وزارة التعليـم العالــي والبحـث العلمي
المركز الجامعي عبد الحفيظ بوالصوف –ميلة
معهدالحقوق

القسم: قانون عام الرقم التسلسلي:.....

الشعبة: الحقوق الرمـــــــــز:.....

التخصص:قانون جنائي

الجريمة الالكترونية و آليات مكافحتها في التشريع الجزائري

مذكرة ضمن متطلبات نيل شهادة ماستر

إعداد الطالبتين:
بن قويدر أمل
بوصبع عفاف

إشراف الأستاذ:
الــدكتور بوصبع فؤاد

أعضاء لجنة المناقشة

د.مجادي نعيمة	الرتبة: أستاذة محاضرة أ	صفته في اللجنة: رئيسا
د. بوصبع فؤاد	الرتبة: أستاذ محاضر أ	صفته في اللجنة: مشرفا ومقررا
د. حمدوني علي	الرتبة: أستاذ محاضر ب	صفته في اللجنة: عضوا مناقشا

السنة الجامعية: 2025/2024


بسم الله الرحمن الرحيم

الشكر و التقدير

بسم الله الرحمن الرحيم، والحمد لله الذي وفقنا لإتمام هذه المذكرة، فله الحمد حتى يرضى، وله الحمد بعد الرضا، والصلاة والسلام على سيدنا محمد وعلى آله وصحبه أجمعين.

في حضرة الكلمات، كثيراً ما تعجز اللغة عن حمل ما يفيض به القلب، لكن الامتنان الحقيقي لا يُخفى، وإن لاذ بالصمت.

حين وضعت أول خطوة في هذه الرحلة، لم نكن ندرك أن الطريق لا يعلّمنا فقط ما نبحث عنه، بل يكشف لنا أيضاً من نحن، ومن يستحق أن يُخلَّد في ذاكرتنا. لذلك، لا يليق أن أضع نقطة النهاية دون أن أُدوِّن شكري، على طريقتي.

إلى عائلتينا، من كانت دعواتهم تصل قبل كلماتهم، ومن حملونا على أكتافهم دون أن يشعروا بالثقل، أنتم الجذور التي أنبتت هذا الثمر.

إلى أستاذنا المشرف و أساتذتنا الأفاضل، من غرسوا فينا بذور الفكر، وسقوها بصبر، وسهر، وإيمان بأن الكلمة قادرة على أن تصنع فرقاً... شكراً لأنكم كنتم النور الذي لا يُطفأ، والنبض العلمي الذي لا يخبو

الإهداء

"أود أن أتوجه بجزيل الشكر والعرفان إلى عائلتي الكريمة، التي كانت دائمًا مصدر دعمي وإلهامي في كل خطوة من خطوات حياتي. شكراً لأمي وأبي على محبتهم اللامحدودة، ولإخوتي الأعزاء على تشجيعهم ووقوفهم بجانبي في الأوقات الصعبة.

كما أخص بالشكر والتقدير صديقتي الغالية، التي كانت شريكتي في إعداد هذه المذكرة، والتي ساعدتني وساندتني بكل جهدٍ وحب. كان لوجودكِ بجانبي دور كبير في إتمام هذا العمل على أكمل وجه، وأنتِ دائمًا مصدر إلهامي ودعمي.

وأتوجه أيضًا بخالص الشكر والتقدير إلى أستاذي المشرف على هذا العمل، الذي قدم لي الإرشاد والنصيحة القيمة طوال فترة إعداد المذكرة. شكرًا لإيمانك بي ومساعدتك المستمرة. "

" عفاف.. "

الإهداء

إلى من كانت الحياة بجوارهم أكثر احتمالاً، وأكثر دفئا...

إلى والديّ، من كان حضنهما ملاذاً، وكلماتهما دعماً، ونظرتهما فخراً

يا من حملتموني بدعائكم، وبذلتم من أجلي دون انتظار مقابل...

إن كان لهذا الإنجاز معنى، فأنتم معناه

وإلى رفيقتي في المذكرة، من لم تكن فقط شريكة في العمل، بل كانت رفيقة في كل تفاصيل الرحلة... هذا العمل يحمل بصمتك كما يحمل بصمتي

إلى كل من مرّ في طريقي، وترك أثراً جميلاً، أو درساً مفيداً...

وإلى نفسي، التي صبرت، وكافحت، وآمنت أن كل تعب له وقتٌ للحصاد.

إليكم جميعاً، أُهدي ثمرة هذا العمل المتواضع، عربون حب وامتنان لا يُقدّر بثمن..

