جامعة غرداية

كلية الحقوق والعلوم السياسية

قسم الحقوق

الجرائم الماسة بالنظم المعلوماتية

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي حقوق تخصص

قانون جنائي وعلوم جنائية

إعداد الطالبين:

- موسى دبري.
- يوسف عنيشل.

إشراف الأستاذ:

- د. مختار بن حمودة.

لجنة المناقشة:

لقب واسم الأستاذ	الرتبة	الجامعة	الصفة
محمد الطيب سكيريفة	أستاذ محاضر ب	جامعة غرداية	رئيسا
مختار بن حمودة	أستاذ محاضر أ	جامعة غرداية	مشرفا مقررا
نسيم هوام	أستاذ مساعد أ	جامعة غرداية	مناقشا

نوقشت بتاريخ: 2022/09/18م

السنة الجامعية:

1442-1443هـ/2021-2022م

جامعة غرداية

كلية الحقوق والعلوم السياسية

قسم الحقوق

الجرائم الماسة بالنظم المعلوماتية

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي حقوق تخصص

قانون جنائي وعلوم جنائية

إعداد الطالبين:

- موسى دبري.
- يوسف عنيشل.

إشراف الأستاذ:

-د. مختار بن حمودة.

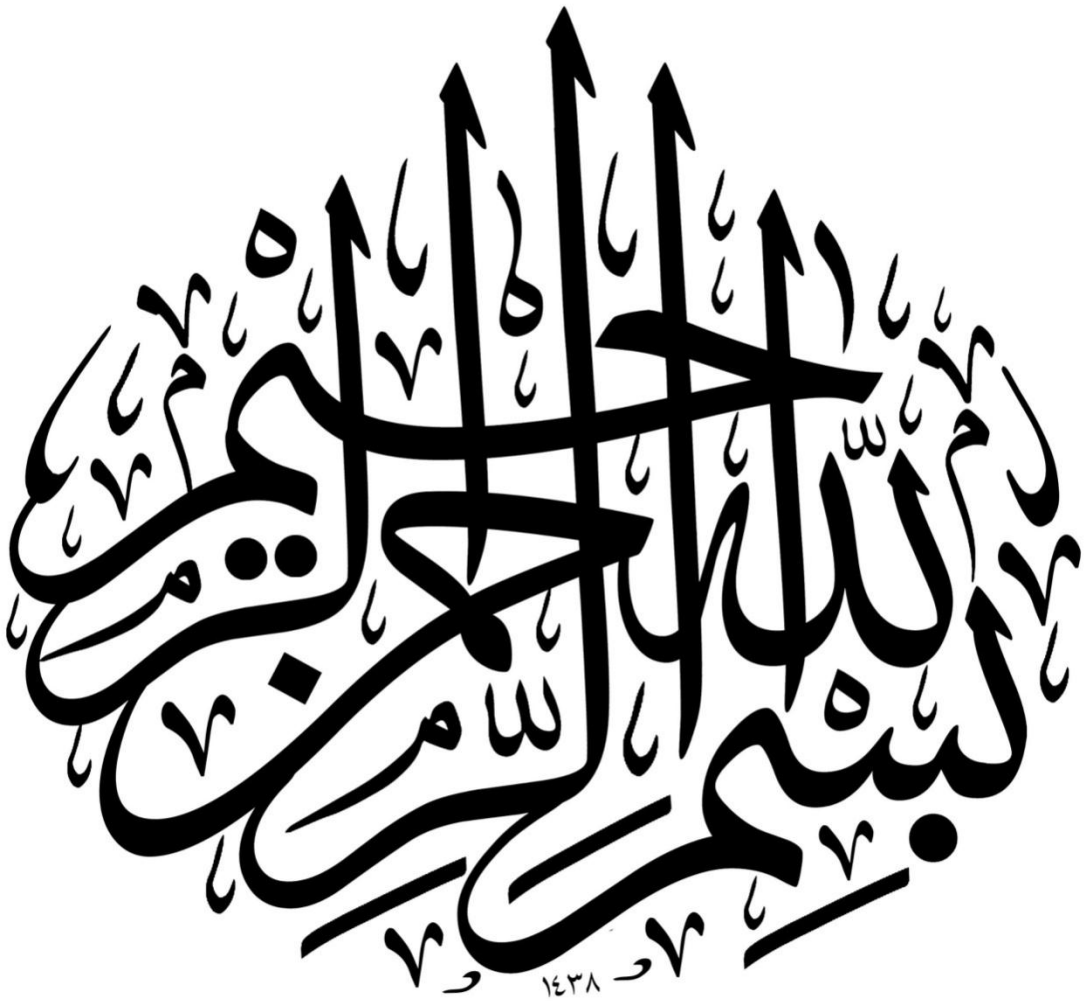
لجنة المناقشة:

لقب واسم الأستاذ	الرتبة	الجامعة	الصفة
محمد الطيب سكيريفة	أستاذ محاضر ب	جامعة غرداية	رئيسا
مختار بن حمودة	أستاذ محاضر أ	جامعة غرداية	مشرفا مقررا
نسيم هوام	أستاذ مساعد أ	جامعة غرداية	مناقشا

نوقشت بتاريخ: 2022/09/18م

السنة الجامعية:

1442-1443هـ/2021-2022م


بسم الله الرحمن الرحيم
١٤٣٨

شكر وعرفان

نرى لزاما علينا تسجيل الشكر وإعلامه ونسبة الفضل لأصحابه، استجابة لقول النبيّ ﷺ :«من لم يشكر الناس لم يشكر الله».

وكما قيل:

علامة شكر المرء إعلان حمده فمن كتم المعروف منهم فما شكر

فالشكر أولا لله عز وجل على أن هدانا لسلوك طريق البحث والتشبه بأهل العلم وإن كان بيننا وبينهم مفاوز.

كما نخص بالشكر أستاذنا الكريم ومعلمنا الفاضل الدكتور *مختار بن حمودة* على هذا البحث، فقد كان حريص على قراءة كل ما نكتب ثم يوجهنا إلى ما يرى بأرق عبارة وألطف إشارة، فله منا وافر الثناء وخالص الدعاء.

كما نشكر السادة الأساتذة وكل الزملاء وكل من قدم لنا فائدة أو أعاننا بمرجع، نسأل الله أن يجزيهم عنا خيرا وأن يجعل عملهم في ميزان حسناتهم.

موسى ويوسف

الإهداء

أهدي ثمرة جهدي إلى أعز الناس إلى فيض الحنان وينبوع المحبة...

إلى من تهدأ حياتي بقربها ويبتهج قلبي بعذوبة صوتها...

إلى الحضن الدافئ إلى التي الجنة تحت أقدامها...

أمي أمي أمي

إلى من يعلو به إسمي وتزهوا به نفسي...

إلى المصباح الذي لم يبخل في إمدادي بالنور الذي أنار مسيرتي...

وعلمني بسلوكه خصالا أعتز بها في حياتي حتى وصلت إلى هدفي هذا

أبي العزيز رحمه الله تعالى

إلى من تقاسمت معهم حلو الحياة ومرها، الذين كانوا معي في مسيرتي

إخوتي وأخواتي...

وإلى جميع الأساتذة الذين أشرفوا على تدريسي عبر مختلف الأطوار

التعليمية، فهم كالشموع التي تحترق لتضيء الآخرين.

إلى كل من ارتبط بيني وبينهم مودة.

إلى زملاء وزميلات الدراسة، إلى كل من ساعدني في انجاز هذا العمل.

إلى كل من تعرّفت عليهم يوماً وكانوا سبباً في إسعادي.

إلى هؤلاء جميعا أهدي هذا العمل المتواضع.

موسى

قائمة المختصرات

(ص): الصفحة

(ق): قانون

(ق.ع): القانون العقوبات

(ط): طبعة

(د): دكتور

(أ): أستاذ

(د.ط): دون طبعة

(د.د.ن): دون دار نشر

(د.ب.ن): دون بلد النشر

(د.س.ن): دون سنة نشر

(ج. ر): الجريدة الرسمية

(د.ت): دون تاريخ

مقدمة

مقدمة:

إن من النعم التي وهبها الخالق سبحانه وتعالى لبني البشر في العصر الحديث التقدم العلمي والمعرفي في شتى مجالات الحياة، والتي من ضمنها الثورة المعلوماتية والتكنولوجيا الرقمية والفضاء الإلكتروني، فالتطور الهائل في استخدام وانتقال المعلومات والبيانات غير ملامح عيش البشر في العالم، وباتت تلك الثورة المعلوماتية ثروة إنسانية تساوي في قيمتها المادية والمعنوية الثروات الأخرى، وتكمن أهميتها في ارتباطها بجميع مناحي الحياة، بحيث أصبحت جزءا لا يتجزأ منها، سواء في المجال العلمي أو الصحي أو السياسي أو الاقتصادي أو العسكري، وكما هو حال ابن آدم في الكفر بنعم الله وإساءة استخدامها من ما عليه من العلوم والمعارف، فقد عمل على تطويع التكنولوجيا الرقمية والفضاء الإلكتروني للإضرار بالآخرين والتعدي عليهم وارتكب الجرائم الشديدة الخطورة عبر هذه التقنيات المعلوماتية، فأتلف الأموال وسرقها وانتهك الأعراض وحقوق الغير وسفك الدماء وجهر بالمحرمات واكتسب الأموال القذرة الملوثة، وأقلق السكينة العامة للدول وأضر بالمجتمعات وباتت تعرف تلك الأفعال بالجرائم الإلكترونية.

وهو ما دفع بالدول وبفقهاء التشريع التصدي لتلك الجرائم باعتبارها جريمة مستحدثة معاصرة شديدة الخطورة للضرر الذي اكتنف لظهورها، وأصبحت دراسة ماهيتها وطبيعتها وظواهرها وتحليلها والأثر المترتب عليها ضرورة ملحة، فأقيمت المؤتمرات والندوات العلمية التي أوصت وحثت الدارسين والباحثين على التعمق والإكثار من البحث في هذا النوع من الجرائم مقارنة بين الفقه والنظام، حيث تعتبر من المستجدات التي تستحق الاهتمام في عصر تكنولوجيا المعلومات التي أصبحت تتطور وبسرعة هائلة حيرت العقول،ومما أثبته الواقع العملي أن الإجراءات الجنائية التقليدية قد عجزت عن استيعاب تلك الجرائم بسبب الطبيعة الخاصة لها، وهو ما نتج عنه ظهور جملة من الصعوبات والمشكلات الشرعية والقانونية في مرحلة جمع الإستدلالات والتحقيق الإبتدائي وحجية الأدلة الجنائية في الإثبات للتصدي لمثل تلك الجرائم.

1) الإشكالية:

فإن من النتائج الحتمية لتطور التكنولوجيا وتقنية المعلومات والعالم الافتراضي الرقمي ظهور عالم إجرامي يستغل ذلك التطور لتنفيذ أعمال إجرامية مع ما يصاحبها من تهديدات أمنية وتحديات تشريعية وقانونية، ومما لا شك فيه أن الجرائم الإلكترونية كغيرها من الجرائم الأخرى لا بد لها من إجراءات جنائية معينة تسبق البدء في سير الدعوى الجنائية منذ لحظة ارتكاب الجريمة وتشمل مرحلة جمع الأدلة وأعمال التحقيق ووسائل إثبات مشروعة لها حجيتها الشرعية لإثبات ذلك، وذلك باعتبار أن الدعوى الجنائية هي مجموعة الإجراءات التي يحددها القانون وتستهدف الوصول إلى حكم قضائي يقرر تطبيقا صحيحا للقانون في شأن وضع إجرامي معين، والذي الهدف منه هو تحقيق العدالة الجنائية التي نصت عليها كل الشرائع والديانات والقوانين الوضعية.

أما من الناحية القانونية فالجرائم الإلكترونية قد استعصى إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية، سواءا من حيث ما يرتبط بشاشة نظام الملاحقة الإجرائية التي تبدوا قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة سواءا على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية.

ومعنى ذلك أننا أمام ظاهرة إجرامية مستحدثة تقف فيها القواعد الإجرائية الجنائية في التشريعات القانونية التقليدية عاجزة جزئيا أو كليا عن استيعاب تلك الجرائم نظرا للطبيعة الخاصة التي تتميز بها الجرائم الإلكترونية عن غيرها من الجرائم، سيما أنها تتخطى حدود الزمان والمكان ولا تعترف بالحدود الجغرافية بين الدول،هذا ما يؤدي إلى تعارض القوانين الجنائية للدول التي تأخذ بمبدأ إقليمية القوانين وتلك التي تأخذ بمبدأ شخصية القوانين أو بالمبدأ المختلط، وهو ما ينعكس سلبا على مرحلة جمع الإستدلالات والتحقيق وحجية الدليل الإلكتروني وإثباته وخصوصياته وعبء الإثبات الإلكتروني.

خاصة بعد أن كشفت الأحداث في وقتنا الحاضر عن تورط دول ومنظمات حكومية في ارتكاب جرائم إلكترونية ودعم وإيواء القراصنة والهاكرز، واستخدامهم لشن هجمات إلكترونية ضد

الدول الأخرى، وهذا تحد جديد يضع العديد من التساؤلات حول مدى فعالية الإجراءات الجنائية التقليدية المتمثلة في إجراءات الاستدلال والتحقيق، أو تلك الموجودة في القوانين الخاصة بالجرائم الإلكترونية ومشروعيتها، وحجية الأدلة الجنائية في الإثبات للتصدي لمثل تلك الجرائم، أضف إلى ما سبق أن الخصائص التي تميز الجريمة المعلوماتية قد أدت إلى صعوبة التعامل مع النشاطات الإجرامية المستحدثة وتكييفها على أساس النصوص الجنائية التقليدية مع ما قد يشكله ذلك من مساس بمبدأ الشرعية.

وعليه من خلال هذا التقديم تبادر إلى أذهاننا التساؤل الرئيسي الذي يرمي إلى:

إلى أي مدى ساهم المشرع الجزائري في معالجة آثار وانعكاسات الجرائم الإلكترونية؟وماهي القوانين التي أقرها في التصدي ومكافحة تلك الجرائم؟

وبناء على هذه الإشكالية الرئيسية اتضحت لدينا مجموعة من التساؤلات الفرعية الآتية:

- ✓ ماهية الجريمة الإلكترونية.
- ✓ ما هي خصائص ومميزات الجريمة الإلكترونية.
- ✓ ماهي الوسائل المنتهجة في تتبع آثار الجريمة الإلكترونية.
- ✓ ماهي القوانين التي أقرت مبدأ مكافحة الجريمة الإلكترونية.

2) أهمية الدراسة:

فمع ظهور التطور الرقمي والتكنولوجي، والطفرة المعرفية والثورة المعلوماتية التي صاحبت هذا التطور، وارتباط العالم بتقنية تكنولوجيا المعلومات، وتوظيف واقتران تلك التكنولوجيا في شتى مناحي الحياة الإنسانية، حيث وفرت الخدمات وطورت البحوث العلمية والطبية، وأنعشت الإقتصادات والصناعات العسكرية والمدنية وأسهمت في تطور وسائل النقل، وشبكات المواصلات وخطوط الطاقة والنقل، إلا أنه ترافق مع ذلك التطور ظهور عالم إجرامي رقمي يستغل ذلك التطور ويطوعه لإرتكاب جرائم تحدد النظام المعلوماتي العالمي، ويتسبب بتدميره وإعطابه وشل قدراته وتنفيذ أفعال غير

مشروعة تطال بضررها الدول والمجتمعات، وحتى الأشخاص، وأضحى قطاع كبير من البشر عرضة بطريقة أو بأخرى لأن يكون ضحية لجريمة إلكترونية.

والجرائم الإلكترونية باعتبارها ظاهرة مستحدثة ودخيلة على النظام القانوني والقضائي،والمدارس القانونية الجنائية العتيقة التي استقرت مبادئها وقواعدها منذ فترة زمنية طويلة،وهو الأمر الذي جعل تلك الأنظمة القانونية عاجزة جزئيا أو كليا عن ملاحقة هذه الجرائم بسبب قصور النصوص التشريعية في مواجهة تلك الجرائم، وبما أن شراح القانون قد عرفوا الجريمة عموما على أنها كل عمل أو امتناع يجرمه النظام القانوني ويقرر له جزاء جنائي،وهو العقوبة التي توقعها الدولة عن طريق الإجراءات التي رسمها المشرع.

ولتحقيق ذلك لابد من اتخاذ الإجراءات الجنائية المقررة في التشريعات الجنائية منذ اللحظة التي تتم فيها ارتكاب الجريمة، وتشمل مرحلة جمع الإستدلالات وأعمال التحقيق ووسائل إثبات مشروعة لها حجيتها حتى تنسب تلك الجرائم لمرتكبها ومواجهته بها، مع ضمان حقوقه الأساسية والحكم عليه ومعاقبته بناء على أدلة وبراهين وحجج شرعية، بغية الوصول إلى الحقيقة لنصل في نهاية المطاف إلى حكم شرعي صائب لا يعتريه نقص، ولا يشوبه بطلان يتم بمقتضاه تحقيق العدالة الجنائية عملا بقول الله سبحانه وتعالى:(... وإذا حكمتم بين الناس أن تحكموا بالعدل...) صدق الله العظيم.[1]

وبناء على ذلك فإن من الأهمية بمكان رفع وإثراء المكتبة الجامعية بدراسات متخصصة لما لها من فوائد جمة تعود على المجتمعات بالكثير من الفوائد، ولعل أهمها المقارنة بين القوانين الوضعية وإثبات مرونتها وقدرتها على استيعاب تلك الجرائم المستحدثة التي لا يتجاوز عمرها الثلاثة عقود، ومعرفة مدى فعالية أحكامها لحماية المجتمع من تلك الجرائم، ومن جهة أخرى إحقاق الحق وضمان معاقبة المجرم في محاكمات مشروعة وعادلة يكفلها القانون، أضف إلى ما سبق أهمية التعرف على مواطن الضعف والقوة والخلل في القوانين، واقتراح حلول عملية لمواجهة تلك الجرائم من خلال صياغة مواد قانونية تواكب الطبيعة الخاصة التي تنفرد بها عن غيرها من الجرائم.

[1] سورة النساء، الآية 58

3) أهداف البحث:

نستهدف من خلال هاته الدراسة إلى تحقيق الأهداف التالية:

- ✓ دراسة وتحليل إجراءات الإستدلال في الجرائم الإلكترونية من منظور القوانين الجزائرية.
- ✓ دراسة وتحليل إجراءات التحقيق الإبتدائي في الجرائم الإلكترونية من منظور القوانين الجزائرية.
- ✓ دراسة وتحليل أثر مرحلة جمع الإستدلالات والتحقيق الإبتدائي في الجرائم الإلكترونية على حجية أدلة الإثبات دراسة شرعية وقانونية مقارنة.
- ✓ صياغة مشروع قانون جديد مقترح خاص بالجرائم الإلكترونية للجمهورية الجزائرية الديمقراطية الشعبية يشمل أحكاما تنظم الإجراءات الجنائية لها وطرق إثبات وحجية الجرائم الإلكترونية.

