الثالثة الموثوقة والسهر على تطبيقها .

1 صبرينة جبايلي ، 01-12-2017 ، النظام القانوني للسلطة الوطنية للتصديق الالكتروني ، تم الإطلاع عليه في 21/09/2020م على الساعة 00.44 ، نسخة إلكترونية ، رابط الموقع :
http://revue.umc.edu.dz/index.php/h/article/view/2668

- الإحتفاظ بشهادات التصديق الإلكترونية المنتهية صلاحيتها والبيانات المرتبطة بمنحها من قبل الطرف الثالث الموثوق بغرض تسليمها إلى السلطات القضائية المختصة.

- نشر شهادة التصديق الإلكتروني للمفتاح العمومي للسلطة.

- إرسال كل المعلومات المتعلقة بنشاط التصديق الإلكتروني إلى السلطة دوريا او بناءا على طلب منها.

- القيام بعملية التدقيق على مستوى الطرف الثالث الموثوق عن طريق الهيئة الحكومية المكلف بالتدقيق طبقا لسياسة التصديق.

2/- السلطة الإقتصادية للتصديق الإلكتروني :

حدد المشرع الجزائري صلاحية تعيين السلطة الإقتصادية للتصديق الإلكتروني من قبل السلطة المكلّفة بضبط البريد والمواصلات السلكية واللاسلكية طبقا لما نصت عليه المادة 29 من هذا القانون.[1]

وتتمثل مهمتها في مراقبة ومتابعة مؤدي خدمات التصديق الإلكتروني لصالح الجمهور .

وقد حدد المشرع مجموعة من المهام التي تختص بها هذه الهيئة في الفقرة الثاني من المادة 30 وتتمثل في ما يلي :

- إعداد سياستها للتصديق الالكتروني وعرضها على السلطة للموافقة عليها والسهر على تطبيقها.

- منح تراخيص لمؤديين خدمات التصديق الإلكتروني بعد موافقة السلطة.

- الموافقة على سياسات التصديق الصادرة عن مؤديي خدمات التصديق الإلكتروني والسهر على تطبيقها.

[1] صبرينة جبايلي ، نفس المرجع السابق مادة 16 و مابعدها.

- الإحتفاظ بشهادات التصديق الإلكترونية المنتهية صلاحيتها.

- نشر شهادة التصديق الإلكتروني للمفتاح العمومي للسلطة.

- إتخاذ التدابير اللازمة لضمان إستمرارية الخدمات في حالة عجز مؤدي خدمات التصديق الإلكتروني عن تقديم خدماته.

- إرسال كل المعلومات المتعلقة بنشاط التصديق الإلكتروني إلى السلطة دوريا أو بناء على طلب منها

- التحقق من مطابقة طالبي التراخيص مع سياسة التصديق الإلكتروني بنفسها أو عن طريق مكاتب تدقيق معتمدة.

- السهر على وجود منافسة فعلية ونزيهة باتخاذ كل التدابير اللازمة لترقية أو استعادة المنافسة بين مؤديي خدمات التصديق الإلكتروني.

- التحكيم في النزاعات القائمة بين مؤديي خدمات التصديق الإلكتروني فيما بينهم أو مع المستعملين طبقا للتشريع المعمول به.

- مطالبة مؤديي خدمات التصديق الإلكتروني أو كل شخص معني بأي وثيقة أو معلومة تساعدها في تأدية المهام المخولة لها.

- إعداد دفتر الشروط الذي يحدد شروط وكيفيات تأدية خدمات التصديق الإلكتروني وعرضه على السلطة للموافقة عليه.[1]

- إجراء كل مراقبة طبقا لسياسة التصديق الإلكتروني ودفتر الشروط الذي يحدد شروط وكيفيات تأدية خدمات التصديق الإلكتروني.

[1] صبرينة جبايلي ، نفس المرجع السابق مادة 16 و مابعدها.

- إصدار التقارير والإحصائيات العمومية وكذا تقرير سنوي يتضمن وصف نشاطاتها مع إحترام مبدأ السرية.

وفي الأخير تقوم السلطة الإقتصادية بتبليغ النيابة بكل فعل ذو طابع جزائي تقوم باكتشافه أثناء تأديتها لعملها طبقا لما تصت عليه الفقرة الأخير من نفس المادة.

الفصل الثاني

إجراءات المتابعة الجنائية في مكافحة الجرائم المعلوماتية

– المبحث الأول :اجراءات المتابعة القانونية في الجرائم المعلوماتية

نظرا لخصوصية الجرائم المعلوماتية وتطورها السريع ومرونتها مع العولمة والتكنولوجية على المستوى[1] الوطني والعالمي أدت بالمشرع إلى استحالت تطبيقه للنصوص التقليدية في هذا المجال لتميزها وانفرادها على الجرائم العادية بحيث أن إجراءات المتابعة العادية وقفت عاجزة أمامها. وهذا ما نادى إلى ضرورة تكاثف وتعاون دولي وعقد إتفاقات ومعاهدات لردع هذه الجرائم .

– المطلب الأول: أجهزة المتابعة القانونية في الجرائم المعلوماتية .

– الفرع الأول: الضبطية القضائية في الجرائم الإلكترونية.

أولا : الإختصاص المكاني للضبطية القضائية في الجرائم الإلكترونية.

لقد أنهى المشرع الجزائري مشكلة تنازع الإختصاص حول الجرائم الإلكترونية في نص المادة[2] 16 من قانون الإجراءات الجزائية وفتح الباب مفتوحا للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي تعد جزءا من الجرائم الماسة بالمعاملات التجارية الإلكترونية بحيث تمتد على المستوى الوطني وهذا ما يحسب على المشرع الجزائري لفطنته لأن التحقيق التمهيدي أو الإبتدائي تتقيد بإختصاصها الإقليمي وتتقيد بحدوده ففي هذه الحالة يتطلب إجراء التحقيق والتحري والبحث في هذه المواقع مساسا بسيادة الدولة المتواجد فيها ذلك الموقع أو الجهاز، وهو موقف المجلس الأوروبي في إحدى تقاريره حيث اعتبر هذا النوع من الإختراق المباشر انتهاكا لسيادة الدولة ما لم توجد اتفاقية . غير أن محكمة النقض الفرنسية لها رأي آخر حيث اعتبرت خروج الضبطية القضائية خارج حدودها الإقليمي خروجاً مادياً فان هذا الإجراء يعد باطلاً، أما إذا قامت الضبطية باستطلاع ملفات عن بعد بقصد القيام بتحريات لازمة حول وقائع معينة فإن ذلك لا

[1] د/ بوقرين عبد الحليم ، مقال بعنوان: (**المكافحة الاجرائية للجريمة المعلوماتية**)، جامعة عمار ثليجي– الأغواط..الصفحة 10

[2] **المرجع نفسه** ، الصفحة 7 وما بعدها.

يعد تنقلاً مادياً وحصول على تلك المعلومات بالوسائل التقنية يعد مشروعاً. وخلاصة القول أنه يتوجب على الضبطية القضائية الإلتزام بالاختصاص الإقليمي حتى لا تكون إجراءاتهم باطلة.

ثانيا: التفتيش في مجال الجريمة الإلكترونية .

يعتبر التفتيش إجراءا هاما من إجراءات التحقيق الذي يهدف إلى البحث عن أدلة الجريمة ويتمتع[1] التفتيش بشروط خاصة ويختلف إجراء التفتيش في الجريمة الإلكترونية عن غيره من الجرائم الأخرى وعليه فإن التفتيش يشمل في بيئة الأعمال الإلكترونية محلين، المحل الأول هو جهاز الحاسوب بمكوناته المادية والمعنوية، والمحل الثاني الشبكة العنكبوتية وقد أجاز المشرع بموجب المادة 5 من القانون 04/09 [2]للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى كل منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها وكل منظومة معلوماتية...

ويبقى الإشكال قائما بشأن تفتيش المكونات المعنوية كالبرامج وقواعد البيانات وكذا المواقع في الشبكة العنكبوتية والبريد الإلكتروني وغيره، فهي تتطلب مهارة عالية وسرعة لفك الشفرات والتعرف على الجناة.

ولا يبقى الإشكال قائما على التفتيش فحسب بل ينتق أيضا إلى الضبط فالضبط بحسب الأصل[3] يرد على أشياء مادية، فلا وجود للصعوبة في ضبط الأدلة في الجرائم الواقعة على المكونات المادية للنظام المعلوماتي ، ولكن تكمن الصعوبة في ضبط الوسائل التقنية المستخدمة في الجريمة

---

[1] د/عبد الحليم بوقرين ، د/ خضراوي الهادي ، (**تجربة الجزائر في مكافحة الجريمة الإلكترونية**) ، مداخلة في مؤتمر علمي بعنوان: المؤتمر العلمي الأول لمكافحة الجريمة الإلكتروني الرياض المملكة العربية السعودية ، كلية الحقوق والعلوم السياسية جامعة عمار ثليجي الأغواط / الجزائر .

[2] قانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ، مرجع سابق

[3] رابحي عزيزة ، **الأسرار المعلوماتية وحمايتها الجزائية** ، أطروحة لنيل شهادة الدكتوراه كلية الحقوق والعلوم السياسية ، قسم القانون الخاص ، جامعة أبي بكر بلقايد– تلمسان ، الصفحة ،281.

وذلك لعدم وجود دليل مرئي في هذه الحالة وهذا ما أدى إلى حدوث جدال فقهي حول الدليل التقني وكيفية ضبط، وقد تدخل المشرع وحل هذه المسألة حيث نص في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المادة 06 [1] منه والتي تنص على": عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهما على دعامة تخزين الكترونية تكون قابلة للحجز، والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية."... فكما يعتبر الضبط هو عملية تتبع التفتيش فيعتبر أيضا تحريز المضبوطات عملية تلي إجراء الضبط وعليه فإن المشرع الجزائري قضى بضرورة إتباع بعض الإجراءات الخاصة للمحافظة على سلامة المضبوطات من العبث وذلك كالتالي:

1- منع المشرع الوصول إلى المعلومات المتحصل عليها والتي تم ضبطها عن طريق ترميزها أو تقييدها

2-ضبط الدعائم الأصلية للمعلومات وعدم الاقتصار على ضبط نسخها.

3-عدم ثني القرص لأن ذلك قد يؤدي إلى تلفه وفقدان المعلومات المسجلة عليه.

4-عدم تعريض الأقراص والأشرطة الممغنطة لدرجات الحرارة العالية ولا الرطوبة.

وما يلاحظ من نص المادة 5 السالف الذكر أن التفتيش يكون بصفة مباشرة عن طريق الإنتقال إلى[2] مسكن المتهم أو المكان الذي تتواجد فيه أجهزته وهنا يجب الإلتزام بشروط التفتيش الواردة

[1] تنص المادة 06 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على : عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهما على دعامة تخزين الكترونية تكون قابلة للحجز، والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية."...

[2] رابحي عزيزة، المرجع السابق، الصفحة 281-286.

في قانون الإجراءات الجزائية سواء من حيث الإذن أو الميعاد أو الكيفية، وقد يكون التفتيش عن بعد كما أشارت المادة السالفة الذكر، ويقضي ذلك الدخول إلى المنظومة المعلوماتية دون إذن صاحبها والولوج إلى حاسوبه والتفتيش فيه وفي برامجه.

وبناءا على ما سبق يمكن القول أن التفتيش في بيئة الأعمال الإلكترونية يشمل محلين، المحل الأول هو جهاز الحاسوب بمكوناته المادية والمعنوية، والمحل الثاني الشبكة العنكبوتية وما تتضمنه من مكونات كالمواقع والبريد الإلكتروني وغيرها . ولا يختلف الشروط أثناء التفتيش في الجريمة الإلكترونية عن الجريمة العادية و يرتبط بثلاثة شروط مهمة جدا وهي الإذن، والمدة، وحضور صاحب المحل. وفي رأيي الشخصي والمتواضع كان على المشرع أن يقوم بتنظيم إجراءات خاصة أثناء التحقيق في الجرائم الإلكترونية لما يتطلب هدا النوع من الجرائم من السرعة في التنفيد لأنها ذات طابع تقني .

