الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة محمد بوضياف المسيلة

كلية الحقوق والعلوم السياسية
قسم الحقوق

ميدان الحقوق
تخصص قانون جنائي

مذكرة مكملة لنيل شهادة ماستر أكاديمي
بعنوان

الجريمة الإلكترونية في التشريع الجزائري

إعداد الطلبة:
بلقليل شـــــوقي
بن شارف يوسف

إشراف الأستاذة:
بوضياف إسمهان

لجنة المناقشة

الاسم واللقب	الرتبة	الصفة
برابح السعـــــيد	أستاذ محاضر قسم-أ-	مناقشـــــــا
بوضياف إسمهان	أستاذ محاضر قسم-أ-	مشـــــــرفا
لجلط فـــــواز	أستاذ التعـــليم العالي	رئيســـــــا

السنة الجامعية : 2022/2021

ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ديسمبر 2020

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي: جامعة محمد بوضياف - المسيلة -

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): بلقليل شوقي الصفة: طالب. أستاذ. باحث طالب

الحامل(ة) لبطاقة التعريف الوطنية رقم: 200839485 والصادرة بتاريخ 2016/12/14

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم الحقوق

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج. مذكرة ماستر. مذكرة ماجستير. أطروحة دكتوراه).

عنوانها: الجريمة الإلكترونية في التشريع الجزائري

أصرح بشرفي أني التزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 12 جوان 2022

توقيع المعني (ة)

ملحق بالقرار رقم .....1082..... المؤرخ في ..... 27 ديسمبر 2020

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي: جامعة محمد بوضياف - المسيلة -

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): بن شارف يوسف الصفة: طالب. أستاذ. باحث طالب

الحامل(ة) لبطاقة التعريف الوطنية رقم: 200360690 والصادرة بتاريخ 25/04/2016

المسجل(ة) بكلية / معهد الحقوق والعلوم السياسية قسم الحقوق

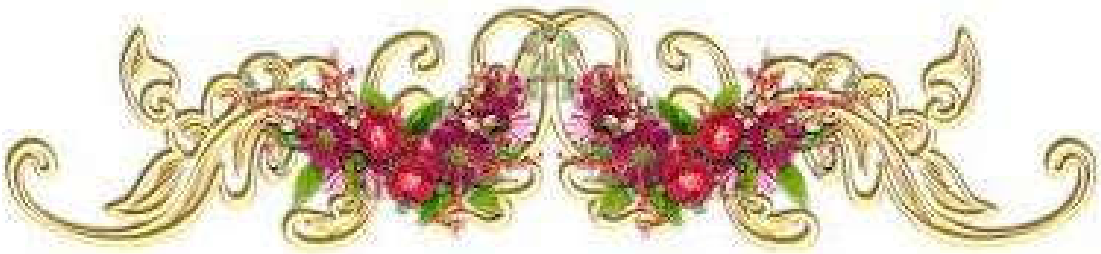
والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج. مذكرة ماستر. مذكرة ماجستير. أطروحة دكتوراه).

عنوانها: الجريمة الإلكترونية في التشريع الجزائري

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 20/12/2020

توقيع المعني (ة)



تشكـــرات

نتقـــدم بالشكـــر الجزيـــل إلـــى الأستـــاذة المشـــرف

- *بوضياف اسمهان *التي أشرفت على هذا البحث وتابعته من بدايته إلى نهايته ممدة إيانا بالنصح والتوجيه القيمين.
- و نتقدم بالشكر الجزيل لأعضاء اللجنة لقبولهم مناقشة هذه المذكرة .
- وفي الأخير نشكر كل من ساعدنا من قريب أو بعيد ولو بكلمة تشجيعية.

إهـــــداء

بسم الله الرحمن الرحيم

﴿ أن أشكر لي ولوالديك إلي المصير ﴾

الآية 14 من سورة لقمان.

- **إلى الوالدين الكريمين حفظهما الله.**
- **إلى إخوتي وأخواتي الأعزاء.**
- **إلى زوجتي حفظها الله وأولادي جواد وأنس .**
- **إلى كل من ساعدنا على إنجاز هذا العمل المتواضع.**

.....نرفع هذا العمل.

بلقليل شوقي

إهـــــداء

بسم الله الرحمن الرحيم

﴿ أن اشكر لي ولوالديك إلي المصير ﴾

الآية 14 من سورة لقمان.

- **إلى الوالدين الكريمين حفظهما الله خاصة الأم أطال الله في عمرها.**
- **إلى إخوتي وأخواتي الأعزاء.**
- **إلى كل العاملين بمكتبة الحقوق لجامعة المسيلة.**
- **إلى كل من ساعدنا على إنجاز هذا العمل المتواضع.**

.....نرفع هذا العمل.

بن شارف يوسف

مقدمـــــــــة

إن الثروة المعلوماتية في عصرنا أضحت متاحة للجميع، من خلال تقنية الحوسبة وتقنية الاتصال ومع التطور الحديث لتكنولوجيا الإعلام والاتصال والاستعمال السيئ لهما أصبح العالم مهددا بخطر انتشار الجرائم عن طريق التقنيات المتطورة، حيث كان يقتصر استخدام شبكة الإنترنت على الحاسب الآلي دون سواه ،لكن ما نلاحظه في زمننا هذا تنوع وسائل الاتصال من هواتف ذكية ولوحات رقمية وغيرها من الوسائل المتاحة للعامة،حيث يمكن لأي شخص وهو يتجول أن يستخدم الإنترنت عبر هاتفه الذكي مع العروض الهائلة التي تقدمها مصلحة الشبكة،وهذا يفتح أبوابا كانت مغلقة ويوسع من الحدود التي أصبحت بلا حراسة، ويساهم في ظهور الجرائم المعلوماتية التي دقت أجراس الخطر لتنبه المجتمعات على مدى خطورتها،فالجريمة المعلوماتية أو الإلكترونية هي سلوك غير مشروع يتخذه المجرم في بيئة رقمية لأهداف يرغبها.

الجريمة الإلكترونية تختلف عن الجرائم الأخرى كونها جريمة يصعب اكتشافها ويثار الجدل حول البلد المختص في الفصل فيها كونها جريمة عابرة للحدود تتم في البيئة الرقمية.

أهمية دراسة موضوع الجريمة الإلكترونية تكمن في معرفة هاته الجريمة الحديثة التي انتشرت انتشار النار في الهشيم في كافة دول العالم عامة والجزائر خاصة وتبيان أركانها، ومحاولة إيجاد حلول للحد من هاته الجريمة .

وما دفعنا لاختيار موضوع الجريمة الإلكترونية هو كثرتها في زمننا والتي نسمع عنها بكثرة في الجرائد والتلفزيون وفي أخبار منصات التواصل الاجتماعي، فالفضول لدراستها جذبنا لإختيار موضوعها.

ومن الدراسات السابقة التي تناولت هذا الموضوع نجد أطروحة الطالب فايز محمد راجح غلاب والتي كانت دراسة مقارنة بين الجريمة الإلكترونية في الجزائر واليمن حيث كان

عنوان الأطروحة الجرائم المعلوماتية في القانون الجزائري واليمني من كلية الحقوق والعلوم السياسية جامعة الجزائر(1) لسنة 2009-2010.

أهداف الموضوع تكمن في دراسة موقف المشرع الجزائري من ظاهرة الإجرام الإلكتروني ومحاولته القضاء عليها.

وهذا ما يجرنا إلى طرح التساؤل الآتي:

ما مدى نجاعة النصوص القانونية في التشريع الجزائري للحد من الجريمة الإلكترونية؟.

ويمكن أن تنجر عنها الإشكاليات الفرعية الآتية:

كيف عرف المشرع الجزائري الجريمة الإلكترونية؟.

وما هي الآليات المتخذة للحد منها؟.

وللإجابة على هاته التساؤلات قسمنا بحثنا إلى فصلين تناولنا في الفصل الأول ماهية الجريمة الإلكترونية الذي قسمناه بدوره إلى مبحثين مبحث لمفهوم الجريمة الإلكترونية ومبحث ثاني لأنواع الجريمة الإلكترونية وخصائصها

وفي الفصل الثاني الآليات القانونية لمكافحة الجريمة الإلكترونية مقسمينه إلى مبحثين الأول تناول القواعد الموضوعية المنظمة للجريمة الإلكترونية والمبحث الثاني الحماية الإجرائية للنظام المعلوماتي معتمدين في ذلك على المنهج الوصفي التحليلي الذي يتماشى مع موضوع البحث.

الفصل الأول:

ماهية الجريمة الإلكترونية

الفصل الأول: ماهية الجريمة الإلكترونية

إن من نتائج التطور التكنولوجي في الوقت الراهن، وجود ثمة علاقة ارتباط قوية بين استخدامات الحاسب الآلي وارتكاب بعض الجرائم المستحدثة، أي استخدام الحاسب الآلي كأداة لارتكاب الأفعال غير المشروعة، وسواء كانت الحاسبات الآلية محلا للجريمة المعلوماتية أو وسيلة لها، فإن الجوهري في الأمر أن انتشار الوسائل المعلوماتية نتيجة لثورة المعلومات والتي تنشر بسرعة هائلة وتغزو مختلف مجلات الحياة أصبح يزيد من فرص انتشار هذا النوع من الجرائم المستحدثة.

هناك تلازم حتمي بين مستوى تطور نظام المعلوماتية وما يرتبط به من وسائل وتقنيات، وبين دقة الاطار القانوني المتعلق بمكافحة الاجرام المعلوماتي ذلك أن الوعي بمخاطر ومضار المعلوماتية على المصالح الاجتماعية المختلفة من شأنه أن يضع أمام المشرع تصورا واضحا بما يسمح له بتأطير الأفعال التي يمكن أن تحمل وصف الجريمة المعلوماتية، باعتبارها أفعال مستحدثة تتميز بالضرورة عن غيرها من الأفعال المكونة للجرائم الأخرى الواقعة على الأشخاص أو الأموال، وهو ما من شأنه أن يخفف من حدة تزايد خطر الاجرام المعلوماتي خاصة مع عدم إمكانية القضاء عليه بشكل نهائي.[1]

[1] يعيش تمام شوقي،" الجريمة المعلواتية " دراسة تأصيلية مقارنة، ط 1،سلسلة مطبوعات المخبر، جامعة بسكرة، جانفي 2019، ص 12.

المبحث الأول: مفهوم الجريمة الإلكترونية

ترتبط الجريمة المعلوماتية ارتباطا وثيقا لايقبل التجزئة، بتقدم الدول والشعوب في استخدام تكنولوجيا الكمبيوتر والانترنت، إذ كلما زاد ذلك كلما كان مؤشرا رئيسيا على زيادة معدل الجريمة المعلوماتية.[1]

المطلب الاول: تعريف الجريمة الإلكترونية وطبيعتها القانونية

لم يتفق الفقه الجنائي على إيراد تسمية موحدة للجريمة الإلكترونية، فهناك عدة تسميات لها منها الجريمة المعلوماتية، جرائم إساءة إستخدام تكنولوجيا المعلومات والإتصال، جرائم الكمبيوتر والأنترنت، الجرائم المستحدثة ،الجريمة الناعمة، إجرام ذوي الياقات البيضاء،وتجدر الإشارة إلى أن هناك فارق بين ميدان جرائم الحاسب الآلي وميدان جرائم الأنترنت، فبينما تتحقق الأولى بالإعتداء على مجموعة الأدوات المكونة للحاسب الآلي وبرامجه والمعلومات المخزنة به، فإن جرائم الأنترنت تتحقق بنقل المعلومات والبيانات بين أجهزة الحاسب الآلي عبر خطوط الهاتف أو الشبكات الفضائية.[2]

الفرع الأول: تعريف الجريمة الإلكترونية والمصطلحات المتعلقة بها

قبل التطرق إلى تحديد أهم التعاريف التي أدلى بها الفقه بخصوص الجريمة المعلوماتية من الضروري والمفيد استحضار أهم المفاهيم والمصطلحات المرتبطة بحقل المعلوماتية والتي كثيرا

---

[1] خالد ممدوح إبراهيم،"أمن الجريمة الإلكترونية"،الدار الجامعية للنشر،الإسكندرية،2008،ص11.

[2] نايري عائشة،" الجريمة الإلكترونية في التشريع الجزائري"،مذكرة لنيل شهادة الماستر في القانون الإداري،جامعة أحمد دراية،كلية الحقوق والعلوم السياسية،أدرار،2017/2016، ص5.

ما تستخدم بمناسبة الحديث عن الاجرام المعلوماتي، وذلك على النحو التالي:

أولا – تعريف المصطلحات المتعلقة بالجريمة الإلكترونية:

1- تقنية المعلومات: يقصد بها عملية تغذية ومعالجة وتخزين، ثم بث واستخدام المعلومات الرقمية والنصية والمصورة والصوتية عن طريق تقنيات الحاسب الآلي والاتصالات، وبالتالي فهي تتضمن توظيف أدوات وأساليب، وتجهيزات متطورة لنقل المعلومات من المرسل الى المستقبل بأقل وقت وجهد وتكلفة، وبأقصى قدر من الدقة.[1]

2- الحاسب الآلي:

هو جهاز إلكتروني كيميائي بصري أوجهاز إعداد معلومات ذات سرعة عالية يؤدي وظائف منطقية حسابية أو تخزينية، ويشتمل على أي تسهيل لتخزين المعلومات أو تسهيل الإتصالات مباشرة سواء المختزنة أو التي تعمل بالختزان مع هذا الجهاز.[2]

وعرف بأنه مجموعة متداخلة من الأجزاء لديها هدف مشترك من خلال التعليمات المخزنة.[3]

ويعرف جانب من الخبراء الحاسب بأنه:"نظام معالجة كهربائي سريع ودقيق يستخدم في تداول البيانات ومصمم لتقبل وتخزين هذه البيانات ومعالجتها واعطاء النتائج تبعا للبرنامج المخزن الذي يتألف بدوره من مجموعة أوامر موضحة خطوة خطوة".[4]

---

[1] يعيش تمام شوقي، مرجع سابق،ص13.

[2] أسامة أحمد المناعسة،وجلال محمد الزعبي،"جرائم تقنية نظم المعلومات الإلكترونية"، ط.1، دار الثقافة للنشر والتوزيع،عمان(الاردن)، ، 2010،ص27.

[3] الشحات إبراهيم محمد منصور،"الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية"، ط.1 ، دارالفكر الجامعي، ،الاسكندرية،2011، ص15.

[4] علي جعفر،" جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة"، ط.1،منشورات زين الحقوقية، ،دون بلد نشر،2013،ص36.

3– شبكة الأنترنت:

الأنترنت هي شبكة دولية للإتصالات يمكن الدخول إليها عن طريق جهاز الكمبيوتر المتواجد في أي بقعة من بقاع العالم، وقد استخدمت هذه الشبكة ابتداء لتجميع المعلومات العسكرية وكانت تابعة لوزارة الدفاع الأمريكية، وذلك حتى السبعينات، ثم تطور الأمر وأصبحت تقدم خدمات تجارية وغير تجارية.[1]

هي الشبكة الدولية للمعلومات والتي اصطلح على تسميتها بالإنترنت وهي عبارة عن شبكة من أجهزة الحاسوب متصلة ببعضها البعض، عن طريق مزود الخدمة والخادم" السارفر" في جميع دول العالم، فالحاسوب الذي لم يرتبط بمزود الخدمة لايمكن أن يتصل بالشبكة الدولية للمعلومات، ولايستفيد من خدمات الإنترنت، كما أن جريمة الإختراق وما يتبعها من جرائم إلكترونية، لايمكن أن تتم إلا عن طريق هذه الشبكة، فالمعلومات المدونة في الحاسوب الخاص، الذي لم يرتبط بالإنترنت لايمكن اختراقه.(2)

4 – المعلومـات :

تأخذ عدة معاني مختلفة نذكر منها المعلومات هي المعنى الذي يستخلص من البيانات عن طريق العرف أو الإتفاق أو الخبرة أو المعرفة، وقد إقترح الأستاذ catala تعريف للمعلومات بأنها : رسالة ما يعبر عنها في شكل يجعلها قابلة للنقل أو الإبلاغ للغير[3]، قد عرف المشرع

(1) شيماء عبد الغني محمد عطاالله،" الحماية الجنائية للتعاملات الإلكترونية"، دار الجامعة الجديدة ،الإسكندرية،2007،ص 16-17

(2) خالد عياد الحلبي،" إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت"، ط.1، دار الثقافة للنشر والتوزيع، ، 2011،ص 50-51.

(3) بعرة سعيدة،"الجريمة الإلكترونية في التشريع الجزائري"،مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي،جامعة محمد خيضر بسكرة، كلية الحقوق والعلوم السياسية،2016/2015، ص8.