" أمل.."

مقدمة

مقدمة:

شهد العالم مؤخرا تطورا كبيرا في مجال تكنولوجيا المعلومات والاتصالات، حيث أصبحت مختلف وسائط ووسائل الاتصال جزء ضروري في حياة الفرد والمجتمع، لما توفره من خدمات سريعة، تبادل المعلومات، تواصل وغيرها، فقد ساهم هذا التطور في تسهيل الكثير من المجالات كالتجارة، الإدارة، التعليم، والخدمات الصحية، وبالرغم من إيجابياته المتعددة إلا أنه أدى إلى ظهور أنماط جديدة من الجرائم وعلى رأسها ما يعرف بالجرائم الالكترونية فهي تشكل تهديدا كبيرا للأفراد والمجتمعات والدول.

كما تتميز الجرائم الالكترونية بصعوبة متابعتها حيث إنها في الغالب لا تترك أثرا، فليست هنالك أموال أو ممتلكات مفقودة،وإنما هي أرقام تتغير في السجلات،ومعظم الجرائم الالكترونية ربما يتم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، كما أن الجرائم الالكترونية تتميز بالدقة والتعقيد التقني، وغالبا من يرتكب تلك الجرائم يتمتع بالذكاء، ومكافحة هذه الجرائم تتطلب جهود خاصة تتعدى الوسائل التقليدية المتعارف عليها في مكافحة الجريمة. كما سعى المشرع الجزائري الى إيجاد إطار قانوني وتنظيمي يمكنه من مواجهة هذه الظاهرة الحديثة، سواء من خلال تعديل النصوص القانونية أهمها ما ورد في قانون العقوبات، وكذا القوانين الخاصة كقانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال لسنة 2023، أو من خلال استحداث أجهزة متخصصة.

تظهر أهمية هذا البحث من خلال رفع مستوى الثقافة القانونية لدى المجتمع الجزائري حول سبل الوقاية من الجريمة الإلكترونية وكيفية الإبلاغ عنها ويسعى هذا البحث على تسليط الضوء على هذه الجريمة كظاهرة حديثة وتأثيرها على الأمن في الجزائر وتسليط الضوء على مرتكب هذه الجريمة ويسهم هذا الموضوع في فهم الجريمة الإلكترونية وتطوراتها في العصر الرقمي وتقديم رؤية للحد من آثار هذه الظاهرة ويعد من المواضيع الحديثة و المعقدة و الخطيرة التي جاء بها التطور التكنولوجي السريع مما أدى إلى كثرة التعرض للابتزاز الرقمي و الاختراق و التجسس و إلحاق الضرر بالناس.

تم اختيار موضوع الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري بناء على رغبة شخصية من الباحثين ونظرا للأهمية الكبيرة لهذه الظاهرة في هذا العصر الرقمي وتأثيراتها السلبية التي باتت تشكل خطرا مباشرا على مستخدمين شبكة الاعلام والاتصال كذلك نقص الدراسات الأكاديمية في هذا الموضوع الذي تناول تحليل الجريمة الإلكترونية و سبل مكافحتها في التشريع الوطني الجزائري و مع تزايد هذه

الظاهرة و سرعة انتشارها بسبب التطور الحاصل و السريع في مجال التكنولوجيا من المهم دراستها و الوقوف على مدى قدرة التشريع الجزائري في التصدي لها و تسليط الضوء على كل جوانبها.

تهدف الدراسة إلى التعرف ودراسة العديد من النقاط و هي:

- التعرف على الجريمة الالكترونية.
- التعرف على أهداف ارتكاب الجريمة الالكترونية.
- دراسة أركان الجريمة الالكترونية في التشريع الجزائري.
- التعرف على الهيئات المختصة لمكافحة الجريمة الالكترونية.
- التعرف على إجراءات التحقيق للكشف عن الجريمة الالكترونية.

تركز هذه الدراسة القانونية العلمية على الجريمة الاليكترونية والمسؤولية الجنائية المرتبطة بها، وذلك من خلال تحليل التشريع الجزائري. ولتحقيق هذا الهدف، يتم استعراض مفهوم الجريمة الاليكترونية، أنواعها، الأركان التي تقوم عليها، بالإضافة إلى وسائل مكافحتها والصعوبات التي تواجه المكافحة.