فبالنسبة للإذن نجد أن المشرع قد فصل في المسألة بموجب المادة الأولى الفقرة الرابعة من القانون04/09[1] السالف الذكر حيث جاء فيها (لا يجوز إجراء عمليات في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة) .

وإذا كان قانون الإجراءات الجزائية يحظر التفتيش من الثامنة ليلا إلى الخامسة صباحا، نظرا لتعلق الأمر بتفتيش المساكن وهو مستقر الإنسان ومكمن أسراره وحياته الخاصة، فإن الأمر يختلف نوعاً ما عن التفتيش في بيئة الأعمال الالكترونية، ومع ذلك لم يشر المشرع إلى مسألة ميقات التفتيش في القانون 04/09 ولكنه أحال ذلك إلى قانون الإجراءات الجزائية وهو ما يفهم من نص المادة 5 حيث جاء فيها (يجوز للسلطات القضائية المختصة وكذا ضابط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي حالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش

1 قانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ، مرجع سابق .

...) وهو ما يفضي بالضرورة إلى وجوب احترام ميعاد التفتيش الوارد في قانون الإجراءات الجزائية .

أما فيما يخص حضور صاحب المحل الذي يجري فيه التفتيش والذي يعد من الشروط الشكلية المعروفة في مجال التفتيش العادي، فإن الولوج إلى المواقع الإلكترونية أو البريد الإلكتروني يتطلب نوعاً من السرعة والسرية حتى لا يتم التلاعب بالأدلة، ورغم هذه الصعوبات إلى أن البعض ينادي بضرورة حضور المتهم أثناء التفتيش فإذا تعذر حضوره ينوب عنه شاهدين كضمانة للمتهم.

وما يميز التفتيش في البيئة الإلكترونية عن نظيرتها من الجرائم هو قابليتها للتفتيش عن بعد وذلك نتيجة لطبيعة التكنولوجيا الرقمية، وهنا نميز بين ثلاث احتمالات:

آ-الاحتمال الأول :اتصال حاسب المتهم بحاسب أو نهاية طرفيه موجودة في مكان آخر داخل الدولة.

ب-الاحتمال الثاني :اتصال حاسب المتهم بحاسب أو نهاية طرفية موجودة في مكان آخر خارج الدولة لأن من المتصور طبقا لهذا الاحتمال أن يقوم مرتكبوا الجرائم بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة عن طريق شبكات الاتصال البعيدة بهدف عرقلة سلطات الإدعاء في جميع الأدلة .

ج-الاحتمال الثالث :التصنت والمراقبة الإلكترونية لشبكات الحاسب الآلي، فالتصنت والأشكال الأخرى للمراقبة الالكترونية رغم أنها مثيرة للجدل إلا أنه مسموح بها تحت ظروف معينة في جميع الدول تقريبا، مثلما هو الأمر بالنسبة للمشرع الجزائري في المادة 04 [1] في الفقرة" ج "من القانون 04/09 أجاز النص استثناء المراقبة الالكترونية للوصول إلى الحقيقة واشترط أن تكون هي الحل الوحيد للوصول إلى الحقيقة.

[1] تنص المادة 04 من القانون 04/09 الفقرة ج: استثناء المراقبة الالكترونية للوصول إلى الحقيقة واشترط أن تكون هي الحل الوحيد للوصول إلى الحقيقة.

-ثالثا :الخبرة.

تعتبر الخبرة أمرا لا مناص منه خاصة في مثل هذا النوع من الجريمة لأنها ذات طابع تقني وفني متطور[1] ومتغير يتطلب من الخبير اشتقاقها و كشف أنماطها في هذا المجال الفني و التقني والذي يحتاج مهارات عالية منه، ولطالما تم ندب هؤلاء الخبراء من طرف القضاة للاستعانة بهم في أمور فنية تتطلب خبرة خاصة.

وتعتبر الخبرة وسيلة تفسير الأدلة داخل النظام المعلوماتي بالاستعانة بالمعلومات العلمية ، ومن الأمور التي تميز بها الخبرة كذلك المهارة في كشف الجريمة المعلوماتية والخبرة المطلوبة من أجل إثبات هذه الجريمة يجب أن تكون من نوع خاص يتماشى وخصوصية الجريمة المعلوماتية وقد تعمل بعض البلدان على إعادة تأهيل بعض ما يسمى بالمجرمين المعلوماتيين من أجل الاستفادة من خبراتهم في الاختراق، ويجب أن يتوفر الخبير على مؤهلات عالية فنية بالأمور التقنية المتعلقة بالكمبيوتر، معرفة شاملة لشبكة الانترنت، التعامل مع الجريمة التي خلفتها التقنية الحديثة، كيفية عزل النظام المعلوماتي والحفاظ على الأدلة دون تلف.

ويشير الفقه الجنائي إلى أهمية الخبرة في التحقيق في الجريمة المعلوماتية والكشف عنها إذ تستعين أجهزة العدالة الجنائية الشرطة وسلطات التحقيق والمحاكمة بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الالكتروني، وذلك بغرض كشف غموض الجريمة أو تجميع أدلتها والمحافظة عليها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات ومن بعض النماذج التي يستعمل فيها المجرمين في مكافحة الجريمة الإلكترونية نجد الولايات المتحدة الأمريكية التي تقوم بإعادة دمج المجرم المعلوماتي في المجتمع ومحاولة الإستفادة منه ومن خبرته في هذا المجال.

[1] رابحي عزيزة ، المرجع السابق، الصفحة 282-285.

وتبرز أهمية الخيرة كذلك في التحقيق في الجريمة المعلوماتية والكشف عنها إذ تستعين أجهزة العدالة[1] الجنائية الشرطة وسلطات التحقيق والمحاكمة بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الالكتروني، وذلك بغرض كشف غموض الجريمة أو تجميع أدلتها والمحافظة عليها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات.

وتكمن أهميتها في المساعدة لسائر السلطات المختصة (سلطات الإستدلال و التحقيق[2]والمحاكمة) بالدعوى العمومية لتحقيق العدالة ، لذا فقد اهتم المشرع الجزائري بالخبراء ومساعدتهم لجهات التحقيق المختلفة ، خاصة في مجال استخلاص دليل إثبات جرائم الاعتداء على نظم المعلوماتية، فهي تتعلق بمسائل فنية معقدة ، والتطور في أساليب ارتكابها سريع ومتطور، والتي لا يكشف غموضها إلا متخصص وعلى درجة كبيرة من التميز في مجال.

– رابعا: تدريب الكوادر .

أضحى إدماج الكوادر على مستوى الوطن لمواجهة الجريمة الإلكترونية ظرورة لا بد منها نظرا لطبيعة[3] الجريمة الإلكترونية وخطورتها ولابد من توفر كفاءات ذوي معرفة خاصة بالوسائل التقنية والحاسبات الآلية ولا تتحقق هذه المعرفة التقنية إلا بتدريب القائمين على أعمال التحري، والمباشرين للتحقيق في مجال الجرائم المعلوماتية بصفة عامة، ونلاحظ أن الجزائر قد بدأت بخطوات متقدمة في تطوير هذا المجال فمثلا على مستوى جهاز الشرطة أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بالجزائر العاصمة ومخبرين جهويين في كل من قسنطينة ووهران، أما على مستوى الدرك الوطني فإنه يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية.

1 المرجع نفسه، الصفحة 271

[2] مليابي عبد الوهاب، المرجع السابق، الصفحة 312

[3] رابحي عزيزة ، المرجع السابق، الصفحة 274/173

لابد وأن تسعى الأجهزة الأمنية المعنية بالتحقيق إلى استقطاب المتخصصين والكفاءات في المجال المعلوماتي وضمهم إليها ليكونوا ضمن كوادرها والاستفادة منهم ومن أجل ذلك ينبغي على كليات الشرطة من جهة أن تقوم بدمج دفعات من الجامعين من خريجي كليات الحاسبات الآلية لتخرجهم ضباطاً مؤهلين قانونيا وتقنيا، كذلك يتعين على الكليات المعينة بتدريس القانون أن تسعى جاهدة إلى تدريس الحاسبات الآلية وكل ما يتعلق به إلى الطلبة ، لأن من شأن ذلك أن تتكون لدي خريجي هذه الكليات ثقافة قانونية وثقافة حاسوبية

ويجب أن يشتمل التدريب على كيفية تشغيل الحاسبات وكل الوسائل الالكترونية وكذلك التعرف على أنواعها ونظمها المختلفة، لاكتساب مهارات ومعارف في هذا المجال ، والمعالجة الإلكترونية للمعطيات في الجرائم التي تقع على الأنظمة المعلوماتية، أو تستخدم الحاسبات وسيلة لارتكابها، وأساليب ارتكاب هذا النوع من الجرائم، فضلا عن أمن المعلومات ووسائل اختراقها، مع دراسة سابقة سلفا لإكتساب الخبرة وكيف تم مواجهتها.

ومن أهم المراجع التي نستدل بها في مجال إدماج الكوادر نجد في هرمها الإتحاد الأوروبي الذي يتمتع بتجربة في مجال التدريب على مكافحة الجرائم المعلوماتية حيث يعتبر هذا الأخير من أهم الجهات التي قامت بالمشروعات والبرامج التدريبية الهادفة لمكافحة الجرائم عالية التقنية من خلال أحد مؤسساتها وهو مركز التدريب الوطني.

وكذلك نجد في بعض الدول يقومون بإرسال أعضاء النيابة العامة من مختلف الدرجات في برامج خارجية وذلك بالتعاون مع أجهزة النيابة العامة في الدول الأخرى والهيئات الدولية بهدف الإطلاع على أحدث النظم المقارنة. وقد يتم التعاون الدولي في مجال تدريب الكوادر من خلال عقد ندوات ومؤتمرات أو ورش العمل الجماعي، متخصصة في مواجهة تلك الجرائم تعقد على المستوى الدولي أو الإقليمي، حيث تقدم هذه الفعاليات العلمية من أبحاثها ودراستها وموضوعات محاورها الضوء على المستجدات المتعلقة بالجرائم المستحدثة من خلال تحليل ومناقشة أبعادها

بعقلية ناجحة مما يمكن المعنيين بالوقاية ومكافحة هذه الجرائم من التعرف على أساليب ارتكابها وأخطارها ووسائل الوقاية بأساليب تتناسب وتفوق أساليب ووسائل مرتكبيها، وعلى هامش هذه المؤتمرات أو الندوات أو ورش العمل الجماعي تعقد اللقاءات وتبادل الآراء. والخبرات وباعتبار أن التعاون الدولي يتحقق في مجال تدريب الكوادر العاملين في أجهزة العدالة الجزائية والمعنيين بمكافحة الجريمة على المستوى الدولي، ومنه يمكننا القول أن هذه الصورة تعد الأكثر تطورا للتعاون الدولي ونلاحظ أن الجزائر بدأت مؤخرا بإرسال كفاءاتها إلى الخارج للتكون في مجال مكافحة الجرائم الإلكترونية على مستوى أجهزة الدرك الوطني.

– خامسا: التسرب .

لقد نص المشرع الجزائري على إجراء التسرب كآلية لردع العديد من الجرائم المستحدثة من بينها[1] الجرائم الإلكترونية في ميدان التحقيق بموجب القانون 22/06[2] المعدل لقانون الإجراءات الجزائية حيث خصص له الفصل الخامس من الباب الثاني تحت عنوان " التسرب".

وتناول من خلال هذه المواد مفهوم عملية التسرب وشروطها وإجراءاتها فأصبح لوكيل الجمهورية ولقاضي التحقيق بعد إخطار وكيل الجمهورية صلاحية منح الإذن بإجراء عملية التسرب لأجل مراقبة الأشخاص لإيهامهم من قبل المتسرب بأنه فاعل معهم أو شريك، وذلك بموجب المواد من 65 مكرر 11 إلى المادة 65مكرر 18 .