الأمريكي المعلومات في قانون المعاملات التجارية الإلكترونية لسنة 1999بالفقرة العاشرة من المادة الثانية بأنها تشمل البيانات والكلمات والصور والأصوات و الرسائل وبرامج الكمبيوتر الموضوعة على الأقراص المرنة وقواعد البيانات أو شابه دلك، وفي فرنسا ووفقا للقانون رقم 82ـ 652الصادر في 26يوليو 1982 تعرف المعلومات بأنهاً صوت أو صورة أومستند أو معطيات أو خطايا أيا كانت طبيعتها.

ثانيا: تعريف الجريمة الإلكترونية

تعددت التعاريف بخصوص الجريمة الإلكترونية، وذهبت أغلبها إلى الإنطلاق من وسيلة إرتكاب الجريمة، إذ أن أصحاب هذا الإتجاه يعتبرون أن جريمة الكمبيوتر تتحقق بإستخدام الجهاز، وهو الشيء الذي تم انتقاده على أساس أن تعريف الجريمة يستدعي الرجوع إلى العمل الأساسي المكون لها وليس فحسب إلى الوسائل المستخدمة لتحقيقه، بمعنى أنه ليس مجرد ان إستخدام جهاز الحاسوب في جريمة ما يمكن أن نعتبرها من الجرائم الإلكترونية.[1]

بينما يذهب اتجاه آخر في تعريفه للجريمة المعلوماتية إلى ربطها بالمعرفة الفنية باستخدام الحاسوب، حيث تعتبر المعرفة الفنية شرطا ضروريا للقول بكون جريمة ما تدخل ضمن زمرة الجرائم المعلوماتية، كمثال لأخذ التعاريف الذي قدمه هذا الإتجاه، هي:" جريمة تتطلب لاحترافها أو لارتكابها أن تتوفر لدى فاعلها معرفة بتقنبة النظام المعلوماتي".

[1] امحمد اقبلي وعابد العمراني الميلودي،" القانون الجنائي الخاص المعمق"، ط.1، مكتبة الرشاد سطات للنشر والتوزيع، ،د.ب.ن،2020، ص285.

1-التعريف الفقهي والقانوني للجريمة الإلكترونية:

لم يتفق فقهاء القانون الجزائي في القوانين المقارنة على الوصف القانوني والسليم أو التسمية الدقيقة لهذا المصطلح، أي الجريمة الإلكترونية لوجود مجموعة من المفاهيم المتقاربة والمشتقة من الإجرام الإلكتروني والغش المعلوماتي والإنحراف الذي يقع بواسطة الجانب الآلي، كما لم يتوصل الفقه إلى تعريف جامع مانع للجريمة الإلكترونية، وبالتالي تعددت التعريفات بشأنها وفق المنظور الذي تبناه الفقه، وفي هذا الإطار يشير الفقيه" فان دير هلست وونيف" إلى أن : هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة...وفي أغلب الأحيانت تستخدم مصطلحات الإفتراضية والحاسوب والإلكترونية والرقمية وكلها تعكس فجوات مهمة في التعريف".[1]

1-1 الإتجاه المضيق لتعريف الجريمة الإلكترونية

عرف أنصار هذا الإتجاه الجريمة الإلكترونية بأنها: "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم لإرتكابه من ناحية، لملاحقته وتحقيقه من ناحية أخرى"، حسب هذا التعريف يجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة، بل كذلك لملاحقتها، والتحقيق فيها وهذا التعريف يضيق بدرجة كبيرة من الجريمة الإلكترونية[2]، بمعنى يجب أن يتوافر قدر كبير من العلم بهذه التكنولوجيا لدى الجناة،والمختصين بملاحقتها من قضاة وضباط الشرطة وغيرهم. وهناك من يعرفها على أنها

[1] محمد الصغير مسيكة،: مفهوم الجرائم المستحدثة وطبيعتها القانونية(الجرائم الإكترونية)،مجلة الدراسات القانونية والسياسية، العدد01،جامعة أحمد بن يحي الونشريسي، تيسمسيلت،تاريخ النشر:2022/01/05،ص ص 133-134.
[2] نايري عائشة، مرجع سابق،ص06.

"الفعل غير المشروع الذي يتورط في ارتكابه الحاسب، أو هي الفعل الإجرامي الذي يستخدم في اقترافه الحاسوب باعتباره أداة رئيسية." كما يرى الأستاذ tredmannأن الجريمة المعلوماتية تشمل أي جريمة ضد المال، مرتبطة باستخدام المعالجة الآلية للمعلومات، ويرى الاستاذ Rosenblatt بأن الجريمة الإلكترونية هي "نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو التي تحول عن طريقه."

حسب هذا التعريف فإن الأفعال غير المشروعة التي يستخدم فيها الحاسب الآلي كأداة لارتكابها تخرج من نطاق التجريم، ويرى الأستاذ باركار أن الجريمة الإلكترونية هي كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل.[1]

1-2 الإتجاه الموسع لتعريف الجريمة الإلكترونية:

عللى عكس الإتجاه السابق، يذهب فريق من الفقهاء إلى التوسع في مفهوم الجرائم الإلكترونية أو المعلوماتية وعدم حصرها في الحاسوب وحده أو في موضوع الجريمة أو في شخص مستخدمه، وإنما بالتقنية ذاتها المستخدمة في كافة الأجهزة المعلوماتية أو الإلكترونية، فيعرفونها على أنها" كل فعل إجرامي أو متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة بالمجني عليه، أو كسبا يحققه الفاعل"[2]، كما عرفتها منظمة التعاون الإقتصادي والتنمية(OCDE) بأنها "كل فعل أو امتناع من شأنه الإعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة

[1] نايري عائشة، المرجع سابق،ص07.
[2] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة، الأسكندرية،2019،ص 50.

أو غير مباشرة عن تدخل التقنية المعلوماتية"، كما تعرف أيضا على أنها:" تلك الجرائم المرتكبة ضد الأملاك باستعمال التقنية المعلوماتية".

إن هذه التعريفات واسعة تتيح الإطاحة الشاملة قدر الإمكان بظاهرة جرائم التقنية، كما أنه يتيح إمكانية التعامل مع التطورات التقنية المستقبلية، ويعرفها آخرون على أنها" كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها".[1]

2- التعريف القانوني للجريمة الإلكترونية:

تبنى المشروع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي لابد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام فإن ثبت تخلف هذا الشرط الأولي فلا يكون هناك مجال لهذا البحث. [2]

لم يتخلف المشرع الجزائري بدوره عن ركب التشريعات التي وضعت تعريفا لنظام المعلومات حيث أنه عرف من خلال نص المادة 2 من الفقرة من القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

مسميا إياه ":المنظومة المعلوماتية " وهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة ، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات

[1] يزيد بوحليط، مرجع سابق،ص50.
[2] بعرة سعيدة، مرجع سابق،ص30.

تنفيذا لبرنامج معين " .

جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتي من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل وهذا دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 15-04 المؤرخ في العاشر من نوفمبر 2004 المتمم للأمر رقم 156-66 المتضمن قانون العقوبات والذي افرد القسم السابع مكرر منه تحت عنوان : المساس بأنظمة المعالجة الآلية للمعطيات ، والذي تضمن 08مواد من المادة 394مكرر وحتى المادة 394مكرر7 .[1]

وفقا المشرع الجزائري في تعريفه لنظام المعالجة الآلية للمعطيات مقارنة مع التشريعات الأخرى اشترط ضرورة الترابط بين مكونات أو أجهزة النظام أو بين الأنظمة فيما بينها ، وركز على وظيفة المعالجة الآلية للمعطيات موسعا بذلك المجال ليشمل كلا من المعالجة الآلية للمعطيات.

الفرع الثاني: الطبيعة القانونية للجريمة الإلكترونية

تكمن الطبيعة الخاصة لهذه الجرائم في قدرة شبكة المعلومات على نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحد مما يؤدي إلى ارتكاب الفعل ،والسبب في ذلك توسع بنوك المعلومات بأنواعها علاوة على رغبة الأفراد وسعيهم إلى ربط حواسبهم بالشبكة [2]،على أساس أن هذه الجرائم ترتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء أكان في تجميعها أو

[1] بعرة سعيدة، المرجع السابق،ص31.

[2] بوضياف اسمهان،" الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"،مجلة الأستاذ الباحث للدراسات القانونية والسياسية،جامعة محمد بوضياف،العدد الحادي عشر 2018،ص353.

تجهيزها أو في إدخالها إلى الحاسب المرتبط بشبكة المعلومات ولغرض الحصول على معلومات معينة كما قد ترتكب هذه الجرائم في مجال معالجة النصوص ،وصعوبة التكييف القانوني لهذه الجرائم تكمن في طبيعتها الخاصة.

بحيث أن القواعد التقليدية لم تكن مخصصة لهذه الظواهر الإجرامية المستحدثة ، وبالتالي تطبيقها على هذا النوع من الجرائم يثير مشاكل عديدة في مقدمتها مسألة الإثبات ،ومتابعة مرتكبيها وعلى ضوء الاعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة.[1]

ولقد تبنى المشرع للدلالة على الجريمة المعلوماتية ،مصطلح المساس بأنظمة المعالجة الآلية للمعطيات، حيث يمثل نظام المعالجة الآلية للمعطيات المسألة الأولية، أو الشرط الأولي الذي يلزم تحقيقه حتى يمكن البحث في توافر أو عدم توافر أركان أي جريمة من جرائم الاعتداء على هذا النظام فإذا تخلف هذا الشرط الأولي ، لايكون هناك مجال لهذا البحث فنظام المعالجة الآلية للمعطيات تعبير فني تقني يصعب على المشتغل بالقانون وإدراك حقيقته بسهولة، فضلا عن أنه تعبير يخضع للتطورات السريعة والمتلاحقة في مجال فن الحاسبات الآلية، لذلك فالمشرع الجزائري على غرار التشريع الفرنسي لم يعرف نظام المعالجة الآلية للمعطيات فأوكل بذلك مهمة تعريفه لكل من الفقه والقضاء.[2]

[1] نفس المرجع السابق،ص353.

[2] رائد مروان محمود عاشور،" المحددات النظرية والقانونية للجريمة المعلوماتية الماسة بالأطفال"،مجلة تحولات،المجلد الثالث،العدد الثاني ديسمبر 2020، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة،ص ص91-92.

يمكن القول بأن الجرائم الإلكترونية لها طبيعة خاصة، فهي تتم في فضاء يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر لحدود، سواء ماتعلق بالجانب الموضوعي كتحديد أركان الجريمة بدقة، أو ماتعلق بإجراءات ملاحقة مرتكبيها لأنها تتم في بيئة افتراضية يصعب معها تطبيق الإجراءات التقليدية كالتفتيش والحجز مثلا، وهذا ما عمل عليه المشرع الجزائري بمراعاته لهذه الطبيعة الخاصة أثناء سنه للنصوص القانونية المتعلقة بمكافحتها.[1]

المطلب الثاني: أركان الجريمة الإلكترونية ودوافع ارتكابها

لكل جريمة من الجرائم المرتكبة أركان تقوم عليها وأسباب تدع المجرم يقوم بها وهو ماسنتطرق إليه في الفرعين الموالين.

الفرع الأول: أركان الجريمة الإلكترونية

مهما كان التعريف الذي يمكن أن نعطيه للجريمة، فإنها من وجهة نظر قانونية لابد من أركان تؤسس عليها، سواء أكانت أركانا عامة لابد منها في أية جريمة ،أو أركانا خاصة يثبتها المشرع ويتطلبها في أنواع معينة من الجرائم.[2]

وأركان الجريمة هي تلك العناصر التي لا وجود للجريمة دونها حيث تدور الجريمة معها وجودا أو عدما.

[1] يزيد بوحليط ، مرجع سابق،ص ص 78-79.
[2] أسامة أحمد المناعسة وجلال محمد الزعبي،"جرائم تقنية نظم المعلومات الإلكترونية"،مرجع سابق،ص43.

أولا: الركن الشرعي:

يقصد بالركن الشرعي للجريمة وجود نص يجرم الفعل ويوضع العقاب المترتب عليه وقت وقوع هذا الفعل، يبنى على ذلك عدم جواز ملاحظة الشخص عن فعل ارتكبه قبل صدور نص التجريم، وعن فعل ارتكبه بعد إلغاء نص التجريم كما لا يجوز قياس افعال لم ينص المشرع على تجريمها وأفعال أخرى ورد نص التجريم عليها مهما يكن بينها من تشابه من حيث لدوافع أو الفاعلية أو النتائج أو العناصر، ذلك أنه لا يجوز أيضا التوسع في تفسير النصوص الجزائية.[1]

انطلاقا من مبدأ الشرعية وفقا لأحكام المادة الأولى من قانون العقوبات التي تنص على:"**لاجريمة ولا عقوبة أو تدابير أمن بغير قانون**"، جرم القانون رقم 04-15 بعض صور الجريمة العلوماتية المقررة لمرتكبيها في القسم السابع مكرر تحت عنوان" المساس بأنظمة المعالجة الآلية للمعطيات" من الفصل الثالث المعنون" الجنايات والجنح ضد الأموال من الباب الثاني المتعلق "بالجنايات والجنح ضد الأفراد وذلك في المواد من 394 مكرر إلى 394 مكرر 08 من قانون العقوبات المعدل والمتمم.[2]

في حين جاء القانون 09-04 متضمنا للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها كجانب وقائي يحد من وقوع الجرائم المعلوماتية، من خلال وضع

[1] يوسف جفال،"التحقيق في الجريمة الإلكترونية"،مذكرة مقدمة لنيل شهادة الماستر أكاديمي،تخصص قانون جنائي،جامعة محمد بوضياف المسيلة،كلية الحقوق و والعلوم السياسية،2017/2016، ص14.

[2] خضري حمزة وعشاش حمزة،"خصوصية اركان الجريمة المعلوماتية في التشريع الجزائري،مجلة الدراسات القانونية،المجلد 06، العدد 02، جامعة محمد بوضياف المسيلة،جوان 2020،ص 173.

ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتسجيل وتجميع محتواها في حينها والقيام بإجراءات التفتيش داخل المنظومة المعلوماتية.

ولجوء المشرع إلى تقنين أو النص على مثل هذه الجرائم وجعلها في نطاق مبدأ الشرعية يمنع القاضي من اللجوء إلى القياس، بمعنى عدم جواز لجوء القاضي الجنائي الى قياس فعل لم يرد نص على تجريمه على فعل ورد نص بتجريمه، فيقرر القاضي الجنائي للأول عقوبة الثاني بسبب التشابه بين الفعلين.[1]

2- الركن المادي:

من المشكلات العملية التي تثيرها الجريمة الالكترونية طبيعة الركن المادي فيها، ذلك أن مفهوم أو مناط التجريم ينصب على نظام إلكتروني يساء استعماله أو يتم اقتحامه على نحو غير مشروع، بما يكون لذلك الاستعمال أو الاقتحام من أثر مادي ملموس يظهر إما في صورة تدمير للمعلومات، وهو مايثير إمكانية الإتلاف العمدي للمنقولات، أو السرقة وذلك عن طريق إساءة استعمال بطاقات الائتمان، أو يثير شبهة التزوير عن طريق التلاعب في بيانات الحاسب الآلي.[2]

إن السلوك الإجرامي في الجريمة الالكترونية يرتبط دائما بالمعلومة المخزنة على الحاسب الآلي،أو تلك التي يتم إدخالها للحاسب الآلي، وصعوبة المشكلة أن السلوك الإجرامي قد يتحقق

[1] خضري حمزة وعشاش حمزة، المرجع السابق،ص173.
[2] عبد الله دغش الجمعي،" المشكلات العملية والقانونية للجرائم الالكترونية دراسة مقارنة"،رسالة مكملة للحصول على شهادة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014 ،ص 26.

بمجرد ضغط زر في الحاسب فيتم تدمير النظام المعلوماتي أو حصول التزوير أو السرقة عن طريق التسلل إلى نظام أرصدة العملاء في البنوك أو إساءة استعمال بطاقات الائتمان.