4) منهج البحث:

إعتمدنا من خلال مجال دراستنا هذه على المنهج العلمي البحثي التالي:

- ✓ المنهج الاستقرائي:وذلك من خلال البحث عن المعلومات والمواد المتعلقة بالموضوع والرجوع للمراجع والمؤلفات والقضايا العملية التي طرحت أمام القضاء.
- ✓ المنهج التحليلي: وذلك عن طريق جمع المعلومات من خلال الدراسية المكتبية والسوابق والدراسات القضائية،وجل ما ورد بشأن موضوع الدراسة في المواقع الإلكترونية على الشبكة المعلوماتية وتحليلها وتفسيرها،ثم رصد مواطن الخطأ والصواب،ثم نقدها بناءا على الأصول والثوابت العلمية المقررة،ومن ثم الخروج بأحكام جديدة تساهم في حل مشكلة البحث.
- ✓ المنهج الإستنباطي:ذلك من خلال عرض الأحكام الشرعية في القضايا الفقهية للوصول إلى أحكام شرعية خاصة بإجراءات الإستدلال والتحقيق الإبتدائي وحجية أدلة الإثبات في الجرائم الإلكترونية، وكذا في القانون الجزائري محل الدراسة.

- ✓ المنهج المقارن:وذلك من خلال المقارنة بين القوانين الجزائرية والقوانين الدولية معا بخصوص موضوع الدراسة.

5) الدراسات السابقة:

1.من مجمل الدراسات السالفة نأخذ على وجه المثال كتاب للباحثة نبيلة هبة هروال ماجستير في القانون،" الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات "لدراسة مقارنة،وهذاعبارة عن كتاب من منشورات دار الفكر الجامعي، الإسكندرية، العام 2013م.

حيث تكلمت الباحثة في المبحث التمهيدي لها عن جرائم الإنترنت وماهياتها،وناقشت النقد الموجه لتعريفات جرائم الإنترنت،ثم ألقت الضوء على خصائص جرائم الإنترنت وأركانها وأنواعها والفرق بين جريمة الإنترنت وجريمة الحاسب الآلي.

وفي الفصل الثاني تناولت الباحثة موضوع تكوين أو هيكلة الضبطية القضائية في جرائم الإنترنت،وحددت الإشكال الذي عبرت عنه بتساؤلات حول إمكانية وجود ضبطية قضائية متخصصة في البحث والتنقيب عن هذا النوع المتميز من الجرائم المستحدثة، وهل توجد هناك ضبطية إدارية متخصصة للحيلولة دون وقوع مثل تلك الجرائم، وما الفرق بين الضبطية القضائية المختصة بالبحث والتنقيب عن ذلك النوع من الجرائم وتلك المختصة بالبحث والتنقيب عن الجرائم التقليدية،وما هي الأجهزة المختصة بمكافحتها على المستوى الوطني والدولي.

ثم تكلمت عن الضبط الإداري بصفة عامة وضرورته ومرونته، وعن دور الضبط الإداري المختص بمكافحة جرائم الإنترنت، وكذا الضبط القضائي بصفة عامة، والمقصود بالضبطية القضائية والضبط القضائي المختص بمكافحة جرائم الإنترنت، وتحدثت أيضا عن أجهزة الضبط القضائي المختصة بمكافحة الجرائم والوحدات المتخصصة في مكافحة جرائم الإنترنت على المستوى الوطني وعلى المستوى الأوروبي والدولي، ثم خصصت الفصل الثاني للحديث عن اختصاصات الضبطية القضائية في مكافحة جرائم الإنترنت، والصعوبات التي تواجه مأمور الضبط القضائي أثناء مكافحته الجرائم الإنترنت واختصاصات الضبطية القضائية في مكافحة جرائم الإنترنت في ظل

الظروف العادية، وأنهت البحث بالحديث عن اختصاصات الضبطية القضائية في مكافحة جرائم الإنترنت في ظل الظروف الاستثنائية.

والفائدة التي عادت على الباحث من هذا الكتاب، هي في الإطلاع على الجوانب الإجرائية لجرائم الإنترنت، والتي من ضمنها دور الضبط الإداري في مكافحة جرائم الإنترنت وضرورته لارتباطه بالمجتمع المدني المنظم وجودا وعدما، وباعتبار أن الضبط القضائي لا يفني عن الضبط الإداري فالوقاية خير من العلاج بحسب تعبيرها، كما تعرف الباحث على أجهزة الضبط القضائي المختصة في مكافحة الجرائم، والوحدات المتخصصة في مكافحة جرائم الإنترنت على المستوى الوطني وعلى المستوى الأوروبي والدولي، واختصاصات الضبطية القضائية في مكافحة جرائم الإنترنت، والصعوبات التي تواجه مأمور الضبط القضائي أثناء مكافحته لجرائم الإنترنت، وشددت على ضرورة التنسيق الدولي والسياسات الجنائية من أجل وضع قانون لمكافحة ومتابعة مرتكبي جرائم الإنترنت توضح فيه إجراءات التفتيش والضبط في العالم الافتراضي.

2." تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية" و هاته دراسة تطبيقية على المحققين في هيئة التحقيق والإدعاء العام بمدينة الرياض لعبد الله حسين القحطاني، فإن هذا البحث عبارة عن رسالة مقدمة لنيل متطلبات الحصول على درجة الماجستير في قسم العلوم الشرطية، بجامعة نايف العربية للعلوم الأمنية بالرياض، سنة 2014م، تحت إشراف الدكتور محمد حسن السراء.

إذ تكلم الباحث عن مفهوم وأهمية ومشروعية التحقيق الجنائي، وكذا الأهداف التي تتحقق من التحقيق الجنائي، ثم انتقل للحديث عن عناصر التحقيق الجنائي في الجرائم المعلوماتية، والتي تتمثل في تحديد وقت ومكان ارتكاب الجريمة المعلوماتية، والركن المادي والمعنوي للجرائم المعلوماتية، وكذا علانية التحقيق وطرق اكتشاف الجرائم المعلوماتية، من ثم تكلم عن أهم المهارات الأساسية الواجب توافرها لدى المحققين في هيئة التحقيق والإدعاء العام للتحقيق الجنائي في الجرائم المعلوماتية،التي من أهمها مهارات استخدام التقنية في التحقيق الجنائي ومهارات تقييم الجريمة المعلوماتية والتعرف على المكونات المادية للأجهزة الرقمية والتعامل المبدئي معها.

ثم استعرض أهم المعوقات التي قد تواجه القائمين على التحقيق الجنائي في الجرائم المعلوماتية، وهي معوقات تتعلق بالجريمة المعلوماتية ذاتها، ومعوقات مرتبطة بالمجني عليه، ومعوقات أخرى مرتبطة بالتحقيق الجنائي، ومعوقات مرتبطة بالدليل الرقمي، واختتم الباحث باستخدام المنهج الوصفي حيث تكون مجتمع الدراسة من (256) محققا من محققي هيئة التحقيق والإدعاء العام بعد أن استخدم الباحث رابط المعادلة الأمريكي، وكانت العينة هي 156 محققا، وصمم الباحث الإستبانة وبناها إنطلاقا من موضوع الدراسة وأهدافها وأسئلتها، وطبيعة البيانات والمعلومات المرغوب الحصول عليها.

وقد استفاد الباحث من هذا البحث الإطلاع على ما ورد بشأن عناصر التحقيق الجنائي، والطرق والأساليب التي تساعد على تنمية مهارات التحقيق في الجرائم المعلوماتية، بالإضافة إلى تقييم المعوقات التي وردت في هذا البحث باعتبارها معوقات تواجه سلطات التحقيق في الجرائم المعلوماتية، وما سيضيفه الباحث في بحثه هو دراسة الآثار المترتبة على حجية أدلة الإثبات من الإجراءات الجنائية الخاصة بجمع الإستدلالات والتحقيق الابتدائي في الجرائم الإلكترونية، ودراستها دراسة شرعية ومقارنتها بأحكام القانون اليمني والقانون الكويتي والقانون القطري.

3-"التحقيق الجنائي في الجرائم الإلكترونية" لجمال براهيمي، فهذا البحث عبارة عن أطروحة مقدمة لنيل درجة الدكتوراه علوم في الحقوق، تخصص قانون، من كلية الحقوق والعلوم السياسية، قسم الحقوق جامعة مولود معمري، جمهورية الجزائر الديمقراطية الشعبية، سنة 2018م، إشراف الدكتور إقلولي محمد.

حيث تطرق الباحث في دراسته إلى الحديث عن الثورة العلمية والتكنولوجية في مجال الإتصالات والمعلومات والإنعكاسات الإيجابية والسلبية على كثير من جوانب الحياة المعاصرة، ثم تكلم عن الصعوبات والمشكلات التي تثيرها ظاهرة الإجرام الإلكتروني باعتبارها لا تقتصر على القانون الجنائي الموضوعي فقط، وإنما امتدت إلى نطاق القانون الجنائي الإجرائي، وعدد المشكلات الإجرائية في مجال الجرائم الإلكترونية والتي من ضمنها التحديات القانونية والعملية التي تثيرها عملية البحث والتنقيب أمام سلطات التحقيق بجميع مستوياتها وباختلاف أدوارها.

ففي الباب الأول تحدث الباحث عن آليات التحقيق في الجرائم الإلكترونية، وخصص الفصل الأول لدراسة إجراءات التحقيق في الجرائم الإلكترونية من حيث محدودية سريان إجراءات التحقيق المألوفة على الجرائم الإلكترونية، سواء عند إجراء التفتيش في البيئة الإلكترونية، أو عند ضبط الأدلة في الجرائم الإلكترونية، ثم عند إجراء المعاينة في العالم الإفتراضي، وأخيرا دور الخبرة التقنية في الجريمة الإلكترونية، أما الفصل الثاني فخصصه الباحث لإبراز القيمة الثبوتية للدليل الإلكتروني وأثرها على تكوين قناعة القاضي الجنائي، حيث قام بدراسة الطبيعة القانونية للدليل الإلكتروني من خلال الوقوف على تعريفه وأهم الخصائص التي تميز الدليل الإلكتروني عن غيره من الأدلة التقليدية، ثم بيان أشكال وأصناف الأدلة الإلكترونية التي تصلح لأن تكون وسيلة إثبات أمام القضاء الجنائي.

أما الباب الثاني فخصصه للحديث عن عقبات التحقيق الجنائي في الجرائم الإلكترونية والنتائج المترتبة عليها،والتي من ضمنها تنازع الإختصاص بالتحقيق في الجرائم الإلكترونية،ومشكلة احترام سيادة الدولة،وصعوبات الإستدلال والإثبات في الجرائم الإلكترونية،وأختم بحثه بالحلول المقترحة لتجاوز عقبات التحقيق في الجرائم الإلكترونية.

وقد استفاد الباحث من هذه الدراسة بالإطلاع على الصعوبات والمشكلات التي تثيرها ظاهرة الإجرام الإلكتروني، التي تناولها الباحث من خلال دراسته،وإلى الإجراءات التي ناقشها باستفاضة عند إجراء التحقيق الإبتدائي في الجرائم الإلكترونية، كما أنه تعرف على القيمة الثبوتية للدليل الإلكتروني في التشريعات الجنائية الفرنسية والجزائرية، في الأخير اطلع الباحث على الحلول المقترحة لتجاوز عقبات التحقيق في الجرائم الإلكترونية التي تناولها من خلال دراسته لموضوعه.

الفصل الأول: التأصيل النظري للجرائم الإلكترونية في الجزائر

تمهيد:

سنقوم بإستعراض أبرز تعريفات الفقهاء السابقين والمعاصرين للمبادئ العامة للإجراءات الجنائية بشكل عام عند أهل الفقه والتشريع، وتعريف وافي لقانون الجرائم الإلكترونية وما نصت وأتت به كل من النظم الأنجلوسكسونية والنظم الفرانكفونية، وذلك من خلال مجريات دراستنا هاته تمهيدا للخوض في صلب موضوع الدراسة،والذي أتى على مبحثان على النحو التالي:

المبحث الأول: مدخل عام حول الجريمة الإلكترونية.

المبحث الثاني: الأساس القانوني للجرائم الإلكترونية في التشريع الجزائري

المبحث الأول:مدخل عام حول الجريمة الإلكترونية

في بداية حديثنا عن تعريف الجريمة الإلكترونية تجدر الإشارة إلى أن هذه الجريمة تكاد تستعصي على التعريف، ذلك أن الأبحاث والدراسات التي تتعلق بها قد أوردت لها تعريفات مختلفة ومتنوعة، بحيث اتفقت جميعها على ألا تتفق على تعريف محدد لهذه الجريمة، وتكشف النماذج المعروضة لتعريفات هذه الجريمة عن تعدد المصطلحات المستخدمة للدلالة عليها وتحديد مفهومها، فغالبية الفقهاء والمعاصرين يطلقون عليها جرائم الحواسيب أو جرائم الأنترنت أو جرائم النظم المعلوماتية، وعليه فعبر هذا التقديم البسيط سوف نتطرق من خلال هذا المبحث إلى مطلبين، حيث أنه في المطلب الأول (تعريف الجرائم الإلكترونية في النظم المقارنة)، أما في المطلب الثاني (خصائص وسمات الجريمة الإلكترونية).

المطلب الأول:تعريف الجرائم الإلكترونية في النظم المقارنة

تعتبر الجريمة الإلكترونية من أبرز الجرائم التي أفرزها التطور العلمي التقني في مجال التكنولوجيا المعلومات والإتصالات، وقد تعددت مسميات الجريمة الإلكترونية، فمنهم من أطلق عليها جرائم الحاسبات، ومنهم من سماها الجرائم الإلكترونية نظرا لعلاقتها بالمعلومات المدمجة من خلال الحاسبات المرتبطة على شبكة الأنترنت، وعليه من خلال هذا المطلب سنتطرق محاولين دراسة وتحليل التعريفات لدى كل من النظم الأنغلوسكسونية من خلال الفرع الأول، وفي الفرع الثاني إلى ما أتت به النظم الفرنكوفونية من خلال تعريفاتها.

الفرع الأول: النظم الأنغلوسكسونية:

وقد عرفت الولايات المتحدة الأمريكية والتي تتبنى النظام الأنغلوسكسوني بشكل خاص الجريمة الإلكترونية بأنها " تلك الجرائم التي تحوز دورا كبيرا في قواعد البيانات الحاسوبية والبرامج الإلكترونية دورا جوهريا في إختراق ممتلكات الغير بغرض الفساد أو السياسة المادية.[1]

ومن مفهوم آخر هي:" كل استعمال للحوسبة الإلكترونية ومعطيات البيانية والشبكة الإلكترونية بغرض استغلال تلك الخدمات التي يؤديها دون أن يكون للمستخدم الحق بذلك.[2]

وفي مفهوم آخر هي: " أعمال غير مشروعة حيث أنها تستهدف شريحة وفئة من المجتمع بغرض الإستفادة الكلية من المعلومات المخزنة داخل النظام الخاص بهم بغرض الإبتزاز أو السرقة أو التهديد،ويندرج هذا النوع تحت جرائم المعالجة الآلية للبيانات".[3]

وفي مفهوم آخر أيضاهي:"جريمة تتطلب لإقترافها أن تتوافر لدى فاعلها معرفة بتقنية النظام المعلوماتي".[4]

ويأخذ الخبير الأمريكي (Parker) مفهوما واسعا للجريمة المعلوماتية، حيث يشير إلى أنها: "هي تلك الأفعال الإجرامية الإلكترونية المقصودة أيا كانت صلتها بالمجال المعلوماتي، والتي تؤذي بدورها إلى خسائر مادية أو معنوية تلحق بالمجني عليه، أو كسب يحققه الفاعل".[5]

وقد تطرق الأساتذة (Vivantو Lestane) لمفهوم الجريمة الإلكترونية على أنها: "هي مجموعة من وسائل اختبار الإختراق الغير مشروعة والتي تركز على استهداف الحواسيب سواء خاصة

---

[1]– عبد الجبار الحليص– الاستخدام غير المشروع النظام الحاسوب من وجهة نظر القانون الجزائي بحث منشور في مجلة جامعة دمشق للعلوم القانونية والاقتصادية – المجلد 27– العدد الأول 2011م ص 191.

[2]–المرجع نفسه، ص 191.

[3]– المرجع نفسه ، ص 191.

[4]–المرجع نفسه ، ص191.

[5] –الشوا سامي، ثورة المعلومات وإنعكاساتها على قانون العقوبات، ط1، القاهرة،دار النهضة العربية ،1994،ص07.

بالشركات أو المؤسسات أو المجتمع من خلال الشبكة العنكبوتية بشتى أنواع أدوات الإختراق بغية الفساد أو المصلحة الخاصة والأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب".[1]

الفرع الثاني:النظم الفرنكوفونية:

ويرى واضعوا هذه التعريفات في النظام الفرنكوفوني الذي أستوحي اسمه من النظام الفرنسي والمعمول بهذا النظام في بعض مستعمراته القديمة بأن الجريمة المعلوماتية ليست هي التي يكون النظام المعلوماتي أداة ارتكابها، بل هي التي تقع على النظام أو داخل نطاقه.

وفي تقرير الجرائم المتعلقة بالحاسوب أقر المجلس الأوروبي بقيام مخالفة الجريمة في كل حالة يتم فيها تغيير معطيات أو بيانات أو برامج الحاسوب،أو محوها أو كتابتها أو أي تدخل آخر في مجال إنجاز البيانات،أو معالجتها وتبعا لذلك تسببت في ضرر اقتصادي أو فقد حيازة ملكية شخص آخر، أو بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص آخر.[2]

ومن جهة فقد عرفها المشرع الفرنسي على أنها السلوك السيئ المتعمد الذي يستخدم نظم المعلومات لإتلاف المعلومات أو إساءة استخدامها مما يتسبب (أو يحاول التسبب)، إما بإلحاق الضرر بالضحية، أو حصول الجاني على فوائد الإستحقاق.[3]

وقد تناولت منظمة التعاون الاقتصادي للتنمية CCDEO بأنها "هو كل فعل غير قانوني وإجرامي يترتب عليه إختراق ممتلكات الغير والإعتداء على خصوصياتهم، سواء كانت مادية أو معنوية بغية الوصول للفساد، ويكون عادة بطريقة غير مباشرة وتارة مباشرة من خلال الشبكة الإلكترونية.[4]

---

[1]--الشوا سامي، المرجع السابق، ص07

[2] -السعيد كمال، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، دار النهضة العربية،القاهرة، 1993، ص324-325.