وقد عرف المشرع الجزائري عملية التسرب من خلال المادة 65 مكرر 12 [3]

---

1 رابحي عزيزة ، المرجع السابق، الصفحة 296/295

2 القانون رقم 22/06 المؤرخ في 2006/09/20 ، المعدل والمتمم لقانون الإجراءات الجزائية ،

[3] المادة 65 مكرر 12 من القانون رقم 22/06 تنص على :" يقصد بالتسرب قيام ضباط أوعون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف."

كما سمحت الفقرة الثانية من المادة 65 مكرر 12 أن يستعمل لغرض إجراء التسرب هوية مستعارة[1] أو أن يرتكب عند الضرورة الأفعال المنصوص عليها في المادة 65 مكرر 14 وهذه الأفعال هي:

- إقتناء أو نقل أو حيازة أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.

- إستعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال.

كما يجب أن يكون الإذن بالتسرب مكتوبا ولا يمكن القيام به دون المرور على الجهاز القضائي[2] طبقا لنص المادة 65 مكرر 15 من قانون الإجراءات الجزائية بقولها " يجب أن يكون الإذن المسلم طبقا للمادة (65 مكرر 11) أعلاه مكتوبا ... تحت طائلة البطلان".

كما تتجسد صور عملية التسرب في نطاق جرائم الاعتداء على نظم المعلوماتية في دخول ضابط أو عون الشرطة القضائية إلى البيئة الافتراضية واشتراكه مثلا في محادثات غرف الدردشة أو حلقات النقاش والاتصال المباشرة في كيفية قيام أحدهم باختراق شبكات أو بث الفيروسات مستخدما في ذلك أسماء وصفات هيئات مستعارة ووهمية كما لو كان فاعل مثلهم لاستفادة منهم حول كيفية اقتحام الهاكر لموقع ما مثلا .

ويعد إجراء التسرب من أخطر الإجراءات انتهاكا لحرمة الحياة الخاصة للمتهم لذا فقد أحاط المشرع جملة من الضمانات التي يتعين مراعاتها عندما تقتضي ضرورات التحري أو التحقيق وعملا بمبدأ الشرعية يجب أن تتوفر في هذا الإجراء الإذن وهذا ما نصّت عليه المادة 65 مكرر 11 من قانون الإجراءات الجزائية كما يلي .... " يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار

[1] العاقل فريال، مرجع سابق، الصفحة 80/79

[2] مليايي عبد الوهاب، المرجع السابق، الصفحة 318/317

وكيل الجمهورية، أن يأذن تحت "... فالجهة المختصة لإصداره كما هو مبين من نص المادة إما وكيل الجمهورية أو قاضي التحقيق وذلك حماية للحقوق الأساسية المكرسة دستوريا.

ويجب التنويه على أن عملية التسرب لا يمكن أن تتجاوز 4 أشهر إلا إذا وجدت ضرورة لمقتضيات التحري أو التحقيق، ويجوز للقاضي الذي رخص بإجرائه بأن يأمر في أي وقت بوقفه قبل انقضاء هذه المدة.

وإذا تقرر وقف عملية التسرب وفي حالة عدم تمديدها يمكن للعون المتسرب مواصلة نشاطاته للوقت الضروري الكافي لتوقيف المراقبة في ظروف تضمن أمنه، دون أن يكون مسؤولاً جزائياً..، على ألا يتجاوز ذلك مدة أشهر.

– الفرع الثاني: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

أحدثت الجرائم الإلكترونية طوارئ ان صح التعبير في أجهزة القضاء وأجهزة الضبط القضائي[1] والتحقيق، ولذلك تعالت الأصوات بضرورة إنشاء أجهزة خاصة بهذه الجرائم تختلف تماماً عن الضبط العادية، الأمر الذي يمكنها من التحري والاستدلال في العالم الافتراضي ومطاردة المجرمين في البيئة الالكترونية .

وهو ما جعل اتفاقية بودابيست للإجرام المعلوماتي تنادى بضرورة إنشاء مثل هذه الأجهزة على المستوى الوطني وسن الإجراءات التشريعية اللازمة لذلك ومن هذه النماذج نجد الولايات المتحدة الأمريكية قد تبنت هذا المنهج وأحدثت عدة جهات متخصصة لمتابعة جرائم الانترنت و نذكر منها :

– المكتب المركزي لمكافحة المرتبطة بتكنولوجيا المعلومات و الإتصالات .

– قسم جرائم الحاسوب وجرائم حقوق الملكية الفكرية ت إنشاؤه سنة

– معهد امن الحواسيب.

[1] د/بوقرين – مداخلة : المؤتمر العلمي الأول لمكافحة الجريمة الإلكترونية الرياض المملكة العربية السعودية، مرجع سابق .

- وحدة جرائم الانترنيت .

- مكتب رئيس التكنولوجيا .

كما قام مكتب التحقيقات الفدرالي بالاشتراك مع المركز الوطني بإنشاء مركزاً لتلقي الشكاوى من الإحتيال الإلكتروني وتلي ذلك إنشاء وكالة تابعة لمكتب التحقيق الفدرالي تهدف إلى التنسيق في مكافحة القرصنة المعلوماتية .

ونجد أن المشرع الجزائري قد نظم الجرائم الواقعة في بيئة الأعمال الإلكترونية بموجب القانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والتي من شأنها تنظيم الجانب الإجرائي به هي المنصوص ولكنه لم يحدث جهة تختص بالجرائم الإلكترونية رغم حداثة هذا القانون وجعل مسألة التفتيش المذكورة في المادة 05 من هذا القانون تختص به الجهات المنصوص عليها في القواعد العامة.

وهذا ما يدل على نقص الخبرة والكفاءة في مجال مكافحة الجريمة الإلكترونية في الدولة الجزائرية و في إطار مسايرت الحكومة الجزائرية للتطور التكنولوجي والعولمة بدأت في تكوين فرق للدرك والشرطة في التكوين في الخارج خاصة فرنسا ويتم المناداة على إستحداث سلطة قضائية لهذا النوع من الجرائم من خلال الندوات والأيام الدراسية . وقد أنشأ المشرع الجزائري هيئة وطنية خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و أحال على التنظيم لبيان الهياكل البشرية والقاعدية لهذه الهيئة وتتمثل مهمتها في تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريمها، بما في ذلك جمع المعلومات وإجراء الخبرة، كما تعمل الهيئة على تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريمها، بما في ذلك جمع المعلومات وإجراء الخبرة، كما تعمل الهيئة على نطاق دولي في تبادل المعلومات مع نظيراتها في سبيل التعرف على مرتكبي هذه الجرائم...،

ورغم الكل الجهود المبذولة من قبل هذه الهيئة إلا أن المشرع لم يستطع بعد إدراك هذا الكم الهائل من التطور الناتج على هذا النوع من الجرائم لذلك من الضروري الإسراع في تكوين فرق متخصصة للبحث والتحري في مثل هذه الجرائم.

– المطلب الثاني : الجرائم التي تتم باستخدام الحواسب الآلية ونظم المعلومات:

– الفرع الأول: الإعتداء على سرية الخطابات والمراسلات الخاصة.

تعتبر جريمة الإعتداء على حرمة الحياة الخاصة من أخطر الجرائم الواقعة على النظم المعلوماتية نظرا[1] لجديتها وسهولة إرتكابها في ظل عدم وجود حماية قانونية فعالة ورادعة لمثل هذه الجرائم التي تتميز بمرونتها ومهارة مرتكبيها في إستعمال الحاسبات الآلية .

وتندرج هذه الجريمة تحت عدة صور منها :

التنصت أو التسجيل، أو نقل لحديث صدر عن شخص أو مراسلة دون رضاه بواسطة جهاز معين، أو إلتقاط أو نقل صورة شخص تواجد في مكان معين دون رضاه.

ومن الطرق التي تتم في الإنترنت للتنصت على الآخرين استخدام برنامج معين يقوم بفتح منفذ في جهاز الشخص المعتدى عليه عن طريق البريد الالكتروني، أو عن طريق مواقع مغرية يمكن من خلاله الاطلاع والاستماع إلى جميع المحادثات والمراسلات الصادرة منه (المعتدى عليه).

وتزداد خطورة هذه الجريمة إذا ما قام المعتدي بعد إنتهاكه للمعتدي عليه بنشر التسجيل على العامة من الناس الذي يتعاملون بالإنترنت ، ونرى أن يتم التعاون دوليا لوضع بروتوكولات وأن يتم عقد إتفاقيات دولية للتسليم في جرائم إنتهاك الخصوصية، وأن لا تخضع مثل هذه الجرائم للتقادم سواء للدعوى أو للعقوبة .

[1] محمد نصر محمد ، **المسئولية الجنائية لإنتهاك الخصوصية المعلوماتية** ، مركز الدراسات العربية ، الطبعة الأولى ، مصر، 2016، الصفحة 41

وسنعرض لذلك من خلال التالي:

أولا: التشهير بالأشخاص التشهير في اللغة، مأخوذ من شهره، بمعنى: أعلنه وأذاعه، وشهر[1] به: أذاع عنه السوء.

والأصل أن تشهير الناس بعضهم ببعض بذكر عيوبهم ومثالبهم والتنقص منهم حرام، فإذا كان المشهر به بريئا مما يشاع عنه ويقال فيه، فإن التشهير به محرم لقول الله تعالى : (إن الذين يحبون أن تشيع الفاحشة في الذين آمنوا لهم عذاب أليم في الدنيا والآخرة والله يعلم وأنتم لا تعلمون) ، ولقد قال النبي صلى الله عليه وسلم: (أيها رجل أشاع على رجل مسلم كلمة وهو منها بريء، يرى أن يشينه بها في الدنيا، كان حقا على الله تعالى أن يرميه بها في النار).

وقد ذم الله عز وجل الذين يفعلون ذلك، وتوعدهم بالعذاب الأليم قال ابن كثير (ه) في قول الله تعالى : (والذين يؤذون المؤمنين والمؤمنات بغير ما اكتسبوا فقد احتملوا بهتانا وإثما مبينا): أي ينسبون إليهم ما هم برآء منه لم يعملوه و لم يفعلوه، يحكون عن المؤمنين والمؤمنات ذلك على سبيل العيب والتنقص منهم، حدثنا أحمد بن سلمة، حدثنا أبو كريب، حدثنا معاوية بن هشام، عن عمران بن أنس، عن ابن أبي مليكة، عن عائشة، قال: قال رسول الله لأصحابه :"أي الربا أربى عند الله ؟"، قالوا: الله ورسوله أعلم قال: " أربى الربا عند الله استحلال عرض امرئ مسلم ، ثم قرأ: (والذين يؤذون المؤمنين والمؤمنات بغير ما اكتسبوا فقد احتملوا بهتانا وإثما مبينا) وقد قيل في معنى قول النبي : (من سمع، سمع الله به) أي من سمع بعيوب الناس وأذاعها أظهر الله عيوبه .

حتى وإن كان المشهر به يتصف بها يقال عنه ولكنه لا يجاهر به، ولا يقع به ضرر على غيره، فالتشهير به حرام لأنه من الغيبة التي نهى الله سبحانه وتعالى عنها في قوله: (يا أيها الذين آمنوا اجتنبوا كثيرا من الظن إن بعض الظن إثم ولا تجسسوا ولا يغتب بعضكم بعضا أيحب أحدكم أن يأكل لحم أخيه ميتا فكرهتموه واتقوا الله إن الله تواب رحيم) ، ومن المقرر شرعا أ الستر على

[1] المرجع نفسه ، الصفحة 43.

المسلم واجب لمن ليس معروفا بالأذى والفساد، فقد قال النبي صلى الله عليه وسلم : (من ستر مسلما ستره الله عز وجل يوم القيامة).