يغطي البحث التطورات التشريعية والمؤسساتية في الجزائر حتى تاريخ فبراير 2025:

تم إجراء العديد من الدراسات حول الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، من أبرزها:

- دراسة بعنوان "**جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري:**" ركزت هذه الدراسة على الإطار القانوني والتنظيمي للأجهزة المكلفة بالتحقيق في هذا النوع من الجرائم، مع تحليل لكفاءة هذه الأجهزة وتحدياتها الميدانية.
- دراسة بعنوان "**إشكالية الجرائم الالكترونية في التشريع الجزائري:** "عالجت هذه الدراسة مسالة التكييف القانوني للجرائم الالكترونية في ظل القواعد التقليدية للقانون الجنائي، مبرزة الصعوبات المرتبطة بتحديد الأركان المادية والمعنوية لهذه الجرائم.
- دراسة بعنوان "**آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري:**" تطرقت هذه الدراسة إلى مختلف الآليات القانونية والمؤسساتية المعتمدة للوقاية من الجرائم الإلكترونية ومكافحتها، مع تقديم تقييم نقدي لمدى فعاليتها و ملائمتها للواقع التكنولوجي المتطور.

إلى أي مدى تصدى المشرع الجزائري للجريمة الإلكترونية وماهي آليات مكافحتها؟

1-ما هي الجريمة الإلكترونية؟

2-ما هي أنواع الجريمة الإلكترونية؟

3-ما هي إجراءات التحقيق في الجريمة الإلكترونية؟

4-هل للجريمة الإلكترونية أركان؟

5-هل يكفي الإطار القانوني الجزائري في مكافحة الجريمة الإلكترونية؟

6-هل يستطيع التشريع الجزائري الحد من الجريمة الإلكترونية؟

بالنسبة للمنهج المعتمد في هذه الدراسة فقد اخترنا المنهج الوصفي والذي يتطرق من جهة إلى وصف الجريمة الإلكترونية من خلال التعريف وذكر خصائصها وأركانها وأنواعها، بالإضافة إلى منهج تحليل المضمون الذي يتضمن التحليل من خلال دراسة الأساليب التي تستخدم في التحري عن هذه الجريمة ومدى مشروعيتها، وهذا ما يتم استخلاصه من تحليل النصوص القانونية ودراسة الجوانب الإجرائية الخاصة بها.

حتى نتمكن من معالجة الإشكالية المطروحة ارتأينا إلى تقسيم الخطة إلى فصلين معتمدين على تقسيم ثنائي للخطة، حيث سنتناول في الفصل الأول ماهية الجريمة الإلكترونية وقسمناه إلى مبحثين، تناولنا في المبحث الأول مفاهيم الجريمة الإلكترونية والمبحث الثاني عن أركانها ودوافع ارتكابها.

بينما تكلمنا في الفصل الثاني عن طرق وآليات مكافحة الجريمة الإلكترونية وقسمناه إلى مبحثين، تناولنا في المبحث الأول الأجهزة المختصة بالمكافحة أما المبحث الثاني إجراءات المتابعة في الجريمة الإلكترونية بين التحري والمحاكمة.

و خلصنا هذه الدراسة بخاتمة أجبنا فيها عن الإشكالية المطروحة ومجمل النتائج والتوصيات التي توصلنا إليها .

خطة البحث

الفصل الأول:ماهية الجريمة الالكترونية.

المبحث الأول: مفهوم الجريمة الالكترونية.

المطلب الأول: تعريف الجريمة الالكترونية وطبيعتها القانونية.

المطلب الثاني:خصائص الجريمة الالكترونية و أنواعها.

المبحث الثاني:أركان الجريمة الالكترونية ودوافع ارتكابها.

المطلب الأول:أركان الجريمة الالكترونية.

المطلب الثاني: دوافع الجريمة الالكترونية.

الفصل الثاني:طرق وآليات مكافحة الجريمة الالكترونية.

المبحث الأول: الأجهزة المختصة بالمكافحة.

المطلب الأول:الأجهزة الوطنية.

المطلب الثاني: الأجهزة الدولية.

المبحث الثاني:إجراءات المتابعة في الجريمة الالكترونية بين التحري والمحاكمة.

المطلب الأول:إجراءات التحقيق والتحري في الجريمة الالكترونية.

المطلب الثاني:إجراءات المحاكمة والصعوبات التي تواجه مكافحة الجريمة الالكترونية.