[3]-حسن طاهر دود – جرائم نظم المعلومات – أكاديمية نايف العربية للعلوم الأمنية.الرياض – ط2000 م ص 32.

[4]أحمد خليفة الملط "الجرائم المعلوماتية"، ط2 ، دار الفكر الجامعي، الإسكندرية،2006، ص 83 . 84.

وفي تعريف آخر بأنها"مجموعة من الوسائل والسلوكيات الغير مبررة وغير المشروعة التي تضر بمصالح المجتمع من خلال استعمال الحاسوب والأنترنت.[1]

ومن جانبنا فنحن نتفق مع هذه التعريفات من جانب أنها حاولت أن تلم بين كل جوانب الجريمة الإلكترونية في ظل تعريف شامل لها، ومن خلال ما سبق بيانه يمكن ملاحظة أن أغلب التعريفات السالفة الذكر حاولت الإحاطة قدر الإمكان بجميع الأشكال الإجرامية للجريمة الإلكترونية، سواء التي قد تقع بواسطة النظام المعلوماتي، أو داخل هذا النظام أي على المعطيات والبرامج والمعلومات، كما شملت جميع الجرائم التي من الممكن أن تقع في بيئة إلكترونية، إلا أن هذه التعريفات لم تركز على فاعل الجريمة ومقدرته التقنية، ولا على وسيلة ارتكاب الجريمة، أو على الغاية والنتيجة التي تسعى لها الجريمة المعلوماتية، بل إنه حاول عدم حصر الجريمة المعلوماتية في نطاق ضيق يتيح المجال أمام إفلات العديد من صور هذه الجريمة من دائرة العقاب.

المطلب الثاني:خصائص وسمات الجريمة الإلكترونية

سوف نتولى من خلال هذا المطلب شرح أهم الخصائص والسمات التي تتميز بها الجرائم الإلكترونية عن غيرها من الجرائم، وما يميز تلك الجرائم كونها تنفرد بطبيعة خاصة، أي لا وجود لها في عالم الجرائم التقليدية والذي بدوره ساعد في انتشار تقنية البيانات والتطور التكنولوجي، ما أضفى عليها مجموعة من الخصائص والسمات خاصة بها.

الفرع الأول: خصائص وسمات خاصة بالجريمة الإلكترونية (الفعل):

أولا: الجريمة الإلكترونية عابرة للحدود:إن المجتمع الإلكتروني وإن صح التعبير لا يعترف بالحدود الموضوعية أو الجغرافية، نظرا لكونه مجتمع تكنولوجي تولد عبر شبكات تخترق الزمان والمكان دون أن تخضع لضوابط قيام الحدود الإقليمية أو القانونية الخاصة بكل دولة في العالم، التي بدورها تحمي الأمن القومي للمجتمع لكل منها، ومن جهة أخرى قيام مقومات الأمن المعلوماتي المتصدر لفكرة الحدود المعلوماتية، فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام

[1]– محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2011، ص 56.

نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال، قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد[1]، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى[2].

وهذه الطبيعة التي تتميز بها الجريمة الإلكترونية كونها جريمة عابرة للحدود، خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه، بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.[3]

فكانت القضية المعروفة باسم مرض نقص المناعة المكتسبة (الإيدز) من القضايا التي لفتت النظر إلى البعد الدولي للجرائم المعلوماتية، وتتلخص وقائع هذه القضية التي حدثت عام 1989 في قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي هدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طروادة)، إذ كان يترتب على تشغيله تعطيل جهاز الحاسوب عن العمل ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل على عنوان معين حتى يتمكن المجني عليه من الحصول على مضاد للفيروس، وفي الثالث من فبراير من عام 1990 تم إلقاء القبض على المتهم جوزيف بوب في أوهايو بالولايات المتحدة الأمريكية.[4]

فتقدمت المملكة المتحدة بطلب تسليمه لها لمحاكمته أمام القضاء الإنجليزي، حيث إن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة، وبالفعل وافق القضاء الأمريكي على تسليم المتهم، وتم

---

[1]–فورة، نائلة، جرائم الحاسب الإقتصادية، ط1،دار النهضة العربية، القاهرة، 2004، ص21.

[2]–أحمد هلالي عبد السلام، إلتزام الشاهد بإعلام في الجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 1997، ص13.

[3]–نهلا عبد القادر المومني، الجرائم المعلوماتية، ط1، دار المكتبة الوطنية للمملكة الأردنية الهاشمية، عمان ،2008، ص51

[4]-نهلا عبد القادر المومني،المرجع السابق، ص 51.

توجيه إحدى عشرة تهمة ابتزاز إليه وقعت معظمها في دول مختلفة، إلا أن إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية، ومهما كان الأمر فإن لهذه القضية أهميتها من ناحيتين:[1]

- الأولى: حيث لأول مرة في التاريخ يتم إلقاء القبض وتسليم جاني في قضية جريمة إلكترونية.
- الثانية: حيث لأول مرة في التاريخ يسلم الجاني للمحاكمة بإتهامه بإنجاز فيروس إختراق وزرعه في الحواسيب (فيروسا).[2]

ونتيجة لهذه الطبيعة الخاصة للجريمة المعلوماتية،ونظرا للخطورة التي تشكلها على المستوى الدولي، والخسائر التي قد تتسبب بها، تعالت الأصوات الداعية إلى التعاون الدولي المكثف من أجل التصدي لهذه الجرائم،فأتى التعاون الدولي متمثلا في المعاهدات والإتفاقيات الدولية التي تعمل على توفير جو من التنسيق بين الدول الأعضاء، الأمر الذي يكفل الإيقاع بمجرمي المعلوماتية وتقديمهم للقضاء العادل.[3]

وتجدر الإشارة هنا إلى أن أهم المصاعب والعراقيل التي تعرقل مراكز التعاون الدولي حول الجريمة الإلكترونية،أنه لا يوجد تفاهم وتكاثف فعال،ولا مفهوم شامل مترابط بين الدول حول صور النشاط المكون لهذه الجريمة، بالإضافة إلى أن نقص الخبرة لدى أجهزة الشرطة وجهات الإدعاء والقضاء في هذا المجال لتمحيص عناصر الجريمة إن وجدت، وجمع الأدلة عنها للإدانة فيها،فهذا يشكل عائقا كذلك أمام التعاون في مجال مكافحة هذا النوع من الجرائم.[4]

ثانيا: صعوبة اكتشاف الجريمة الإلكترونية: إذ تتميز الجريمة الإلكترونية بصعوبة اكتشافها وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة[5]، حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة إذا قورنت بما يتم اكتشافه من الجرائم التقليدية.

---

[1]– نهلا عبد القادر المومني، المرجع السابق، ص52

[2]–المرجع نفسه، ص52.

[3]–المرجع نفسه، ص52.

[4]–المرجع نفسه، ص52.

[5]-الصغير، جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، ط1، القاهرة، 1992، ص 17.

ويمكن رد الأسباب التي تقف وراء الصعوبة في اكتشاف الجريمة الإلكترونية إلى عدم ترك هذه الجريمة لأي اثر خارجي بصورة مرئية، كما أن الجاني يمكنه ارتكاب هذه الجريمة في دولة وقارة مغايرة لموقع الجريمة، إذ أن الجريمة الإلكترونية كما سبق وأشرنا إليه أنها جريمة عابرة حدود الدول (دولية)، وكذلك فإن قدرة الجاني على تدمير دليل الإدانة في أقل من الثانية الواحدة، يشكل عاملا إضافيا في صعوبة اكتشاف هذا النوع من الجرائم.[1]

فالجرائم الإلكترونية في أكثر صورها خفية لا يلاحظها المجني عليه،أو لا يدري حتى بوقوعها والإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي والنبضات أو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها، أمر ليس عسيرا في الكثير من الأحوال بحكم توافر المعرفة والخبرة في مجال الحاسبات غالبا لدى مرتكبها، كما أن المجني عليه يلعب دورا رئيسيا في صعوبة اكتشاف وقوع الجريمة الإلكترونية، حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للإنتهاك أو تمنى بخسائر فادحة من جراء ذلك على عدم الكشف حتى بين موظفيها عما تعرضت له، وتكتفي عادة بإتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها.[2]

ويرى البعض أن للمجني عليه دور مثير للشبهة في بعض الأحيان، فهو قد يشارك بطريق غير مباشرة في ارتكاب الفعل بطريقة غير مباشرة، وذلك بسبب تواجده داخل الشبكة العنكبوتية أو داخل النظام المراد إلحاق الضرر به، في ظروف تحمل تعرضه للجريمة المعلوماتية أمرا مرتفعا بشكل كبير، ويرجع ذلك بشكل أساسي إلى القصور الأمني الذي يعتري الأنظمة المعلوماتية، الأمر الذي قد يساعد على ارتكاب الفعل الإجرامي بشكل مباشر أو غير مباشر،فيترتب على ذلك نتيجة أخرى تميز الجريمة الإلكترونية، وهي أن هناك إمكانية للحيلولة دون وقوع هذه الجريمة مقارنة بغيرها من الجرائم، إذ يعتمد ذلك أساسا على تطوير نظم الأمن الخاصة بأنظمة الحاسبات وشبكاتها.[3]

---

[1]-المرجع نفسه، ص 17.

[2]–رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، ط1، 1994، ص 25–26.

[3]–قورة، المرجع السابق ،46.

والواقع أن إحجام المجني عليه من الإبلاغ عن وقوع الجرائم الإلكترونية يبدو أكثر وضوحا في المؤسسات المالية، مثل البنوك والمؤسسات الإدخارية ومؤسسات الإقراض والسمسرة، حيث تخشى مجالس إدارتها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها، حيث أن الجانب الأكبر من الجرائم الإلكترونية لا يتم الكشف أو التبليغ عنه فإن ذلك يؤثر سلبا في السياسة التي يمكن أن توضع لمكافحتها، وقد تم طرح عدة اقتراحات تكفل تعاون المجني عليه وكشف هذه الجرائم، وبالتالي إنقاص حجم الإجرام المعلوماتي الخفي.[1]

وإلى جانب ذلك فإن المجني علية يتردد أحيانا في الإبلاغ عن هذه الجرائم خفية من الكشف عن أسلوب ارتكاب هذه الجرائم،فقد يؤدي ذلك إلى تكرار وقوعها بناء على تقليدها من قبل أشخاص آخرين، كما أن الإعلان عن هذه الجرائم يؤدي أحيانا إلى الكشف عن مواطن الضعف في برنامج المجني عليه ونظامه المعلوماتي مما يسهل عملية اختراقه.[2]

ثالثا: صعوبة إثبات الجريمة الإلكترونية: بما أن اكتشاف الجريمة المعلوماتية أمر كما "سبق وأشرنا إليه" ليس بالسهل ولكن حتى في حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها، فإن إثباتها أمر يحيط به كذلك الكثير من الصعاب،فالجريمة الإلكترونية تتم في بيئة غير تقليدية، حيث تقع خارج إطار الواقع المادي الملموس، ولتقوم أركانها في بيئة الحاسوب والإنترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة، ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي، مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل امرا في غاية السهولة.[3]

---

[1]–رستم، الجوانب الإجرائية، مرجع سابق، ص25–27.

[2]-البيتي، محمد حماد، التكنولوجيا الحديثة والقانون الجنائي، ط1، دار الثقافة للنشر والتوزيع، عمان،2004، ص152.

[3]–نهلا عبد القادر المومني، المرجع السابق، ص56.

ففي إحدى الحالات التي شهد ألمانيا أدخل أحد الجناة في نظام الحاسوب تعليمات أمنية لحماية البيانات المخزنة داخله من المحاولات الرامية إلى الوصول إليها، والتي من شأنها محو هذه البيانات بالكامل بواسطة مجال كهربائي،وذلك إذا تم اختراقه من قبل الغير.[1]

وتجدر الإشارة إلى أن وسائل المعاينة وطرقها التقليدية لا تفلح غالبا في إثبات هذه الجريمة نظرا لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية، فالأخيرة لها مسرح تجري عليه الأحداث، حيث تخلف آثارها المادية التي تقوم عليها الأدلة، وهذا المسرح يعطي المجال أمام سلطات الإستدلال والتحقيق الجنائي في الكشف عن الجريمة، وذلك عن طريق المعاينة والتحفظ على الآثار المادية التي خلفتها الجريمة، لكن فكرة مسرح الجريمة في الجريمة الإلكترونية يتضاءل دوره في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة وذلك لسببين:[2]

- الأول: أن الجريمة المعلوماتية لا تخلف آثارا مادية.
- الثاني: أن كثيرا من الأشخاص يرتادون إلى مسرح الجريمة خلال الفترة من زمان وقوع الجريمة، وحتى اكتشافها أو التحقيق فيها هي فترة طويلة نسبيا، الأمر الذي يعطي مجالا للجاني أو للآخرين أن يغيروا أو يتلفوا أو يعبثوا بالآثار المادية إن وجدت، الأمر الذي يورث الشك في مصداقية الأدلة المستسقاة من المعاينة في الجريمة الإلكترونية.

بالإضافة إلى ذلك فإن نقص الخبرة الفنية والتقنية لدى الشرطة وجهات الإدعاء والقضاء يشكل عائقا أساسيا أمام إثبات الجريمة الإلكترونية، ذلك أن هذا النوع من الجرائم يتطلب تدريب وتأهيل هذه الجهات في مجال تقنية المعلومات، وكيفية جمع الأدلة والتفتيش والملاحقة في بيئة الحاسوب والإنترنت، فنتيجة لنقص الخبرة والتدريب في هذا المجال، كثيرا ما تخفق أجهزة الشرطة في تقدير أهمية الجريمة المعلوماتية فلا تبذل لكشف غموضها وضبط مرتكبيها جهودا تتناسب وهذه الأهمية،

[1]–رستم، الجوانب الإجرائية، المرجع السابق، ص 23.

[2]–حجازي، عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الإلكترونية والأنترنت، ط1، دار الكتب القانونية، القاهرة 2002، ص59.

بل إن المحقق قد يدمر الدليل بمحوه محتويات الأسطوانة الصلبة عن خطأ منه أو إهمال أو بالتعامل بخشونة مع الأقراص المرنة.[1]

الفرع الثاني: خصائص وسمات خاصة بالمجرم الإلكتروني(الفاعل):

أولا:أسلوب ارتكاب الجريمة الإلكترونية:ذاتية الجرائم المعلوماتية تبرز بصورة أكثر وضوحا في أسلوب ارتكابها وطريقة تنفيذها، فإذا كانت الجرائم التقليدية تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف، أو في صورة الخلع أو الكسر أو تقليد المفاتيح كما هو الحال في جريمة السرقة، فإن الجرائم الإلكترونية هي جرائم هادئة بطبيعتها (soft crime) لا تحتاج إلى العنف لتنفيذها، بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة.[2]

وتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الإنترنت)، مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو التغرير بالقاصرين، كل ذلك دون حاجة لسفك الدماء.[3]

ثانيا: الجريمة الإلكترونية تتم عادة بتعاون أكثر من شخص: حيث تتميز الجريمة المعلوماتية أنها تتم عادة بمشاركة وتعاون أكثر من شخص على ارتكابها، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والإنترنت يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو من خارج مؤسسة المجني عليه لتغطية

[1]-حجازي، الدليل الجنائي، المرجع السابق، ص 28 و29؛ أنظر كدالك القبائلي، سعد حماد، ضوابط الحماية الإجرائية لبرامج الحاسب الآلي، بحث مقدم لمؤتمر القانون والحاسوب المنعقد في جامعة اليرموك، أريد من 26-2004/04/27، ص 24.

[2]- القبائلي سعد حماد، المرجع نفسه، ص 24.

[3]-القبائلي سعد حماد، المرجع السابق، ص 24.

عملية التلاعب وتحويل المكاسب إليه[1]،والإشتراك في إخراج الجريمة الإلكترونية إلى حيز الوجود قد يكون اشتراكا سلبيا وهو الذي يترجم بالصمت من جانب من يعلم بوقوع الجريمة محاولة منه لتسهيل إتمامها، وقد يكون اشتراكه ايجابيا وهو غالبا ما يكون عبارة عن مساعدة فنية أو مادية.[2]

ثالثا: خصوصية المجرم المعلوماتي:المجرم الذي يقترف الجريمة الإلكترونية والذي يطلق عليه المجرم الإلكتروني،يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية (المجرم التقليدي)، فإذا كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكابها، فإن الأمر يختلف بالنسبة للجرائم الإلكترونية فهي جرائم فنية تقنية في الغالب الأعم، ومن يرتكبها عادة يكون من ذوي الإختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الإنترنت.

فعلى سبيل المثال فإن الجرائم الإلكترونية ذات الطابع الاقتصادي مثل التحويل الإلكتروني غير المشروع للأموال يتطلب مهارة وقدرة فنية تقنية عالية جدا من قبل مرتكبها، كذلك فإن البواعث على ارتكاب المجرم الإلكتروني هذا النوع من الإجرام الإلكتروني قد تكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي[3].

[1]–عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، الأردن، 2007، ص 32.

[2]–الشوا، ثورة المعلومات وإنعكاساتها، المرجع السابق، 46.

[3]-الشوا، ثورة المعلومات وإنعكاساتها، المرجع السابق، 46.

المبحث الثاني: الأساس القانوني للجرائم الإلكترونية في التشريع الجزائري

إن النظام القانوني في التشريع الجزائري يرتكز في طياته بما يثار أمامه من قضايا أو منازعات سواء كانت مدنية أو شخصية أو جنائية، وعليه فإن تلك المصادر والأدوات المساعدة له تحيله إلى الإجتهاد،ولا يوجد ما يمنع من تقسيم القضايا على أساس التخصصات طالما لا تتعارض مع تلك المصادر وأدواتها، وعليه فمن خلال هذا المبحث سنتطرق إلى التكييف الدستوري للجريمة الإلكترونية في المطلب الأول، وفي المطلب الثاني إلى الجريمة الإلكترونية في القوانين العامة والأنظمة الخاصة.