أما إن كان التشهير على سبيل النصيحة للمسلمين وتحذيرهم، كجرح الرواة والتحذير من أرباب البدع والتصانيف المضلة لئلا يغتر بهم، فلي الستر هنا بمرغوب فيه ولا مباح)، فأرباب البدع والتصانيف المضلة ينب أن يشتهر في الناس فسادها وعيبها، وأنهم على غير الصواب، ليحذرها الن فلا يقعوا فيها، بشرط أن لا يتعدى فيها الصدق، ولا يفتري على أهلها .

ثانيا :حماية المعلومات غير المعلنة.

إن هذه الشبكة مع حداثتها فإن عدد المستخدمين قد بلغ مطلع 2002م أكثر من 2133 مليون[1] مستخدم على مستوى العالم.

ولا يعني الإستخدام مجرد الولوج إلى المعلومات المتاحة فقط، بل إختراق المواقع غير المتاحة أو التعدي إلى البرامج المحمية طبقا للأنظمة الخاصة بحماية الملكية الفكرية.

– الفرع ثاني : جريمة غسيل الأموال المرتكبة عن طريق الإنترنت أو عن طريق الحاسب الآلي

يعرف غسيل الأموال بأنه أي عملية من شأنها إخفاء المصدر الغير المشروع الذي اكتسبت منه[2] الأموال وتتعدد عدة مصطلحات لهذه الجريمة ومن مرادفاتها تبييض الأموال أو تطهير الأموال وتنظيف الأموال، وتنصب في معنى واحد.

ولا تقتصر جريمة غسل الأموال الإتجار بالمواد المخدرة كما يعتقد البعض إذ أنه يشمل كل عمل الأموال سواء كان أصلها من المخدرات أو أي أمر آخر غير مشروع.

1 محمد نصر محمد مرجع سابق ، الصفحة 47.

2 عبد العزيز بن غرم الله آل جار الله ، **جرائم الإنترنت وعقوباتها** ، دار الكتاب الجامعي ، الطبعة الأولى ، السعودية، 2017، الصفحة 276 .

وقد ظهر هذا المصطلح وإنبثق أولا من الولايات المتحدة الأمريكية وهي إلى اليوم تعد من الجرائم المستحدثة والأحدث منه هو إرتكابها على الأنترنت وأجهزة الكمبيوتر وتنسب هذه الجريمة إلى مؤسسات الغسيل التي تمتلكها المافيا في أمريكا، وهي مؤسسات نقدية كان يتاح فيها مزج الإيرادات المشروعة وغير المشروعة إلى حد تظهر عنده كل الإيرادات وكأنها مستحصلة من مصدر مشروع، فيقوم صاحب الجريمة بممارسة بعض الأنشطة المشروعة كشراء الذهب أو العقارات والمنقولات وبيعها ، ليقطع كل صلة له بأصل المال غير المشروع وصورته المعروفة أمام المجتمع.

وقد تطورت عمليات غسيل الأموال، وأصبحت أكثر تعقيدا، واستخدمت أحدث الوسائل التكنولوجية والخداعية لإخفاء طابع الأموال، أو مصادرها أو استخدامها الحقيقي.

فمن ذلك أنه أصبحت البنوك من وسائل غسيل الأموال، خاصة بنوك الإنترنت أو ما يسمى بمقدمي خدمة الكارت الذهبي، والتي يستطيع من خلالها العميل أن يقوم بتحويل أي مبالغ مع استحالة مراقبته أو كشفه، أو تتبعه في أي بنك على مستوى العالم.

– الفرع الثالث : جريمة إنتحال الشخصية المرتكبة عن طريق الإنترنت.

تتمثل جريمة انتحال الشخصية في استخدام شخص هوية شخص آخر بطريقة غير شرعية، إما[1] لغرض ومن هوية الضحية أو لإخفاء هوية شخصية المجرم ، وتعتبر هذه الجرائم الأكثر شيوعا على شبكة الأنترنت نظرا لسهولة إرتكابها.

ولذلك بدأت العديد من المؤسسات والشركات التجارية الإعتماد على وسائل متينة لتوثيق الهوية كالتوقيع الرقمي والتي تجعل من الصعب إرتكاب هذه الجريمة ويتخذ إنتحال الشخصية لشبكات الإنترنت صورة متعددة ، فقد تكون صورة هذا الفعل انتحال شخصية فرد كما يمكن أن يكون انتحال هوية موقع، وانتحال شخصية الأفراد يتم عبر بعض المعلومات المتعلقة بشخص ما، وغالبا ما تكون شخصية مشهورة أ للوصول إلى أغراض أهداف متعددة فمثلا قد يستطيع

1 عبد العزيز بن غرم الله آل جار الله ، المرجع السابق ، الصفحة 309-311

الشخص أن يجد الرقم السري للبطاقة الائتمانية أو للبريد الإلكتروني أو لإدارة موقع ، أو حتى اسم المستخدم ورقم السري للتحدث باسم هذا الشخص المشهور معلومات أو تصريحات خاطئة الغرض منها الإضرار بهذا الشخص في ماله

وقد لا يكون الغرض هو السرقة بقدر ما يكون تشويه سمعة ذلك الشخص ويكون ذلك بإرسال رسالة من بريده الإلكتروني إلى مديره العام مثلا والقيام بسبه وشتمه والتنقص منه، وقد يكون الانتحال بإرسال بلاغ وهمي للسلطات للوشاية بهذا الشخص المرسل.

– الفرع الرابع : جرائم الإختراق والتسلل عبر الإنترنت.

الاختراق: هو مجموعة من الأعمال التي تؤدي إلى الإخلال بنظام وسرية الجهاز. ويقوم بالاختراق[1] شخص أو أكثر عن طريق شبكة الإنترنت باستخدام برامج متخصصة تعمل على فك الرموز والكلمات السرية، التسلل هو : السلوك المصاحب لهذا الفعل وتتعدد صور الإختراق في عدة أوجه منها الإختراق الموجه نحو البريد الإلكتروني، وقد يكون اختراقا لمواقع، وأكثر الاختراقات شيوعا هو اختراق الأجهزة الشخصية، فيما يعد أشدها خطورة اختراق الشبكات وقوا البيانات الحساسة. ويهدف الإختراق في أغلب الحالات إلى اختراق الأجهزة الشخصية للتطفل والعبث بمحتوياتها، وقد يمتد غرض المخترق إلى أبعد من مجرد التطفل والفضول إلى قصد سرقة محتويات الجهاز واشتراك الإنترنت الخاص بالمستخدم.

ومن الإجراءات الوقائية التي يوصى بها لتجنب الاختراق هي إخفاء الملفات وإغلاقها بكلمات سرية[2] وعدم ترك أي ملفات مهمة على الجهاز، بل تحفظ في اسطوانة خارجية وتشغل عند الحاجة، فلا يجد المخترقون إليها سبيلا .لكن ليس هذا بالحل المثل لأنه كفيل بتجريد المستخدم من منافع الحاسب الآلي.

[1] كتاب عبد العزيز بن غرم الله آل جار الله ، المرجع السابق، الصفحة 206/205.

[2] رابحي عزيزة ، المرجع السابق، ص 119/118

– الفرع الخامس : جرائم الإرهاب والجريمة المنظمة المرتكبة عن طريق الإنترنت.

لم تتفق التشريعات العالمية على إيجاد تعريفا موحد للإرهاب فقد عرف الإرهاب بتعريفات كثيرة من[1] أمثلها : أنه إستراتيجية عنف منظم ومتصل تمارسه دولة أو مجموعة سياسية ضد دولة أو مجموعة سياسية أخرى من خلال جملة من أعمال القتل والاغتيال، وخطف الطائرات واحتجاز الرهائن وزرع المتفجرات أو ما شابه ذلك من أفعال، أو التهديد بها، وذلك لإيجاد حالة من الرعب العام بقصد تحقيق أهداف سياسية.

ومن الأمثلة التي يذكرها خبراء الأمن ومكافحة الإرهاب جرائم الإرهاب الإلكتروني التي يمكن أن تصل إلى جهات حيوية بالغة الحساسية في المجتمع كأن يقوم الإرهابيين بالدخول على أنظمة المصانع الدوائية مثلا لتحريف المعادلات الطبية أو بالدخول على مصانع حليب الأطفال لتغيير نسب الحديد، ذلك .

– الفرع السادس : جريمتي التزوير والإختلاس عبر الإنترنت.

1/– **جريمتي التزوير:** تنتشر على شبكة الإنترنت الكثير من جرائم العدوان على المال ومن جرائم[2] التزوير والاختلاس والاحتيال في سبيل تحصيل كل منهما، ويوما بعد آخر يكتشف المسئولون في دول العالم صورا وأنواعا مستجدة في كيفية ارتكاب الجرائم مستغلة تقدم التقنية، وتنوع استخداماتها.

ومن أكثر الجرائم شيوعا في مجال التزوير نجد التزوير في بيانات الحاسب الآلي لأنه لا تكاد تخلو جريمة من جرائم أنظمة المعلومات من عملية تزوير للبيانات بشكل أو بآخر ويتم هذا التزوير إما بإدخال بيانات مغلوطة إلى قواعد البيانات، أو بتعديل البيانات الموجودة عمدا بهدف ارتكاب

[1] كتاب عبد العزيز بن غرم الله آل جار الله ، المرجع السابق، الصفحة 196/194

[2] كتاب عبد العزيز بن غرم الله آل جار الله ، المرجع السابق، الصفحة 181/179/178.

جريمة من جرائم نظم المعلومات المتنوعة. ويعد الموظفون هم الشريحة الأكثر إرتكابا لهذه الجريمة لسهولة وصولهم إليها .

2/- **جريمة الإختلاس** : أما في ما يخص الإختلاس فهي معروفة منذ القدم وموجودة حتى في هذا العصر الحديث فمن الوسائل التقنية الحديثة للاختلاس استخدام الحاسب في التلاعب بالبيانات إما بإدخال أسماء ومعلومات زائفة للتمويه وفتح حسابات لهؤلاء الأشخاص الوهميين وتحويل الأموال إليها، أو بالتلاعب بالبرامج لصالح المتحايل، ويحدث ذلك مثلا بإدخال بيانات زائفة لاصطناع دائنين معينين وجعل الأموال المختلسة كأموال يجب دفعها لهم بحكم المديونية، أو بصنع فواتير يجب سدادها، وأخذ الأموال التي ترصد لها.

- الفرع السابع : جرائم النصب والإحتيال المرتكبة عبر الإنترنت.

تعتبر جرائم النصب والاحتيال من قبيل جرائم العدوان على المال، والتي تعتمد على الحيلة والدهاء[1] وتتنوع لتشمل عدة صور نذكر منها :

- **النصب والاحتيال على العملاء:** هو الفعل الذي يقوم على التلاعب في نظم المعالجة الآلية للمعلومات بهدف الحصول على خدمات أو أموال أو أصول معينة دون وجه حق.

ومن جرائم الاحتيال والنصب على العملاء تلك المواقع الموجودة على شبكة الإنترنت الخاصة بالمزادات والتي تعرض منتجات بأسعار منخفضة جدا، وبعد أن يقرر مشاهدو هذه المنتجات اقتناءها ويرسلوا أرقام بطاقات الائتمان أو شيكات تختفي هذه المواقع .

- **التهديد والإبتزاز** : يقصد بالابتزاز ما يمارسه بعض المحتالين من مجرمي الإنترنت من تخويف وتهديد لكي يجبروا الضحية سواء كان فردا أو شركة أو حكومة للخضوع لمطالبهم وغالبا ما تكون مطالب المبتزين هي المال،

[1] كتاب عبد العزيز بن غرم الله آل جار الله ، المرجع السابق، الصفحة 150-153

- **التهرب الضريبي** : صورة التهرب الضريبي عن طريق الإنترنت أن البائع والمشتري في التجارة الإلكترونية يخفون تعاملاتهم عن مصلحة الضرائب ويدلون بمعلومات كاذبة ذات قيم منخفضة لأنهم بذلك يجعلون مأمور الضرائب لا يعلم عن حجم التعامل الحقيقي الممول التي يتم على أساسها حساب قيمة الضريبة المستحقة بشكل حقيقي.