ويمثل الركن المادي النشاط الذي يصدر عن الفاعل ويبرز إلى العالم الخارجي، ويرتب آثار قانونية معينة، ويقوم على عناصر ثلاثة تشكل الهيكل المادي للجريمة وهي، سلوك خارجي قد يكون سلبيا أو إيجابيا، والنتيجة التي يفضي إليها سواء تحققت أم لم تتحقق، والعلاقة السببية التي تربط بينهما.[1]

ثالثا: الركن المعنوي

الجريمة ليست ركنا ماديا خالصا قوامه تافعل وآثاره، ولكنها كذلك ركن نفسي، ويمثل الركن المعنوي الأحوال النفسية لماديات الجريمة والسيطرة النفسية عليها،[2]

لم يعرف المشرع الجزائري القصد الجنائي على غرار غالبية التشريعات واكتفى بالنص في الجرائم على العمد، كما لايكفي لقيام الجريمة ارتكاب عمل مادي فقط، بل لابد من أن يصدر أيضا عن إرادة الجاني، هذه العلاقة التي تربط العمل المادي بالفاعل تسمى بالركن المعنوي،اي يتمثل في نية داخلية يضمرها الجاني في نفسه، ومن ثمة يتخذ الركن المعنوي صورتين أساسيتين هما: صورة الخطأ العمد أي القصد الجنائي، وصورة الخطأ غير العمد: أي الاهمال وعدم الاحتياط، إن الركن المعنوي في مختلف الاعتداءات الماسة بأنظمة المعالجة الآلية

[1] عبد الرحمان خلفي،" محاضرات في القانون الجنائي العام" محاضرات موجهة لطلبة السنة الثانية ل م د قسم التعليم القاعدي"،كلية الحقوق والعلوم السياسية، جامعة ميرة عبد االرحمان،2017/2016، ص 67.
[2] أسامة أحمد المناعسة وجلال محمد الزعبي، المرجع السابق،ص60.

للمعطيات تتخذ صورة القصد الجنائي إضافة إلى نية الغش، فالجرائم الإلكترونية هي من جرائم التقنية العالية تتطلب من المجرم الإلكتروني قدرا من المعرفة والتخصص، فكان من المتصور غالبا وقوعها في صورة واحدة هي صورة العمد.[1]

الفرع الثاني: دوافع ارتكاب الجريمة الإلكترونية

مما لاشك فيه أن وراء كل فعل سواء كان يحمل في طيانه جانب الخير أم الشر إلا وخلفه دافع أو غرض أو غاية، ولهذا ولذاك فإن، الدافع (الباعث)، الغرض، الغاية، تعبيرات لكل منها دلالاته الاصطلاحية في القانون الجنائي، تتصل بما يعرف بالقصد الخاص في الجريمة[2]

بالنسبة للجريمة الإلكترونية، فثمة دوافع عديدة تحرك الجناة لارتكاب أفعال الاعتداء المختلفة المنطوية تحت هذا المفهوم ،وأهم هذه الدوافع سيتم بيانها من خلال دوافع شخصية واخرى موضوعية

1-الدوافع الشخصية:

لايخفى على أحد أن المجرم يرتكب جريمته نتيجة دوافع معينة، تختلف هذه الدوافع من مجرم لآخر كما قد تكون مشتركة بينهم، والأمر نفسه بالنسبة للمجرم الإلكتروني الذي يرتكب جريمته في بيئة إلكترونية تختلف تماما عما نعرفه عن البيئة التقليدية،[3] إذ يمتلك دوافع شخصية عديدة، وعموما يمكن تقسيمها إلى دافعين رئيسيين هما:

---

[1] يزيد بوحليط ، مرجع سابق،ص134.
[2] عبد الحكيم رشيد توبة،" جرائم تكنولوجيا المعلومات"، ط1، دار المستقبل للنشر والتوزيع، عمان(الأردن)،2009،ص166.
[3] يزيد بوحليط، مرجع سابق،ص37.

أ- دوافع مادية:

يعتبر الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة الإلكترونية، وذلك لأن الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم الإلكتروني إلى تطوير نفسه حتى يواكب كل جديد يطرأ على التقنية المعلوماتية، ويستغل الفرص ويسعى إلى الإحتراف حتى يحقق أعلى المكاسب وبأقل جهد دون أن يترك أثر ورائه، فيتعمد الجاني رغبة منه في تحقيق الربح إلى التلاعب بأنظمة المعالجة الآلية للبنوك والمؤسسات المالية إن كان أحد موظفيها، أو اختراق نظم المعالجة الألية لها من خلال اكتشافه لفجواتها الأمنية، فيعمل على استغلالها وبرمجتها لتحويل مبالغ مالية لحسابه، أو لحساب شركائه، أو لحساب من يعمل لحسابهم إن كان من خارج المؤسسة. كما يمكن الحصول على مكاسب مادية من خلال المساومة على البرامج أو المعلومات المتحصل عليها بطريق الاختلاس من جهاز الحاسوب.[1]

ب- دوافع ذهنية ونمطية:

الصورة الذهنية لمرتكبي جرائم الحاسوب والإنترنت غالبا هي صورة البطل والذكي يستحق الإعجاب لاصورة المجرم الذي يستوجب محاكمته، فغالبا ما يكون الدافع لدى مرتكبي جرائم المعلومات هي الرغبة في اثبات الذات وتحقيق انتصار على تقنية المعلومات، وهم فئة غير خطيرة لأن دافعهم هو الفضول بالدرجة الأولى وليس الربح ولا يملكون أية نوايا سيئة.[2]

[1] نايري عائشة، مرجع سابق،11.

[2] سليمة ذياب وبلال بوترعة،" الجريمة الإلكترونية: الأسس والمفاهيم" مجلو تطوير العلوم الإجتماعية، المجلد 13، العدد 01، جامعة زيان عاشور، الجلفة،ص15.

2-**دوافع موضوعية:** تتعدد هذه الدوافع ويمكن تقسيمها إلى مايلي:

أ- دوافع الإنتقام:

يكون دافع الانتقام مؤثرا في ارتكاب هذه الجرائم، حيث يعد من أخطر الدوافع التي يمكن أن تدفع شخص يملك معلومات عن المؤسسة أو الشركة التي يعمل بها لأنه غالبا مايكون أحد موظفيها، ويقوم بهذا الدافع نتيجة اما لفصله من العمل أو تخطيه في الحوافز أو الترقية، فهذه الأمور تجعله يقدم على ارتكاب جريمته.[1]

ب- دافع جنون العظمة أو الطبيعة التنافسية:

ويكون ذلك من خلال الموظفين داخل المؤسسة بغية إظهار ملكاتهم الفنية في هذا المجال لخلق جو من المنافسة قصد الوصول للمراكز المرموقة داخل المؤسسة.

ج- **دافع التعاون والتواطؤ على الأضرار:**

يحدث هذا كثيرا في الجرائم المعلوماتية، حيث يقوم متخصص في الأنظمة المعلوماتية يعمل لدى المؤسسة بالتعاون مع شخص آخر من محيط أو خارج المؤسسة بتغطية عمليات التلاعب وتمويل المكاسب المادية، عن طريق اختراق الأنظمة المعلوماتية وتبادل المعلومات فيما بينها.[2]

[1] صغير يوسف،" الجريمة المرتكبة عبر الإنترنت"، مذكرة لنيل شهادة الماجستير في القانون تخصص القانون الدولي للأعمال،كلية الحقوق والعلوم السياسية، جامعة مولود معمري(تيزي وزو)،ص 42.
[2] يزيد بوحليط، مرجع سابق،ص38.

المبحث الثاني: أنواع الجريمة الإلكترونية وخصائصها

تتعدد أنواع الجريمة الإلكترونية وتمتاز بخصائص يمكن توضيحها فيما يلي:

المطلب الأول: أنواع الجريمة الإلكترونية:

نظرا لصعوبة حصر أنواع الجريمة المعلوماتية بصورة دقيقة، تعددت محاولات الفقه لتحديد أنواعها، فهناك من قسمها على أساس معيار الآداة المستعملة في ارتكاب الجريمة (الحاسب الآلي)، وهناك من قسمها اعتبارا على أنماط السلوك المختلفة التي تمثل الجريمة المعلوماتية ومدى اتفاقها او اختلافها مع القواعد التي تحكم القانون الجنائي، بالإضافة إلى اتجاه ثالث قسمها بالاعتماد على محل الجرائم المعلوماتية التي تنصب على معطيات الحاسوب بالإضافة إلى الإعتماد على الدور الذي يقوم به الحاسب الآلي في الجريمة وهذا الأخير يعد الاتجاه الراجح في تقسيم الجرائم المعلوماتية إذ صنفها ضمن طائفتين الأولى تمثل الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي، أما الطائفة الثانية تتمثل في الجرائم المعلوماتية الواقعة على النظام المعلوماتي[1]

الفرع الأول: الجريمة الإلكترونية المرتكبة باستخدام النظام المعلوماتي:

تتنوع الجرائم التي ترتكب بواسطة النظام المعلوماتي مابين جرائم اقتصادية أو قرصنة المعلومات أو ذات طابع سياسي، أو متعلقة بالأمن القومي، وقد تقع على الأشخاص الطبيعية أو الإعتبارية.

[1] عبد الحكيم مولاي ابراهيم،" الجرائم الإلكترونية"، مجلة الحقوق والعلوم الإنسانية، المجلد الثاني ،العدد 23،جامعة زيان عاشورالجلفة،2015، ص ص 214-215.

أولا: الجريمة الإلكترونية الواقعة على الأشخاص الطبيعية:

ويمكن التطرق إليها من خلال:

1- الجريمة الإلكترونية الواقعة على حقوق الملكية الفكرية:

يكون النظام المعلوماتي وسيلة للإعتداء على حقوق الملكية الفكرية، ومثاله السطو على بنك المعلومات وتخزين واستخدام هذه المعلومات دون إذن صاحبها، لأن استخدام معلومة معينة دون إذن صاحبها يعتبر اعتداء على حق معنوي، إضافة إلى كونه اعتداء على قيمتها المالية كون أن للمعلومة قيمة أدبية بجانب قيمتها المادية، ويندرج ضمن الحقوق الفكرية كذلك براءات الإختراع، إذ تمثل فكرة للمخترع تحتوي على حق معنوي وآخر مالي للمخترع، وقد نص المشرع الجزائري على حقوق الملكية الفكرية من خلال نصوص قانونية وهي الأمر رقم03-05 الصادر في 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، والأمر رقم 03-07 الصادر في 2003 المتعلق ببراءات الإختراع.[1]

2-الجريمة الالكترونية المتصلة بانتهاك حرمة الحياة الخاصة:

لقد اعتمد الأستاذ (Sieber) في تحديد صور التهديد المعلوماتي للحياة الخاصة على معيار موضوعي قوامه تحديد الوسيلة المستخدمة في انتهاك الخصوصية.[2]

[1] نايري عائشة، المرجع السابق،ص25.
[2] علي جعفر، مرجع سابق،ص87.

وتشمل جرائم الاعتداء على المعطيات السرية أو المحمية وجرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة.[1]

3- جريمة اتلاف المعلومات المبرمجة آليا بواسطة الفيروسات:

تستخدم كلمة فيروس في مجال المعلوماتية للدلالة على كل البرامج الخبيثة التي تسبب اتلافا لأنظمة المعالجة الآلية للمعلومات،ويوجد منها أنواع كثيرة مثل ،فيروس البكتيريا والديدان وحصان طروادة والقنابل المنطقية، وهي تسبب في اتلاف المكونات المنطقية للحاسب الآلي[2]، ولاسيما فيما يخص الحذف الكلي، الذي يمكن أن يؤدي إلى تعطيل الحاسب الآلي عن آداء وظائفه.[3]

ثانيا: الجريمة الإلكترونية الواقعة على الأموال:

باستثناء جريمة السرقة، تشمل هذه الطائفة أنشطة الدخول أو التواصل غير المصرح به مع نظام الكمبيوتر أو الشبكة

1- جرائم الاحتيال والسرقة:

وتشمل جرائم الاحتيال عن طريق التلاعب بالمعطيات والنظم واستخدام الكمبيوتر للحصول على أو البطاقات المالية للغير دون ترخيص، والاختلاس عبر الكمبيوتر أو بواسطته،وسرقة معلومات الكمبيوتر وقرصنة البرامج.

---

[1] يزيد بوحليط، مرجع سابق،ص62.
[2] خالد ممنوح ابراهيم، مرجع سابق،ص73.
[3] محمد حماد مرهج الهيتي،" جرائم الحاسوب"، ط.1، دار المناهج للنشر والتوزيع، ،عمان (الاردن)،2006،ص154.

2-التحويل الالكتروني غير المشروع للأموال:

غالبا مايتم ولوج مخترقي شبكات الانترنت الى بيانات حساب الآخرين من خلال الحصول على كلمة مرور مدرجة في ملفات انظمة الكمبيوتر الخاصة بالمجني عليه، فإذا ما تم الاستيلاء على كلمة المرور وادخالها في انظمة الحاسب الآلي فإنها سوف تنسجم وتقترن بالملف ومن ثم تسمح للمستخدم بالولوج إلى النظام المعلوماتي.

وقد قام بالفعل مبرمج في أحد البنوك منوط به اعداد البرامج المتعلقة بإعادة المال الزائد من مالكي بطاقات الفيزا باستخدام طريقة salami، باستقطاع (25 سنت) من حاملي البطاقة وبطريقة عشوائية وادخالها في حساب الفيزا الخاص به.[1]

3- جريمة غسيل الأموال عبر الانترنت:

من الجرائم التي ترتكب عبر النظام المعلوماتي جريمة غسيل الأموال، وهي عملية يقصد بها نقل أموال مستمدة من مصدر غير مشروع بقصد تطهيرها، فعملية التحويل الإلكتروني لهذه الأموال لايشوبها أي تلاعب إلا صفة عدم المشروعية يرجع إلى مصدر هذه الأموال، وتتم عبر الانترنت عن طريق البنوك حيث تتم العمليات المصرفية بطريقة إلكترونية سريعة.[2]

الفرع الثاني: الجريمة الإلكترونية المرتكبة على النظام المعلوماتي:

من أجل سد الفراغ الذي عرفه التشريع الجزائري في هذا المجال، جاء القانون رقم 04-15 الصادر في 10 نوفمبر ،2004 المتضمن قانون العقوبات بتجريم كل أنواع الإعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، وقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وذلك في المواد 394مكرر إلى 394مكرر08 ،وتأخذ صور الإعتداء صورتين وهما:[3]

[1] محمد أمين الشوابكة، مرجع سابق، ص ص178-179.
[2] خالد ممنوح ابراهيم ،مرجع سابق،ص76
[3] نايري عائشة،مرجع سابق،ص27.

الدخول والبقاء في منظومة معلوماتية، المساس بمنظومة معلوماتية، كما تضمن صور أخرى للغش.

اولا: الدخول او البقاء غير المشروع في نظام المعالجة الالية للمعطيات او الشروع في ذلك

نصت الدادة 394 مكرر في قانون العقوبات على ان الدخول او الدخول والبقاء غير المشروع في نظام المعالجة الالية للمعطيات او الشروع في ذلك يشكل فعلا إجراميا ولهذا الفعل حسب المادة المذكورة صورتين كالتالي:

1- الصورة البسيطة:

يتمثل النشاط الاجرامي في هذه الصورة في الافعال الاتية:

أ_ فعل الدخول: يتحقق فعل الدخول بمجرد الوصول الى امعلومات المخزنة داخل النظام ودون علم ورضا صاحبه، لان هذا النظام لا يسمح للدخول فيه إلا لأشخاص معينين او يسمح بالدخول لكن مقابل نفقات.

ب_ البقاء: معنى البقاء هو التواجد داخل نظام المعالجة الالية للمعطيات ضد ارادة من له الحق في السيطرة على هذا النظام، او بتجاوز المدة المسموح له بالبقاء فيها، او عدم الانسحاب فورا وقطع وجوده في نظام البيانات او يطبع معلومات حتُ يسمح لو بالرؤية فقط.

2-الصورة المشددة:

نصت المادة 942 مكرر في الفقرتين الثانية والثالثة من قانون العقوبات على ظروف تشديد عقوبة فعل الدخول والبقاء غير المشروع عندما ينتج عن هذين الفعلين اما محو أو تحويل المعطيات التي يحتويها النظام، وإما عدم صلاحية النظام لأداء وظائفه من خلال تخريب نظام اشتعال المنظومة.[1]

[1] حمزة خضري وعشاش حمزة،" خصوصية اركان الجريمة الالكترونية في التشريع الجزائري"،مرجع سابق،ص174.

3-افعال اجرامية اخرى:

جرمت المادة 394 مكرر 02 من قانون العقوبات السابق الذكر الأعمال الأتية: تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي السابقة الذكر ، ويقصد بتصميم المعطيات هنا الفيروسات المعلوماتية، برامج القرصنة التي يمكن أن تستعمل في ارتكاب جرائم معلوماتية إما ضد الأنظمة المعلوماتية، أو المعطيات المعوماتية في حد ذاتها، كما جرم المشرع كذلك أفعال الحيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصلة منإحدى جرائم الغش المعلوماتي لإي غرض.

ثانيا: جريمة المساس بمنظومة معلوماتية

نصت المادة 394مكرر 01 من قانون العقوبات رقم 04/15 بمعاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية، أو أزال أو عدل هذه المعطيات وذلك عن طريق استعمال الغش،هذا السلوك الإجرامي يتجسد في ثلاث صور هي الإدخال، المحو، التعديل، كما أن المشرع لم يشترط اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداهما فقط لكي يتوافر الركن المادي، و أفعال الإدخال و الإزالة و التعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات، سواء بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل، كما أن هذا السلوك يجسد فعل التخريب و إفساد المعطيات التي يتضمنها نظام المعالجة الآلية، مثال ذلك إدخال فيروس المعلوماتية في البرامج من أجل إتلافها.[1]

[1] نايري عائشة، مرجع سابق،ص29.