المطلب الأول: التكيف الدستوري للجريمة الإلكترونية

كفل دستور الجزائر لسنة 1996 وكذا التعديل الطارئ عليه بموجب القانون المعدل له سنة 2016 حماية الحقوق الأساسية والحريات الفردية، وعلى أن تضمن الدولة عدم انتهاك حرمة الإنسان.[1]

وقد ألم المشرع الجزائري من خلال المبادئ والأسس المعمول بها دستوريا تطبيق الإجراءات الدستورية من خلال تطبيق النصوص التشريعية، والتي أقرها قانون الإجراءات الجنائية وقانون العقوبات،وقوانين خاصة أخرى،والتي تحمي السلامة والأمن القومي والمجتمع،ومن أهم هاته المبادئ الدستورية العامة:

- المادة3: الحريات الأساسية وحقوق الإنسان والمواطن مضمونة.
- المادة 4: حرية الإبتكار الفكري والفني والعلمي مضمونة للمواطن وحقوق المؤلف يحميها القانون.
- لا يمكن بأي حال من الأحوال تعليق وحجز أي من (المطبوعات أو التسجيلات أو أية أدوات أو وسائل مستخدمة من وسائل الإرشاد والتوجيه والإعلام والتبليغ، إلا بتصريح أو أمر قضائي.
- الحريات الأكاديمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون.

[1]-القانون رقم 01/16 المؤرخ في 06-2016/03 المتضمن تعديل الدستور، الجريدة الرسمية العدد 14.

- تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة للتنمية المستدامة للأمة، ولا يجوز انتهاك حرمة حياة المواطن الخاصة وشرفه، وسرية المراسلات والإتصالات الخاصة بكل أشكالها مضمونة.
- إن القانون يحمي حقوق المؤلف ولا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بأمر قضائي.

المطلب الثاني: الجريمة الإلكترونية في القوانين العامة والأنظمة الخاصة

من خلال هذا المطلب سنستعرض جزءا من القوانين الخاصة والمعمول بها في التشريع الجزائري،والتي تندرج ضمن القوانين العامة والخاصة للجرائم الإلكترونية، حيث سنتحدث هنا عن الجريمة الإلكترونية المقترنة بالقوانين العامة، ومن جهة أخرى سنتطرق إلى الهياكل الخاصة للتصدي للجرائم الإلكترونية كما يلي:

الفرع الأول: الجريمة الإلكترونية مقترنة بالقوانين العامة:

أولا: قانون البريد والإتصالات السلكية واللاسلكية:باستقراء القانون الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات بحيث لاحظنا أنه تسارع مواكبة التطور الذي تشهده التشريعات العالمية ومسايرة التطور التكنولوجي، لذلك بات من السهولة بمكان اجراء التحويلات المالية عبر الطريق الإلكتروني ذلك ما نصت عليه المادة 87 منه[1]،كما نصت المادة 84 مكرر2 منه على استعمال حوالات دفع عادية أو إلكترونية أو برقية[2]، كما نص في المادة10 منه على إحترام المراسلات.[3]

[1]–المادة 87 من قانون البريد والمواصلات والإتصالات السلكية واللاسلكية رقم 2000–03 المؤرخ في 2000/08/05 على أنه " يمكن أن ترسل الأموال ضمن النظام الداخلي بواسطة الحوالات الصادرة عن المتعامل والمحولة عن البريد أو البرقيات أو عن طريق البريد الإلكتروني

[2]–المادة 02/84 من نفس القانون " تطبق أحكام المادة 89 من هدا القانون عند إستعمال الحوالات دفع عادية أو إلكترونية أو برقية.

[3]–أنظر المادة 105 من نفس القانون لا يمكن في أي حال من الأحوال إنتهاك حرمة المراسلات.

بينما أتت المادة 127 منه لتبين جزاء كل من تسول له نفسه بحكم مهنته، أن يفتح أو يحول أو يخرب البريد أو ينتهكه، بمعاقبة الجاني بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات.[1]

ثانيا: قانون التأمينات: قد تطرق هذا القانون كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي[2]، ففي نصوص قانونية عديدة تخص البطاقة الالكترونية التي تسلم للمؤمن له إجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني، وكذا للجزاءات المقررة في حالة الإستعمال غير المشروع،أو من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا، أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لأمين الصحة للبطاقة الإلكترونية حسب المادة93 مكرر02[3].

ثالثا: القوانين الخاصة المتعلقة بتكنولوجيا الإعلام والإتصال والتصدي لها :جاء هذا القانون منظما للجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وكل ما يتعلق بالمنظومة المعلوماتية، والمعطيات المعلوماتية،ومقدموا الخدمات، والمعطيات المتعلقة بتسيير الإتصالات الإلكترونية[4] من مراقبة وتفتيش المنظومات المعلوماتية عند الضرورة، وحجز المعطيات المعلوماتية، وحفظ المعطيات المتعلقة بحركة السير على الإلتزامات الخاصة بمقدمي خدمات الإنترنت، وأخيرا على إنشاء مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

[1]–المادة 127 من قانون البريد والمواصلات رقم: 2000–03، المرجع السابق.

[2]–المادة 06 مكرر 01، والمادة 65 مكرر 01 من القانون 2008/08/01 والمعدل والمتمم لقانون 83–01 المتعلق بالتأمينات.

[3]–المادة 93 مكرر 2 و3 من نفس القانون.

[4]-المواد من المادة الثانية حتى 14 من قانون رقم 09–04 المؤرخ في 2009/08/05 والمتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.

الفرع الثاني: الجريمة الإلكترونية مقترنة بالقوانين الخاصة

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: وقد أنشئت بموجب القانون رقم 09-04 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، ومن مهام الهيئة الوطنية تفعيل التعاون القضائي والأمني الدولي، وإدارة وتنسيق عمليات الوقاية والمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية، في حالة الإعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني[1].

ثانيا: الهيئات القضائية الجزائية المتخصصة: أنشئت بموجب القانون 14/04 المؤرخ في 2004/01/10 المعدل والمتمم لقانون الإجراءات الجزائية التي تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد322، و4 من ق إ.ج ج، تتمتع باختصاص إقليمي موسع طبقا للمرسوم التنفيذي رقم 34 المؤرخ في 2006/01/05،بحيث تنظر في القضايا المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون رقم 04/09.[2]

ثالثا: المعاهد الوطنية المتخصصة في مجال الأمن المعلوماتي: حيث تندرج ضمن مستويات عالية وهي من أرقى عشرة دوائر متخصصة في مجالات الأمن المعلوماتي والسيبيراني، ولديها من الكفاءات العالية في مجال الجرائم الإلكترونية والتقنية، بحيث تمتلك على أجهزة جد متطورة في المركز الوطني،وتقدم جميع المساعدات الإلكترونية والتقنية، والأهم أنها تقوم بمعالجة وتحليل الرقمنة وجمع الأدلة الرقمية،والتي بدورها تساعد الأمن القومي والمحققين في مجال الجرائم الإلكترونية.[3]

---

[1]-القانون رقم 09-04 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافتحتها

[2]-هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية وعلم الإجرام، كلية الحقوق،جامعة بسكرة،2016، ص03.

[3]-حملاوي عبد الرحمان، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية، كلية الحقوق، جامعة بسكرة، 2016، ص15.

رابعا: المديرية العامة للأمن الوطني: تتصدى هذه المديرية للجريمة الإلكترونية من عدة جوانب، والتي منها الجانب التوعوي بحيث لم تغفل المديرية العامة للأمن الوطني عن الوقاية عن طريق التوعية الإجتماعية، وهذا من خلال برمجتها لتنظيم دروس توعوية في مختلف الأطوار الدراسية، وكذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم الإلكترونية، ودائما في إطار مكافحة الجريمة الإلكترونية ونظرا للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم، إذ أكدت عضويتها الفعالة في المنظمة الدولية للشرطة الجنائية INTERPOL، فهاته الأخيرة تتيح مجالات للتبادل المعلوماتي الدولي، وكذا تسهيل الإجراءات القضائية المتعلقة بتسليم المجرمين، ومباشرة الإنابات القضائية الدولية ونشر أوامر القبض المبحوث عنهم دوليا.[1]

[1]-علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة للطبع والنشر، بيروت، 1999، ص120

خلاصة الفصل الأول:

تطرقنا من خلال هذا الفصل إلى المفاهيم العامة حول الجريمة الإلكترونية،وقلنا بأنها تعتبر من الظواهر الحديثة وذلك بإرتباطها بتكنولوجيا حديثة، بما نصطلح عليها تكنولوجيا المعلومات والإتصالات والحاسوب، وقد أحاطت بتعريفات الجريمة الإلكترونية الكثير من الغموض، حيث تعددت الجهود الرامية إلى وضع مفهوم محدد وجامع لها، لكن القوانين الوضعية لم تتفق على تعريف محدد، بل إن البعض ذهب إلى ترجيح عدم وضع تعريف بحجة أن هذا النوع من الجرائم ما هو إلى جريمة تقليدية ترتكب بأسلوب إلكتروني.

الفصل الثاني: الوسائل التقنية والعقابية لمكافحة الجريمة الإلكترونية

تمهيد:

إن الإستدلال والتحقيق في الجرائم الإلكترونية صراع بين المحقق والمجرم، حيث أن الأول ينشد إلى الحقيقة بالكشف عن ملابسات الجريمة، والثاني يحاول التضليل وطمس الحقائق حتى يفلت من العقاب، ولكن بقدر ما يكون للمحقق الجنائي من خبرة وفراسة وإلمام بالعلوم الجنائية والنفسية، وبقدر ما يتمتع به من كفاءة ومقدرة وسيطرة على المواقف التي يواجهها،بقدر ما تكون النتيجة في صالح التحقيق إرساءا لقواعد الحق والعدل والتحقيق بمعناه العام، يعني اتخاذ جميع الإجراءات والوسائل المشروعة التي توصل إلى كشف الحقيقة، وعليه فإن الإستدلال والتحقيق في الجرائم الإلكترونية علم متمم لقانون العقوبات والإجراءات الجنائية، فمن وجهة نظر قانون العقوبات فإنه يرشدنا هذا العلم إلى الطرق والوسائل التي يمكن بها استكمال وإثبات أركان الجريمة، ويساعدنا في الوصول إلى معرفة الوثائق التي تحدد وصفها القانوني، ويبين لنا كذلك الوسائل التي تكشف بها عن الظروف المحيطة بكل جريمة، ويكون من شأنها تشديد أو تخفيف العقوبة.

وعليه فمن خلال هذا التقديم سنتطرق من خلاله لمبحثين:

المبحث الأول: أركان الجريمة الإلكترونية وسريان القانون.

المبحث الثاني: مكافحة الجريمة الإلكترونية في القانون الدولي والمشرع الجزائري.

المبحث الأول: أركان الجريمة الإلكترونية وسريان القانون

بالرجوع لنصوص القانون المشرع الجزائري محل الدراسة،فإنه خلا من أي تحديد مباشر لأركان الجريمة الإلكترونية، إلا أنه يوجد بين ثنايا مواده ما يشير إلى تلك الأركان بطريقة أو بأخرى.

وبما أن المشرع الجزائري قد أحال فيما لا يوجد به نص لبعض القوانين المتفرقة في قانون العقوبات،والتي نصت على بيان أركان الجريمة بصفة عامة، وهذا الأمر يثير إشكالية للباحثين والقضاة عند تطبيقها على الواقع لتفرد الجرائم الإلكترونية بخصوصية وذاتية متميزة عن بقية الجرائم، وتطور أنماطها بشكل دائم حيث تعجز فيه النظريات والأحكام القائمة عن مواجهة هذا النوع من الجرائم، الأمر الذي يتطلب معه وضع قواعد إجرائية خاصة بها تنسجم مع خصوصيتها وطبيعتها.

وعليه سنتطرق من خلال هذا المبحث إلى مطلبين على النحو التالي:

المطلب الأول: أركان الجريمة الإلكترونية.

المطلب الثاني: سريان القوانين العقابية في مجال الجريمة الإلكترونية.

المطلب الأول: أركان الجريمة الإلكترونية.

تتخذ الجريمة المرتكبة عبر الانترنت من الفضاء الافتراضي مسرحا لها، مما يجعلها تتميز بخصوصيات تنفرد بها، إلا أن ذلك لا يعني عدم وجود تشابه لها مع الجريمة المرتكبة في العالم التقليدي أو المادي، فهي تشترك بوجود الفعل الغير المشروع، والمجرم يقوم بهذا الفعل من خلال هذا التشابه،الذي سنتطرق إلى تبيان الأركان التي تقوم عليها هذه الجريمة، وبالتالي نعمد إلى تبيان مدى انطباق مبدأ الشرعية على الجريمة الإلكترونية في الفرع الأول، وبشكل جامع سنوضح الركن المادي لها مع تحديد الركن المعنوي للجريمة الإلكترونية في الفرع الثاني.

الفرع الأول: الركن الشرعي للجريمة الإلكترونية:

إن الجريمة هي نتيجة الأفعال المادية الصادرة عن الإنسان،فهذه الأفعال تختلف حسب نشاطات الإنسان، وهذا ما جعل المشرع يتدخل لتجريم هذه الأفعال الضارة بموجب نص قانوني يحدد فيه الفعل الضار أو المجرم والعقوبة المقررة لارتكابه[1].

فالركن الشرعي للجريمة الذي هو الصفة غير المشروعة للفعل الذي يقوم به الجاني له ركنين أساسين،وهما تطابق الأفعال التي يجرمها القانون مع النصوص التشريعية الموجودة وعدم خضوع الفعل المرتكب لأي سبب من أسباب الإباحة.[2]

الفرع الثاني: الركن المادي والمعنوي للجريمة الإلكترونية:

يقصد بالركن المادي للجريمة كل فعل أو سلوك إجرامي صادر من إنسان عاقل سواء كان إيجابيا أو سلبيا، يؤدي إلى نتيجة تمس حقا من الحقوق، التي يكفلها الدستور والقانون فهذا الإعتداء يكون في ثلاثة أشكال وهي:

أولا: الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات: فيكون هذا الشكل من الإعتداء في صورتين وهو ما تنص عليه في المادة 394 مكرر من قانون العقوبات الجزائري، فيكون على صورة جريمة بسيطة تتمثل في الدخول أو البقاء غير المشروع،وأخرى مشددة تحقق

[1]-احسن بوسقيعة، الوجيز في القانون الجزائي العام، ط10 ،دار هومة، الجزائر، 2011، ص 27.

[2]-بلعيات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، ط1، دار الخلدونية، الجزائر2007، ص95

بتوافر الظرف المشدد المتمثل في حصول نتيجة الدخول أو البقاء غير المشروع إما بمحو أو تغيير في المعطيات الموجودة في النظام أو تخريب نظام اشتغال المنظومة.[1]

ثانيا: الإعتداء العمدي على سير نظام المعالجة الآلية للمعطيات: المشرع الجزائري لم يورد نصا خاصا بالإعتداء العمدي على سير النظام، واكتفى بالنص على الإعتداء العمدي على المعطيات الموجودة داخل النظام، وهذا راجع إلى تفسير أن الإعتداء على المعطيات قد يؤثر على صلاحية النظام و وظائفه، فقد وضع الفقه معيارا للتفرقة بين الإعتداء على المعطيات والإعتداء على النظام على أساس ما إذا كان الإعتداء وسيلة أم غاية، فإذا كان الإعتداء مجرد وسيلة فإن الفعل يشكل جريمة الإعتداء العمدي على النظام، أما إذا كان الإعتداء غاية فإن الفعل يشكل جريمة اعتداء عمدي على المعطيات[2].

ثالثا:الإعتداءات العمدية على المعطيات: إن جريمة الإعتداء العمدي على المعطيات جريمة عمدية يتخذ فيها القصد الجنائي بعنصريه العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، كما يجب أن يعلم الجاني بأن نشاطه الإجرامي يترتب عليه التلاعب في المعطيات، ويعلم أيضا أنه ليس له الحق في القيام بذلك وأنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته.

فلتوافر الركن المعنوي يشترط القصد الجنائي العام والمتمثل في نية الغش، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل توافر الجريمة،والتي يتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه، وإن كان الضرر قد يتحقق في الواقع نتيجة للنشاط الإجرامي إلا أنه ليس عنصرا في الجريمة.[3]

---

[1]-نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية، دارسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، 2005، ص189، .Loi n°92-683 du juillet 1992

[2]المرجع نفسه، ص 190.

[3]–أمال قارة، الحماية الجزائرية للمعلوماتية في التشريع الجزائري، دار هومة الجزائر، ط2، 2007،ص125.

المطلب الثاني: سريان القوانين العقابية في مجال الجريمة الإلكترونية

سنستعرض من خلال هذا المطلب سريان القوانين العقابية في مجال الجريمة الإلكترونية،وهذا من خلال الفروع التالية:

أولا سريان القانون العقابي للأشخاص الطبيعية، ثانيا سريان القانون العقابي للأشخاص المعنوية.

الفرع الأول: سريان القانون العقابي للأشخاص الطبيعية:

حيث أوضحت النصوص القانونية سواء في التشريع الجزائري أو في التشريعات المقارنة العقوبات الأصلية المقررة لمختلف الجرائم الإلكترونية، وإضافة إلى ذلك العقوبات التكميلية للجريمة الإلكترونية.

أولا: العقوبات الأصلية: العقوبات الأصلية هي كل عقوبة لا توقع إلا إذا نطق بها القاضي وحدد نوعيتها ومقدارها،وهي السجن أو الحبس أو الغرامة المالية التي تكون كافية بذاتها لتحقيق معنى الجزاء وهي العقاب الأساسي للجريمة.[1]

ويحدد القانون لكل جريمة عقوبة، وتشدد العقوبة إذا اقترنت بظرف من ظروف التشديد المنصوص عليها، لذلك سوف نحاول توضيح العقوبات التي تخضع لها كل جريمة من الجرائم التي نص عليها التشريع العقابي الجزائري، مقارنة مع التشريع العقابي الفرنسي لتوضيح أكثر.

فهي تشمل العقاب على الجرائم الآتية:

أ. **عقوبة جرائم المساس بأنظمة المعالجة الآلية للمعطيات:**وهي تتضمن الجرائم الآتية:

1.عقوبات جريمة الدخول أو البقاء غير المصرح بهما:تختلف العقوبة في هذه الجريمة بحسب ما ترتب أو لم يترتب عن الدخول أو البقاء، أو أضرار مست المعلومات وأنظمة المعالجة الآلية في التشريع الجزائري والتشريعات المقارنة محل الدراسة وفقا لما يلي: [1]

[1]–راضية مشري، الحماية الجزائية للمصنفات الرقمية في ظل قانون حق المؤلف، مجلة التواصل لكلية الحقوق، جامعة 08 ماي 45، قالمة، عدد 34، جوان 2013، ص 144.