الفصل الأول

ماهية الجريمة الإلكترونية

تمهيد:

أسهم الانتشار الواسع و الاستعمال المكثف لوسائل التكنولوجيا الحديثة و شبكة الانترنت بين فئات متعددة من المجتمع في مختلف الميادين في ظهور نوع جديد من الجرائم لم يكن معروفا من قبل و هو ما يعرف بمسمى الجريمة الإلكترونية ولعل هذا الانتشار الواسع و التطور المستمر للانترنت ساعد على خلق بيئة سرية ملائمة للإجرام الإلكتروني بعيدا عن أعين الجهات الأمنية و سيتم في هذا الفصل التطرق إلى الإطار المفاهيمي للجريمة الإلكترونية من خلال مبحثين في المبحث الأول مفهوم الجريمة الإلكترونية و الثاني تم تخصيصه إلى أركان الجريمة الإلكترونية و أسباب انتشارها.

المبحث الأول:مفهوم الجريمة الإلكترونية

باتت التكنولوجيا في العصر الرقمي الحديث تلعب دورًا محوريا في مختلف جوانب الحياة ومع هذا الاعتماد المتزايد للانترنت نشأت تهديدات جديدة تمثلت في الجريمة الإلكترونية التي أخذت بدورها حيزا واسعا وكبيرا من الدراسات من أجل تحديد مفهوم لها.

المطلب الأول:تعريف الجريمة الإلكترونية وتحديد طبيعتها القانونية

يكتسب موضوع تعريف الجريمة الإلكترونية وتحديد طبيعتها القانونية أهمية كبرى لفهم ماهيتها.

الفرع الأول: تعريف الجريمة الإلكترونية

تعددت وتنوعت صيغ وألفاظ التعريف بالجريمة الإلكترونية ومنها أصبح من الصعب الاتفاق على تعريف موحد لها واختلفت الاجتهادات في ذلك اختلاف كبير.

أولا: التعريف اللغوي للجريمة الإلكترونية

الجريمة في اللغة مأخوذة من كلمة (الجرم) معناه التعدي أو الذنب،وجمعها إجرام وهو الجريمة فيوصف الفاعل ب المجرم أو الجريم[1].

والجريمة والمجرم بمعنى الكاسب ارتكب فلان الجرم أي اكتسب الإثم[2].

كلمة الإلكترونية تشير إلى الحاسب أو شبكات الاتصالات مثل شبكة الانترنت.

ثانيا: التعريف الاصطلاحي للجريمة الإلكترونية

للتعرف على الجريمة الإلكترونية اصطلاحا لابد من التعرض إلى التعريف الفقهي ثم التعريف القانوني حسب المشرع الجزائري:

1. **التعريف الفقهي:** أكدّ علماء الفقه كدا مكثفا وواسعا في محاولة تحديد ووضع تعريف شامل وموحد لمصطلح الجريمة الإلكترونية وانقسم الفقه إلى اتجاهين الأول يضيق لمفهومها والثاني يوسع منه[3]

---

[1]– هبة نبيلة هروال، جرائم الأنترنت، دراسة مقارنة، أطروحة دكتوراه، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة تلمسان الجزائر ،2014/2013 ص 12

[2]–سامية عزيز،ما زياعيساوي، الجريمة من منظور سوسيولوجي، الأسباب الآثار، مجلة دراسات في سيكولوجية الانحراف، السنة 2021، المجلد 6، العدد 1، ص 128

[3] – عادل محمد فريد نائلة، جرائم الحاسب الآلي الاقتصادية، ط1، منشورات الحلبي الحقوقية، بيروت لبنان 2005، ص 7

أ- التعريف المضيق للجريمة الإلكترونية:

تعرف على أنها كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكاب الجريمة من ناحية ولملاحقته والتحقيق معه من ناحية أخرى.

- يرى الأستاذ mass أن المقصود بالجريمة المعلوماتية هي الاعتداءات القانونية التي ترتكب بواسطة بغية تحقيق الربح.[1]
- أما عن الفقيه الألماني Tiedmann فهو يرتكز في تعريفه على وسيلة إرتكاب الجريمة : "هي كل أشكال السلوك الغير مشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب".
- كذلك يعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية أنها: "الجرائم التي تلعب فيها البيانات و البرامج المعلوماتية دورا رئيسيا".
- ويعرف David Thompson جريمة الحاسب بأنها: :"أي جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب"، وارتكز هذا الفقيه في تعريفه على توافر المعرفة بتقنية المعلومات. [2]
- أما بالنسبة للفقه المصري، فهي تنشأ عن الاستخدام الغير مشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال أو الأشياء المعنوية.[3]