المطلب الثاني: خصائص الجريمة الإلكترونية

إن للجريمة الإلكترونية خصائص متعددة نوجزها فيمايلي:

الفرع الأول: صعوبة اكتشاف جرائم المعلوماتية وإثباتها:

لا تحتاج جرائم المعلوماتية إلى أي عنف أو سفك للدماء، أو آثار اقتحام لسرقة الأموال، وإنما هي أرقام وبيانات تتغير أو تمحى تماما من السجلات المخزونة في ذاكرة الحاسبات الآلية، ولأن هذه الجرائم – في أغلب الأحيان– لا تترك أي أثر خارجي مرئي لها، فإنها تكون صعبة الإثبات، ومما يزيد من صعوبة إثبات هذه الجرائم أيضا ارتكابها عادة في الخفاء، وعدم وجود أي أثر كتابي لما يجري خلال تنفيذها من عمليات أو أفعال إجرامية[1]، حيث يتم بالنبضات الكهربائية نقل البيانات والمعلومات، كما ان هذه الجرائم ترتكب غالبا بصورة منظمة،على صعيد أكثر من دولة باستخدام شبكة الاتصالات والمعلومات(الانترنت) و دون تحمل عناء الانتقال، أضف إلى ذلك إحجام مجتمع الأعمال عن الإبلاغ عنها تجنبا للإساءة إلى سمعة وهز الثقة في كفاءة المنظمات والمؤسسات المجني عليها، فضلا عن ذلك إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الزمنية.[2]

الفرع الثاني: جرائم عابرة للحدود:

إن تعبير جرائم عابرة للدول أو جرائم عبر وطنية هي تلك الجرائم التي تقع بين أكثر من دولة، بمعنى أنها لا تعرف بالحدود الجغرافية للدول كجرائم تبييض الأموال، والمحذرات، وغيرها.

وفي عصر الحاسب الآلي ومع انتشار شبكة الاتصالات العالمية (الانترنت)، أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة بحيث يغدو أمر التنقل والاتصال

[1] محمد عبد الله أبوبكر،" موسوعة جرائم المعلوماتية"،المكتب العربي الحديث،الاسكندرية،2007،ص 97.
[2] نفس المرجع السابق، ص97.

فيما بينها أمرا سهلا، طالما حدد عنوان المرسل إليه،أو أمكن معرفة كلمة السر، وسواء تم ذلك بطرق مشروعة أو غير مشروعة.[1]

وفي هذه البيئة يمكن أن توصف جرائم التقنية بأنها جرائم عابرة للدول، إذ غالبا ما يكون الجاني في بلد، والمجني عليه في بلد لآخر، كما قد يكون الضرر المتحصل في بلد ثالث في الوقت نفسه، وعليه تعتبر جرائم التقنية شكلا جديدا من الجراالعابرة للحدود الوطنية أو الإقليمية أو القارية.[2]

الفرع الثالث: جريمة ناعمة:

تختلف الجرائم المعلوماتية عن الجرائم التقليدية التي تتطلب أحيانا استخدام العنف، كما في جرائم القتل والضرب والجرح والسرقة وجرائم الإرهاب، إلا أن الجرائم المتصلة بالكمبيوتر تمتاز بأنها جرائم ناعمة لا تتطلب عنفا، بل تتطلب مواصفات خاصة كالذكاء وامتلاك الوسائل المناسبة وقدرة على التعامل مع شبكة الانترنت، فنقل بيانات من كمبيوتر إلى آخر أو المساس بأنظمة المعالجة الآلية للمعطيات، أو الدخول غير المشروع للحاسوب أو القرصنة والسطو الإلكتروني على الأرصدة وبيانات بطاقات الائتمان،لا يتطلب أي عنف سواء مادي أو معنوي ولا يبذل فيه الجاني أي جهد عضلي، فهي جرائم هادئة بطبيعتها، فلا يحتاج المجرم الإلكتروني إلى العنف، وإنما يحتاج إلى مهارة وفن ودقة في استعمال تقنية المعلومات مثلك استخدام ما يعرف بالقنابل المنطقية والفيروسات المعلوماتية...،كما أن معظم هؤلاء من الشباب المثقفين ذوي الاختصاصات العالية في مجال الحاسوب مما يخلق صعوبات إضافية لملاحقتهم.[3]

---

[1] أسامة أحمد المناعسة وجلال محمد الزعبي، مرجع سابق،ص95.
[2] نفس المرجع السابق ،ص95.
[3] يزيد بوحليط ، مرجع سابق،ص ص83-84.

الفرع الرابع : جريمة مستحدثة:

تعد الجرائم الالكترونية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطارا جسيمة في ظل العولمة، فلا غرابة أن تعتبر الجرائم المعلوماتية- سواء التي تتعرض لها أجهزة الكمبيوتر أو التي تسخر تلك الأجهزة في ارتكابها- من الجرائم المستحدثة، حيث أن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة ، بحيث يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقيبة ، بل انه اضعف من قدراتها في تطبيق قوانينها ، بالشكل الذي أصبح يهدد أمنها وامن مواطنيها.[1]

وعلى الرغم من المرايا والمنافع الايجابية المرتبة على هذه العولمة وثورة المجتمع الالكتروني ، وإلا أنها ساعدت على ظهور وتعزيز أنواع جديدة من الجرائم ، من أبرزها جرائم غسيل الأموال ، وتهريب المخدرات ، واختراق قطاع الأعمال ، والإفلاس بالتدليس والغش، والفساد ورشوة الموظفين العموميين و وسرقة الملكيات الفكرية ، والاتجار غير المشروع في الأسلحة وفي النساء والأطفال ، والاتجار غير المشروع في الأعضاء البشرية، وسرقة المقتنيات الفنية و الثقافية، والغش في التامين ، وجرائم الحاسب الآلي أو الجرائم الالكترونية .[2]

الفرع الخامس: امتناع المجني عنهم عن التبليغ:

لا يتم في الغالب الأعم الإبلاغ عن جرائم الانترنت إما لعدم اكتشاف الضحية لها وإما خشية من التشهير، لذا نجد أن معظم جرائم الانترنت تم اكتشافها بالمصادفة، بل وبعد وقت طويل من ارتكابها، زد على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها، فالرقم المظلم بين الحقيقة عدد هذه الجرائم المرتكبة والعدد الذي تم اكتشافه، هو رقم خطير، وبعبارة أخرى، الفجوة بين عدد هذه الجرائم الحقيقي وما تم اكتشافه فجوة كبيرة.[3]

---

[1] خالد ممنوح إبراهيم، مرجع سابق،ص ص51-52

[2] نفس المرجع السابق، ص52.

[3] صغير يوسف، مرجع سابق، ص18.

تتبدى هذه الظاهرة على نحو أكثر حدة في المؤسسات المالية كالبنوك والمؤسسات الادخارية ومؤسسات الإقراض والسمسرة، حيث تخشى مجالس إدارتها عادة من تؤدي الدعاية السلبية التي تنجم عن كشف الجرائم أو اتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها وانصرافهم عنها.[1]

[1] نفس المرجع السابق، ص 18.

الفصل الثاني:

الآليات القانونية لمكافحة الجريمة الالكترونية في التشريع الجزائري

الفصل الثاني: الآليات القانونية لمكافحة الجريمة الالكترونية في التشريع الجزائري

بالرغم من المزايا الهائلة التي تحققها تقنية المعلومات في شتى ميادين الحياة المعاصرة, فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل ظهور الجرائم المعلوماتية، التي تمتاز بسمات متميزة عن الجرائم التقليدية، الأمر الذي أثار مشكلة عدم إمكانية تطبيق النصوص الموضوعية التقليدية لقانون العقوبات، فتبلورت فكرة وضع نصوص قوانين خاصة إلا أنها اختلفت في أسلوب المعالجة التشريعية لذلك.[1]

كما تثير الجريمة المعلوماتية من جهة أخرى نظرا لخصوصيتها، مشكلة عدم كفاية إجراءات التحري والتحقيق التقليدية في الحصول على الدليل الرقمي الناتج عن ارتكابها، مما أدى إلى ضرورة التطوير في هذه الإجراءات من خلال التطوير في الأحكام العامة للإجراءات التقليدية ، وعن طريق خلق إجراءات حديثة مختلفة عن تلك المتبعة في سبيل مكافحة الجرائم العادية.[2]

المبحث الأول: القواعد الموضوعية المنظمة للجريمة الالكترونية

لم تعرف الجزائر قبل 2004 قوانين تطبق على نظم المعلوماتية أو على تكنولوجيا الإعلام والاتصال، لكن أمام تزايد الإجرام المعلوماتي كان لابد للمشرع من إيجاد الإطار القانوني المناسب الذي يمنع الاعتداء على هذه النظم أو الاستعمال السيئ لها.[3]

---

[1] شرف الدين وردة، بلجراف سامية،" الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري"، مجلة المنار للبحوث والدراسات القانونية والسياسية ،العدد الثالث ،كلية الحقوق والعلوم السياسية ،جامعة يحي فارس المدية، ديسمبر 2017، ص 23.

[2] المرجع نفسه، ص23.

[3] سعيدة بوزنون،" مكافحة الجريمة الالكترونية في التاشريع الجزائري"، مجلة العلوم الانسانية،عدد 52، المجلد ب، جامعة الإخوة منتوري، كلية الحقوق ،قسنطينة،2019، ص49.

عالج المشرع الجزائري جرائم المعالجة الآلية للمعطيات في العديد من القوانين، والتي سنستعرضها وفقا للآتي:

المطلب الأول: مكافحة الجريمة بموجب قانون العقوبات ونصوص الملكية الفكرية

سنطرق في الفرع الأول كيف عالج المشرع هذه الجريمة في قانون العقوبات وفي الفرع الثاني في نصوص الملكية الفكرية.

الفرع الأول: بموجب قانون العقوبات

قام المشرع الجزائري في تعديله لقانون العقوبات بمقتضى القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 بإدراج القسم السابع مكرر خصصه للاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، مواكبة للتشريعات الغربية في مكافحة الجريمة المعلوماتية فاتجه اتجاها ايجابيا لحماية الحياة الخاصة التي أصبحت عرضة للانتهاكات عن طريق الحسابات الآلية بأفعال مستهجنة عواقبها جد خطيرة، بتعديل آخر لقانون العقوبات بالقانون 23/06 المؤرخ في 20 ديسمبر 2006 والذي مس المادة 303 من ق.ع لسنة 2004 وإدراجه المواد 303 مكرر إلى 303 مكرر 3 .[1]

أولا: تجريم الاعتداء على نظام المعالجة الآلية للمعطيات

عرف المشرع الجزائري نظام المعالجة الآلية للمعطيات بأنه:" كل نظام أو مجموعة من الأنظمة منفصلة كانت أم متصلة بعضها البعض أو المرتبطة والتي يقوم واحد منها أو أكثر بمعالجة

[1] طرشي نورة ،"مكافحة الجريمة المعلوماتية"، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي"، كلية الحقوق، جامعة الجزائر1، 2012/2011 ،ص53.

آلية للمعطيات تنفيذا لبرنامج معين" وهو نفس التعريف الذي جاءت به الاتفاقية الدولية للإجرام المعلوماتي المبرمة ببودابست في 2001، وجعل من وجود نظام المعالجة الآلية شرطا أساسيا للبحث عن مدى تحقق الاعتداء أم لا.[1]

وهذه بعض صور الاعتداء على نظام المعالجة الآلية للمعطيات:

1- جريمة التوصل أو الدخول غير المصرح به عن طريق الغش

تقوم هذه الجريمة بمجرد ما يتم الدخول غير المصرح به وعن طريق الغش إلى المنظومة المعلوماتية، سواء مس ذلك الدخول أو البقاء كامل المنظومة أو جزء منها فقط، وهو ما أشارت إليه المادة 394 مكرر من قانون العقوبات[2].

أورد المشرع ظرفين لتشدد عقوبة الدخول غير المشروع إلى المنظمات المعلوماتية، أو له حذف أو تغيير المعطيات، والظرف هو تخريب نظام اشتغال المنظومة، وقد أشار المشرع في المادة المذكورة أعلاه على تجريم فعل الشروع في جريمة الدخول غير المصرح به وذلك بقوله أو يحاول ذلك.[3]

[1] براهيمي جمال،"مكافحة الجرائم الالكترونية في التشريع الجزائري"،المجلة النقدية، كلية الحقوق ،جامعة مولود معمري،تيزي وزو،ص126.
[2] المادة 394 مكرر:" يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 د ج إلى 200.000 د ج كل من يدخل أو يبقى عن طريق الغش في كل جزء أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.
تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة."
[3] صغير يوسف،"الجريمة المرتكبة عبر الانترنت"، مرجع سابق،ص108.

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

نصت عليها المادة (394 مكرر1)[1] من قانون العقوبات، حيث اعتبر المشرع الجزائري أن إزالة أو تعديل المعطيات التي يتضمنها النظام بطريق الغش عملان إجراميان ويقصد بإزالة المعطيات سواء جزئيا أو كليا أو محوها أو إتلافها أو تخريبها من أجل منع النظام بالقيام بمهامه أو تعطيل النظام المعلوماتي ، أما تعديل المعطيات ويقصد به إدخال معلومات وهمية أو تزوير في النظام المعلوماتي.[2]

3- جرائم نشر أو حيازة أو الإتجار بالمعطيات المخزنة أو المعالجة:

نصت عليها المادة (394 مكرر2) [3] من قانون العقوبات، حيث تعد هذه الجريمة من أكثر الجرائم وقوعا في العالم الافتراضي ولقد اعتبر المشرع الجزائري عملية اصطناع برنامج مخصص لارتكاب فعل الغش المعلوماتي أو إعداد برنامج ناقص من الناحية الفنية وخاصة المبرمج من أجل خلق فجوات وثغرات فيه لممارسة فعل الغش أو تجميع أو التقاط البيانات بغرض استغلالها أو نشرها خاصة عن طريق الإنترنت أو الاتجار فيها من الجرائم المعاقب عليها، بحكم أن جريمة الإفشاء والنشر تتسم بخطورة على الحياة الخاصة.[4]

---

[1] المادة 394 مكرر1:" يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 د ج إلى 4000.000 د ج ، كل من أدخل بطريق الغشمعطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها."

[2] فاروق خلف،" الآليات القانةنية لمكافحة الجريمة المعلوماتية"، مجلة الحقوق والحريات،العدد الثاني 2015، كلية الحقوق جامعة حمة لخضر، الوادي، ص16.

[3] المادة 394 مكرر2:" يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1000.000 د ج إلى 10000.000 د ج ، كل من يقوم عمدا وعن طريق الغش:

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

- حيازة أو إفشاء أو نشر أو استعمال لأيس غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم.

[4] فاروق خلف، مرجع سابق، ص16.

يستخلص من استقراء البند أعلاه (المادة 394 مكرر 2) أن المشرع الجزائري يعمل على تقرير حماية جنائية لكل المعطيات داخلية أو خارجية.

ويقصد المشرع بالمعطيات المحزنة إما تلك المفرغة في دعامة مادية خارج النظام كالأقراص، أو تلك المخزنة داخل النظام ذاته كذاكرته أو قرصه الصلب.[1]

ويقصد بالمعطيات المعالجة إما تلك التي أصبحت جزاءا من النظام بعد أن تحولت إلى إشارات أو رموز تمثل المعطيات المعالجة، أو تلك المعطيات المرسلة عن طريق منظومة معلوماتية مثل تبادل إرسال المعلومات بين أجهزة المنظومة المعلوماتية، فالأولى تعتبر معطيات داخلية للنظام والأخرى معطيات خارجية للنظام.[2]

وعليه فأي تلاعب بالمعطيات أعلاه، وبحسب المادة 394 مكرر2 يعد جريمة اعتداء على المعطيات، وبالتالي يعاقب صاحبها طبقا للقانون.

4- إذا ارتكبت هذه الجرائم ضد الدفاع الوطني أو الهيئات والمؤسسات العامة:

اتسمت السياسة الجنائية للمشرع الجزائري بخصوص جرائم المساس بأنظمة المعالجة الآلية للمعطيات ضد الدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام بالتشدد[3]، حيث أصبحت هذه المؤسسات تعتمد في تسيير شؤونها على التقنية المعلوماتية مثل استعمال نظم معلوماتية مختلفة كقواعد البيانات.

---

[1] ناجية شيخ،" حول مكافحة الجريمة الإلكترونية في التشريع الجزائري"، مجلة العلوم القانونية والسياسية، المجلد 9، العدد 2، جامعة مولود معمري، تيزي وزو، جوان 2018، ص 693.

[2] المرجع نفسه، ص 693.