1.1-العقوبة في التشريع الجزائري: حددتها المادة 394 مكرر من قانون العقوبات والمعدلة بموجب القانون 06-23 الذي شدد عقوبة الغرامة في صورتها البسيطة والمشددة، وعليه تكون العقوبة الحبس من ثلاثة (03) أشهر إلى سنة والغرامة من خمسون ألف (50000) إلى مائتي ألف (200000) دينار جزائري في حالة الدخول أو البقاء غير المصرح به، ولم ينشأ عن ذلك أي ضرر أو إفساد أو تعطيل للنظام المعلوماتي المخترق أو للمعلومات المتضمنة فيه، وذلك بعد ما كانت عقوبة الغرامة قبل التعديل لقانون العقوبات سنة 2006 تتراوح بين خمسون ألف (50000) إلى مائة ألف (100000) دينار جزائري كحد أقصى، ولا شك أن هدف المشرع من وراء تشديد ومضاعفة الحد الأقصى للغرامة، هو مكافحة ومحاولة الحد من انتشار جرائم الإختراق المعلوماتي خاصة والجريمة الإلكترونية عامة، لاسيما إذا تم اختراق نظام يحتوي على معلومات سرية أو تتعلق بأمن الدولة ومؤسساتها، مما يشكل خطورة على الأشخاص وعلى الدولة الجزائرية التي تتوجه مؤخرا نحو إرساء حكومة إلكترونية تقيدا بمبدأ العصرنة والتوجه نحو التكنولوجيا الرقمية والإنفتاح عليها.[2]

أما إذا ترتب على فعل الدخول أو البقاء أضرار تمس المعلومات أو النظام فإن المادة 394 مكرر من قانون العقوبات المعدل وفي فقرتها الثانية والثالثة تنص على أنه " ... تضاعف العقوبة إذا ترتب على حذف أو تغيير المعطيات المنظومة، وإذا ترتب على الأفعال المذكورة أعلاه تخريب اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 300000 دج، وما هو ملاحظ في هذه الصورة لجريمة الدخول والبقاء المترتب النتيجة، أن جعل المشرع الضرر الناتج عن ذلك الفعل ظرفا لتشديد العقوبة في حالتين اثنتين وهما :

---

[1]-وهذا ما أكد عليه المشرع الجزائري وأخذه بعين الإعتبار، عندما لم يقصر الحماية على المعلومات بمختلف أنواعها وبغض النظر عن الجهات التي تنتمي إليها، بتشديده للعقوبة إذا كانت المعلومات التي تم الاعتداء عليها تتعلق بالدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام وذلك بموجب المادة 394 مكررة من قانون العقوبات المعدل.

[2]-يظهر توجه الجزائر نحو تفعيل الحكومة الالكترونية من خلال إصدار تشريعات للتواصل في المسائل الإدارية وغيرها مع المواطنين من خلال القانون رقم 15-03 مؤرخ في أول فبراير سنة 2015 يتعلق بعصرنة العدالة،والقانون رقم 15-04 مؤرخ في أول فبراير سنة 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني، ج.ر عدد 06 بتاريخ السادس من فبراير 2015، ص 4-6.

* إذا ترتب عن الدخول أو البقاء حذف أو تغيير المعلومات المنظومة: فإن العقوبة تضاعف عن تلك المقررة لعقوبة الدخول أو البقاء المجرد ليصبح الحبس في حده الأدنى (06) ستة أشهر وفي حده الأقصى (02) سنتين، والغرامة لتتراوح بين (100000) مائة ألف دينار جزائري إلى (400000) أربعمائة ألف دينار جزائري.

* إذا ترتب عن فعل الدخول أو البقاء تخريب نظام اشتغال المنظومة: وفي هذه الحالة تكون عقوبة الحبس من (06) ستة أشهر إلى (02) سنتين، أما الغرامة فتكون بين (50000) دينار جزائري إلى حدها الأقصى (300000) ثلاثمائة ألف دينار جزائري.

والملاحظ أن المشرع لم يعطي للقاضي الفاصل في منازعة الحكم بإحدى العقوبتين الحبس أو الغرامة باستعمال حرف "و" للربط بدلا من " أو" الإختيارية، دون ترك المجال للسلطة التقديرية للقاضي في إمكانية الجمع من عدمه، ويكون المشرع الجزائري في ذلك قد جانب الصواب، لأنه يمكن للقاضي الحكم بإحدى العقوبتين مما قد يجعل العقاب أقل ردعا، وبإمكان القاضي أن يحكم بالحبس أو الغرامة أو كلاهما معا موقوفة النفاذ طبقا لنص المادة 592 من قانون إجراءات جزائية[1]، فضلا عن إمكانية تطبيق عقوبة العمل للنفع العام بدلا من الحبس طبقا للمادة 05 مكرر من قانون العقوبات، ويكون للقاضي سلطة تقديرية في الحكم بالعقوبات بين الحد الأدنى والحد الأقصى بحسب ما تطلبه كل حالة اختراق.

1.2- العقوبة في التشريع الفرنسي: حدد المشرع الفرنسي عقوبات مختلفة وعدلها في كل مرة بتشديدها بداية من أول قانون لسنة 1988 المتعلق بالغش المعلوماتي،وإدخاله في قانون العقوبات

[1] – المادة 592 من الأمر رقم المتضمن قانون الإجراءات الجزائية الجزائري تقضي:" يجوز للمجالس القضائية وللمحاكم، في حالة الحكم بالحبس أو غرامة إذا لم يكن المحكوم عليه قد سبق الحكم عليه بالحبس لجناية أو جنحة من جرائم القانون العام، أن تأمر بحكم مسبب بالإيقاف الكلي أو الجزئي لتنفيذ العقوبة الأصلية" معدلة بموجب القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004، ج.ر عدد 71، ص 06.

لسنة 1992وبدأ العمل به بداية من 1994[1]، وكذا التعديل الذي جاء في سنتي 2004 و2012، والعقاب عليها في صورتها البسيطة والمشددة.

فكانت عقوبة الدخول أو البقاء غير المشروع في صورتها البسيطة في أول قانون للغش المعلوماتي رقم 88-19 تقدر ب (02) شهرين حبس إلى (01) سنة أو بغرامة من (2000) ألفين فرك فرنسي إلى (50000) خمسين ألف فرك فرنسية[2]، فكان الحد الأدنى والأقصى منخفضا مع ترك السلطة التقديرية للقاضي في تقدير عقوبة ما بين الحدين مع حريته في الحكم بإحدى العقوبتين فقط.

ليأتي المشرع الفرنسي بقانون العقوبات الجديد سنة 1994 ويجعل عقوبة هذه الجرائم في حد واحد سواء كانت الحبس لمدة (01) سنة وبغرامة (15000) خمسة عشر ألف يورو ليسلب القاضي سلطته التقديرية في التحرك بالعقوبة.[3]

و في حالات أخرى ولأن جرائم المعالجة الآلية للمعطيات في انتشار وتطور مستمر تبعا لتطور التقنية الرقمية، وكذا النمو وازدياد الخسائر الناجمة عنها خاصة أن التقارير الأخيرة توضح تأثر فرنسا من ضمن الدول الأوروبية بهاته الجرائم، وكذا قيامها بكل الإجراءات والتدابير لدراسة واقع الجريمة الإلكترونية، ومكافحة جرائم الأنترنت لحماية شعبها من هذا الخطر المتلون وغير المحدود، إضافة إلى تشجيعها القيام بحملات تحسيسية وتوعية من قبل مهنيين ومتخصصين في هذا المجال، وضع برامج وخطط استراتيجية ومن ذلك تقديم تقرير حول حماية مستخدمي الانترنت[4]، الأمر الذي

[1] Loi n° 92-683 du 22 juillet 1992, portant réforme du code pénal, text origine au 01 mars 1994.

[2]-Art 462-2 du A.C.P. F dispose que ; « quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de deux mois à un an et d'une amende de 2000 f à 50000 f ou de l'une de ces deux peines… » Loi n°88-19 du 05 janvier 1988 relative à la fraude informatique, JORF du 06 janvier 1988, P 231.Sur le site ;www.legifrance.gouv.fr

[3]-Art 323-1 ; « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 100 000 f d'amende… » Loi n° 92-683 du 22 juillet 1992, portant réforme du code pénal, texte origine au 01 mars 1994.

[4] -Remise du Rapport «Protéger les internautes» remettre par Marc Robert, Procureur général prées la cour d'appel de Riom, le rapport du group de travail interministériel sur la lutte contre la cybercriminalité, communiqué de presse, No 185, Paris, le 30 juin 2014,sur le site: www.presse.justice.gouv.fr

قام به فريق عمل وزاري تحت إشراف مارك روبرت النائب العام للمحكمة استئناف[1]، والملاحظ أن المشرع الفرنسي لم يدخر أي جهد في مكافحته لجرائم أنظمة المعالجة الآلية في كل فرصة تسمح بالتعديل، فقد بدأ مبكرا في مواجهته لهذه الجرائم، ولم يتأخر،عن أي إجراء تعديلي كلما تطلب الأمر ذلك.

وقام المشرع الفرنسي مرة أخرى بتشديد العقوبة، وذلك بموجب المادة 45 من الفصل الثاني من القانون رقم 4-57 في سنة 2004المتعلق بالثقة في الإقتصاد الرقمي لتصبح العقوبة ضعف عما كانت عليه، وهي الحبس (02) سنتين والغرامة (30000) ثلاثون ألف يورو.[2]

أما عقوبة الدخول أو البقاء غير المصرح به وفي صورته المشددة، حيث جعل المشرع ما يترتب عن الدخول أو البقاء بدون قصد من أضرار كظرف مشدد، فكانت في قانون الغش المعلوماتي السنة 1988 محدد بالحبس لمدة من (02) شهرين إلى (02) سنتين وبغرامة من (10000) عشرة ألاف فرك فرنسي إلى (100000) مائة ألف فرك فرنسي وذلك في حالة ترتب عن الدخول أو البقاء حذف أو تعديل للبيانات وتعطيل النظام.[3]

وكذا في قانون العقوبات الجديد لسنة 1994 ليحتفظ بالحد الأقصى العقوبة الحبس ورفع الغرامة إلى (30000) ثلاثون ألف يورو، أما قانون العقوبات لسنة 2004 كذلك زاد من عقوبة الحبس إلى (03) ثلاثة سنوات والغرامة لتصبح (45000) خمسة وأربعون ألف يورو[4].

[1]-Art 462-2/2 ; «Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de deux mois à deux ans et l'amende de 10000 F à 100000 F >> la loi n° 88-19 précédente, www.presse.gouv.fr.

[2] --رشيدة بوبكر، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، ط1، منشورات الحلبي الحقوقية، بيروت –لبنان،2012، ص319.

[3]-Art 462-2/2 ; « Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de deux mois à deux ans et l'amende de 10000 F à 100000 F >> la loi no 88-19 précédente.

[4] Art 323-1 alinéa 2, « Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros

ليأتي المشرع الفرنسي في سنة 2012 بفقرة جديدة من نفس المادة، ويتفرد بها على غرار المشرع الجزائري وغيره من المشرعين، ويعاقب بعقوبة أشد إذا كان الدخول أو البقاء سواء في صورته البسيطة أو المشددة يرتكب على نظام معالجة آلية للبيانات الشخصية التي تنفذها الدولة.[1]

2-عقوبة جريمة الإتلاف المعلوماتي أو تخريب منظومة معلوماتية:

2.1- في التشريع الجزائري: اخضع المشرع الجزائري لمن تعمد منذ البداية الإضرار بالمعلومات المتضمنة في نظم المعالجة الآلية،أو تخريب المنظومة في حد ذاتها لعقوبة أشد عن من دخل أو بقي بدون تصريح وترتب عن ذلك ضرر وفقا للمادة 394 مكرر 1، ولا شك أن المشرع قد شدد العقوبة في هذه الصورة عن العقوبة في الصورة الأولى لجريمة الإختراق المعلوماتي، وذلك راجع إلى توفر عنصر القصد منذ بداية ارتكاب فعل الإتلاف، حددت العقوبة ب (06) ستة أشهر حبس إلى (03) ثلاثة سنوات وغرامة من (500000) خمسمائة ألف إلى (2.000.000) اثنان مليون دينار جزائري لكل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش، ولم ينص على إتلاف أو تخريب نظام اشتغال منظومة المعالجة الآلية للمعطيات مكتفيا بنص المادة 394 مكرر عقوبات، إن كان إدخال معلومات فيها مثل بعض الفيروسات قد يترتب عنه تعطيل اشتغالها.

2.2- في التشريع الفرنسي: كذلك المشرع الفرنسي نص على عقوبات إتلاف المعطيات والمعلومات المتضمنة في أنظمة المعالجة الآلية، وعلى إتلاف أو تعطيل تلك الأنظمة بموجب المادتين 462-3 و462-4 من القانون 88-19 فكانت عقوبة إتلاف أو تعطيل نظام المعالجة

d'amende » Du code pénal français modifié par la loi n° 2004-575 du juin 2004 pour la confiance dans l'économie numérique, art 45, JORF n°0143 du 22 juin 2004, P11168, texte n°02

[1]- Art 323-1 alinéa 3 du code pénal ; « Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende » Modifié par LOI n°2012-410 du 27 mars

الآلية للمعلومات هي الحبس من (03) ثلاثة أشهر إلى (03) ثلاثة سنوات وغرامة (10000) عشرة آلاف فرك إلى (100000) مائة ألف فرك فرنسي أو بإحدى العقوبتين[1].

وعقوبة إتلاف معلومات متضمنة في نظام معلوماتي هي بالنسبة للحبس نفس عقوبة تعطيل النظام الحبس من (03) ثلاثة أشهر إلى (03) ثلاثة سنوات،والغرامة اقل منها مقارنة بسابقتها بالنسبة لحدها الأدنى والضعف خمس مرات بالنسبة لحدها الأقصى وهي(2000) ألفين فرك إلى (500000) خمس مائة ألف فرك فرنسي أو بإحدى هاتين العقوبتين[2] .

وبعد تعديله لقانون العقوبات الجديد الذي أصبح ساريا بداية من مارس 1994، جعل العقوبات في حدها الأقصى فقط وهي واحدة سواء بالنسبة لإتلاف المعلومات أو إتلاف النظام وتعطيله، بأن أصبحت عقوبة الحبس (03) ثلاثة سنوات وبغرامة (45000) خمس وأربعون ألف يورو دون أن تكون للقاضي سلطة تقديرية بين العقوبتين وذلك بموجب المادتين 232-2 و323-3 من قانون العقوبات الفرنسي المعدل والمتمم، ليعود المشرع الفرنسي من جديد ويستجيب للمستجدات بتعديله لهاته المواد بموجب القانون رقم 2004-575 ويرفع العقوبات السابقة بالنسبة لجريمة الإتلاف سواء بالنسبة للمعطيات أو البيانات أو بالنسبة لتشغيل النظام بأن يعاقب على ذلك بالحبس لمدة (05) خمس سنوات وغرامة (75000) خمس وسبعون ألف يورو.

ولقد فسر تقارب العقوبتين بالنسبة لصور الإتلاف المعلوماتي من قبل الجمعية الوطنية الفرنسية بالتقارب الكبير بين الجريمتين، ويتعذر التمييز بينهما في بعض الأحيان، كما فسر أن فعل إعاقة النظام يكون نتيجة إدخال معلومات وهي صورة من صور إتلاف أو التلاعب بالمعلومات[3].

[1]-Art 462-3 ; « quiconque aura intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 10 000 F à 100 000 F ou de l'une de ces deux peines ». Loi n°88-19 précédent.

[2]-Art 462-4 ; «quiconque aura intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 2000 F à 500000 F ou de l'une de ces deux peines» L

[3] - محمد خليفة، الحماية الجنائية المعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، 2007، ص192.

ومؤخرا في 2014 عاد ليعدل المادة 233-3[1] ويضيف المشرع الفرنسي في المادتين 323-2 و323-3 زيادة عقوبة الحبس (07) سبع سنوات وغرامة (100000) مائة ألف يورو إذا وقع الإتلاف المعلوماتي أو جريمة التلاعب المعلوماتي على نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة.

3: عقوبة جريمة التعامل في معلومات غير مشروعة:

هذه الجريمة نص عليها كل من التشريع الجزائري والتشريع الفرنسي:

3.1-التشريع الجزائري: عاقب على هذه الجريمة بالحبس من (02) شهرين إلى (03) ثلاثة سنوات وبغرامة من (1.000.000) مليون دينار إلى (5.000.000) خمسة ملايين دينار جزائري، وذلك بموجب المادة 394 مكرر 2 الفقرة 1 عقوبات المعدل والمتمم، ويلاحظ أن عقوبة هذه الجريمة مقارنة مع الجريمتين السابقتين، أن المشرع خفض من الحد الأدنى لعقوبة الحبس بداية من شهرين ورفع من عقوبة الغرامة كحد أقصى هو خمسة ملايين دينار جزائري، وقد يرجع السبب في ذلك إلى أن الأضرار المترتبة عن جريمة التعامل في معلومات غير مشروعة قد تفوق بكثير الأضرار المترتبة عن الجريمة الأولى والثانية.

3.2- التشريع الفرنسي: يعاقب عليها المشرع الفرنسي بموجب المادة 323-3-1 عقوبات المضافة بموجب القانون 2004-575 المتعلق بالثقة في الإقتصاد الرقمي، والمعدلة بموجب القانون رقم 2013-1168،وأن العقاب على هذه الجريمة يكون بنفس العقوبة المقررة للجريمة نفسها، أي العقوبة المقررة لجريمة الدخول أو البقاء غير المصرح بهما أو جريمة إتلاف المعلومات، أو نظم المعالجة الآلية التي يمكن أن تؤدي البرامج والأجهزة والوسائل المتعامل فيها إلى ارتكابها أو بعقوبة أشد.[2]

[1]-Art 323-3 ; « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de

[2]-Art 323-3-1 du C.P.F« Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction ellemême ou pour

اعتبر المشرع الفرنسي وهو ما لم يقم به المشرع الجزائري، أن هذه الجريمة من الأعمال التحضيرية لجريمة أخرى قد تكون للتحضير للقيام بدخول غير مصرح أو إتلاف معلوماتي لذلك عاقب بنفس عقوبة الجريمة المحضر لها، أو بعقوبة أشد وقد أحسن الفعل المشرع الفرنسي في ذلك.

ثانيا: العقوبات التكميلية: نص القانون على عقوبات تكميلية يحكم بها إلى جانب العقوبات الأصلية والمتمثلة في المصادرة والغلق وهو ما سيتم شرحه كما يأتي:

المصادرة: يتم مصادرة الأشياء التي يتم حيازتها واستخدامها لأغراض إجرامية، حيث تشمل الأجهزة والبرامج والوسائل المستخدمة في إرتكاب جريمة من الجرائم الماسة بأنظمة المعالجة الآلية، ولقد نص المشرع الجزائري في المادة 394 مكرر 6 على أنه: مع الإحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة،وكذلك المشرع الفرنسي نص على عقوبة مصادرة الأشياء التي استخدمت في ارتكاب جرائم المعالجة الآلية بموجب المادة 323-5 الفقرة الثالثة من قانون العقوبات الفرنسي[1].