– الفرع الثامن: تجريم وعقوبة التجسس وإنتهاك حرمة الحياة الخاصة على الإنترنت.

تستطيع شبكة الإنترنت أن توفر للمستخدم العابث تسهيلات كبيرة أدت إلى تخطي الخصوصية من[1] قبل مجرمي الإنترنت والإعتداء على الحياة الخاصة بالأفراد كانوا أو شركات ونذكر أهم أنواع التجسس و هي:

- **التجسس على أجهزة المستخدمين أو الشبكات ذات الخصوصية:**

تمتلئ البيئة الإلكترونية بالعديد من ببرامج التجسس التي تزرع في أجهزة المستخدمين دون شعور منهم، وتأتيهم إما عن طريق البريد الإلكتروني، أو عند تحميل بعض البرامج المجانية، وغير ذلك ولعل من أشرس هذه البرامج برنامج طروادة الذي ينقل كل المعلومات المطلوبة من الضحية إلى من أرسله من الجناة، بل إنه يلتصق بالجهاز إلى الحد الذي يؤدي فيه حذفه من الجهاز إلى حذف البرنامج التشغيلي للجهاز نفسه، وما ينتج عن ذلك من أضرار جسيمة.

- **نشر المعلومات الخاصة والتشهير بأصحابها :**

يشكل ما يتم الحصول عليه من معلومات بطريق التجسس جريمة، كما أن نشر هذه المعلومات على شبكة الإنترنت أخرى مستقلة، ويدخل في هذه الجريمة التهديد بإفشاء الأسرار والمعلومات فيه مساس خطير بحق الأفراد في الحياة الخاصة إذ أن الضرر المترتب عليها قد لا يقتصر على مجرد الإزعاج والمضايقة العارضة، بل قد يمتد إلى أن يشوه سمعة هذا الشخص ويقضي على مستقبله.

[1] المرجع نفسه، ص138-141.

- **التجسس العسكري :**

كما يمس التجسس الأفراد فإنه يمس الحكومات والشركات بصورة أكبر، وتصرح العديد من الدول الكبيرة كروسيا وأمريكا بخشيتها من تجسس الدول بعضها على بعض بما قد يؤدي لإشعال حرب معلوماتية فادحة الخسائر في نفس الوقت التي تبسط فيه هذه الدول هيمنتها التقنية على دول العالم بشبكة تجسسية واسعة النطاق .

وعلى النطاق الصناعي فإن الشركات والمنشئات الصناعية تلاقي الأمرين؛ فهي من جهة لا تستطيع الحفاظ على وثائقها السرية ومن جهة أخرى لا تستطيع حتى التذمر والشكوى لدى الجهات الرقابية خوفا من تشويه سمعتها لدى عملائها.

- **اعتراض الرسائل والمعلومات**

يقصد باعتراض الرسائل والمعلومات، ما يقوم به البعض من التعرض الرسائل البريد الإلكتروني لمنع وصولها أو الإطلاع على تلك الرسائل قبل إرسالها .[1]

[1] المرجع نفسه، ص138-141.

– المبحث الثاني : الإجراءات القانونية في متابعة الجرائم المعلوماتية على النطاق الدولي.

إن ما تتميز به الجرائم المعلوماتية من سرعة التنفيذ وحداثة الأسلوب وأنها عابرة للحدود وأنها ذات[1] طبيعة عالمية وهذا أمر طبيعي خاصة إذا ما علمنا أن شبكة الإنترنت ذاتها لا تعرف الحدود كما أن هذا النشاط الإجرامي لم يعد قاصرا على إقليم معين بل أمتد إلى أكثر من إقليم، بحيث بات المجرم يشرع في التحضير لارتكاب جريمته في بلد معين، يشرع في التنفيذ في بلد آخر ويهرب إلى بلد ثالث.

أصبح لا مناص من البحث عن وسيلة أخرى تساعد على إيجاد تعاون دولي يتفق مع طبيعة هذا[2] النوع المستحدث من الجرائم ويخفف من غلو الفوارق بين الأنظمة العقابية الداخلة ، وتتمثل هذه الوسيلة في تحديث التشريعات المحلية المعنية بالجرائم المعلوماتية و إبرام اتفاقيات خاصة يراعى فيها هذا النوع من الجرائم وضرورة القضاء على الصعوبات التي تواجه التعاون الدولي فيما يتعلق بالعقبة الأولى المتمثلة في عدم وجود نموذج موحد للنشاط الإجرامي فإن الأمر يقتضي توحيد هذه النظم القانونية.

ولقد أثبت الواقع العملي أن – أي دولة – لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا[3] التطور الملموس والمذهل في كافة ميادين الحياة، فنتيجة للتطور المذهل في الاتصالات وتكنولوجيا المعلومات أدى إلى ظهور أشكال وأنماط جديدة من الجرائم منها الجرائم المتعلقة بشبكة الإنترنت التي باتت تشكل خطرا لا على سرية النظم الحاسوبية أو سلامتها.

[1] رابحي عزيزة ، مرجع سابق، الصفحة 302

[2] كتاب أمير فرج يوسف، مرجع سابق، الصفحة 419

[3] كتاب محمد نصر محمد، مرجع سابق، الصفحة 111.

وتظهر مشكلة الإختلاف بين التشريعات الإجرائية في دول العالم ومنها الجهات المختصة بالتفتيش[1] وضرورة مكافحة جرائم المعلوماتية تقتضي إذا توحيد التشريعات الإجرائية وهو أمر يستحيل تحقيقه لذلك فضرورة تحقيق تعاون دولي أمر لا مناص منه ولابد من إبرام إتفاقيات دولية خاصة بمكافحة هذا النوع من الجرائم.

– المطلب الأول: التعاون الدولي في مجال مكافحة الجرائم المعلوماتية.

– الفرع الأول : التعاون القضائي الدولي في مكافحة الجرائم المعلوماتية.

التعاون القضائي الدولي هو الآلية الرئيسية للكفاح ضد الجريمة بجميع أطيافها، ويقصد بالتعاون في[2] موضوع دراستنا ما تقدمه سلطات دولة لدولة أخرى من مساعدة وعون في سبيل ملاحقة الجناة والقبض عليهم سواء في التحقيق أو في تسليم المجرمين أو في غيرها من الإجراءات.

وينبع التعاون القضائي من الضرورة ذاتها التي ينبع منها التعاون التشريعي فغالبا ما تقتضي تتبع أثر النشاط الإجرامي من خلال مقدمي خدمات الانترنت أو الشركات المقدمة لتلك الخدمات مع توصيل أجهزة الحاسب الآلي بالأنترنت .وحتى ينجح المحققون في ذلك فعليهم أن يتتبعوا أثر قناة الاتصالات بأجهزة الحاسب الآلي المصدرية والجهاز الخاص بالضحية أو بأجهزة أخرى تعمل مع مقدمي خدمات وسطاء في بلدان مختلفة.

إذ لا يمكن لها أن تتجاوز حدود سلطاتها ويمتنع عليها القيام بأي عمل قضائي أو إجراء جزئي في دولة أخرى إذن لابد من التعاون الدولي.

ومن أهم صور التعاون القضائي نجد :

[1] حسن طوالبة ، (**التعاون القضائي الدولي في مجال مكافحة جرائم الإلكترونية**) ، كلية الحقوق ، جامعة العلوم التطبيقة ، الصفحة 2 .

[2] رابحي عزيزة ، المرجع السابق، الصفحة 303 – 305

– أولا: التعاون الدولي على المستوى الأمني:

لا يمكن تصور مكافحة الجرائم المعلوماتية إلا[1] بوجود تعاون دولي على المستوى الإجرائي الجنائي بحيث يسمح بالإتصال بين أجهزة الشرطة في الإجراء الجنائي ويسمح بالإتصال المباشر بين أجهزة الشرطة في الدول المختلفة . وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالإنترنت وتعميمها فمثلا في جرائم البث والنشر الفيروسي قد يكون مرتكب الهجوم يحمل جنسية دولة ما، ويشن الهجوم الفيروسي من حواسيب موجودة في دولة أخرى ، وتقع الآثار المدمرة لهذا الهجوم في دولة ثالثة فمن البديهي أن تقف مشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها و يستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود لأن جهاز الشرطة في هذه الدولة أو تلك لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابع لها بمعنى آخر أن متى ما فر المجرم خارج حدود الدولة يقف الجهاز الشرطي عاجزا لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بها المهمة وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة.

– ثانيا: جهود المنظمة الدولية للشرطة الجنائية" الإنتربول: "البدايات الأولي للتعاون الدولي[2] الشرطي ترجع إلى عام 1904م عندما تم إبرام الاتفاقية الدولية الخاصة بمكافحة الرقيق الأبيض والتي نصت في مادتها الأولى على "" تتعهد كل الحكومات المتعاقدة بإنشاء أو تعين سلط الجمع المعلومات الخاصة باستخدام النساء والفتيات لغرض الدعارة ف الخارج ، ولهذه السلطة الحق في أن تخاطب مباشرة الإدارة المماثلة لها ف كل الدول الأطراف المتعاقدة ."ولم تمر سنة على إبرام هذه الاتفاقية وكانت سبع دول من الدول المتعاقدة تنشي مثل تلك الأجهزة وتتبادل من خلالها المعلومات والبيانات الخاصة باستخدام النساء والفتيات لغرض الدعارة في الخارج من أجل القضاء

[1] أمير فرج يوسف، المرجع السابق، الصفحة 426/425.

[2] المرجع نفسه ، الصفحة 426-429.

على هذه الجريمة في أقاليمها بعد ذلك أم التعاون الشرطي الدولي يأخذ صورة المؤتمرات الدولية أولها وأسب تاريخيا كان مؤتمر موناكو والذي ضم رجال الشرطة والقضاء والقانون من 14 دولة ، وذلك لمناقشة ووضع أسس التعاون الدولي في بعض المسائل الشرطية ، وتقع الأمانة العامة للأنتربول في ليون بفرنسا، وهي تعمل على مدار الساعة وطوال أيام السنة وللأنتربول ستة مكاتب إقليمية في مختلف أرجاء العالم، ومكتب لتمثيله في مقر الأمم المتحدة في نيويورك، ولكل بلد عضو في الأنتربول مكتب مركزي وطني يعمل فيه موظفوا شرطة وطنيون مؤهلون أفضل تأهيل.

– **ثالثا: تبادل المعاونات لمواجهة الكوارث والأزمات والمواقف الحرجة** : تتعرض كافة دول العالم لإحتمالات وقوع كوارث ضخمة ، الأمر الذي يحتاج إلى تكثيف خاص للجهود والخبرات والإمكانيات بشكل لا يمكن تحقيقه إلا بتضافر الجهود الدولية .

وتعتبر هذه الصورة من أهم صور التعاون الأمني لا سيما أن أجهزة العدالة الجزائية ليست بنفس المستوى والجاهزية بين جميع الدول إذ هنالك تفاوت في ما بينها فبعض الدول متقدمة تكنولوجيا ولها الخبرة في التصدي للجرائم الإلكترونية ومنها الجرائم المتعلقة بالإنترنت تشريعيا وفنيا ، والبعض الآخر تفتقد ذلك . من هنا كان لابد من التعاون بين الدول.

– **رابعا : القيام ببعض الأعمال الشرطية والأمنية المشتركة** : تتمثل في تعقب مجرمي الأنترنت[1] عامة وشبكة الأنترنت خاصة ، وكذا تعقب الأدلة الرقمية وضبطها والقيام بعمليات التفتيش العابرة للحدود لمكونات الحاسب الآلي المنطقية والأنظمة المعلوماتية وشبكات الإتصال بحثا عن ما تحتويه من أدلة على إرتكاب الجريمة المعلوماتية ، كلها أمور تستدعي القيام ببعض العمليات الشرطية والفنية والأمنية المشتركة، وهي من شانها صقل مهارا وخبرات القائمين على مكافحة تلك الجرائم، وبالتالي وضع حد لها.