[3] يزيد بوحليط، مرجع سابق، ص 197.

ونظرا لأن هذه المؤسسات تمثل سيادة الدولة فيمكن لهذه الجرائم الإخلال بأمن وسلامة الدولة ومؤسساتها خاصة في ظل توجه الجزائر وبخطوات ثابتة نحو تحقيق الحكومة الالكترونية بغية عصرنة خدماتها والقضاء على مشكلات البيروقراطية، تجلى ذلك في إنجاز جواز السفر البيومتري وبطاقة التعريف البيومترية، وإمكانية استخراج الوثائق الإدارية عبر الإنترنت..إلخ.

في هذا الصدد المادة (394 مكرر 3)[1] من قانون العقوبات، من خلالها يتضح لنا أن المشرع الجزائري حرص على توفير الحماية المطلقة لمؤسسة الدفاع الوطني ولمؤسسات الدولة وتوسع في ذلك، ومنها جرائم الخيانة والتجسس التي نص عليها في قانون العقوبات بموجب المواد من (61–65) والتي تتم ضد الدولة أو مؤسساتها الدفاعية كما في حالة تسليم معلومات أو أشياء أو مستندات أو تصميمات [2] فلم يكتف المشرع بتجريم التجسس بالطرق التقليدية فقط، وإنما نص على جريمة التجسس الإلكتروني باستعمال التقنية المعلوماتية وضاعف من العقوبة عليها دون الإخلال بعقوبات أشد،وعليه يمكن للقاضي تطبيق العقوبات الأشد المنصوص عليها من المادة 60 إلى المادة 87 مكرر من قانون العقوبات خاصة المتعلقة بجرائم المساس بأمن الدولة ومؤسساتها ووحدتها.[3]

[1] المادة 394 مكرر 3:" تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد".
[2] يزيد بوحليط ، مرجع سابق، ص 197.
[3] المرجع نفسه، ص 198.

5- إذا ارتكبت هذه الجرائم من طرف الشخص المعنوي:

نصت المادة (394 مكرر 4)[1] من قانون العقوبات على توقيع العقوبة على الشخص المعنوي الذي يرتكب إحدى الجرائم الواردة في الفصل السابع مكرر بغرامة تعادل 5 مرات الحد الأقصى للغرامة المحددة للشخص الطبيعي، غير أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء في نفس الجريمة.[2]

6- عقوبة الشروع والاشتراك في الجريمة الإلكترونية:

الجرائم الماسة بالأنظمة المعلوماتية لها وصف جنحي، وباعتبار أمه لا عقاب على الشروع في الجنح إلا بنص، فقد أقرت المادة(394 مكرر7)[3] من قانون العقوبات على ذلك، بالتالي يبدو من خلال هذا النص رغبة المشرع الجزائري في توسيع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية.[4]

وفي هذا الإطار انقسم الفقه بين من يذهب بين من يذهب إلى أنه لا يوجد شروع في الاتفاق الجنائي لكونه حالة نفسية تتم بتلاقي الإرادات[5] ولا تحتمل لا بداية ولا نهاية وهو يقع إلا كاملا ولا يحتمل البدء في التنفيذ، خاصة وأن المشرع لا يعتبر الدعوة إلى الاتفاق روعا ولكن يعاقب عليها كجريمة قائمة بذاتها، في حين يرى جانب آخر أنه طالما كانت أركان الشروع قائمة ولم

---

[1] المادة 394 مكرر 4:" يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".

[2] صغير يوسف، مرجع سابق، ص 111.

[3] المادة 394 مكرر 7:" يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".

[4] خاليدة بن بعلاش، علي عثماني،" الأحكام الموضوعية والإجرائية لمكافحة الجريمة الالكترونية في التشريع الجزائري"، مجلة أبحاث قانونية وسياسية ،المجلد 6، العدد 2، ديسمبر 2021، بدون كلية وجامعة، ص704.

[5] دمان ذبيح عماد، بهلول سمية،" الآليات العقابية لمكافحة الجريمة الالكترونية في الجزائر"، مجلة الحقوق والعلوم السياسية، العدد 13، جانفي 2020، جامعة عباس لغرور خنشلة، ص 145.

يكن القانون يتضمن نصا خاصا يعاقب عليه فلا داعي للأخذ بالرأي السابق لكونه غير صحيح أن الشروع في الاتفاق غير متصور.

هذا وقد نصت المادة(394 مكرر 5)[1] على الاشتراك.

7- عقوبة مقدمو خدمة الانترنت عند عدم امتثاله لأوامر الهيئة المختصة:

نصت المادة(394 مكرر 8)[2] من قانون العقوبات على عقوبة "مقدم خدمات الانترنت"[3] كما عرفته المادة 2 من القانون 09-04 عند عدم القيام بأوامر الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[1] المادة 394 مكرر 5:" كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها."

[2] المادة 394 مكرر 8:" دون الإخلال بالعقوبات الإدارية المنصوص عليها في التشريع والتنظيم الساري المفعول، يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من 2000.000 د ج إلى 10.000.000 د ج ، أو بإحدى هاتين العقوبتين فقط، مقدم خدمات " الانترنت" بمفهوم المادة 2 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الذي لا يقوم رغم إعذاره من الهيئة الوطنية المنصوص عليها في القانون المذكور أو صدور أمر أو حكم قضائي يلزمه بذلك:
أ- بالتدخل الفوري لسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول إليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا.
ب- بوضع ترتيبات تقنية تسمح بسحب أو تخزين المحتويات التي تتعلق بالجرائم المنصوص عليها في الفقرة(أ) من هذه المادة أو لجعل الدخول إليها غير ممكن."

[3] المادة 2 فقرة د من القانون 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها تنص على :" مقدمو الخدمات: 1-أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/ أو نظام للاتصالات .
2- و أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.

ثانيا: حماية الحياة الخاصة

من خلال التعديل الذي جاء في القانون رقم 06-23 المتعلق بقانون العقوبات في المادة(303 مكرر)[1] منه وكذا المادة (303 مكرر 1)[2].

ثالثا: حماية حرمة رموز الدولة[3]

من خلال التعديل الذي جاء في القانون رقم (14/11) المتعلق بقانون العقوبات، في نص المادة (144 مكرر)[4] منه

[1] المادة 303 مكرر :" يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 د ج إلى 300.000 د ج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك:
- بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة، أو سرية، بغير إذن صاحبها أو رضاه
- بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه.
- يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة.
ويضع صفح الضحية حدا للمتابعة الجزائية."

[2] المادة 303 مكرر 1:"يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير، أو استخدم بأي وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون
عندما ترتكب الجنحة المنصوص عليها في الفقرة السابقة عن طريق الصحافة، تطبق الأحكام الخاصة، المنصوص عليها القوانين ذات العلاقة لتحديد الأشخاص المسؤولين.
يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة."

[3] فاروق خلف، مرجع سابق، ص 17.

[4] المادة 144 مكرر:"يعاقب بغرامة من 100.000 د ج إلى 500.000 د ج كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأية آلية لبث الصوت أو صورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى.
تباشر النيابة العامة إجراءات المتابعة الجزائية تلقائيا.
وفي حالة العود تضاعف الغرامة.

الفرع الثاني: بموجب قانون الملكية الفكرية الجزائري

نظرا لنسبية الحماية المقررة من خلال النصوص التقليدية في قانون العقوبات سنتطرق إلى مدى إمكانية الحماية من خلال نصوص الملكية الفكرية من خلال: قانون الملكية الصناعية وقانون الملكية الأدبية والفنية

أولا: مواجهة الجريمة المعلوماتية من خلال قانون الملكية الصناعية

1- من خلال أحكام العلامات التجارية:

ينظمها الأمر 06/03 المؤرخ في : 2003/07/19 المتعلق بالعلامات المعدل والمتمم للأمر 57/66 المؤرخ في 1966/03/19 المتعلق بعلامات المصنع والعلامات التجارية والمعدل للأمر رقم 223/67 المؤرخ في 1967/10/19 المتضمن أحكام العلامات التجارية و العلامات التجارية هي كل ما يتخذ من تسميات أو رموز أو أشكال توضع على البضائع التي يبيعها التاجر أو يصنعها المنتج أو يقوم بإصلاحها أو تجهيزها أو ختمها لتمييزها عن بقية المبيعات أو المصنوعات أو الخدمات ،ويشترط في العلامة أن تكون مميزة وجديدة وغير مخالفة للنظام والآداب [1]

السؤال المطروح: هل تستفيد برامج الحاسب الآلي من الحماية الجنائية للعلامات التجارية ؟

[1] فشار عطاء الله،" مواجهة الجريمة المعلوماتية في التشريع الجزائري"، بحث مقدم إلى الملتقى المغاربى حول القانون والمعلوماتية المزمع عقده بأكاديمية الدراسات العليا بليبيا، جامعة زيان عاشور بالجلفة كلية الخقوق والعلوم السياسية،2009، ص 11.

نعلم أن كل برنامج يحمل اسما خاصا به، لذلك فقد عمد أصحاب البرامج إلى تسجيل هذا الاسم كعلامة تجارية للبرنامج، ولما كانت هذه الحماية قاصرة على الاسم دون المحتوى فقد لجا أصحاب البرامج إلى وضع الاسم مقترنا به.

الحماية بإحكام العلامات التجارية قد تكون فعالة بالنسبة للنسخ البسيط، لكن ليس الأمر كذلك بالنسبة للنسخ المعقد.

2 – من خلال أحكام براءة الاختراع :[1]

عرفت المادة 02 من الأمر 07/03 الاختراع بأنه فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية. وبشان الشروط التي يجب توافرها في الاختراع فتتمثل فيما يلي:

- شرط الابتكار
- شرط الجدة
- القابلية للتطبيق الصناعي
- المشروعية

في حال توافر هذه الشروط يتحصل المخترع على براءة الاختراع وهي الوثيقة التي تمنحها الدولة للمخترع فتخول له حق استغلال اختراعه والتمتع بالحماية القانونية المقررة لهذا الغرض وذلك لمدة محدودة وبشروط معينة والجهاز المانح لهذه الشهادة هو المعهد الجزائري لحماية الملكية الصناعية .

[1] نفس المرجع السابق، ص 11.

السؤال المطروح هل تستفيد برامج الحاسب من الحماية بواسطة براءات الاختراع ؟

التشريعات المعاصرة بصفة عامة تستبعد البرامج المعلوماتية من مجال الحماية بواسطة براءات الاختراع لأحد سببين أساسين هما:

– إما تجرد البرامج من أي طابع صناعي

– إما صعوبة البحث في مدى جدة البرنامج لتقدير مدى استحقاق البرنامج للبراءة فليس من الهين توافر شرط الجدة في البرمجيات وليس من الهين إثبات توافر هذا الشرط، إذ يجب أن يكون لدى الجهة التي تقوم بفحص طلبات البراءة قدرا معقولا من الدراية لتقرر ما إذا كان قد سبق تقديم اختراعات مشابهة للاختراع المقدم الطلب بشأنه أم لا ، الأمر يتطلب أن تكون هذه الجهة على درجة عالية من الكفاءة والتمييز في المجال الذي تتولى بحثه.[1]

و الجهة المكلفة بتقرير توافر شرط الجدة في الجزائر هي المعهد الجزائري لحماية الملكية الصناعية إذ يأخذ المشرع الجزائري بمبدأ الجدة المطلقة الذي يتنافى مع وجود أية سابقة دون تحديد زماني أو مكاني، إنما يشرط أن تتوافر علانية هذه السابقة.[2]

إضافة إلى التحفظ العملي لمنتجي برامج الحاسب على استعمال قوانين براءة الاختراع ، ويتمثل هذا التحفظ في الإجراءات المعقدة للحصول على البراءة والتكلفة العالية والمدد الطويلة التي يستغرقها هذا التسجيل ، فعمر البرنامج قصير نسبيا لا يتعدى ثلاثة سنوات بينما قد تمتد

[1]) نفس المرجع السابق ، ص 12.
[2] المرجع نفسه، ص12.

إجراءات تسجيل البراءة مثل ذلك أو أكثر وعليه بمكن للغير الوصول إلى سر البرنامج واستغلاله قبل صدور البراءة .

ثانيا: مواجهة الجريمة المعلوماتية من خلال قانون الملكية الأدبية والفنية

شهد النصف الأخير من القرن العشرين تطورا ملحوظا في مجال الاتصال رافقه تطور في وسائل نقل الإنتاج الفكري على اختلاف صوره من علوم وفنون وآداب، مما أوجد مصنفات جديدة جديرة بحماية حق المؤلف كانت محل اهتمام ودراسة من قبل المختصين في مجال الملكية الفكرية، وقد كان من أهم هذه المصنفات، المصنفات الخاصة ببرامج الحاسبات الإلكترونية، وقواعد البيانات التي كانت طبيعتها التقنية تختلف عن المصنفات التقليدية، الأمر الذي تطلب متابعتها باستمرار ووضع قواعد قانونية محددة وثابتة.[1]

جاء الأمر رقم 03-05 المتعلق بحق المؤلف والحقوق المجاورة باستخلاص ما يلي: - أن المشرع وسع قائمة المؤلفات المحمية، حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية والتي عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي- تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين، لاسيما المصنفات المعلوماتية ، حيث تنص المادة 05 من القانون رقم 03-05على أنه: " تعتبر أيضا مصنفات محمية الأعمال الآتية....مجموعات من مصنفات التراث الثقافي التقليدي وقواعد البيانات سواء كانت مستنسخة على دعامة قابلة للاستغلال [2]بواسطة آلة أو بأي شكل من الأشكال الأخرى...تكفل الحماية لمؤلف المصنفات

[1] صغير يوسف، مرجع سابق، ص106.
[2] نايري عائشة ، مرجع سابق، ص35.

المشتقة دون المساس بحقوق مؤلفي المصنفات الأصلية." والمادة رقم 04من نفس القانون نصت على أنه:" تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يلي: المصنفات الأدبية المكتوبة مثل...وبرامج الحاسوب...."كما أن مدة الحماية تحدد ب 50 سنة بعد وفاة المبدع وفقا للمادة 58 فقرة الأولى من نفس القانون، ويعتبر كل اعتداء على الحق المالي أو الأدبي لمؤلف برنامج فعلا من أفعال التقليد[1]، حيث نص المشرع في المادة 151 من الأمر رقم 05/03على قيام جنحة التقليد في حالة الكشف غير المشروع عن مصنف أو أداء فني أو في حالة المساس بسلامة مصنف أو أداء فني، أو في حالة استنساخ مصنف أو أداء فني بأي أسلوب في شكل نسخ مقلدة أو في حالة استيراد نسخ مقلدة أو تصديرها أو بيع نسخ مزورة من مصنف أو أداء فني و أخيرا في حالة تأجير مصنف أو أداء فني أو عرضه للتداول. وقد قرر المشرع جزاءات لجرائم التقليد، حيث ربط المشرع الجزائري حماية المصنف بتاريخ الانتهاء من الابتكار أو تاريخ النشر أو التوزيع لأول مرة، كما خول المشرع لصاحب المصنف

المعتدى عليه القيام بإجراء تحفظي يتمثل في حجز التقليد، وبواسطته يتم حجز الوثائق والنسخ الناتجة عن الاستنساخ غير المشروع أو التقليد[2]، والعقوبات المقررة للاعتداء على حقوق الملكية الأدبية والفنية تشمل المواد من 153/156إلى 159من نفس القانون السابق الذكر، حيث قدرت العقوبة الأصلية بالحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500.000دج إلى 1.000.000دج سواء تمت عملية النشر داخل الجزائر أو خارجها، ومنح المشرع للقاضي سلطة تقرير عقوبات تكميلية تتمثل في مصادرة المبالغ المساوية لمبلغ

[1] نفس المرجع السابق، ص35.
[2] المرجع نفسه، ص 35.

الإيرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو أداء محمي، ومصادرة و إتلاف كل عتاد أنشأ خصيصا لمباشرة النشاط غير المشروع، وكل النسخ المقلدة والمصادرة في هذه الحالة تكون وجوبية، كما للقاضي أن يضاعف العقوبة في حالة العود مع إمكانية غلق المؤسسة التي يستغلها المقلد أو شريكه مدة لا تتعدى ستة أشهر.

المطلب الثاني: مكافحة الجريمة بموجب القانون 04/09 والقانون 03/2000

حاول المشرع الجزائري سن قوانين خاصة للحد من الجريمة المعلوماتية من خلال القانون 04/09 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والقانون 03/2000 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.