الغلق: إلى جانب عقوبة المصادرة نص المشرع على عقوبات تكميلية أخرى وهي الغلق، ويقصد بها وفقا لما جاء في المادة 394 مكرر 6: إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على ذلك إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.

غير أن المشرع لم يحدد مدة الغلق، وهل يكون الغلق نهائيا؟،وبالنسبة للمشرع الفرنسي نص عليها في المادة 323-5 الفقرة 4 على "الغلق لمدة (5) خمس سنوات أو أكثر للمؤسسات أو الواحد أو أكثر من فروع المشروع الذي أستخدم في ارتكاب الجريمة وإضافة إلى عقوبة الغلق والمصادرة،

l'infraction la plus sévèrement réprimée » Modifié par Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JORF n'0294 du 19 décembre 2013 page 20570 texte n° 1

[1]-I-Art 323-5 alinéa 3 du C.P.F: «Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes: 3. La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

نص المشرع الفرنسي على عقوبات أخرى تكميلية وجوبية وحسب طبيعة كل جريمة وظروفها بموجب نفس المادة.[1]

الفرع الثاني: العقوبات بالنسبة للأشخاص المعنوية:

كرس القانون مبدأ المسؤولية الجزائية للشخص المعنوي، وقرر له عقوبات، حيث أقر المشرع الجزائري بذلك بموجب المادة 51 مكرر من قانون العقوبات واستثنى الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام كونها هي الحامية للمجتمع وتحافظ على أمن وسلامة الأشخاص.

ويكون الشخص المعنوي مسؤولا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون عليه،وقد نص المشرع في المادة 394 مكرر 4 على الحد الأقصى للعقوبة المقررة للشخص المعنوي وهي غرامة تعادل (05) خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

أما إذا ارتكبت إحدى الجرائم السابقة من شخص معنوي على إحدى الجهات العامة أو استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، بتطبيق عقوبات أشد حسب المادة 394 مكررة عقوبات، وبالتالي تضاعف العقوبة مرتين إذا كانت من شخص معنوي ضد شخص معنوي أو أحد الجهات العامة، وبذلك يكون مجموع الغرامة 10 مرات أضعاف الغرامة المقررة للشخص الطبيعي.

[1]- Art 323-5 du C.P.F « Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes:

1 L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26;

2 L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

4 La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5 L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;

6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7* L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35

أما بخصوص المشرع الفرنسي، نجده قد ضاعف الغرامة إلى 05 أضعاف ما يفرض على الشخص الطبيعي بموجب الفقرة الأولى من المادة 323-6 والتي أحالت في تحديد العقوبات وكيفيتها إلى مواد أخرى من قانون العقوبات.[1]

[1]-Art 323-6 du C.P.F Modifié par LOI n°2009-526 du 12 mai 2009.

المبحث الثاني:مكافحة الجريمة الإلكترونية في القانون الدولي والمشرع الجزائري

إن التحقيق هو إجراء من أهم الإجراءات التي تتخذ بعد وقوع الجريمة، ذلك لما له من أهمية في التثبت من حقيقة وقوعها وإقامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف أنواعها من أجل استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه، وهناك تشابه بين التحقيق في الجرائم الإلكترونية وبين التحقيق في الجرائم التقليدية، فهي جميعا تحتاج إلى إجراءات تتشابه في عمومها مثل المعاينة والتفتيش والخبرة والإستجواب والشهود وجمع وتحليل الأدلة، إلا أن التحقيق في الجرائم المعلوماتية له خصوصية خاصة، لأنه يتم في بيئة رقمية.

المطلب الأول: إجراءات التحقيق و وسائل الإثبات في الجريمة الإلكترونية

جمع الأدلة و وسائل الإثبات في الجرائم الإلكترونية يستخلص من البيئة الرقمية، والتي تعتبر مسرحا للجريمة، وبما أن الدليل يقوي من إثبات الجريمة، يستلزم أن يكون من ذات طبيعتها التقنية، وتحيط بعملية جمع الأدلة العديد من الصعاب، إلا أنه لا مناص من مواصلة جمع الأدلة و وسائل إثبات مع التطوير المستمر لوسائل البحث، والتكيف مع طبيعة الجرائم المعلوماتية.

الفرع الأول: إجراءات التحقيق:

أولا: مرحلة التقصي والمعاينة: وهي ملاحظة وفحص حسي مباشر لأي شيء له علاقة بالجريمة لإثبات حالتها، والكشف والتحفظ على كل ما قد يفيد من الأشياء في كشف الحقيقة.

وتكمن أهمية المعاينة في دورها لتصور كيفية وقوع الجريمة وظروف ملابساتها وتوفير الأدلة،والمعاينة في مسرح الجريمة تتيح أمام المحقق الكشف عن طريق معاينة الآثار المادية التي خلفها ارتكاب الجريمة من مخبر الحقوق والحريات في الأنظمة المقارنة والجريمة، والتحفظ على الأشياء التي تفيد التحقيق، لكن بالنسبة للجرائم الإلكترونية قلما تخلف آثار مادية، لذلك وجب مراعاة قواعد وإرشادات فنية خاصة مثل: تصوير الحاسوب وملحقاته، إثبات التوصيلات، عدم نقل مادة المعلوماتية من مسرح الجريمة.[1]

[1]–عبد الفتاح بيومي حجازي، مبادي في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2006، ص192.

ثانيا: مرحلة التفتيش وضبط الأدلة:

أولا: التفتيش:وهو إجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة، تحقق وقوعها في محل يتمتع بحرمة، وذلك وفقا للضمانات والقيود المقررة قانونا، ويعد التفتيش في نظم المعالجة الآلية من أخطر المراحل، لأنه يكون على طابع غير مادي، ولا يعدو إلا أن يكون معلومات إلكترونية ليس لها مظهر محسوس خارجيا، والتفتيش بنصب على الجانب المادي والمنطقي للحاسوب معا.[1]

تفتش المكونات المادية للحاسوب: إن التفتيش الواقع على المكونات المادية للحاسوب لا توجد فيه مشكلة في التنفيذ، لأنه يرد على أشياء مادية لا خلاف فيها لقواعد القانون، لأنه تطبق عليه القواعد التقليدية، لكن مع الأخذ بعين الإعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وإمكانية إتلافها، ونظام التفتيش تنطبق عليه الضمانات المقررة قانونا.[2]

تفتيش المكونات المنطقية للحاسوب: ولقد اختلف الفقه الجنائي في مسألة مدى قابلية البيانات المعلوماتية لأن تكون موضوعا للتفتيش من عدمه طبقا للنصوص التقليدية، وهو ما أخذ بالمشرعين إلى سن قوانين إجرائية جديدة تنص على إمكانية تفتيش المكونات المنطقية للحاسوب، وهذا ما ذهب إليه المشرع الفرنسي في تعديله للنصوص التي تحكم التفتيش، وكما نص المشرع الإنجليزي على جواز تفتيش نظم الحاسوب المادية والمعنوية، وقد صرحت الإتفاقية الأوروبية المتعلقة بجرائم تقنية المعلومات، أنه يحق للدول الأعضاء تفتيش نظام الحاسوب أو جزء منه أو المعلومات المخزنة فيه و وسائط التخزين،والتفتيش في البيئة الرقمية التي تخضع لشروط شكلية وأخرى موضوعية تختلف عن شروط التفتيش في البيئة التقليدية.[3]

---

[1]–المرجع نفسه، ص 192.

[2]– عبد الفتاح بيومي حجازي، المرجع نفسه، ص 192.

[3]–محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، رسالة ماجستير، قسم علوم الشرطة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص76–80

ثانيا: مرحلة ضبط الأدلة: أما عن مرحلة ضبط الأدلة فهو وضع اليد على الشيء المتصل بالجريمة ويفيد في كشف الحقيقة وعن مرتكبيها، ويفيد في ضبط الأدلة في التحقيق الجاري بشأن الجريمة.[1]

وضبط الأدلة في الجرائم الإلكترونية يتصل بضبط المكونات المادية لأنظمة الحاسوب، وضبط المكونات المنطقية والبرمجيات، وكذا ضبط المعطيات التي تتناقل أو يجري تبادلها في نطاق شبكة المعلومات التي تربط الحواسيب وما يتصل بها[2]، وعلى هذا الأساس فإن من الأشياء التي يتم ضبطها والتحفظ عليها في الجرائم الإلكترونية والتي لها قيمة في إثبات تلك الجرائم ونسبتها إلى المتهم هي جهاز الحاسوب وملحقاته، وضبط المعدات المستعملة في الشبكة كجهاز المودم، ووسائط تخزين البيانات والمعطيات، وضبط البرمجيات.

الفرع الثاني: وسائل الإثبات في الجريمة الإلكترونية:

إن وسائل الإثبات في الجرائم الإلكترونية لها طبيعتها الخاصة بالمقارنة بوسائل الإثبات التقليدية، فوسائل الإثبات تدخل في إطار اختصاص القضاء، والذي يثبت ويدعم من خلالها القضاء في الجريمة الإلكترونية المرتكبة من طرف المجرمين، والتي هي محل التحقيق.

أولا: الخبرة:وهي إجراء بمقتضاه يكلف القاضي شخصا من ذوي الإختصاص يسمى خبيرا بمهمة معينة تتطلب تحقيقات واستقصاءات قد تكون على جانب من التعقيدات، توصلا لإعطاء القاضي معلومات ورأي فني بشأن أمور واقعية لا يمكن الحصول عليها بنفسه، ويثبت الخبير تحقيقه مع الرأي الذي توصل إليه في تقرير خطي إلى القاضي.

فالخبرة هي أحد أهم وسائل جمع الأدلة، وتأخذ حكم الشاهد من حيث الحجية أو القوة في الإثبات، وبالنظر إلى الطبيعة الخاصة للجرائم المعلوماتية فإن إماطة اللثام عنها تحتاج إلى خبرة

[1] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2001، ص170-171.

[2] - المرجع نفسه، ص281-282.

فنية منذ بدء مرحلة التحري عن هذه الجرائم، وتستمر إليها في مرحلتي التحقيق والمحاكمة، وتخضع لشروط شكلية وشروط موضوعية لابد من الالتزام بها لتعتمد لدى القضاء.[1]

ثانيا: الإستجواب وسماع الشهود:

الإستجواب: ويعرف بأنه مساءلة المتهم ومناقشته عن وقائع القضية المنسوبة إليه ارتكابها ومجابهته بالأدلة وسماع ما لديه من دفوع للتهمة المنسوبة إليه، والهدف من الإستجواب هو كشف الحقيقة واستظهارها بالطرق القانونية، واستجواب المتهم في الجرائم الإلكترونية تحكمه ذات القواعد العامة لإستجواب متهم في أي جريمة تقليدية، إلا أنه لابد أن تكون السلطة المختصة التي تتولى الإستجواب مؤهلة للتحقيق في الجرائم المعلوماتية حتى يمكن الإستيعاب والتعامل مع مفردات الجريمة الإلكترونية، وقد أحاط المشرع الإستجواب بعدة ضمانات لابد من الإلتزام بها لضمان حقوق المتهم[2].

سماع الشهود:سماع الشهود كسائر إجراءات التحقيق في الطريقة التقليدية، فالقاضي له أن يسمع الشهود أو يستغني عنهم، فإذا قرر سماعهم فهو الذي يحدد من يجب الإستماع إليه ومن يمكن الإستغناء عنه، والأمر متروك للسلطة التقديرية للقاضي، فالشاهد في الجرائم الإلكترونية يطلق عليه اسم الشاهد المعلوماتي أو الإلكتروني تميزا له عن الشاهد التقليدي، والمقصود بالشاهد في الجريمة الإلكترونية هو الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسوب، والذي تكون لديه معلومات جوهرية، أو هامة لازمة للولوج في نظام المعاجلة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة[3]، وتضم طائفة الشهود: مشغلوا الحاسوب، خبراء البرمجة، محللوا البيانات، مهندسوا الصيانة، مديروا النظم.

المطلب الثاني: مكافحة ومواجهة الجرائم الإلكترونية في القوانين الدولية والتشريع الجزائري

مع تزايد صور وحجم الخسائر والأضرار الناجمة عن الجرائم الإلكترونية، والتي تتخطى في أغلب أحيانها الحدود لتطال اعتداءها دول ومؤسسات أخرى، ومع تميزها بالعالمية، وبكونها عابرة

[1]- محمود الشنكيات، الإثبات بالمعاينة والخبرة في القانون المدني، دار الثقافة للنشر والتوزيع، الأردن، 2008، ص98

[2]–عبد الأمير العكيلي وسليم حربة، أصول المحاكمات، ج1 و2، دار الكتب للطباعة والنشر، القاهرة، 1980، ص44

[3]–عبد الفتاح بيومي حجازي، المرجع السابق، ص 339.

للحدود، وأثبت الواقع العملي أن أي دولة لا تستطيع بجهودها المنفردة مواجهة الجريمة الإلكترونية، لذلك عملت الدول على توحيد جهودها لمكافحتها.

الفرع الأول: مكافحة الجرائم الإلكترونية في القوانين الدولية

إن مكافحة الجرائم الإلكترونية لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي والجنائي، وفي إطار الجهد الدولي المبذول، فإن هناك العديد من الهيئات والمنظمات الدولية التي تلعب دورا ملحوظا في إطار إبرام الإتفاقيات في محاولة منها لترسيخ وجوب التعاون الدولي لمواجهة الجرائم الإلكترونية.

أولا: جهود الأمم المتحدة: تبذل الأمم المتحدة جهودا لا يستهان بها في مجال محاولة التصدي للجرائم الإلكترونية،وتؤكد على وجوب تعزيز العمل المشترك بين أعضاء المنظمة من أجل التعاون للحد من انتشارها وتعاظم آثارها، وقد حظيت الجرائم الإلكترونية بإهتمام مؤتمرات الأمم المتحدة، وأبرزها ما جاء في هذا المجال مايلي:

عقد منظمة الأمم المتحدة المؤتمر الثالث عشر[1] لمنع الجريمة والعدالة الجنائية من 12 إلى 19 أفريل 2015 بدولة قطر، وكان الموضوع الرئيسي للمؤتمر "إدماج منع الجريمة والعدالة الجنائية في جدول أعمال الأمم المتحدة الأوسع للتصدي للتحديات الإجتماعية والإقتصادية، وتعزيز سيادة القانون على الصعيدين الوطني والدولي، ومشاركة الجمهور"، وقررت الجمعية العامة قرارها (67/184) فيما يلي:

- ✓إنشاء حلقات عمل من بينها تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدي للأشكال المتطورة للجريمة، منها الجرائم المعلوماتية.
- ✓ عقد منظمة الأمم المتحدة المؤتمر الثاني عشر[2] من 12 إلى 19 أفريل 2010 بالبرازيل تحت عنوان "استراتيجيات شاملة لتحديات عالمية لنظم منع الجريمة والعدالة الجنائية وتطورها في عالم

[1] حكومة قطر الإلكترونية، صفحة المؤتمر ،مجلة الحقوق والحريات:
http://www.moi.gov.qa/UNCCPCJDoha/Arabic/Previous_Congresses.html

[2] –موقع خاص بقرارات الأمم المتحدة

متغير"، وتضمن جدول أعمال المؤتمر ثمانية بنود من بينها جرائم الإنترنت، حيث دعت لجنة منع الجريمة والعدالة الجنائية إلى عقد اجتماع لفريق من خبراء حكوميين دولي مفتوح العضوية لدراسة شاملة لمشكلة الجريمة المعلوماتية وتدابير التصدي لها.

- قرارات وتوصيات الجمعية العام للأمم المتحدة:[1]

✓القرار (45/121) العام 1990، وكذلك نشر دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها في العام 1994- القرار رقم (55/63) المؤرخ في 2000/12/04، والقرار رقم (56/121) المؤرخ في 2001/12/19 بشان" مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات ".

✓يدعو هذا القرار الدول الأعضاء، إلى عقد وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، على أن تأخذ بالإعتبار عمل لجنة منع الجريمة والعدالة الجنائية،القرار رقم (57/2397) في 2003/01/31 والقرار رقم (58/199 المؤرخ في 2004/01/30 بشأن " إنشاء ثقافة عالمية للأمن السيبراني،ودعوة الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني، قرار لجنة مكافحة المخدرات (48/5) حول تعزيز التعاون الدولي من أجل منع استخدام شبكة الإنترنت لإرتكاب الجرائم المتصلة بالمخدرات".

✓التوصيات والمبادئ التوجيهية للهيئة الدولية لمراقبة المخدرات (INCB) التي نشرت عام 2005 توصيات للحد من انتشار المبيعات غير المشروعة من المواد الخاضعة للرقابة ولاسيما المستحضرات الصيدلانية عبر الإنترنت.

ثانيا: جهود الإتحاد الدولي للإتصالات:[2] يوفر الإتحاد الدولي للإتصالات الذي يضم 192 دولة و700 شركة من القطاع الخاص والمؤسسات الأكاديمية، منبرا استراتيجيا للتعاون بين أعضائه

---

http://www.un.org/arabic/documents/instruments/subj_ar.asp

[1]–المرجع نفسه.

[2]- موقع الاتحاد الدولي للاتصالات:

http://www.itu.int/osg/csd/cybersecurity/gca/global-strategic, report/index.htm

باعتباره وكالة متخصصة داخل الأمم المتحدة، وقد وضع الإتحاد الدولي للإتصالات مخططا لتعزيز الأمن الإلكتروني العالمي، ومن أهم أهدافه الرئيسية ما يلي:

✓وضع استراتيجيات لتطوير نموذج التشريعات السيبرانية يكون قابلا للتطبيق محليا وعالميا بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة.

✓وضع استراتيجيات لتهيئة الأرضية الوطنية والإقليمية المناسبة لوضع الهياكل التنظيمية والسياسات المتعلقة بجرائم الإنترنت.

ثالثا: جهود المنظمة الدولية للشرطة الجنائية الإنتربول: وتهدف المنظمة إلى تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأعضاء وعلى نحو فعال في مكافحة الجريمة الإلكترونية، من تجميع للبيانات والمعلومات المتعلقة بالمجرم والجريمة الإلكترونية كحد سواء وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول الأعضاء وتبادلها لتلك المعلومات والبيانات فيما بينها، بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأعضاء، ومدها بالمعلومات المتوفرة لديها على إقليمها وخاصة بالنسبة للجرائم المتشعبة في عدة دول ومنها جرائم الإنترنت.