[1] أمير فرج يوسف، المرجع السابق، الصفحة 429 .

– الفرع الثاني : مركز الشكاوى الخاصة بجرائم الأنترنت في العالم :

يعتبر مركز الشكاوى الخاصة بجرائم الإنترنت في العالم من اهم الأطر المؤسسية لمكافحة جرائم[1] المعلوماتية والانترنت.

فالنظام المعروف باسم (IC3) هو كناية عن نظام تبليغ وإحالة لشكاوي الناس في الولايات المتحدة والعالم أجمع ضد جرائم الإنترنت. ويخدم المركز المشار اليه وعبر استمارة للشكاوي مرسلة على الإنترنت وبواسطة فريق من الموظفين والمحللين، الجمهور ووكالات فرض تطبيق القوانين الأميركية والدولية التي تحقق في جرائم الإنترنت ".

– أولا : هيكلية المركز.

نشأ مركز الشكاوى الخاصة بجرائم الإنترنت كمفهوم سنة 1998 بإدراك ملائم بأن الجريمة بدأت[2] تدخل الإنترنت لأن الأعمال التجارية والمالية كانت قد بدأت تتم عبر الإنترنت، ولأن مكتب التحقيقات الفدرالي أراد أن يكون قادرا على تعقب هذه النشاطات وعلى تطوير تقنيات تحقيق خاصة بجرائم الإنترنت.

ولم يكن هناك آنذاك أي مكان واحد معين يمكن للناس التبليغ فيه عن جرائم الإنترنت، وأراد مكتب التحقيقات الفدرالي التمييز بين جرائم الإنترنت والنشاطات الإجرامية الأخرى .

وقد تم تأسيس أول مكتب للمركز سنة 1999 في مورغانتاون بولاية وست فرجينيا، وسمي مركز شكاوى الاحتيال على الإنترنت. وكان المكتب عبارة عن شراكة بين مكتب التحقيقات الفدرالي والمركز القومي لجرائم موظفي المكاتب، وهذا الأخير مؤسسة لا تبغي الربح متعاقدة مع

[1] عبد الله عبد الكريم عبد الله ، **جرائم المعلوماتية والأنترنت** ، منشورات الحلبي القانونية ، الطبعة الأولى ، لبنان، 2007 ، الصفحة 115.

[2] عبد الله عبد الكريم عبد الله ، المرجع السابق ، الصفحة 116- 118.

وزارة العدل الأميركية مهمتها الأساسية تحسين قدرات موظفي أجهزة تطبيق القانون على صعيد الولاية والصعيد المحلي، على اكتشاف جرائم الإنترنت أو الجرائم الاقتصادية ومعالجة أمرها.

وفي العام 2002، وبغية توضيح نطاق جرائم الإنترنت التي يجري تحليلها، بدءا من الاحتيال البسيط إلى تشكيلة من النشاطات الإجرامية التي أخذت تظهر على الأنترنت أعيدت تسمية المركز وأطلق عليه اسم مركز الشكاوى الخاصة بجرائم الإنترنت أصبح هناك اليوم في مركز الشكاوى ستة موظفين فدراليين وحوالى أربعين محللا من القطاع الأكاديمي وقطاع صناعة الكمبيوتر وبإمكان الناس من كافة أنحاء العالم تقديم شكاوى بواسطة موقع مركز الشكاوى الخاصة بجرائم على الإنترنت.[1]

– ثانيا : نطاق اعمال المركز.

هدف عمليات المركز الرئيسي هو أخذ شكوى المواطن الفرد وضمها إلى المعلومات المبلغ عنها من جانب 100 أو 1000 ضحية أخرى من مختلف أنحاء العالم، فقدت أموالا نتيجة جرائم الأنترنت ويساعد مركز الشكاوى الخاصة بجرائم الإنترنت أحيانا وكالات تطبيق القانون من خلال إجراء الأبحاث وإعداد ملف القضية الأولى. وقد وجد محققوا المركز، خلال السنتين والنصف الأوليتين من عمر المشروع، وعلى الرغم من جهود إعداد القضايا وإحالتها بسرعة إلى وكالات تطبيق القوانين أن فرق العمل الخاصة بمكافحة جرائم الإنترنت ملف القضية الأولى. وقد وجد محققوا المركز، خلال السنتين والنصف الأوليتين من عمر المشروع، وعلى الرغم من جهود إعداد القضايا وإحالتها بسرعة إلى وكالات تطبيق القوانين أن فرق العمل الخاصة بمكافحة جرائم الإنترنت لم تكن جميعا مجهزة لمتابع هذه الجرائم أو التحقيق فيها بسرعة. وقد لا تملك بعض فرق العمل هذه القدرة على القيام بعمليات سرية، أو قد لا تملك التجهيزات اللازمة لاقتفاء الآثار الرقمية للأدلة .

[1] عبد الله عبد الكريم عبد الله ، المرجع السابق ، الصفحة 116- 118.

– ثالثا : مظاهر التعاون الدولي للمركز .

يعمل مركز الشكاوى الخاصة بجرائم الإنترنت أيضا مع منظمات دولية مثل هيئة الجرائم الاقتصادية[1] والمالية (EFCC) في نيجيريا، حيث توجد مستويات عالية من الجرائم الاقتصادية والمالية كتبييض الأموال والاحتيال بقبض أموال مسبقة المشاريع وهمية، أو ما يسمى احتيال (419)، مما كانت له عواقب سلبية شديدة على ذلك البلد .

وقد أدى خطر هذه الجرائم في نيجيريا إلى تأسيس لجنة الجرائم الاقتصادية والمالية هناك. وخلال السنة الماضية، قام مركز الشكاوى الخاصة بجرائم الإنترنت بعدة عمليات جديدة صودرت فيها بضائع وتم إلقاء القبض على أشخاص في أفريقيا الغربية نتيجة لهذا التحالف بين المركز ولجنة الجرائم الاقتصادية والمالية، ونتيجة التحالفات أخرى.

وهناك مجموعة متنامية من الوكالات الدولية المنخرطة في محاربة جرائم الإنترنت. ويعمل مركز الشكاوى الخاصة بجرائم الإنترنت مع المسؤولين عن تطبيق القانون في بلدان عديدة، بينها أستراليا والمملكة المتحدة. كما يحضر ممثلو مركز الشكاوى أيضا اجتماعات دورية للمجموعة الفرعية حول جرائم التكنولوجيا المتقدمة التابعة لمجموعة الثماني (كندا، فرنسا، ألمانيا، إيطاليا، اليابان، روسيا والمملكة المتحدة والولايات المتحدة). ويعمل قسم من هذه المجموعة الفرعية على محاربة جرائم الإنترنت وتعزيز التحقيقات بشأنها.

– المطلب الثاني : الصعوبات التي تواجه التعاون الدولي وكيفية القضاء عليها :

بعد دراستنا للتعاون الدولي والوقوف أمام أهم نماذجه وصوره سنحاول التطرق في هذا المطلب بنوع من الإختصار إلى المعوقات التي تشوب التعاون الدولي وكيفية القضاء عليها.

[1] د. عبد الله عبد الكريم عبد الله، المرجع السابق، الصفحة 122

– الفرع الأول : الصعوبات التي تواجه التعاون الدولي .

التعاون الدولي بكافة صوره في مجال مكافحة ومواجهة الجرائم المتعلقة بشبكة الإنترنت وإن كان[1] يعد مطلبا تسعى إلى تحقيقه أغلب الدول إن لم يكن كلها ، إلا أنه ثمة صعوبات ومعوقات تقف دون تحقيقه أهمها :

1/– عدم وجود نموذج موحد للنشاط الإجرامي : من بين الصعوبات التي تطرأ على التعاون الدولي يتضح لنا تناقض الكثير من الدول و عدم وجود إتفاق عام مشترك لمواجهة الجرائم المعلوماتية ومنها الجرائم المتعلقة بشبكة الإنترنت و نماذج إساءة استخدامها ، فما يكون مباحا في أحد الأنظمة قد يكون مجرما و غير مباح في نظام آخر ويمكن إرجاع ذلك إلى عدة أسباب و عوامل كاختلاف البيئات والعادات والتقاليد والديانات والثقافات بين الدول.

2/– تنوع واختلاف النظم القانونية الإجرائية : بسبب تنوع وإختلاف النظم القانونية الإجرائية، نجد أن طرق التحري و التحقيق و المحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها، فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلال أو التحقيق أنها قانونية في دولة ما، قد تكون ذات الطريقة غير مشروعة في دولة أخرى، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح بإستخدام أي دليل إثبات جرى الحصول عليه بطرق تري هذه الدولة طرق غير مشروعة، حتى وإن كان هذا الدليل تم الحصول عليه في اختصاص قضائي وبشكل مشروع.

3/– عدم وجود قنوات اتصال :

إن ضرورة وجود قنوات إتصال أمر لا بد منه لتحقيق التعاون الدولي فلا يمكن تحقق هذا الشرط إلا[2] بتحقيق الإتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة . ومن أبرز أهداف

[1] أمير فرج يوسف الجريمة الإلكترونية، المرجع السابق، الصفحة 436/435

[2] محمد نصر محمد ، المسؤولية الجنائية، المرجع السابق، الصفحة 112- 114..

هذا التعاون في مجال مكافحة الجريمة والمجرمين، الحصول على المعلومات والبيانات المتعلقة بهم فعدم وجود مثل هذا النظام يعني عدم القدرة لجمع الأدلة والمعلومات العملية التي غالبا ما تكون مفيدة في التصدي لجرائم معينة ولمجرمين معينين . وبالتالي تنعدم الفائدة من هذا التعاون .

4/- مشكلة الاختصاص في الجرائم المتعلقة بالإنترنت: الجرائم المتعلقة بالإنترنت من أكبر الجرائم التي تثير مسألة الاختصاص على المستوى المحلي أو الدولي ولا توجد أي مشكلة بالنسبة للاختصاص على المستوى الوطني أو المحلي حيث يتم الرجوع إلى المعايير المحددة قانونا لذلك.

ولكن المشكلة تثار بالنسبة للاختصاص على المستوى الدولي حيث اختلاف التشريعات والنظم القانونية والتي قد ينجم عنها تنازع في الاختصاص الدول بالنسبة للجرائم المتعلقة بالإنترنت التي تتميز بكونها عابرة للحدود يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استنادا إلى مبدأ الإقليمية ، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبيه ، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية كما تثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية ، كما لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة وتم الإطلاع عليها في دولة أخرى ، ففي هذه الحالة يثبت الاختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة.

5/- التجريم المزدوج: التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين ، فهو[1] منصوص عليه في أغلب التشريعات الوطنية والصكوك الدولية المعنية بتسليم المجرمين ، وبالرغم من أهميته تلك نجده عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية سيما وأن بعض الدول لا تجرم هذه الجرائم ، بالإضافة إلى أنه من الصعوبة أن نحدد فيما إذا كانت

[1] أمير فرج يوسف ، المرجع السابق، الصفحة438/437.

النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم المتعلقة بشبكة الإنترنت أو لا الأمر الذي يعوق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين ، ويحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم المتعلقة بالإنترنت.

6/- المساعدات القضائية بين الدول : الأصل في الإنابة القضائية الدولية والتي تعد من أهم صور المساعدات القضائية الدولية في المجال الجنائي أن تسلم بالطرق الدبلوماسية وهذا بالطبع يجعلها تتسم بالبطء والتعقيد، والذي يتعارض مع طبيعة الإنترنت وما تتميز به من سرعه ، وهو الأمر الذي انعكس على الجرائم المتعلقة بالإنترنت .