الفرع الأول: بموجب القانون 04/09 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

أطلق المشرع الجزائري على الجرائم المعلوماتية [1]مصطلحي:" جرائم المساس بأنظمة المعالجة الآلية للمعطيات" و" الجرائم المتصلة بتكنولوجيا الإعلام والاتصال" وقد عرفها ضمن القانون رقم 09-04 المؤرخ في 5 أوت 2009، في المادة 2- أ على أنه يقصد بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال :(جرائم المساس بأنظمة المعالجة الآلية للمعطيات)المحددة في قانون العقوبات و أي جريمة أخرى

[1] شرف الدين وردة و بلجراف سامية، مرجع سابق، ص 35.

ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الالكترونية.

يتميز القانون 09-04 السابق الإشارة إليه بأنه القانون الأكثر ملائمة مع الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت.[1]

حيث أتى بتدابير متنوعة بعضها وقائي وبعضها تدابير إجرائية

أولا: التدابير الوقائية المستحدثة:

لقد جاء في القانون 09-04 مجموعة من التدابير الوقائية التي يتم اتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية أو الكشف عنها وعن مرتكبيها في وقت مبكر وهي كالتالي:

1- مراقبة الاتصالات الالكترونية:

لقد نصت المادة 04 من القانون 09 على أربع حالات التي يجوز فيها لسلطات الأمن القيام بمراقبة المراسلات والاتصالات الإلكترونية، وذلك بالنظر إلى خطورة التهديدات المحتملة وأهمية المصلحة المحمية.[2]

2-إقحام مزودي خدمات الاتصالات الالكترونية في مسار الوقاية من الجرائم المعلوماتية:

وذلك من خلال فرض عليهم مجموعة من الالتزامات مذكورة في المواد 10،11 و 12 من نفس القانون بالشكل التالي:

الالتزام بالتعاون مع مصالح الأمن المكلف بالتحقيق القضائي عن طريق جمع أو تسجيل المعطيات المتعلقة بالاتصالات والمراسلات ووضعها تحت تصرفها مع مراعاة سرية

[1] ناجية شيخ، مرجع سابق، ص697.

[2] حنان مسكين،" واقع مكافحة الجرائم المعلوماتية واتجاهاتها التشريعية في الجزائر"، المجلة الأكاديمية للبحوث القانونية والسياسية،المجلد الرابع، العدد الأول،جامعة الدكتور مولاي الطاهر، سعيدة، 2020، ص 621.

هذه الإجراءات والتحقيق .

الالتزام بحفظ المعطيات المتعلقة بحركة السير وكل المعلومات التي من شأنها أن تساهم في الكشف عن الجرائم ومرتكبيها، وهذين الالتزامين موجهين لكل مقدمي خدمات الاتصالات الالكترونية دون استثناء.[1]

الالتزام الفوري لسحب المحتويات التي يسمح لهم الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقانون، وتخزينها أو جعل الوصول إليها غير ممكن.

الالتزام بوضع ترتيبات تقنية للحد من إمكانية الدخول إلى الموزعات التي تحتوي على معلومات متنافية مع النظام العام والآداب العامة مع إخطار المشتركين لديهم بوجودها، ونشير إلى أن هذين الالتزامين يخصان فقط مقدمي الدخول إلى الانترنت.[2]

ثانيا: التدابير الإجرائية

أضاف المشرع إلى جانب تلك التدابير الوقائية الواردة في القانون الخاص رقم 09-04 إجراءات جديدة تدعم تلك المنصوص عليها في قانون الإجراءات الجزائية[3]، ولاسيما تلك المتعلقة بمكافحة الجريمة الالكترونية، ويمكن تلخيص هذه الإجراءات في:

جواز التفتيش ولو عن بعد للمنظومة المعلوماتية أو لجزء منها من طرف الجهات القضائية المختصة وضباط الشرطة القضائية.

---

[1] راهيمي جمال، مرجع سابق، ص152.
[2] المرجع نفسه، ص 153.
[3] ناجية شيخ، مرجع سابق، ص698.

إمكانية تمديد آجال التفتيش بإذن السلطة المختصة.

إمكانية الاستعانة بالسلطات الأجنبية المختصة للحصول على المعطيات محل البحث المخزنة في منظومة معلوماتية موجودة خارج الإقليم الوطني، وذلك طبقا للاتفاقيات الدولية ومبدأ المعاملة بالمثل.[1]

توسيع دائرة اختصاص الهيئات القضائية الجزائرية لتشمل النظر في الجرائم المتصلة بتكنولوجية الإعلام والاتصال المرتكبة من طرف الأجانب خارج الإقليم الوطني، عندما تكون مؤسسات الدولة الجزائرية والدفاع الوطني والمصالح الإستراتيجية للدولة الجزائرية مستهدفة.[2]

السماح للسلطات الجزائرية المختصة باللجوء إلى التعاون المتبادل مع السلطات الأجنبية في مجال التحقيق وجمع الأدلة للكشف عن الجرائم المتصلة بتكنولوجية الإعلام والاتصال عبر الوطنية ومرتكبيها، وذلك عن طريق تبادل المعلومات أو اتخاذ تدابير احترازية في إطار الاتفاقيات الدولية ومبدأ المعاملة بالمثل.[3]

تجدر الإشارة أنه أنشئت بموجب القانون رقم 09-04 المذكور سابقا هيئة تعرف في صلب القانون بـــ : " الهيئة الوطنية للوقاية من الجرام المتصلة بتكنولوجيا الإعلام والاتصال ".[4]

اهتمت هذه الهيئة بمهام متعددة ، أهمها:

تفعيل التعاون القضائي والأمني والدولي وإدارة وتنسيق العمليات الوقائية.

---

[1] حنان مسكين، مرجع سابق، ص622

[2] براهيمي جمال،، مرجع سابق، ص154.

[3] المرجع نفسه، ص154.

[4] ناجية شيخ، مرجع سابق، ص698.

المساعدة التقنية للجهات القضائية و الأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية في حالة الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.[1]

يستنتج في الأخير أن أحكام القانون رقم 09-04 جاءت عامة ومطلقة في مكافحة الجرائم المتصلة بتكنولوجية الإعلام والاتصال، بحيث تجرم كل الأفعال المخالفة للقانون التي ترتكب عبر وسائل الإعلام والاتصال، ويطلق على كافة التكنولوجيات القديمة والجديدة، بما فيها بكة الانترنت وعلى أي تقنية يمكن أن تظهر مستقبلا، وهو الأمر الذي يجعله قانونا فعالا ويساير التطور التكنولوجي السريع.[2]

الفرع الثاني: بموجب قانون رقم 2000-03 المؤرخ في 05 غشت سنة 2000، يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية:

و تتمثل بعض الجرائم المعلوماتية التي نص عليها المشرع الجزائري ضمن هذا القانون في:[3]

- فتح أو تحويل أو تخريب البريد أو انتهاك سرية المراسلات أو المساعدة على ارتكاب هذه الأفعال من قبل:كل شخص يقوم بتقديم خدمة البريد السريع الدولي أوكل عون يعمل لديه وفي إطار ممارستهم لمهامهم، كل شخص مرخص له بتقديم خدمة مواصلات سلكية ولاسلكية، وكل

[1] نفس المرجع السابق، ص698.
[2] حنان مسكين، المرجع السابق، ص622.
[3] شرف الدين وردة و بلجراف سامية، المرجع السابق، ص33.

عامل لدى متعاملي الشبكات العمومية للمواصلات السلكية واللاسلكية وأثناء ممارستهم لمهامهم وغيرهم(المادة 127).[1]

- إنشاء أو استغلال شبكة عمومية لمواصلات السلكية واللاسلكية دون رخصة أو مواصلة ممارسة النشاط خرقا لقرار التعليق أو سحب هذه الرخصة (المادة 131).
- إنشاء أو العمل على إنشاء شبكة مستقلة دون ترخيص (المادة 132).
- إشهار بغرض بيع تجهيزات أو معدات للمواصلات السلكية واللاسلكية دون الحصول على الاعتماد المسبق(المادة 1339.
- تحويل أو العمل على تحويل أو استغلال خطوط المواصلات السلكية واللاسلكية المحولة(المادة 135).

المطلب الثالث: بموجب القانون 12-05 والقانون 08-01

سنحاول تبسيط ما جاءا به القانونين من خلال الفرعين المواليين

الفرع الأول: القانون العضوي رقم 12-05 مؤرخ في 12 يناير سنة ،2012 يتعلق بالإعلام

حيث نص في الباب التاسع على مجموعة من المخالفات المرتكبة في إطار ممارسة النشاط الإعلامي، وتتمثل الجرائم المعلوماتية المذكورة ضمن هذه المواد في:

- نشر وبث بإحدى وسائل الإعلام المنصوص عليها في هذا القانون العضوي، أي خبر أو وثيقة تلحق ضررا بسر التحقيق الابتدائي في الجرائم (المادة 119).

[1] نفس المرجع السابق، ص33.

- نشر وبث بإحدى وسائل الإعلام المنصوص عليها في هذا القانون العضوي، فحوى مناقشات الجهات القضائية التي تصدر الحكم، إذا كانت جلساتها سرية (المادة 120).[1]
- نشر وبث بإحدى وسائل الإعلام المنصوص عليها في هذا القانون العضوي، تقارير عن المرافعات التي تتعلق بحالة الأشخاص والإجهاض (المادة 121).
- نشر وبث بإحدى وسائل الإعلام المنصوص عليها في هذا القانون العضوي، صورا أو رسوما أو أي بيانات توضيحية أخرى تعيد تمثيل كل أو جزء من ظروف الجنايات أو الجنح المذكورة في المواد 255 إلى 263 مكرر و من 333 إلى 342 من قانون العقوبات (المدة 122).
- إهانة بإحدى وسائل الإعلام المنصوص عليها في هذا القانون العضوي، رؤساء الدول الأجنبية وأعضاء البعثات الدبلوماسية المعتمدين لدى حكومة الجمهورية الجزائرية الديمقراطية الشعبية.[2]

الفرع الثاني : القانون العضوي رقم 08-01 مؤرخ في 23 يناير سنة 2008، يتمم القانون 83-11 المؤرخ في: 2 يوليو سنة 1983 والمتعلق بالتأمينات الاجتماعية:

تمم هذا القانون أحكام القانون 83-11 المؤرخ في 2 يوليو سنة 1983 بباب خامس مكرر عنوانه "أحكام جزائية"، يتضمن المواد 93مكرر2 و 93 مكرر3 و 93 مكرر4 و 93مكرر5 و 93مكرر6، وتتمثل الجرائم المعلوماتية التي ترتكب على البطاقة الإلكترونية للمؤمن له اجتماعيا فيما يلي:

[1] نفس المرجع السابق، ص36.
[2] المرجع نفسه،ص 36.

- تسليم أو استلام بهدف الاستعمال غير المشروع البطاقة الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة(المادة 93 مكرر2).
- القيام عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية و/أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهني الصحة(المادة 93 مكرر1/3).
- الإعداد أو التعديل أو النسخ بطريقة غير مشروعة البرمجيات التي تسمحا لوصول أو باستعمال المعطيات المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهني الصحة (المادة 93مكرر 2/3).
- المحاولة في ارتكاب الجنح المذكورة في الفقرتين الأولى والثانية من المادة 93مكرر3 (المادة 93 مكرر 3/3).[1]
- نسخ أو صناعة أو حيازة أو توزيع بطريقة غير مشروعة البطاقة الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الالكتروني لمهني الصحة(المادة 93 مكرر 4).
- ارتكاب الشخص المعنوي إحدى الجنح المنصوص عليها في المادتين 93مكرر3و 93مكرر 4أعلاه (المادة 93 مكرر5).

[1] نفس المرجع السابق، ص34.

- ارتكاب الجنح المنصوص عليها في المادتين 93مكرر 3و 93مكرر 4أعلاه، في حالة علم المالك بذلك.

المبحث الثاني: الحماية الإجرائية للنظام المعلوماتي

بعد أن تناولنا كيف حاول المشرع التصدي للجريمة الالكترونية بسن جملة من القوانين سنحاول في هذا المبحث التطرق للقواعد الإجرائية التي أتى بها المشرع الجزائري لمتابعة مركبي هذه الجريمة.

المطلب الأول: الإجراءات التقليدية لجمع الدليل الإلكتروني

إن الجريمة الإلكترونية تعتبر كأي جريمة من الجرائم المنصوص عليها في قانون العقوبات والقوانين الأخرى فلذلك تتسع الجريمة الإلكترونية بدعوى عمومية وهذه الدعوة تتم بمراحل سنوضحها من خلال الفروع الآتية.[1]

الفرع الأول: تلقي الشكاوى والبلاغات

يناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها[2]، ونعتبر صلاحية تلقي الشكاوى والبلاغات من المراحل المهمة في البدء في إجراء التحقيق الابتدائي، خاصة في مجال مكافحة الجرائم الإلكترونية التي يصعب كشفها نتيجة وجود الدليل في بيئة رقمية يسهل معها محوه أو تدميره.

[1] مرابطن حياة،" الجريمة الإلكترونية في التشريع الجزائري"، مذكرة نهاية الدراسة لنيل شهادة الماستر،كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس،مستغانم،2019/2018، ص34.
[2] يزيد بوحليط، مرجع سابق، ص313.

أولا: تلقي البلاغات في الجريمة الإلكترونية

الأصل أنه يجب على رجال الشرطة قبول البلاغات أو الشكاوي التي تقدم إليهم سواء كانت كتابية أو شفهية، وعند وردها للقسم تقيد في دفتر خاص بتلقي البلاغات، كما يجب على المتحري أو المتحقق إخطار رئاسته في حالة الجرائم الإلكترونية، وإخطار الجهات المختصة مثل: إدارة مكافحة جرائم الحاسبات وشبكات المعلومات، ومن الأخطار الشائعة في هذا المجال، الامتناع عن قبول البلاغ أو الشكوى بدعوى عدم الاختصاص المكاني أو النوعي بها، في حين أن الواجب اتخاذ الإجراءات المقرة بشأنها، ثم إخطار جهة الاختصاص وإحالة المحضر إليها.[1]

ويقوم المتحري بجمع الأدلة وفحص البلاغ أو الشكوى إجراءات معينة تتمثل في المعاينة وجمع الأدلة والتحقيق.

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

[1] محمد بوعمرة وسيد علي بنينال،" جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري"، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، البويرة،2019-2020، ص ص 41-42.
[2] نفس المرجع السابق، ص42.

ثانيا: تلقي الشكاوى في الجريمة الإلكترونية

قد يترتب على الجريمة ضرر خاص يصيب أحد الأفراد ماديا أو معنويا فينشأ له حق في تحريك الدعوى العمومية بتقديم شكوى أمام الجهة المختصة بالتحقيق حيث نص المشرع الجزائري في (المادة 72)[1] من قانون الإجراءات الجزائية على الشكوى المصحوبة بالإدعاء المدني، وقد عرفت الشكوى بأنها البلاغ أو الإخطار الذي يقدمه المجني عليه أو وكيله الخاص إلى السلطات المختصة طالبا تحريك الدعوى العمومية بشأن جرائم معينة، حظر المشرع تحريكها بصددها قبل تقديمه، ولا يوجب القانون للشكوى شكلا معينا و إنما يقتصر فيها المعني بالأمر على ذكر اسمه وسنه وعنوانه وموجز الوقائع، والمواد القانونية التي تعاقب الفعل المرتكب، وإعطاء كافة المعلومات الخاصة بمرتكب الجريمة إذا كان معلوما.[2]

الفرع الثاني: الاستجواب وسماع الشهود في الجريمة الإلكترونية

يستدعى أشخاص للإدلاء بأقوالهم، قد يكونون مشتبه فيهم وهذا ما يطلق عليه الاستجواب، وقد يكون هؤلاء أشخاص خارجين عن الخصومة إلا أنهم يؤثرون على مسار القضية من خلال شهادتهم.[3]

أولا: الإستجواب في الجريمة الإلكترونية

وهو أن يمثل أمام المحقق حتى يتحقق من هويته ومحيطه علما بكل الوقائع المنسوبة إليه

---

[1] المادة 72 من قانون الإجراءات الجزائية:" يجوز لكل شخص متضرر من جناية أو جنحة أن يدعي مدنيا بأن يتقدم بشكواه أمام قاضي التحقيق المختص."

[2] بخي فاطمة الزهراء،" إجراءات التحقيق في الجريمة الإلكترونية"، مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة،2013-2014، ص ص 56-57.

[3] نفس المرجع السابق، ص 63.