رابعا: جهود المنظمة العالمية للملكية الفكرية: تهدف إلى تشجيع النشاط الإبتكاري، وتطوير إدارة الإتحادات في مجال حماية الملكية الصناعية وحماية المصنفات الأدبية والفنية، واهتمت بتوفير الحماية القانونية للبرامج الإلكترونية وقواعد البيانات، وتم الإتفاق على توفيرها بواسطة الإتفاقيات العالمية، وخاصة "اتفاقية التريبس" و"اتفاقية بيرن" اللتان حثت فيهما الدول الأعضاء على ضرورة تطوير تشريعاتها، وخاصة تشريعات حقوق المؤلف، كما يلزم الإتفاق الدولي الأعضاء في المنظمة بوجوب فرض إجراءات تنفيذية، وتدابير مدنية وإدارية، وعقوبات جنائية لمواجهة أي اعتداء على حقوق المؤلف وخاصة القرصنة، وتنص المادة (04) من منظمة العالمية للملكية الفكرية[1]، المعتمدة

[1]– المنظمة العالمية للملكية الفكرية www.wipo.int.

سنة 1996على أنه "تتمتع برامج الحاسوب بالحماية باعتباره مصنفات أدبية وتطبق تلك الحماية على برامج الحاسوب أيا كانت التعبير عنها".

خامسا: جهود منظمة التعاون الإقتصادي والتنمية: تضم هذه المنظمة في عضويتها 34 دولة،حيث وضعت المنظمة توصيات إرشادية بخصوص أمن نظم المعلومات، ومن مجمل أعمال منظمة التعاون الإقتصادي والتنمية حول الجرائم الإلكترونية حصل اتفاق على ضرورة أن يغطي قانون العقوبات في كل دولة الأفعال التالية:

- ✓التلاعب في البيانات المعالجة آليا بما في ذلك محوها.
- ✓التجسس المعلوماتي.
- ✓التخريب المعلوماتي.
- ✓قرصنة البرامج.
- ✓الدخول غير المشروع على البيانات أو نقلها، واعتراض استخدام المعطيات أو نقله.

سادسا: جهود الاتحاد الأوروبي:[1] أعلنت "يوروبول" في2014/09/01، وكالة تطبيق القانون الأوروبية المتخصصة في مكافحة الجرائم والإرهاب في دول الاتحاد الأوروبي، عن إنشائها قوة خاصة لمحاربة الجرائم المعلوماتية في دول الإتحاد، كما أن عملها يمتد إلى دول أخرى.

وستكون مهمة القوة الجديدة التنسيق مع التحقيقات الدولية لإتخاذ التدابير اللازمة في مواجهة التهديدات الرئيسية على الإنترنت، مثل البرمجيات الخبيثة وخاصة ما يستهدف منها القطاعات المالية ومكافحة عمليات الإحتيال الإلكترونية والمواقع التي تبيع الممنوعات وغير ذلك، وستبدأ القوة التي أطلق عليها اسم "J-CAT" وسيكون مقرها ضمن المركز الأوروبي للجرائم الإلكترونية "EC3" التابع لليوروبول، ويتضمن فريق العمل المشترك ضد الجرائم الإلكترونية الأعضاء في الإتحاد الأوروبي، بالإضافة إلى شركاء آخرين لا ينتمون إلى الإتحاد الأوروبي من وكالات تطبيق القانون.

[1]– الموقع الإلكتروني لليروبول: WWW.eurpol.europa.eu.

وانضمت للتعاون مع هذه القوة الجديدة مجموعة من الدول منها كندا واستراليا وألمانيا وفرنسا وهولندا، وإيطاليا وإسبانيا والمملكة المتحدة والولايات المتحدة الأمريكية.

سابعا : جهود اتفاقية المجلس الأوروبي: اعتمد المجلس الأوروبي الطابع الدولي لجرائم الكمبيوتر منذ العام 1976، وفي العام 1996 أنشأت اللجنة الأوروبية لمشاكل الجريمة (CDPC) لجنة خبراء للتعامل مع مشكلة الجريمة السيبرانية، وعملت اللجنة بين سنة 1997 و2000 على الإتفاقية التي اعتمدها البرلمان الأوروبي في الجزء الثاني من جلسته العامة في شهر أفريل 2001، وتم التصديق على الإتفاقية من قبل 30 دولة بحلول العام 2010، واتفاقية جرائم الإنترنت هي المعاهدة الدولية الأولى التي تسعى لمعالجة الجرائم الإلكترونية عبر التنسيق بين القوانين الوطنية وقوانين الدول الأخرى ومن أهم أهداف الاتفاقية.

✓توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية بتوفير الإجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة إلكترونيا، وجمع معلومات عن حركة البيانات وعن إمكان وجود تدخل في محتواها.

✓تتضمن الإتفاقية المبادئ العامة المتعلقة بالتعاون الدولي في: تسليم المجرمين، المساعدة الدولية المتبادلة، إعطاء المعلومات بصورة آلية، وإنشاء الولاية القضائية على أي جريمة.

ثامنا:جهود مجموعة الدول الثماني G8:[1] حيث اعتمد وزارة العدل والداخلية للبلدان الثمانية في اجتماعاتهم المختلفة سياسات المكافحة العديد من جرائم الإنترنت بالإستناد إلى المبادئ التالية:

عدم إتاحة ملاذات آمنة للمعتدين على تكنولوجيا المعلومات، والتنسيق بين جميع الدول المعنية في ملاحقة مرتكبي جرائم الإنترنت ومحاكمتهم، تدريب الموظفين المكلفين بتنفيذ القوانين، وتجهيزهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالية، بالإضافة إلى ذلك دعت دول الثمانية

[1]–موقع مجموعة الثمانية: www.Canadainternationalgc.ca/G8G8 recommandations on transnational crimes, 2011,

إلى مواصلة العمل حتى التوصل إلى حلول دولية ناجحة، من خلال عقد اتفاقات دولية، لمعالجة الجريمة ذات التقنية العالية والإستفادة من عمل المنظمات الدولية المختلفة.

ومن توصيات ال "G8" بالنسبة للجرائم الإلكترونية الموجودة في إطار الباب "D" من المعاهدة وتتلخص بما يلي:[1]

✓يتعين على الدول أن تجرم الإنتهاكات على حقوق الغير على الشبكة العنكبوتية التي تستوجب العقوبات الجزائية، وأن تعالج المشاكل المتعلقة بالتحقيقات القضائية بالتدريب الفعال لمنع الجريمة، وإقامة تعاون دولي فيما يتعلق بمكافحة هذه الانتهاكات وينبغي للدول أن تتخذ خطوات لمنع الجريمة ذات التقنية العالية.

الفرع الثاني: مواجهة الجرائم المعلوماتية في التشريع الجزائري:

سارع المشرع الجزائري كغيره من الدول إلى احتواء الجريمة المعلوماتية من خلال التعديلات التي أدخلها على قانون العقوبات وسن نصوص قانونية أخرى جديدة التي نستعرضها كما يلي:

أولا: الحماية من خلال قانون العقوبات: يعتبر قانون العقوبات وسيلة ردعية للكف عن ارتكاب الجرائم بصفة عامة، وبما أن الجرائم الإلكترونية تلحق أضرار بالغير فقد أقر المشرع عقوبات ردعية لتلك الجرائم وهي كالتالي:

أ. المساس بأنظمة المعالجة الآلية للمعطيات: وهي من أبرز الجرائم التي عالجتها المحاكم الجزائرية، وهذا بموجب القانون رقم (15/04)[2]المتعلق بقانون العقوبات،وذلك من خلال المواد (394 مكرر) إلى (394 مكرر7)، فمن خلال استقراء نصوص المواد حاول المشرع الجزائري حصر هذه الجرائم والعقوبات المقرر لها فيما يلي:[3]

[1]–موقع مجموعة الثمانية، المرجع نفسه (22).

[2]–القانون (04/15 المؤرخ في 10/11/2004المتعلق بقانون العقوبات الرسمية عدد 71 صادر في10/11/2004.

[3]–مولود ديدان، قانون العقوبات، دار بلقيس للنشر، الدار البيضاء، الجزائر، ط2012، مصححة ومحيثة، ص 135–137

✓جريمة دخول معالجة آلية للمعطيات عن طريق الغش: نصت عليها المادة(394 مكرر)[1] من قانون العقوبات، حيث تعاقب بالحبس والغرامة عند الدخول أو البقاء بالغش في المنظومة المعلوماتية، وفرق المشرع في هذه الحالة بين ما إذا كانت الجريمة بسيطة ومضاعفة العقوبة إذا ترتب عنها حذف أو تغيير في المنظومة، وبين ما إذا ترتب على ذلك تخريب لنظام اشتغال المنظومة.

✓جريمة إزالة أو تعديل معطيات في نظام المعالجة الآلية بطرق تدليسية، حيث نصت عليها المادة(394 مكرر1)[2] من قانون العقوبات، واعتبر المشرع الجزائري أن إزالة أو تعديل المعطيات التي يتضمنها النظام بطريق الغش عملا إجراميان ويقصد بإزالة المعطيات سواء جزئيا أو كليا إما بمحوها أو إتلافها أو تخريبها من أجل منع النظام القيام بمهامه أو تعطيل النظام المعلوماتي، وطرق متعددة شرحناها سابقا مثل نشر الفيروسات، أما تعديل المعطيات فيقصد به إما إدخال معلومات وهمية أو تزويرها في النظام المعلوماتي.

✓جرائم نشر حيازة أو الإتجار بالمعطيات المخزنة أو المعالجة التي نصت عليها المادة (394 مكرر2)[3] من قانون العقوبات، حيث تعد هذه الجريمة من أكثر الجرائم وقوعا في العالم الإفتراضي، ولقد اعتبر المشرع الجزائري عملية اصطناع برنامج مخصص لإرتكاب فعل الغش المعلوماتي أو إعداد برنامج ناقص من الناحية الفنية وخاصة المبرمج من أجل خلق فجوات وثغرات فيه لممارسة فعل الغش أو تجميع أو إلتقاط البيانات بغرض استغلالها أو نشرها، خاصة عن طريق الإنترنت أو الإتجار فيها من الجرائم المعاقب عليها، بحكم أن جريمة الإفشاء والنشر تتسم بخطورة على الحياة الخاصة.

✓جرائم المعالجة الآلية الماسة بالدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام: طبقا للمادة (394 مكرر)[4] من قانون العقوبات: حيث اعتبر المشرع الجرائم المعلوماتية التي

[1]–المادة (364 مكرر) من القانون (15/04)،المرجع السابق.

[2]–المادة (394 مكرر1)، المرجع السابق.

[3]– المادة (394 مكرر2)، المرجع نفسه.

[4]–المادة (394 مكرر 3)، المرجع السابق.

تستهدف الدفاع الوطني أو أي مؤسسة رسمية بمثابة ظرف تشديد، ويستخلص من نص المادة (394 مكرر3) من قانون العقوبات أن العقوبة المشددة على جميع الجرائم المنصوص عليها في المادة (394 مكرر) والمادة (394 مكرر1) و(مكرر2) من قانون العقوبات، وحرص المشرع الجزائري على ضمان حماية مطلقة لهيئات الدفاع الوطني ولمؤسسات الدولة الجزائرية، وتوسع في هذه الحماية وذلك بإدراج جميع الجرائم المعلوماتية[1]، المنصوص عليها في المادة (394 مكرر) من قانون العقوبات كلها.

✓الجرائم المعلوماتية للشخص المعنوي: نصت عليها المادة (394 مكرر4)[2]، من قانون العقوبات حيث أقر المشرع الجزائري المسؤولية الجزائرية للأشخاص المعنوية، وشدد عقوبة الغرامة في جرائم الإعتداء على نظم المعالجة الآلية، حيث أن الغرامة المطبقة على الشخص المعنوي تتراوح بين واحد إلى خمس أضعاف الغرامة المقررة على الشخص الطبيعي.

✓جريمة تكوين جمعية أشرار إلكترونيين لغرض التحضير للجرائم الماسة بأنظمة المعالجة الآلية: طبقا للمادة (394 مكررة)[3] من قانون العقوبات يتضح من خلال نص المادة أن العقوبات يطال من يشارك أي مجموعة أو في اتفاق الغرض منه التحضير أو الإعداد لإرتكاب الجرائم الإلكترونية مع توفر القصد الجنائي، كما يستخلص أن مجرد المشاركة أو الإتفاق المجسد بفعل مادي يوحي بالتحضير للجريمة خاصة أن ذلك يمكن أن يتم عبر الشبكات المعلوماتية.

✓العقوبات التكميلية: وفقا للمادة (394 مكرر6)[4] من قانون العقوبات: نص المشرع في هذه المادة على العقوبات التكميلية للجرائم السالفة الذكر، وتمثل في المصادرة للأجهزة المستعملة والبرامج والوسائل المستعملة، مع إلحاق ذلك بغلق المواقع وأماكن الإستغلال شريطة أن تكون بعلم صاحبها.

[1]–زيبحة زيدان، المعلوماتية في التشريع الجزائري، دار الهدى للطباعة والنشر، عين مليلة، الجزائر، 2001، ص100

[2]–المادة (394 مكرر4) من القانون رقم (04/15) المرجع السابق.

[3]– المادة (394 مكررة)، المرجع السابق.

[4]–المادة (394 مكرر6)، المرجع نفسه.

✓العقاب على الشروع في الجريمة الإلكترونية: طبقا لنص المادة (394 مكرر7) من قانون العقوبات[1]،أن فعل الشروع أو البدء في ارتكاب الجريمة يعاقب عليه بنفس العقوبة المقررة للجنحة ذاتها، ونظرا لكون جرائم الإعتداء على نظام المعالجة الآلية ذات وصف جنحوي، إذ أقر المشرع العقاب لها بمثل الجريمة نفسها.

ب. حماية حرمة الحياة الخاصة: من خلال التعديل الذي جاء في القانون رقم (06-23)[2] المتعلق بقانون العقوبات فالمادة (303 مكرر)[3] من قانون العقوبات تعاقب بالحبس والغرامة كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت سواء بإلتقاط أو تسجل أو نقل صور أو مكالمات خاصة أو سرية دون إذن رضا صاحبها، أما المادة (303 مكرر1)[4]، من قانون العقوبات، تعاقب بالعقوبة ذاتها على من يحتفظ أو يضع في متناول الجمهور الصور أو الوثائق بأية وسيلة كانت.

ج. حماية حرمة رموز الدولة: من خلال التعديل الذي جاء في القانون رقم (14/11)[5] المتعلق بقانون العقوبات، حيث نصت المادة (144 مكرر) منه[6]، على عقوبة الغرامة المالية فقط لكل من أساء لرئيس الجمهورية بأية وسيلة كانت أو بوسيلة إلكترونية وفي حالة العود تضاعف الغرامة.

ح. الحماية من خلال قانون الإجراءات الجزائية: حيث أن المادة (16) من قانون الإجراءات الجزائية[7]، وسعت من الإختصاص المحلي لضباط الشرطة القضائية فيما يتعلق بالبحث ومعاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ويمتد الإختصاص إلى كامل الإقليم الوطني، كما

---

[1]- المادة (394 مكرر 7).

[2]-القانون (23/06) المؤرخ في 20/12/2006، المتضمن قانون العقوبات، الجريدة الرسمية، عدد48، الصادرة في 24/12/2006

[3]- -المادة (303 مكرر)، المرجع نفسه.

[4]-المادة (303 مكرر1) من القانون (06/23) المرجع السابق.

[5]-القانون (14/11) مؤرخ في 02/08/2011 المتضمن قانون العقوبات، الجريدة الرسمية، عدد 44، صادرة في 10/08/2011

[6]-المادة (144 مكرر)، المرجع نفسه.

[7]-القانون (22/06) المؤرخ في 20/12/2006المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، عدد 84 صادرة في24/12/2006.

جاءت المادة (37) من قانون الإجراءات الجزائية[1]، والمادة (40) منه لتمكن كل من وكيل الجمهورية وقاضي التحقيق على تمديد الإختصاص المحلي إلى دائرة اختصاص محاكم أخرى في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

ثانيا:الحماية من خلال القوانين خاصة:هذه القوانين الخاصة شملت الحماية في قانون التأمينات الإجتماعية، وكذلك الحماية من خلال نصوص الملكية الفكرية، وأيضا الحماية في نصوص التوقيع الإلكتروني بالإضافة إلى الحماية المتعلقة بالمواصلات السلكية واللاسلكية[2].

أ. الحماية في قانون التأمينات الإجتماعية: بمقتضى أحكام قانون التأمينات الإجتماعية رقم (01/08)[3]المؤرخ في 2008/01/23 شدد العقوبة فيما يتعلق بالمساس غير المشروع للبطاقة الإلكترونية للمؤمن له اجتماعيا، وعاقب المشرع الجزائري كل من يسلك أو يستلم بهدف الإستعمال غير المشروع للبطاقة الإلكترونية للمؤمن له اجتماعيا المفتاح الإلكتروني لهيكل العلاج أو المفتاح لمهنيي الصحة طبقا للمادة (93 مكرر2)[4]، من نفس القانون، كما يشمل العقاب التعديل أو الحذف الكلي أو الجزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية، أو نسخ البرمجيات المتعلقة باستعمال البطاقة الإلكترونية، أو المحاولة على ارتكاب الفعل طبقا لنص المادة (93 مكرر3) منها[5]، كما أقر المشرع أيضا عقوبة للشخص المعنوي تتمثل في الغرامة ضعف المقررة للشخص الطبيعي طبقا لنص المادة (93 مكرر 5)[6] من ذات القانون، ومصادرة الأجهزة والوسائل المستعملة وكذا غلق المحلات وأماكن الاستغلال التي تكون محل الجنح.

---

[1]– المادة (37) والمادة (40) من القانون رقم (14/04) مؤرخ في 10/11/2004 يعدل ويتمم الأمر (155/66) المؤرخ في 08/06/1966المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، عدد، 71 صادرة في،10/11/2004

[2]–وعناد فاطمة زهرة، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، عدد 1، 2013، جامعة جيلالي اليابس سيدي بلعباس، ص 63

[3]–القانون (01/08) المؤرخ في 23/01/2008،المتعلق بالتأمينات الاجتماعية، الجريدة الرسمية، عدد 4)، صادرة في 27/01/2008.

[4]–المادة (93 مكرر2) من القانون رقم (01/08)، المرجع السابق.

[5]–لمادة (93 مكرر3)، المرجع نفسه.

[6]– المادة (93 مكرر 5).