7/- الصعوبات الخاصة بالتعاون الدولي في مجال التدريب: تتمثل في عدم رغبة بعض القيادات الإدارية في بعض الدول في التدريب لإعتقاد هم بدوره السلبي في تطوير العمل من خلال تطبيق ما تعلمه المتدرب في الدورات التدريبية وما اكتسبوه من خبرات ومن الصعوبات أيضا والتي قد تهدد التعاون في مجال التدريب ما يتعلق بالفوارق الفردية بين المتدربين وتأثيرها على عملية الإكتساب المهارات المستهدفة بقوة تامة و متكافئة لمختلف الأفراد المتدربين. سيما في مجال تكنولوجيا المعلومات وشبه الاتصال حيث أنه يوجد بعض الأشخاص ممن لا يعي في هذا المجال شيء وعلى النظير يوجد أناس على درجة كبيرة من المعرفة والثقافة في هذا المجال .

الفرع الثاني : مواجهة المعوقات التي تواجه التعاون الدولي :

-فيما يتعلق بالعقبة الأولى: بالنسبة لعدم وجود **نموذج موحد للنشاط الإجرامي** فإن الأمر[1] يقتضي توحيد هذه النظم القانونية، ولإستحالة هذا الأمر فإنه لا بد من تحديث التشريعات المحلية المعنية بالجرائم المعلوماتية و إبرام اتفاقيات خاصة يراعى فيها هذا النوع من الجرائم .

-وبالنسبة للمعوق الثاني : المتعلق بإختلاف **النظم القانونية الإجرائية** نجد أن المواثيق الدولية الصادرة عن الأمم المتحدة غالبا ما تشجع الأطراف فيها على السماح باستخدام بعض تقنيات

1 كتاب محمد نصر محمد ، المرجع السابق، الصفحة 117 - 123.

التحقيق الخاصة، وهذا ما يخفف من غلو واختلاف النظم القانونية والإجرائية بين الدول ويفتح المجال أمام تعاون دولي فعال.

فمثلا المادة 20 من إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية تشير في هذا الصدد إلى التسليم المراقب، والمراقبة الإلكترونية وغيرها من أشكال المراقبة والعمليات المستترة، والتي تعتبر من أهم التقنيات.

وأدلة الإثبات لإستخدامها فيما بعد في الملاحقات القضائية المحلية منها أو الدولية في دول أطراف في سياق نظم المساعدة القانونية المتبادلة.

وهذا ما أكدت عليه الاتفاقية الأوربية للإجرام المعلوماتي حيث نص المادة 29 على سرية حفظ البيانات المعلوماتية المخزنة وأجازت لكل طرف أن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الإلكترونية الموجودة داخل النطاق المكاني لذلك الطرف الآخر والتي ينوي الطرف طالب المساعدة أن يقدم طلبا للمساعدة بشأنها بغرض القيام بالتفتيش أو الدخول بأي طريقة مماثلة، وضبط أو الحصول الكشف عن البيانات المشار إليها.[1]

كما أكدت المادة 30 من ذات الاتفاقية على الكشف السريع عن البيان المحفوظة حيث نصت على: أنه عند تنفيذ طلب حفظ البيانات المتعلقة بالتجارة غير المشروعة والمتعلقة بإتصال خاص تطبيقا لما هو وارد في المادة 29 فإن الطرف المساند إذا اكتشف وجود مؤدي خدمة في بلد آخر قد شارك في نقل هذا الاتصال فإن عليه أن يكشف على وجه السرعة إلى الطرف طالب المساعدة كمية كافية من البيانات المتعلقة بالتجارة غير المشروعة حتى يمكن تحديد هوية مؤدي الخدمة، وهذا الطريق الذي تم الاتصال من خلاله كما أشارت المادة 31 من هذه الإتفاقية إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة، حيث أجازت لأي طرف أن يطلب من أي طرف آخر أن يقوم بالتفتيش أو أن يدخل بأي طريقة مشابهة أز أن يضبط أو يحصل بطريقة مماثلة و أن يكشف عن

[1] كتاب محمد نصر محمد ، المرجع السابق، الصفحة 117 - 123.

البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكاني لذلك الطرف والتي يدخل فيها أيضا البيانات المحفوظة وفقا للمادة 29، ويجب الاستجابة لمثل هذا الطلب بأسرع ما يمكن في الحالات الآتية:

– **أولا** : إذا كانت هناك أسباب تدعو للإعتقاد أن البيانات المعنية عرضة على وجه الخصوص لمخاطر الفقد أو التعديل.

– **ثانيا** : أو أن الوسائل والإتفاقات والتشريعات الواردة في الفقرة 2 تستلزم تعاونا سريعا.

في حين نجد أن المادة 32 من ذات الاتفاقية سمحت بالدخول للبيانات المخزنة خارج نطاق الحدود بشرط أن يكون ذلك بموجب اتفاق، أو أن تكون هذه البيانات متاحة للجمهور.

أيضا نصت المادة 33 على تعاون الدول الأطراف فيما بينها لجمع البيانات في الوقت الحقيقي عن التجارة غير المشروعة، والمرتبطة بإتصالات خاصة على أرضها تتم بواسطة شبكة معلومات، وفي إطار ما هو منصوص عليه في الفقرة الثانية. وينظم هذا التعاون الشروط والإجراءات المنصوص عليها في القانون الداخلي.[1]

ويمنح كل طرف تلك المساعدة على الأقل بالنسبة للجرائم التي يكون جمع المعلومات بشأنها في الوقت الحقيقي متوافر في الأمور المشابهة على المستوى المحلي.

ونلاحظ مما سبق أن: الاتفاقية الأوربية للإجرام المعلوماتي أوجدت بعض الحلول التي من شأنها التغلب على مشكلة اختلاف النظم الإجرائية أمام التعاون الدولي لمواجهة الجرائم المتعلقة بشبكة الإنترنت.

– **وأما فيما يتعلق بعدم وجود قنوات اتصال بين جهات إنفاذ القانون** : وللحد من هذه ظاهرة فنلاحظ أنه غالبا ما تشجع المواثيق الدولية، الدول إلى التعاون فيما بينها وتدعوها إلى إنشاء قنوات إتصال بين بغية التيسير في الحصول على هذه المعلومات وتبادلها .

[1] كتاب محمد نصر محمد ، المرجع السابق، الصفحة 123-125

ومن الأمثلة على هذه المواثيق الدولية إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية في المادة 27 منها، والمادة 9 من إتفاقية 1988 والمادة 48 من إتفاقية الأمم المتحدة لمكافحة الفساد، والبند الثاني من المادة من الاتفاقية الأوربية بشأن الإجرام المعلوماتي، والمادة 35 من ذات الاتفاقية الأوربية والتي أوجبت على الدول الأطراف فيها ضرورة تحديد نقطة اتصال تعمل لمدة 24 ساعة يوميا طوال أيام الأسبوع لكي تؤمن المساعدة المباشرة للتحقيقات المتعلقة بجرائم البيانات والشبكات.

– **وأما مشكلة الإختصاص** : فثمة حاجة ملحة إلى إبرام إتفاقيات دولية ثنائية كانت أو جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي خاصة بالنسبة للجرائم المتعلقة بالإنترنت ، بالإضافة إلى تحديث القوانين الجنائية والإجرائية حتى يتناسب مع التطور الكبير التي تشهده تكنولوجيا المعلومات والاتصالات.

– **أما مشكلة التجريم المزدوج** : والذي يعد من أهم الشروط الخاصة بنظام تسليم المجرمين ركزت الاتجاهات والتطورات التشريعية الخاصة بتسليم المجرمين على تخفيف التطبيق الصارم لهذا الشرط ، وذلك بإدراج أحكام عامة في المعاهدات والاتفاقيات المعنية بتسليم المجرمين وذلك إما بسرد الأفعال والتي تتطلب أن تجرم كجرائم أو أفعال مخلة بمقتضى قانون الدولتين معا أو بمجرد السماح بالتسليم لأي سلوك يتم تجريمه و يخضع لمستوى معين من العقوبة في كل دولة.

– وأما الصعوبات الخاصة بالمساعدات القضائية الدولية : والتباطئ في الرد فإننا نجد الحاجة ملحة إلى إيجاد وسيلة أو طريقة تتسم بالسرعة من خلالها طلبات النيابة كتعيين سلطة مركزية مثلا أو السماح بالاتصال المباشر بين الجهات المختصة في النظر إلى مثل هذه الطلبات لنقضي على مشكلة البطء والتعقيد في تسليم طلبات الإنابة.[1]

[1] كتاب محمد نصر محمد ، المرجع السابق، الصفحة 126-127

أما بالنسبة للرد على طلبات إلتماس المساعدة فإنه من الضرورة بمكان الإستجابة الفورية والسريعة على هذه الطلبات، لأجل ذلك تنص غالبية المعاهدات والاتفاقيات الخاصة بالمساعدات القضائية المتبادلة على ضرورة الإستجابة الفورية والسريعة على طلبات إلتماس المساعدة.

– **أما فيما يتعلق بالصعوبات الفنية التي تواجه التعاون الدولي في مجال التدريب** : فإنه يمكن التغلب عليها بإجراء المزيد من البرامج التي تعمل على بيان مخاطر الجرائم المعلوماتية والأضرار التي تسببها وبأهمية تدريب رجال العدالة الجزائية على مواجهتها، كما أنه وبمزيد من التنسيق بين الأجهزة المعنية بتدريب رجال تنفيذ القانون إيجاد برامج تدريبية مشتركة تناسب جميع الفئات.

خاتمة

في رأيي الشخصي والمتواضع أعتقد أن أكبر بؤر الإجرامي لا هي في جرائم الأعمال ولا في جرائم الفساد بل هي في الجرائم المعلوماتية لأن أغلب الجرائم المرتكبة في هذا النطاق غالبا ما تكون من طرف أشخاص يمتلكون مهارات فنية وتقنية عالية في مجال نظم الحاسب الآلي والنظم المعلوماتية تمكنهم من إرتكاب جرائمهم باحترافية تامة والإفلات من العقاب ، والأدهى والأمر أن أغلب التشريعات العالمية تقوم بتطبيق النصوص القانونية الوضعية والتقليدية لمثل هذه الجرائم المستجدة خاصة في ما يتعلق بالمجال الإجرائي في متابعة الجرائم الإلكترونية وعليه فإن القضاة في كثير من القضايا المعروضة عليهم المتعلقة بجرائم المعلوماتية يصطدمون بمبدأ الشرعية لأنه لا يوجد سد تشريعي تام لهذه الجرائم .

ومن الصعوبات التي يواجهها المشرع هو عدم إبلاغ الأشخاص المعنوية كالشركات التجارية وغيرها على الجرائم الإختراقات التي تقع على أنظمتهم المعلوماتية وذلك بهدف محافظة الشركة على سمعتها لدى زبائنها و ما يلحقه الإبلاغ من أضرار للشركة نتيجة تلطخ سمعتها قد يكون أكبر من الضرر الذي طرأ عليها من هذه الجريمة ، وقد يرجع السبب في عدم وثوق هذه الأشخاص المعنوية في نجاعة القوانين الإجرائية التي لا يختلف عليها إثنين أنها لا تزال في مسار التطور.

- **ومن خلال بحثنا في هذا الموضع توصلنا لبعض النتائج التي نذكر في ما يلي :**

– عدم تعريف المشرع الجزائري لنظام المعالجة الآلية للمعطيات عكس المشرع الفرنسي والإتفاقية الدولية للإجرام المعلوماتي وترك الأمر للفقه والقضاء ونظرا للطبيعة القانونية للجريمة الإلكترونية كونها من الجرائم المستحدثة كان من الأجدر تحديد تعريف صريح لمصطلح المعالجة الآلية للمعطيات.

– إستعمال المشرع الجزائري مصطلح عن طريق الغش أمر مثير للجدل لأن هنالك أفعال تصدر عن الجاني للدخول إلى النظام المعلوماتي من دون أي وسائل أو برامج للغش مثال فتح

حاسب آلي مفتوح ويقوم بالدخول إلى المعطيات . ولكن قد يكون المشرع قد أراد بذلك أو قصد وراء ذلك بسوء النية .