وينبهه بأنه حر في الإدلاء بأقواله أو عدم الإدلاء بها، كما يجب على المحقق أن يخبر المتهم في أن له الحق في توكيل محامي وان لم يقدر يجوز للمحقق أن يعين له محام من تلقاء نفسه، كما يجب على المتهم إذا ما طرأ تغيير عنوانه أن يخطر المحقق بذلك.[1]

الاستجواب ما هو إلا مناقشة تفصيلية في التهمة المنسوبة إليه من طرف جهة التحقيق ومطالبته بإبداء رأيه في الأدلة القائمة ضده إما تنفيذا أو تسليما وذلك قصد محاولة كشف الحقيقة واستظهارها بالطرق القانونية.[2]

ثانيا: سماع الشهود في الجريمة الإلكترونية

سماع الشهود هو إجراء من الإجراءات التحقيق، يهدف لجمع الأدلة المتعلقة بالجريمة، بحيث يستدعي أشخاص ليست لهم علاقة بالجريمة، إلا أن وجودهم ضروري للكشف عن الجرائم والقبض عن مرتكبها يختلف الشاهد في الجريمة الإلكترونية عن الشاهد في الجرائم العادية لما يتميز به من صفة خاصة تمنحه إياها طبيعة عمله وخبرته في مجال المعلوماتية.[3]

إن مصطلح الشهادة الإلكترونية يطلق على نوع من الشهادة التي لا يكون فيها الشاهد حاضرا فقد يتم مثلا عن طريق وسائل إلكترونية[4]،أو رقمية من خلال شبكة الإنترنت.

---

[1] محمد بوعمرة وسيد علي بنينال، مرجع سابق، ص43.
[2] مرابطن حياة، مرجع سابق، ص43.
[3] محمد بوعمرة وسيد علي بنينال، مرجع سابق، ص43.
[4] ابتسام بغو،" إجراءات المتابعة الجزائية في الجريمة المعلوماتية"، مذكرة مكملة لنيل شهادة ماستر في القانون تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي أم البواقي، 2015-2016، ص 70.

وقد أعطى قانون الإجراءات الجزائية لقاضي التحقيق الحرية في تحديد الأشخاص الذين يرى فائدة من سماع شهادتهم، سواء كان هؤلاء الأشخاص قد ورد ذكرهم في البلاغ عن الجريمة أو الشكوى منها، أو أي شخص آخر،وذلك تطبيقا للمواد 60، 88، 97، 110، من قانون الإجراءات الجزائية الجزائري.[1]

المطلب الثاني : الإجراءات المستحدثة في التحري وجمع الأدلة

يقصد بها مجموع الإجراءات التي يقوم بها التحري عبر شبكة الأنترنت بواسطة التقنية الإلكترونية الرقمية تحت تغطية للحصول على بيانات و معلومات تعريفية أو توضيحية عن الأشخاص أو الأماكن أو الأشياء حسب طبيعتها للحد من الجرائم الإلكترونية ،و نقسمها إلى الوسائل المادية (أولا)، و الوسائل الإجرامية (ثانيا).

الفرع الأول: الوسائل المادية: يمكن تلخيص الوسائل المادية فيما يلي:

أ- عناوينIP، البريد الإلكتروني، و برامج المحادثة [2]

في حالة وجود أي مشكلة أو أية أعمال تخريبية فإن أول ما يجب أن يقوم به المحقق هو البحث عن رقم الجهاز و تحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال غير القانونية و يمكن لمزود خدمة الانترنت أن يراقب المشترك، كما يمكن للشبكة التي تقدم خدمة الاتصال الهاتفي أن تراقبه أيضا إذا ما توفرت لديها أجهزة و برامج خاصة بذلك

[1] نفس المرجع السابق، ص70.
[2] رزيقة بونار،" الجريمة المعلوماتية في التشريع الجنائي الجزائري"، مذكرة مكملة لنيل شهادة الماستر في القانون العام،كلية الحقوق والعلوم السياسية،جامعة محمد الصديق بن يحي، جيجل، 2020-2021 ،ص ص 61-62.

ب- البروكسي (**PROXY**) حيث يعمل البروكسي كوسيط بين الشبكة و مستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة، و ضمان الأمن و توفير خدمات الذاكرة الجاهزة (**Cash Memory**).[1]

ت- برامج التتبع و تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تم اختراق جهازه، و يحتوي هذا البيان على اسم الحدث و تاريخ حدوثه و عنوان (**IP**) الذي تمت من خلاله عملية الاختراق، و اسم الشركة المزودة لخدمة الانترنت المستضيفة للمخترق، و أرقام مداخلها و مخارجها على شبكة الأنترنت و معلومات أخرى، و من الأمثلة على هذه البرامج برنامج(**2 hack tracer**).[2]

ث- نظام كشف الاختراق (**intrusion détection system**) و يرمز له اختصارا بالأحرف (**IDS**) وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسبة الإلكترونية أو الشبكة ،و يتم ذلك من خلال تحليل رموز البيانات أثناء انتقالها عبر الشبكة و مراقبة بعض ملفات نظام التشغيل الخاص تسجيل الأحداث فور وقوعها في جهاز الحاسبة الإلكترونية.

الفرع الثاني: الوسائل الإجرائية

و يقصد بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة و المحددة والمتغيرة، و الغير محددة التي تثبت وقوع الجريمة و تحدد شخصية مرتكبها و منها:

[1] نفس المرجع السابق، ص 62.
[2] نفس المرجع السابق، ص 63.

أ – اقتفاء الأثر من أخطر ما يخشاه مجرم نظم المعلومات تقصي أثره أثناء ارتكابه للجريمة و يمكن تقصي الأثر بطرق عدة سواء عن طريق بريد إلكتروني تم استقباله أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق.

ب - الإطلاع على عمليات النظام المعلوماتي و أسلوب حمايته فينبغي على المحقق و هو بصدد التحقيق في إحدى الجرائم الماسة بالمعطيات الرقمية، أن يطلع على النظام المعلوماتي و مكوناته من شبكات و تطبيقات و خدمات تقدم للعملاء، كما ينبغي الإطلاع على عمليات النظام المعلوماتي، كقاعدة البيانات و إدارتها و خطة تأمينها و معرفة مواد النظام.

ت – الاستعانة بالذكاء الاصطناعي في حصر الحقائق و الاحتمالات والأسباب و الفرضيات من خلال استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسبة الإلكترونية، وفق برامج صممت خصيصا لهذا الغرض.

ث – مراقبة الاتصالات الإلكترونية، و يقصد بها: مراقبة شبكة الإتصالات، و هي وسيلة من وسائل جمع البيانات و المعلومات عن المشتبه فيه، يقوم بها مراقب إلكتروني، يتمثل في مأمور ضبط قضائي ذي كفاءة تقنية عالية تتماشى مع نوع الجريمة التي يتعامل معها، مستخدما في ذلك التقنية الإلكترونية و عبر شبكة الانترنت.[1]

[1] نفس المرجع السابق، ص64

المطلب الثالث: التحقيق في الجريمة الإلكترونية

تعتبر مرحلة جمع المعلومات والمعطيات من أهم مراحل الدعوى الجنائية التي تسبق المحاكمة، فمن خلالها يتم التعرف على من ارتكب الفعل وهذا ما يعرف بالتحقيق.[1]

فالتحقيق هو مجموعة من الإجراءات التي تستهدف التنقيب و الكشف عن الأدلة في شأن الجريمة التي ارتكبت ثم مدى كفايتها لإحالة المتهم للمحاكمة، يقوم به المحقق وهو شخص عهد إليه القانون سلطة اتخاذ كافة الإجراءات القانونية و الوسائل المشروعة فيما يصل إلى علمه من جرائم بهدف الكشف عنها وضبط فاعلها وتقديمه للمحاكمة، وقد عبر عنه المشرع الجزائري بقاضي التحقيق واعطى تعريفه في المادة 68 من قانون الإجراءات الجزائية.[2]

الفرع الأول: الأعوان المكلفون بالتحري وجمع الأدلة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

نظرا لخصوصية الجريمة الإلكترونية كان محتما توفير كوادر، وأجهزة متخصصة تعنى بعملية البحث والتحري عن الجريمة الإلكترونية، وكان ذلك إما على مستوى جهاز الشرطة أو الدرك الوطني، بالنسبة لجهاز الشرطة فقد أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة ومخبرين جهويين بكل من قسنطينة ووهران، تحتوي على فروع تقنية من بينها خلية الإعلام الآلي، بالإضافة إلى فرق متخصصة مهمتها التحقيق في الجريمة الإلكترونية تعمل بالتنسيق مع هذه المخابر توجد على مستوى مراكز

[1] فلاح عبد القادر و أيت عبد المالك نادية،" التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، جامعة الجيلالي بونعامة خميس مليانة،2009، ص1694..

[2] نفس المرجع السابق، ص ص 1694-1695.

الأمن الولائي، أما على مستوى الدرك الوطني فإنه يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني، قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، بالإضافة إلى مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومي للدرك الوطني.[1]

الفرع الثاني: إجراءات التحقيق العادية في الجرائم المعلوماتية

تتم هذه الإجراءات وفقا ل:

أولا: التفتيش كإجراء تحقيق مألوف في الجرائم المعلوماتية

يعتبر التفتيش إجراء من إجراءات البحث والتحقيق ويهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها بمكان يتمتع بالحرمة أو تفتيش شخص، وان لإجراء التفتيش أهمية بالغة وخطورة معتبرة على الحياة الخاصة، ولهذا نص عليه المشرع الجزائري بمقتضى قواعد دستورية، حيث تضمن الدولة عدم انتهاك حرمة منزل، فلا تفتيش إلا بمقتضى القانون[2] وفي إطار احترامه فلا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة

وإذا كان التفتيش يقصد به البحث عن جسم الجريمة والأداة التي استخدمت في ارتكابها وكل ما له علاقة بها أو بفاعلها، فإن عالم التقنية قد يتميز عن الجرائم العادية بكونه يتكون من شقين

هما الكيانات المادية والتي تنطبق عليها القواعد العامة للتفتيش من حيث مكان واجدها بحسب ما إذا كان مكان عام أو خاص كمسكن المتهم مثلا، أما إذا تعلق الأمر بتفتيش الكيانات

[1] نايري عائشة، مرجع سابق، ص41

[2] ابتسام بغو،مرجع سابق، ص 13.

المعنوية كالبرامج ونظم التشغيل وقواعد البيانات وبعيدا عن الآراء الفقهية التي قيلت حولها فقد نص المشرع الجزائري في المادة 47 الفقرة الرابعة من قانون الإجراءات الجزائية بإمكانية التفتيش والضبط على المكونات المعنوية للحاسوب، بنصه على أنه:" إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك.[1]

ثانيا: المعاينة كضابط التحقيق في الجريمة المعلوماتية

يقصد بالمعاينة "إثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة "، أو هي " رؤية بالعين لمكان أو شخص أو لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة[2]، وعليه تعتبر المعاينة عملية التوجه إلى مكان وقوع الجريمة والمحافظة عليه من أجل البحث و أخذ عينة من الآثار التي تركها المجرم.

عند العلم بوقوع الجريمة فإن أول خطوة يقوم بها مأمور الضبط القضائي هو الانتقال إلى مسرح الجريمة، لأن هذا الأخير حجز الزاوية في التحقيق الجنائي ومكمن الآثار والأدلة المادية ، وينبغي التعامل في الإطار مع مسرح الجريمة الالكترونية على أنه مسرحان هما:

[1] سعيدة بوزنون، مرجع سابق،ص 52.
[2] يزيد بوحليط، مرجع سابق، ص321.

المسرح تقليدي : يقع خارج البيئة الإلكترونية لأنه يتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة ، وهو أقرب إلى مسرح الجريمة التقليدية ويترك فيها الجاني عدة أثار كالبصمات وبعض متعلقاته الشخصية أو وسائط تخزين رقمية.[1]

المسرح افتراضي : يقع داخل البيئة الالكترونية ، لأنه يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الأنترنت في ذاكرة الأقراص الصلبة الموجودة بداخله.

ثالثا: الخبرة الفنية من متطلبات التحقيق في الجريمة المعلوماتية

لابد أن يكون الخبير صاحب مقدرة وإمكانيات علمية وفنية في مسألة موضوع الخبرة ويستطيع القيام بدوره والقيام بهذا الأخير عليه أن يبين المكان المحتمل لأدلة الإثبات وشكلها وهيئته والآثار الاقتصادية والمالية دون إتلاف الأدلة أو الأجهزة أو تدميرها.[2]

ويتعين على الخبير في الجرائم المرتكبة عبر الانترنت التنسيق مع المحقق الجنائي في هذه الجريمة، بما في ذلك حصر الأدلة المتوفرة وترتيبها وفقا لأهمية كل دليل أو بيئة أو قرينة، كما يجب على المحقق الجنائي أن يشرح للخبراء العملية بعناصر و أركان الجريمة المقام عنها الدعوى الجنائية ضد المتهم.[3]

[1] بعرة سعيدة، مرجع سابق،ص 76.
[2] مرابطن حياة، مرجع سابق، ص43.
[3] رابح وهيبة ، المرجع السابق، ص329.

الفرع الثالث: إجراءات التحقيق المستحدثة في الجرائم الإلكترونية

يعتبر التسرب أسلوبا حديثا للكشف عن الجرائم وف البيئة الرقمية يمكن أن يكون التسرب رقميا

أولا: التسرب الرقمي

1-تعريفه:

يمكن تصور عملية التسرب في نطاق الجرائم المعلوماتية في دخول ضابط شرطة قضائية أو عون الشرطة القضائية إلى العالم الافتراضي (شبكة الانترنت) وذلك بتسجيله على مواقع معينة (كواقع التواصل الاجتماعي)، أو اشتراكه في محادثات عبر غرف الدردشة أو حلقات الاتصال المباشر لرفع ومعاينة الجرائم أو ربط الاتصال مع المشتبه فيهم و الظهور بمظهر كما لو كان فاعلا مثلهم، مستخدما في ذلك أسماء أو صفات مستعارة ووهمية سعيا منها للتعرف عليهم وتحديد أماكنهم. [1]

2-جهات مراقبته:

أوكل المشرع مهمة منح الإذن بالتسرب إلى وكيل الجمهورية وقاضي التحقيق دون سواهما , وهذا ما جاء صراحة في المادة 65 مكرر11 من القانون 06-22 المعدل والمتمم . لذلك فإن وكيل الجمهورية أوكل له قانون الإجراءات الجزائية بموجب المادة 12 منه كافة الصلاحيات لاتخاذ الإجراءات اللازمة للبحث والتحري عن الجرائم بصفة عامة قبل إحالتها على التحقيق[2]،

[1] فايد فاطيمة، مرجع سابق، ص56.
[2] نفس المرجع السابق، ص.56

وبهذه الصفة يحق له منح الإذن بنفس الشروط إلى ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب، إذا تطلبت ضروريات التحقيق و التحري في الجرائم المحددة قانونا بنص المادة 65مكرر5 السابق ذكرها، وخول له كذلك سلطة اتخاذ هذا الإجراء في حالة التلبس في أي جريمة من الجرائم المحددة قانونا على سبيل الحصر و أما قاضي التحقيق فأنه يمارس صلاحياته بعد إخطاره من قبل وكيل الجمهورية بموجب طلب افتتاحي وفقا لنص المادة 67 من نفس القانون لإجراء التحقيق، لتصبح له الولاية الكاملة في اتخاذ ما يجب قانونا من الإجراءات التي تستوجبها ضروريات البحث والتحري عن الجريمة الالكترونية بغية الكشف عن الحقيقة.[1]

ثانيا: اعتراض المراسلات والمراقبة الالكترونية للتحقيق في الجريمة الالكترونية

إن الجزائر وعلى غرار التشريعات المقارنة قد تبنت ما جاء في مضمون الاتفاقية المتعلقة بمكافحة الجريمة المنظمة عبر الحدود الوطنية لاسيما المادة 20 منها، إذ نص المشرع الجزائري على مصطلح المراقبة في قانون الإجراءات الجزائية بعد تعديله سنة 2006 ليكرس مفهوم المراقبة الاستدلالية في نص المادة 16 مكرر.[2]

وكذا في نص المواد من 65 مكرر إلى 65 مكرر 10 من قانون الإجراءات الجزائية الجزائري والتي جاءت تحت تسمية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

[1] نفس المرجع السابق، ص ص 56-57.
[2] جومي الأمير،" الخصوصية الإجرائية للتحقيق في الجريمة المعلوماتية"، مذكرة مقدمة لاستكمال متطلبات الحصول على شهادة الماستر في العلوم القانونية تخصص القانون الجنائي والعلوم الجنائية،كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج،2020-2021، ص74.

لم ينص المشرع الجزائري في قانون الإجراءات الجزائية على تعريف محدد لأسلوب اعتراض المراسلات واكتفى بوضع النصوص المنظمة له في المواد 65 مكرر5 إلى 65 مكرر10 من ذات القانون[1]، لكن يمكن تعريفه حسب ما عرفته بقية التشريعات المقارنة والتي عرفت الاعتراض يعني الاستيلاء بهذه على محتويات المراسلات والرسائل المنقولة عبر وسائل الاتصال السلكية واللاسلكية هذه الأخيرة التي تعتبر وسيلة تقيد في استقبال أو إرسال الإشارات أو كتابة أو صورة أو صوت أو معلومة من أي نوع كانت عبر الأسلاك أو الألياف البصرية أو الكهرباء لا سلكية أو بمختلف الأنظمة الكهرومغناطيسية أو الأقمار الصناعية.