ب. الحماية من خلال قانون الملكية الأدبية والفنية: حاول المشرع الجزائري مواجهة الجريمة الإلكترونية من خلال قانون الملكية الأدبية والفنية المتعلق بحق المؤلف والحقوق المجاورة الصادر بموجب الأمر رقم (05/03)[1] المؤرخ في 2003/07/23 المتعلق بحقوق المؤلف والحقوق المجاورة، حيث وسع قائمة المؤلفات المحمية، وذلك بإدماج برامج المعلوماتية، ضمن المصنفات الأصلية والتي عبر عنها بمصنفات قواعد البيانات وبرامج المعلوماتية، كما شدد العقوبات على المساس بحقوق المؤلفين خاصة المصنفات الرقمية التي تشملها الحماية.

ج. الحماية في نصوص التوقيع الإلكتروني: أصدر المشرع الجزائري قانون رقم 03/15[2] المتعلق بعصرنة العدالة، حيث تطرق في الفصل الثاني إلى المنظومة المعلوماتية المركزية لوزارة العدل والإشهاد على صحة الوثائق الإلكترونية وضمان حمايتها، أما في الفصل الثالث تعرض إلى إرسال الوثائق والإجراءات القضائية بالطريقة الإلكترونية، أما الفصل الخامس فتعرض إلى الأحكام الجزائية لحماية التوقيع والتصديق الإلكترونيين، حيث أن المادة (17)[3]، منه تعاقب على كل من يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع إلكتروني يتعلق بتوقيع شخص آخر، أما المادة (18)[4]فتعاقب كل شخص حائز على شهادة إلكترونية يستعملها بعد انتهاء صلاحيتها أو إلغائها.

د. الحماية المتعلقة بالموصلات السلكية واللاسلكية: تضمن الفصل الثاني من الباب الرابع من القانون رقم (03/2000)[5] المتعلق بالبريد والمواصلات السلكية واللاسلكية الأحكام الجزئية المترتبة على مخالفة النظام القانوني، فالأشخاص المرخص لهم تقديم خدمة المواصلات السلكية واللاسلكية،

[1]– الأمر (05/03) المؤرخ في 19/07/2003المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، عدد 44، صادرة بتاريخ23/07/2003.

[2]– القانون (03/15) المؤرخ في 01/02/2015المتعلق بعصرنة العدالة الجريدة الرسمية، عدد2، صادرة في 10/02/2015

[3]–المادة (17)، المرجع نفسه.

[4]–المادة (18)، المرجع نفسه

[5]–القانون (03/2000) المؤرخ في 05/08/2000الذي يحدد القواعد العامة المتعلقة بالبريد السلكية واللاسلكية، الجريدة الرسمية، عدد، المؤرخة في06/08/2000

والعمال متعاملي الشبكات العمومية الذين ينتهكون سرية المراسلات السلكية واللاسلكية، أو المساعدة على ذلك يعاقبون طبقا لنص المادة (137) من قانون العقوبات أما غيرهم ممن يرتكب هذه الأفعال يعاقب بالحبس والغرامة.

هـ. الحماية من خلال قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها رقم (04/09)[1]: وتكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية ويبين القواعد الوقائية التي تسمح بالرصد المبكر للإعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها، وقد جرم الأفعال المخالفة للقانون والتي ترتكب عبر وسائل الإتصال عامة وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة بما فيها شبكة الإنترنت، وعلى كل تقنية تظهر مستقبلا وقد حدد القانون الحالات التي يسمح فيها اللجوء إلى المراقبة الإلكترونية، كالأفعال الموصوفة بجرائم الإرهاب أو التخريب، أو الجرائم الماسة بأمن الدولة أو في حالة توفر معلومات عن احتمال الإعتداء على منظومة معلوماتية، وقد تعرض الفصل الأول من القانون إلى أهدافه وتحديد مفهوم التقنية، أما الفصل الثاني فقد تعرض إلى أحكام خاصة بمراقبة الاتصالات الإلكترونية، والفصل الرابع تعرض إلى القواعد الإجرائية الخاصة.

[1]– القانون (04/09) المؤرخ في 05/08/2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد47 الصادرة في ،16/08/2009

خلاصة الفصل الثاني:

نستخلص من خلال هذا الفصل أن الجريمة الإلكترونية والتي هي نوع من أنواع الجرائم في الإجرام المعاصر، تختلف عن باقي الجرائم المألوفة بالإضافة إلى صعوبة وضع تعريف جامع وموحد لها.

بالإضافة إلى أن المشرع الجزائري قام بمكافحتها بموجب تعديل قانون العقوبات رقم 04/15 المؤرخ في 11 ربيع الثاني عام 1436 الموافق 01 فبراير سنة 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، فوضع العديد من النصوص القانونية التي تجرم الإعتداءات الماسة بالنظم المعلوماتية بجميع أشكالها.

الخاتمة

الخاتمة:

لقد تناولنا من خلال الفصلين موضوعا مهما من الموضوعات المستحدثة، ألا وهو موضوع الجريمة الإلكترونية، ورأينا قبل بيان هذه الآليات أن توضيح ماهية الجريمة الإلكترونية، وبينا أيضا الخصائص التي تتميز بها الجريمة الإلكترونية، والتي تميزها عن غيرها من الجرائم، ولاسيما الجرائم التقليدية، كما أوضحنا أركان الجريمة الإلكترونية المتمثلة في الركن الشرعي والركن المادي والركن المعنوي، التي تتشارك فيها مع الجرائم التقليدية من حيث الشكل وتختلف فيه عنها من حيث المضمون، وبعد ذلك تطرقنا إلى سريان العقوبات لدى الأشخاص الطبيعية والأشخاص المعنوية والظروف المشددة للعقوبات لكل منهما، وبعد ذلك عرضا للآليات الوطنية والدولية لمكافحة الجريمة الإلكترونية، والتي قسمناها إلى قسمين هما: الإتفاقيات الدولية، والأجهزة والمنظمات الدولية المعنية بمكافحة الجرائم الإلكترونية في التشريع الجزائري لمكافحة الجرائم الإلكترونية، وقد اختتمنا دراستنا هاته بعدد من التوصيات والنتائج، وذلك على النحو التالي:

أولا: النتائج:

- ✓ بينت الدراسة أن القواعد التقليدية لا تكفي لوحدها لمكافحة الجرائم الإلكترونية.
- ✓ عدم وجود مفهوم مشترك لماهية الجريمة الإلكترونية، وكذلك عدم وجود تعريف قانوني موحد لها.
- ✓ عدم وجود تنسيق دولي كاف في مجال الجريمة الإلكترونية، ويرجع ذلك إلى عدم وجود معاهدة دولية شاملة لمواجهة الجريمة الإلكترونية، أو لإختلاف مفهوم الجريمة تبعا لإختلاف النظم القانونية.

ثانيا: التوصيات:

- ✓ ضرورة إضافة مقرر دراسي لطلاب كليات الحقوق يتضمن معلومات عن الحاسب الآلي وتقنياته وطرق الإثبات والتحقيق في القضايا المتعلقة بالحاسب الآلي.
- ✓ لابد من إيجاد الوسائل المناسبة لتشجيع المجتمع الدولي على مواجهة الجرائم الإلكترونية، والعمل على سن التشريعات الخاصة التي تواجه هذا النوع من الجرائم.

✓ضرورة إبرام المعاهدات التي تحث على تبادل المعلومات والخبرات، وتسليم وتبادل المجرمين، وتلك التي تهدف إلى مكافحة الجرائم الإلكترونية.

و بهذا نصل إلى أن الجرائم الإلكترونية قد أصبحت واقعا معاشا ولا يمكن تجاوزه أو نسيانه أو محاولة التغاضي عنه، لهذا يجب التعامل معها بجدية، وتسخير الوسائل التقنية والعلمية لمكافحتها، من حيث سد كل الثغرات التقنية، وتكوين الخبراء في مجال الكمبيوتر، حتى نستطيع التعامل مع هذا العالم التقني والإفتراضي، علما أن الإعلام الجديد أصبح بيت كل الجرائم التي تفكك الإنسان ومجتمعه، وسيظل هنالك صراع دائم بين طرفي المعادلة الإجتماعية، والسعي للمحافظة على الإنسان من تغلب التقنية عليه في أمنه وعاداته وتقاليده وعقيدته.

قائمة المراجع

قائمة المصادر والمراجع

أولا قائمة المصادر:

1-القرآن الكريم

2-الدستور الجزائري

3-النصوص والمواد القانونية:

1) القانون (03/2000) المؤرخ في 05/08/2000 الذي يحدد القواعد العامة المتعلقة بالبريد السلكية واللاسلكية، الجريدة الرسمية، عدد، المؤرخة في 06/08/2000
2) الأمر (05/03) المؤرخ في 19/07/2003 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، عدد 44، صادرة بتاريخ 23/07/2003.
3) القانون (15/04) المؤرخ في 10/11/2004 المتعلق بقانون العقوبات الرسمية عدد 71 صادر في 10/11/2004.
4) القانون رقم (14/04) مؤرخ في 10/11/2004 يعدل ويتمم الأمر (155/66) المؤرخ في 08/06/1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، عدد، 71 صادرة في،10/11/2004
5) القانون (22/06) المؤرخ في 20/12/2006 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، عدد 84 صادرة في 24/12/2006.
6) القانون (23/06) المؤرخ في 20/12/2006، المتضمن قانون العقوبات، الجريدة الرسمية، عدد48.
7) القانون (01/08) المؤرخ في 23/01/2008، المتعلق بالتأمينات الاجتماعية، الجريدة الرسمية، عدد 4، صادرة في24/12/2006
8) القانون 2008/08/01 والمعدل والمتمم لقانون 83/01 المتعلق بالتأمينات.

9) القانون (04/09) المؤرخ في 05/08/2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد47 الصادرة في 16/08/2009.

10) القانون (14/11) مؤرخ في 02/08/2011 المتضمن قانون العقوبات، الجريدة الرسمية، عدد 44، صادرة في10/08/2011.

11) القانون (03/15) المؤرخ في 01/02/2015 المتعلق بعصرنة العدالة الجريدة الرسمية، عدد2، صادرة في10/02/2015.

12) القانون (04/15) المؤرخ في 2015/02/01 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية، العدد 06، صادرة في 2015/02/10.

13) القانون رقم (01/16) المؤرخ في 2016/03/06 المتضمن تعديل الدستور، الجريدة الرسمية العدد 14.

14) قانون الإجراءات الجزائية الجزائري.

15) Loi n° 92-683 du 22 juillet 1992, portant réforme du code pénal, texte origine au 01 mars 1994.

16) code pénal français modifié par la loi n° 2004-575 du juin 2004 pour la confiance dans l'économie numérique, art 45, JORF n°0143 du 22 juin 2004, P11168, texte n°02

17) C.P.F, Modifié par Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JORF n'0294 du 19 décembre 2013 page 20570 texte n° 1

18) A.C.P. F dispose que ; Loi n°88-19 du 05 janvier 1988 relative à la fraude informatique, JORF du 06 janvier 1988, P 231.Sur le site ; www.legifrance.gouv.fr

19) Loi n° 92-683 du 22 juillet 1992, portant réforme du code pénal, text origine au 01 mars 1994.

20) -rt 323-6 du C.P.F Modifié par LOI n°2009-526 du 12 mai 2009 - art. 124

ثانيا: قائمة المراجع:

1-الكتب:

1) أحسن بوسقيعة، الوجيز في القانون الجزائي العام، ط10، دار هومة، الجزائر، 2011.

2) أحمد خليفة الملط "الجرائم المعلوماتية"،ط2، دار الفكر الجامعي، الإسكندرية، 2006.

3) أحمد هلالي عبد السلام، إلتزام الشاهد بإعلام في الجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 1997.

4) أمال قارة، الحماية الجزائرية للمعلوماتية في التشريع الجزائري، ط2، دار هومة الجزائر، 2007.

5) بلعيات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، ط1، دار الخلدونية، الجزائر 2007.

6) البيتي، محمد حماد، التكنولوجيا الحديثة والقانون الجنائي، ط1، دار الثقافة للنشر والتوزيع، عمان،2004.

7) حجازي، عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الإلكترونية والأنترنت، ط1، دار الكتب القانونية، القاهرة ،2002.

8) حسن طاهر دود – جرائم نظم المعلومات – أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000م.

9) خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2001.

10) رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، ط1، مكتبة الآلات الحديثة، 1994.

11) رشيدة بوبكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، ط1، منشورات الحلبي الحقوقية، بيروت –لبنان، 2012.

12) السعيد كمال، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، دار النهضة العربية، القاهرة، 1993.

13) الشوا سامي، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط1، القاهرة، دار النهضة العربية ،1994.

14) الصغير، جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة، ط1، دار النهضة العربية، القاهرة، 1992.

15) عبد الأمير العكيلي وسليم حربة، أصول المحاكمات، ج 01 و 02، دار الكتب للطباعة والنشر، القاهرة، 1980.

16) عبد الفتاح بيومي حجازي، مبادي في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، 2006.

17) عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، الأردن، 2007.

18) علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة للطبع والنشر، بيروت، 1999.

19) فورة نائلة، جرائم الحاسب الاقتصادية، ط1، دار النهضة العربية، القاهرة، 2004.

20) محمد خليفة، الحماية الجنائية المعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية،2007.
21) محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2011.
22) محمود الشنكيات، الإثبات بالمعاينة والخبرة في القانون المدني، دار الثقافة للنشر والتوزيع، الأردن، 2008.
23) نائلة عادل محمد، فريد قورة، جرائم الحاسب الآلي الاقتصادية، دارسة نظرية وتطبيقية، منشورات الحائي الحقوقية، 2005.
24) نهلا عبد القادر المومني، الجرائم المعلوماتية،ط1، دار المكتبة الوطنية للمملكة الأردنية الهاشمية، عمان ،2008.
25) مولود ديدان، قانون العقوبات، دار بلقيس للنشر، الدار البيضاء، الجزائر، 2012.
26) زيبحة زيدان، المعلوماتية في التشريع الجزائري، دار الهدى للطباعة والنشر، عين مليلة، الجزائر، 2001.

2-البحوث الجامعية:

1) محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، رسالة ماجستير، قسم علوم الشرطة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

3- المقالات العلمية:

1) عبد الجبار الحليص – الاستخدام غير المشروع النظام الحاسوب من وجهة نظر القانون الجزائي بحث منشور في مجلة جامعة دمشق للعلوم القانونية والاقتصادية – المجلد 27- العدد الأول 2011م.
2) راضية مشري، الحماية الجزائية للمصنفات الرقمية في ظل قانون حق المؤلف، مجلة التواصل لكلية الحقوق، جامعة 08 ماي 45، قالمة، عدد 34، جوان 2013.

3) القبائلي، سعد حماد، ضوابط الحماية الإجرائية لبرامج الحاسب الآلي، بحث مقدم لمؤتمر القانون والحاسوب المنعقد في جامعة اليرموك، أريد من 26-2004/04/27.

4) وعناد فاطمة زهرة، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، عدد 1، 2013، جامعة جيلالي اليابس سيدي بلعباس.

5) عبد الجبار الحليص- الاستخدام غير المشروع النظام الحاسوب من وجهة نظر القانون الجزائي بحث منشور في مجلة جامعة دمشق للعلوم القانونية والاقتصادية - المجلد 27- العدد الأول 2011م.

6) راضية مشري، الحماية الجزائية للمصنفات الرقمية في ظل قانون حق المؤلف، مجلة التواصل لكلية الحقوق، جامعة 08 ماي 45، قالمة، عدد 34، جوان 2013.

7) القبائلي، سعد حماد، ضوابط الحماية الإجرائية لبرامج الحاسب الآلي، بحث مقدم لمؤتمر القانون والحاسوب المنعقد في جامعة اليرموك، أريد من 26-2004/04/27.

4-المؤتمرات والندوات العلمية:

1) حملاوي عبد الرحمان، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية، جامعة بسكرة، كلية الحقوق، 2016.

2) هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية وعلم الإجرام، جامعة بسكرة، كلية الحقوق ،2016.

3) حملاوي عبد الرحمان، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية، جامعة بسكرة، كلية الحقوق، 2016.

4) هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية وعلم الإجرام، جامعة بسكرة، كلية الحقوق ،2016.

5-المواقع الالكترونية:

www.presse.justice.gouv.fr

www.moi.gov.qa/UNCCPCJDoha/Arabic/Previous_Congr esses.html

www.un.org/arabic/documents/instruments/subj_ar.asp

www.itu.int/osg/csd/cybersecurity/gca/global-strategic,report/index.html

www.wipo.int

www.eurpol.europa.eu

www.Canadainternationalgc.ca/G8G8recommandationson transnational crimes, 2011

فهرس المحتويات

فهرس المحتويات

الملخص:

تتعرض المؤسسات بصفة عامة إلى عدة مخاطر تمس الوظائف التي تمارسها، ومن بين هذه المخاطر الجريمة الماسة بالأنظمة المعلوماتية التي تطورت بتطور تكنولوجيات الإعلام والاتصال، حيث عملت الدول على سن نصوص قانونية وعقد اتفاقيات دولية لحماية المؤسسات من هذه الجريمة، التي من بينها الدولة الجزائرية التي عملت على حماية المؤسسات من جرائم المعلوماتية عن طريق إدخال تغيرات جذرية في قانون الملكية الفكرية والملكية الصناعية والقانون الجنائي للأعمال، بالإضافة إلى وضع قوانين مكملة تتطور بتطور الجريمة المعلوماتية.

إذ توصلت الدراسات إلى أنه بالرغم من التعديلات التي قام بها المشرع الجزائري في مجال مكافحة الجريمة الماسة بالأنظمة المعلوماتية إلا أن هذه النصوص تبقى غير كافية مقارنة بتطور الاحتراف الإجرامي المعلوماتي.

الكلمات المفتاحية: مخاطر المعلومات؛ الجرائم الماسة بالأنظمة المعلوماتية؛ مكافحة الجرائم الماسة بالمعلوماتية؛ القانون جنائي.

Abstract:

Institutions in general are exposed to several risks affecting the functions they practice, and among these risks is the crime against information systems that have developed with the development of information and communication technologies, as countries have worked to enact legal texts and conclude international agreements to protect institutions from this crime, among which is the Algerian state that worked To protect institutions from information crimes by introducing radical changes in intellectual property law, industrial property and business criminal law, in addition to establishing complementary laws that evolve with the development of information crime.

Studies have concluded that despite the amendments made by the Algerian legislator in the field of combating crime affecting information systems, these texts remain insufficient compared to the development of informational criminal professionalism.

key words: information risk; crimes against information systems; combating cybercrime; The law is criminal.