– تسرع المشرع في إعتبار العلم والإرادة بالنسبة الدخول إلى النظام المعلوماتي مفترض أي لايمكن التصور الدخول إلا بتوفر سوء النية وقد إعتاد بذلك لوجود نظام حماية ولكن ماذا لو دخل المتهم للمعطيات عن طريق السهو أو الخطأ أو الصدفة وكان الحاسب الآلي مفتوحا.

– عدم تحديد مدة زمنية للبقاء داخل النظام من قبل المشرع ينفي حدوث الخطأ من قبل المتهم وقد نوه الفقه إلى ضرورة تحديد مدة زمنية إذا تجاوز المتهم تلك المدة انتفى بذلك الدخول عن طريق الخطأ .

– لم يفرق المشرع الجزائري بين الإعتداء على النظام والإعتداء على المعطيات عكس الإتفاقية الدولية للجرائم المعلوماتية والغريب أنه اعتمد في تعريفه لجرائم الإعتداء على نظم المعلومات في المادة 02 من القانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والإتصال وهو التعريف الذي جاءت به الإتفاقة الدولية لإجرام المعلوماتي .

– نص المشرع الجزائري على جريمة التقليد في المواد 151و154و155 من الأمر 05/03 وما يعاب عليها في رأيي الشخصي والمتواضع هو تحديده لأفعال أو جرائم لا يصلح بوصفها من جرائم التقليد بل هي جرائم ملحقة لجرائم التقليد.

– هناك مشكل كبير في ما يخص بالاستغلال الصناعي بالنسبة للكيان المعنوي إذ أن المشرع في الأمر 07/03 المتعلق ببراءة الإختراع إشترط على أن يكون الإختراع يتمتع بشرط الجدية وهذا الإستغلال الصناعي أوجب المشرع توفره في مجال مادي وهذا ما يتنافى مع برامج الحاسوب وطبيعتها حيث أنها كيان معنوي ولكن ما يعاب على المشرع الجزائري أنه أهمل بعضا من البرامج التي تعد من قبيل الإختراعات وتستعمل في المجال الصناعي المادي حيث أجرت المنظمة العالمية للملكية الفكرية عام 1978 دراسة التي جاء فيها أن 1% فقط من البرامج يستوفي شرط قابلية الاستغلال الصناعي.

– كان يجب على المشرع أن يقوم بالتفريق في إجراءات التحقيق والتفتيش بين الجريمة الإلكترونية والعادية إذ لم يحدد القانون رقم 04/09 ميقات التفتيش وقد حدد المشرع في المادة 05 من القانون 04/09 الإنتقال إلى مسكن المتهم أو المكان المتواجدة فيه الأجهزة من حيث الإذن و الميعاد والكيفية مما يجعل من السلطات المختصة الإلتزام بقانون الإجراءات الجزائية وهذا ما لا يخدم الطبيعة القانونية للجريمة للإلكترونية بحيث يشترط إتخاذ إجراءات سريعة وفورية لضبط الدليل التقني فلا يمكن أن تحظر التفتيش من الساعة الثامنة ليلا إلى الخامسة صباحا لأننا بصدد دليل رقمي و تقني .

– في ما يخص بحظور المتهم أثناء التفتيش فهذا أيضا يضر بإجراءات التحقيق في الجريمة الإلكترونية

– تعتبر الجريمة الإلكترونية من الجرائم التقنية العابرة لحدود الدولة لذلك فمن غير المعقول الإلتزام بالقوانين التقليدية (قانون الإجراءات الجزائية) في المسائل الإجرائية لهذه الجرائم ومن أكبر المعوقات التي تواجه المشرع الجزائري ومختلف التشريعات الدولية هو تصادم القوانين الإجرائية بين دولة وأخرى فترفض الأخيرة التعاون الدولي في المجال الإجرائي وعليه أصبح صدور إتفاقية دولية خاصة بالجرائم المعلوماتية أمرا ضروريا لا يمكن الغنى عنه .

– إجراءات المتابعة عن بعد لا تعد كافية كإجراء تحقيقي حتى ولو أن الجريمة المعلوماتية ذات طابع تقني إلا أن الخروج المادي خارج إختصاص الدولة أمر لا مناص لضبط الدليل التقني .

– صعوبة إثبات الجرائم الالكترونية بالنظر إلى طبيعة الدليل الذي يتحصل منها إذ قد يكون هذا الدليل غير مرئي وقد يسهل إخفاؤه أو تدميره.

– قد يكون الدليل التقني متصلا بدول أخرى فتكون هناك صعوبة للحصول عليه نظرا لتمسك كل دولة بسيادتها.

- يمتاز إجراء التسليم ببعض الإشكاليات من بينها إهدار لحقوق الأفراد الدفاعية بالإضافة إلى المجاملات الدولية التي قد تحدث لصالح الدولة طالبة التسليم ويقع ضحيتها المتهم المطلوب تسليمه كأن يكون الشخص المطلوب تسليمه غير مرتكب لأي فعل إجرامي وإنما أسند إليه إرتكاب الفعل الإجرامي على غير الحقيقة بقصد الحصول على موافقة الدولة المطلوب منها التسليم بحيث عندما يعاد إلى دولته طالبة التسليم تتخذ ضده إجراءات عقابية مختلفة كليا

- **ومن خلال هذه النتائج المتوصل لها سنحاول ذكر بعض التوصيات في ما يلي :**

- ظرورة توسيع النطاق الإقليمي في مجال التفتيش على الأدلة المادية المتعلقة بالجريمة الإلكترونية وعدم الإقتصار على الأدلة التقنية لوحدها.

- نشير إلى أن لهذه الجرائم خصوصية بحيث يقوم القاضي بإجراءات الخبرة ويعتمد عليها إعتمادا مطلقا مع أن القاضي الجنائي هو قاضي أمير يحتكم على قناعته الشخصية وعليه يجب على القضاة التكوين في المسائل التقنية و الفنية للحاسب الآلي وذلك للموازنة بين تقرير الخبرة وإقتناع القاضي الشخصي.

- تكوين منظمة أمنية خاصة تابعة للدولة خاضعة للتكوين الخاص في مجال النظم المعلوماتية ذو كفاءة تقنية عالية في مجال الحاسب الآلي فالولايات المتحدة على سبيل المثال تقوم بظم القراصنة وإدماجهم ضمن مجموعة خاصة بمجال المعلومات .

- ظرورة إبرام إتفاقية دولية خاصة بالجريمة المعلوماتية .

قائمة المصادر

والمراجع

قائمة المراجع:

القرآن الكريم .

الإتقاقيات الدولية :

1/- الاتفاقية الدولية حول الإجرام السيبيري التي أبرمت بتاريخ : 2001/11/08 من طرف المجلس اللأوروبي وتم وضعها للتوقيع منذ تاريخ 2001/11/23.

– القوانين والأوامر :

1/- الأمر رقم 156/66 المؤرخ في 1966/06/08 المتضمن قانون العقوبات المعدل والمتمم .

2/- الأمر رقم 05/03 المؤرخ في 19/ 2003/07 المتعلق بحقوق المؤلف والحقوق المجاورة ، الجريدة الرسمية عدد 44.بتاريخ 2003/07/23.

2/- الأمر 10/97 من الأمر المتعلق بحق المؤلف والحقوق المجاورة المؤرخ في 03/06/ 1997 المعدل والمتمم لحقوق المؤلف والحقوق المجاورة.

3/- الأمر رقم 07/03 المؤرخ في 19/ 2003/07 المتعلق ببراءة الإختراع ، الجريدة الرسمية عدد 44.بتاريخ 2003/07/23.

4/- قانون07/18 المؤرخ في 10/06/2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، الجريدة الرسمية عدد 34.

5/- قانون رقم 04/09 المؤرخ في 2009/07/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها ، الجريدة الرسمية عدد 47بتاريخ 2009/07/16 .

6/- قانون رقم 05/18 المؤرخ في 10/05/2018 المتعلق بالتجارة الإلكترونية ، الجريدة الرسمية عدد 28 بتاريخ 16/05/2018.

7/- قانون رقم 04/18 المؤرخ في 01/02/2015 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين ، الجريدة الرسمية عدد 06 بتاريخ 10/02/201.

8/- القانون رقم 22/06 المؤرخ في 2006/09/20 ، المعدل والمتمم لقانون الإجراءات الجزائية

- الكتب :

1/- أمير فرج يوسف ، **الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر و الإنترنت** ، مكتبة الوفاء القانونية ، الطبعة الأولى ، مصر، 2011.

2/- محمد نصر محمد ، **المسئولية الجنائية لانتهاك الخصوصية المعلوماتية** ، مركز الدراسات العربية ، الطبعة الأولى ، مصر، 2016.

3/- عبد العزيز بن غرم الله آل جار الله ، **جرائم الإنترنت وعقوباتها** ، دار الكتاب الجامعي ، الطبعة الأولى ، السعودية، 2017.

4/- عبد الله عبد الكريم عبد الله ، **جرائم المعلوماتية والأنترنت** ، منشورات الحلبي القانونية ، الطبعة الأولى ، لبنان، 2007.

- رسائل الدكتوراه :

1/- عبد الوهاب مليابي ، **أمن المعلومات في بيئة الأعمال الإلكترونية** ، رسالة لنيل شهادة الدكتوراه ، كلية الحقوق والعلوم السياسية قسم الحقوق ، جامعة أبي بكر بلقايد– تلمسان.

2/- غربي خديجة ، **التوقيع الإلكتروني** ، مذكرة لنيل شهادة ماستر ، كلية الحقوق والعلوم السياسية قسم الحقوق ، جامعة قاصدي مرباح–ورقلة .

- المذكرات :

1/- العاقل فريال ، **الجريمة المعلوماتية في ظل التشريع الجزائري** ، مذكرة لنيل شهادة الماستر ، كلية الحقوق والعلوم السياسية قسم القانون العام ، جامعة أكلي محند اولحاج – البويرة.

2/- رابحي عزيزة ، **الأسرار المعلوماتية وحمايتها الجزائية** ، أطروحة لنيل شهادة الدكتوراه كلية الحقوق والعلوم السياسية ، قسم القانون الخاص ، جامعة أبي بكر بلقايد– تلمسان ، الصفحة 281.

- الملتقيات و المداخلات :

1/- مختارية بوزيدي ، (**ماهية الجريمة الإلكترونية**) ، مداخلة في ملتقى وطني بعنوان : آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري ، جامعة الدكتور مولاي الطاهر- سعيدة ، المنعقد يوم 29 مارس 2017.

2/- عبد الحليم بوقرين، خضراوي الهادي ، (**تجربة الجزائر في مكافحة الجريمة الإلكترونية**) ، مداخلة في مؤتمر علمي بعنوان: المؤتمر العلمي الأول لمكافحة الجريمة الإلكتروني الرياض المملكة العربية السعودية، كلية الحقوق والعلوم السياسية جامعة عمار ثليجي الأغواط / الجزائر .

- المقالات :

1/- بوقرين عبد الحليم، مقال بعنوان: (**المكافحة الاجرائية للجريمة المعلوماتية**)، جامعة عمار ثليجي- الأغواط..الصفحة .

2/- حسن طوالبة ، (**التعاون القضائي الدولي في مجال مكافحة جرائم الإلكترونية**) ، كلية الحقوق ، جامعة العلوم التطبيقية .

– مواقع الإنترنت:

1/- أحمد مسعود, مريم قريشي محمد ، 23/04/2013 ، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال القانون رقم 09/ 04 ، تم الإطلاع عليه بتاريخ 19/09/2020م على الساعة 02:04 ، نسخة إلكترونية، رابط الموقع :
https://dspace.univ-ouargla.dz/jspui/handle/123456789/1467

2/- صبرينة جبايلي ، 01-12-2017 ، النظام القانوني للسلطة الوطنية للتصديق الالكتروني ، تم الإطلاع عليه في 21/09/2020م على الساعة 00.44 ، نسخة إلكترونية ، رابط الموقع :
http://revue.umc.edu.dz/index.php/h/article/view/2668

فهرس