ثالثا: الحفظ والإفشاء العاجلان للمعطيات الالكترونية

يعد الحفظ والإفشاء العاجلان للمعطيات من الإجراءات المستحدثة التي فرضت على مزودي خدمة الإنترنت على غرار باقي التشريعات لمتابعة الجريمة الإلكترونية ومعاقبة مرتكبيها حيث تضمن القانون رقم 09-04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها في نص المادة 10 على عدد من الالتزامات المفروضة على مقدمي خدمة الإنترنت فيما يتعلق بالعمليات التي تنجزها السلطات بالبحث والاستدلال لأغراض التحقيق ومن بينها حفظ المعطيات المعلوماتية بالسير ووضعها تحت تصرفهم.[2]

[1] نفس المرجع السابق، ص74.
[2] نفس المرجع، ص83.

خاتمـــــــة

خاتمة:

من خلال ما سبق دراسته يمكن القول أن الجريمة الإلكترونية هي جريمة حديثة النشأة تطورت بشكل كبير بسبب توفر وسهولة اقتناء الوسائل التي تؤدي إليها، من هواتف ذكية ولوحات رقمية وحواسب آلية، حاول المشرع الجزائري القضاء عليها من خلال سن القوانين واستحداث إجراءات جديدة لمتابعة مرتكبيها، إلا أن الجريمة المعلوماتية لازالت في تزايد كما نسمع ونرى في الواقع، لم تعد تقتصر الجريمة الإلكترونية على سلوك واحد بل تعددت أنواعها فهي سب إلكتروني وسرقة إلكترونية وقذف إلكتروني ...إلخ.

ومن خلال دراسة موضوع الجريمة الإلكترونية في التشريع الجزائري يمكن استخلاص النتائج الآتية:

- القضاء على الجريمة الإلكترونية لا يكمن إلا بإتحاد تشريع ناجع من طرف العديد من الدول من خلال دراسة الظاهرة الإجرامية من كل جوانبها وتحديد الإجراءات التي تحد منها.
- المشرع الجزائري يغفل عن بعض الجرائم المعلوماتية من خلال عدم التطرق إليها وتجريمها مثل التزوير المعلوماتي حيث لم نسمع عليه في التشريع الجزائري.
- الجريمة الإلكترونية ظاهرة إجرامية تتطور مع التطور التكنولوجي.
- آليات المشرع الجزائري للحد من الجريمة الإلكترونية وإن قللت منها فإنها لم تضع لها حدا مثلها مثل باقي الدول.

أما التوصيات التي يمكن طرحها:

- على المشرع الجزائري دراسة ظاهرة الجريمة الالكترونية جيدا ومحاولة فهم المجرم المعلوماتي .

- على الدول أن تتكاتف وتتعاون في سبيل القضاء عليها ووضع قانون يحدد الاختصاص الإقليمي للفصل في قضاياها (تنازع الاختصاص) بحكم أن الجريمة المعلوماتية جريمة عابرة للحدود.
- على الدول المتقدمة والتي تصنع الوسائل التي ترتكب بها الجريمة المعلوماتية أن تضع ميزة تمكن من تحديد المجرم المعلوماتي.
- على المشرع الجزائري أن يتماشى في سن القوانين في مجال الجريمة الإلكترونية مع العصر الحديث دارسا في ذلك دوافع المجرم المعلوماتي.

الفهرس

الفهرس

مقدمــة	أ
الفصل الأول :ماهية الجريمة الإلكترونية	01
المبحث الأول : مفهوم الجريمة الإلكترونية	02
المطلب الأول :تعريف الجريمة الإلكترونية وطبيعتها القانونية	02
الفرع الأول :تعريف الجريمة الإلكترونية والمصطلحات المتعلقة بها	02
الفرع الثاني :الطبيعة القانونية للجريمة الإلكترونية	09
المطلب الثاني :أركان الجريمة الإلكترونية ودوافع ارتكابها	11
الفرع الأول : :أركان الجريمة الإلكترونية	11
الفرع الثاني :دوافع ارتكاب الجريمة الإلكترونية	15
المبحث الثاني :أنواع الجريمة الإلكترونية وخصائصها	18
المطلب الأول :أنواع الجريمة الإلكترونية	18
الفرع الأول :الجريمة الإلكترونية المرتكبة باستخدام النظام المعلوماتي	32
الفرع الثاني :الجريمة الإلكترونية المرتكبة على النظام المعلوماتي	21
المطلب الثاني :خصائص الجريمة الإلكترونية	24
الفرع الأول :صعوبة اكتشاف جرائم المعلوماتية واثباتها	24
الفرع الثاني :جرائم عابرة للحدود	24
الفرع الثالث: جريمة ناعمة	25
الفرع الرابع: جريمة مستحدثة	26
الفرع الخامس: امتناع المجني عنهم عن التبليغ	26
الفصل الثاني: الآليات القانونية لمكافحة الجريمة الالكترونية في التشريع الجزائري	29

المبحث الأول: القواعد الموضوعية المنظمة للجريمة الالكترونية	29
المطلب الأول: مكافحة الجريمة بموجب قانون العقوبات ونصوص الملكية الفكرية	30
الفرع الأول: بموجب قانون العقوبات	30
الفرع الثاني: بموجب قانون الملكية الفكرية الجزائري	38
المطلب الثاني: مكافحة الجريمة بموجب القانون 04/09 والقانون03/2000	43
الفرع الأول: بموجب القانون 04/09الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال	43
الفرع الثاني: بموجب قانون رقم 2000-03المؤرخ في 05غشت سنة ،2000 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية	47
المطلب الثالث: بموجب القانون 12-05 والقانون 08-01	48
الفرع الأول: القانون العضوي رقم 12-05مؤرخ في 12يناير سنة ، 2012يتعلق بالإعلام	48
الفرع الثاني: القانون العضوي رقم 08-01مؤرخ في 23يناير سنة ،2008	49
المبحث الثاني: الحماية الإجرائية للنظام المعلوماتي	51
المطلب الاول: الإجراءات التقليدية لجمع الدليل الإلكتروني	51
الفرع الأول: تلقي الشكاوى والبلاغات	51
الفرع الثاني: الاستجواب وسماع الشهود في الجريمة الإلكترونية	53
المطلب الثاني: الإجراءات المستحدثة في التحري وجمع الأدلة	55
الفرع الأول: الوسائل المادية	55
الفرع الثاني: الوسائل الإجرائية	56

المطلب الثالث: :التحقيق في الجريمة الإلكترونية	58
الفرع الأول: الأعوان المكلفون بالتحري وجمع الأدلة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات	58
الفرع الثاني: إجراءات التحقيق العادية في الجرائم المعلوماتية	59
الفرع الثالث: إجراءات التحقيق المستحدثة في الجرائم الإلكترونية	62
خاتـــمـــــة	65

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

أولا: النصوص القانونية

1- الأمر رقم 66-155 المؤرخ في 08 يونيو سنة 1966 المتضمن قانون الإجراءات الجزائية حسب آخر تعديل له الأمر رقم 21-11 المؤرخ في 25 غشت 2021 (ج.ر رقم:65 المؤرخة في 26 غشت 2021).

2- القانون رقم 20-06 مؤرخ في 28 أبريل سنة 2020 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

ثانيا: الكتب

1- امحمد اقبلي وعابد العمراني الميلودي،" القانون الجنائي الخاص المعمق"، ط.1،مكتبة الرشاد سطات للنشر والتوزيع، ،د.ب.ن، ،2020.

2- أسامة أحمد المناعسة وجلال محمد الزعبي،"جرائم تقنية نظم المعلومات الإلكترونية"، ط.1،دار الثقافة للنشر والتوزيع،عمان(الاردن)، ،2010.

3- الشحات إبراهيم محمد منصور،"الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية"، ط .، 1دارالفكر الجامعي، ،الاسكندرية،،2011

4- يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة، الأسكندرية 2019.

5- يعيش تمام شوقي،" الجريمة المعلواتية " دراسة تأصيلية مقارنة، ط ،1سلسلة مطبوعات المخبر، جامعة بسكرة، جانفي 2019

6- محمد حماد مرهج الهيتي،" جرائم الحاسوب"، ط .،1دار المناهج للنشر والتوزيع، ،عمان (الاردن)،2006.

7- محمد عبد الله أبوبكر،"موسوعة جرائم المعلوماتية"،المكتب العربي الحديث،الاسكندرية ، 2007.

8- عبد الحكيم رشيد توبة،" جرائم تكنولوجيا المعلومات"، ط ،1دار المستقبل للنشر والتوزيع، عمان(الأردن)،2009.

9- علي جعفر،" جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة"، ط.1 منشورات زين الحقوقية، ،دون بلد نشر،2013.

10- شيماء عبد الغني محمد عطاالله،" الحماية الجنائية للتعاملات الإلكترونية"، دار الجامعة الجديدة ،الإسكندرية،2007.

11- خالد عياد الحلبي،" إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت"، ط.1،دار الثقافة للنشر والتوزيع، 2011.

12- خالد ممدوح إبراهيم،"أمن الجريمة الإلكترونية"،الدار الجامعية للنشر،الإسكندرية،2008.

ثالثا: الرسائل العلمية

1-ابتسام بغو،" إجراءات المتابعة الجزائية في الجريمة المعلوماتية"، مذكرة مكملة لنيل شهادة ماستر في القانون تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي أم البواقي، ،2015-2016.

2- بعرة سعيدة،"الجريمة الإلكترونية في التشريع الجزائري"،مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي،جامعة محمد خيضر بسكرة، كلية الحقوق والعلوم السياسية، 2016/2015.

3-بخي فاطمة الزهراء،" إجراءات التحقيق في الجريمة الإلكترونية"، مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، 2013-2014.

4-رزيقة بونار،" الجريمة المعلوماتية في التشريع الجنائي الجزائري"، مذكرة مكملة لنيل شهادة الماستر في القانون العام،كلية الحقوق والعلوم السياسية،جامعة محمد الصديق بن يحي، جيجل، 2020-2021.

5-يوسف جفال،"التحقيق في الجريمة الإلكترونية"،مذكرة مقدمة لنيل شهادة الماستر أكاديمي،تخصص قانون جنائي،جامعة محمد بوضياف المسيلة،كلية الحقوق و والعلوم السياسية،2017/2016.

6-طرشي نورة ،"مكافحة الجريمة المعلوماتية"، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي"، كلية الحقوق، جامعة الجزائر1 ،2012/2011

7-محمد بوعمرة وسيد علي بنينال،" جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري"، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية، تخصص قانون أعمال، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، البويرة، ،2019-2020.

8- مرابطن حياة،" الجريمة الإلكترونية في التشريع الجزائري"، مذكرة نهاية الدراسة لنيل شهادة الماستر،كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس،مستغانم، ،2018-2019.

9- نايري عائشة،" الجريمة الإلكترونية في التشريع الجزائري"،مذكرة لنيل شهادة الماستر في القانون الإداري،جامعة أحمد دراية،كلية الحقوق والعلوم السياسية،أدرار، 2017-2016.

10- عبد الله دغش الجمعي،" المشكلات العملية والقانونية للجرائم الالكترونية دراسة مقارنة"،رسالة مكملة للحصول على شهادة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014.

11- صغير يوسف،" الجريمة المرتكبة عبر الإنترنت"، مذكرة لنيل شهادة الماجستير في القانون تخصص القانون الدولي للأعمال،كلية الحقوق والعلوم السياسية، جامعة مولود معمري(تيزي وزو).

12- جومي الأمير،" الخصوصية الإجرائية للتحقيق في الجريمة المعلوماتية"، مذكرة مقدمة لاستكمال متطلبات الحصول على شهادة الماستر في العلوم القانونية تخصص القانون الجنائي والعلوم الجنائية،كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج، 2020-2021.

ثالثا: المقالات

1- بوضياف اسمهان،" الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"،مجلة الأستاذ الباحث للدراسات القانونية والسياسية،جامعة محمد بوضياف،العدد الحادي عشر2018.

2-براهيمي جمال،"مكافحة الجرائم الالكترونية في التشريع الجزائري"،المجلة النقدية، كلية الحقوق ،جامعة مولود معمري،تيزي وزو.

3-دمان ذبيح عماد، بهلول سمية،" الآليات العقابية لمكافحة الجريمة الالكترونية في الجزائر"، مجلة الحقوق والعلوم السياسية، العدد13 ،جانفي، جامعة عباس لغرور خنشلة،2020.

4-حنان مسكين،" واقع مكافحة الجرائم المعلوماتية واتجاهاتها التشريعية في الجزائر"، المجلة الأكاديمية للبحوث القانونية والسياسية،المجلد الرابع، العدد الأول،جامعة الدكتور مولاي الطاهر، سعيدة،2020.

5-محمد الصغير مسيكة،: مفهوم الجرائم المستحدثة وطبيعتها القانونية(الجرائم الإكترونية)،مجلة الدراسات القانونية والسياسية، العدد،01جامعة أحمد بن يحي الونشريسي، تيسمسيلت،تاريخ النشر2022.

6- ناجية شيخ،" حول مكافحة الجريمة الإلكترونية في التشريع الجزائري"، مجلة العلوم القانونية والسياسية، المجلد9 ،العدد 2،جامعة مولود معمري،تيزي وزو،2018.

7-سليمة ذياب وبلال بوترعة،" الجريمة الإلكترونية: الأسس والمفاهيم" مجلو تطوير العلوم الإجتماعية، المجلد ،13العدد ،01جامعة زيان عاشور،الجلفة.

8- سعيدة بوزنون،" مكافحة الجريمة الالكترونية في التاشريع الجزائري"، مجلة العلوم الانسانية،عدد ،52المجلد ب، جامعة الإخوة منتوري، كلية الحقوق ،قسنطينة، 2019.

9-عبد الحكيم مولاي ابراهيم،" الجرائم الإلكترونية"، مجلة الحقوق والعلوم الإنسانية، المجلد الثاني ،العدد ،23جامعة زيان عاشورالجلفة، 2015.

10- فاروق خلف،" الآليات القانونية لمكافحة الجريمة المعلوماتية"، مجلة الحقوق والحريات،العدد الثاني ،كلية الحقوق جامعة حمة لخضر،الوادي،2015.

11- فلاح عبد القادر و أيت عبد المالك نادية،" التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04،العدد 02،جامعة الجيلالي بونعامة خميس مليانة، 2009.

12- رائد مروان محمود عاشور،" المحددات النظرية والقانونية للجريمة المعلوماتية الماسة بالأطفال"،مجلة تحولات،المجلد الثالث،العدد الثاني ديسمبر،كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة.2020 .

13- شرف الدين وردة، بلجراف سامية،" الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري"، مجلة المنار للبحوث والدراسات القانونية والسياسية ،العدد الثالث ،كلية الحقوق والعلوم السياسية ،جامعة يحي فارس المدية، ديسمبر 2017.

14- خضري حمزة وعشاش حمزة،"خصوصية اركان الجريمة المعلوماتية في التشريع الجزائري،مجلة الدراسات القانونية،المجلد ،06العدد ،02 جامعة محمد بوضياف المسيلة،جوان 2020.

رابعا: الملتقيات

1- فشار عطاء الله،" مواجهة الجريمة المعلوماتية في التشريع الجزائري"، بحث مقدم إلى الملتقى المغاربى حول القانون والمعلوماتية المزمع عقده بأكاديمية الدراسات العليا بليبيا، جامعة زيان عاشور بالجلفة كلية الخقوق والعلوم السياسية، 2009.

خامسا: المحاضرات

1-عبد الرحمان خلفي،" محاضرات في القانون الجنائي العام" محاضرات موجهة لطلبة السنة الثانية ل م د قسم التعليم القاعدي"،كلية الحقوق والعلوم السياسية، جامعة ميرة عبد االرحمان، 2016-2017.

الملخص:

مع التطور التكنولوجي الحديث واعتماد التعاملات الاجتماعية، التجارية و السياسية الشبكة المعلوماتية ، انتشرت الجريمة الإلكترونية بشكل كبير وأصبحت واقعا مفزعا يهدد العالم بأسره، فالمجرم الإلكتروني يمتاز بالمهارة والذكاء والسرعة في تنفيذ الجريمة ،ومع صعوبة اكتشافها وتحديد البيئة الرقمية التي تنفذ فيها الجريمة ، أضحت كافة الدول عامة والجزائر خاصة في حيرة من هاته الجريمة وكيفية سن قوانين تحد منها أو تقلل منها.

Abstract:

With the development of modern technology and the adoption of social and commercial transactions and politics on the, internet electronic crime has spread widely, it has become a terrible reality that threatens the whole world, the cybercriminal is characterized by skill intelligence and speed in executing the crime, and with the difficulty of discovering it and determining the digital environment in with it is implemented.