وهناك فريق آخر يرى أن الجريمة المعلوماتية هي أي فعل أو عدم فعل يمكن أن يسبب ضررًا لمكونات الكمبيوتر وشبكات الاتصال الخاصة به، وهذا محمي بموجب قانون العقوبات الذي يفرض عقوبات لذلك، وقد عرفها محمد علي العريان بأنها: كل فعل إيجابي أو سلبي عمدي يهدف إلى الاعتداء على تقنية المعلوماتية أي كان غرض الجاني.[4]

ب-التعريف الموسع للجريمة الإلكترونية:

على نقيض الاتجاه السابق هناك تعريفات حاولت التوسع في مفهوم الجريمة المعلوماتية فعرفوها كالأتي:

---

[1] – نهلا عبد القادر المومني، الجرائم المعلوماتية، ماجيستير في القانون الجنائي المعلوماتي، دار الثقافة للنشر والتوزيع 1429هـ/2008م، طبعة الأولى، الإصدار الأول / 2008 ص 48

[2] – سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، ماجيستير في القانون، دار الفكر الجامعي، 30 شارع سويتر الإسكندرية،2008، صفحة 38-40

[3]– سامي علي حامد عياد، مرجع سابق، صفحة 38-40

[4]– نشناش منية، مداخلة حول الركن المفترض في الجريمة المعلوماتية، جامعة بسكرة 2015 /2016، صفحة 2-3

- " كل فعل أو امتناع عمدي ينشأ عن استخدام غير مشروع لتقنية المعلوماتية بهدف الاعتداء على الأموال أو الأشياء المعنوية".
- منح الخبير الأمريكيparker مفهوما واسعا للجريمة المعلوماتية على أنها: "كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ، ينشأ عنه خسارة تلحق بالمجني عليه ، أو مكسب يحققه الفاعل".[1]
- وعرفهاالأستاذ vivan بأنها: "مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب".[2]

جرائم الكمبيوتر هو مصطلح شامل أشمل من المصطلح السابق و يقصد فيه كل الجرائم التي يستخدم فيها الكمبيوتر، سواء كأداة للجريمة أو كان هدفا في الجريمة و يدخل في ضمنها جرائم معلوماتية و جرائم الانترنت، كما يدخل الاعتداء على الشبكات المحلية خاصة بالهيئات و المنشآت الخاصة و العامة ، الجريمة الإلكترونية هي ببساطة استخدام التقنيات الرقمية لإخافة الآخرين.[3]

2. التعريف القانوني حسب المشرع الجزائري:

تبنى المشرع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبراً أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلاً 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.[4]

لم يتخلف المشرع الجزائري بدوره عن ركب التشريعات التي وضعت تعريفاً لنظام المعلومات حيث أنه عرفها من خلال نص المادة 2 من القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[5]، ب جرائم المساس بأنظمة المعالجة الآلية للمعطيات

[1] – نهلا عبد القادر المومني، مرجع سابق، صفحة 49

[2] – نفس المرجع صفحة 49

[3] –أمير فرج يوسف، جرائم المعلوماتية على شبكة الأنترنت، دار المطبوعات الجامعية،الإسكندرية، 2009 ص 106

[4]– قانون رقم 04/09 المؤرخ في 14 شعبان 1430 سنة 2009، و يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، صادر بتاريخ 2009/08/16 ، صفحة 05

[5] – المادة 02 الفقرة ب ، قانون 04/09 ،مرجع سابق

المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

قام المشرع الجزائري بتجريم الأفعال التي تضر بأنظمة الحاسب الآلي، وذلك نتيجة لتأثر الجزائر بالثورة المعلوماتية التي أدت إلى ظهور أشكال جديدة من الجرائم لم تعرفها الجزائر سابقًا، هذا الأمر دفع المشرع إلى تعديل قانون العقوبات من خلال القانون رقم 15/04 الصادر في 10 نوفمبر 2004، الذي يعدل الأمر رقم 66-156 المتعلق بقانون العقوبات، حيث خصص القسم السابع مكرر بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات".[1]

وفقًا للمشرع الجزائري في تعريفه لنظام المعالجة الآلية للمعطيات اشترط ضرورة الترابط بين مكونات أو أجهزة النظام أو بين الأنظمة فيما بينها، وركز على وظيفة المعالجة الآلية للمعطيات.[2]

3. موقف المشرع الجزائري من الجريمة الإلكترونية:

من خلال ما تقدم من تعريفات للجريمة الإلكترونية حسب المشرع الجزائري نستنتج موقف المشرع من هذه الجريمة والمتمثل في التطور التكنولوجي وانتشار التكنولوجيا الحديثة أدى إلى ظهور إجرام فني في حلة جديدة، مما استدعى ضرورة معاقبة هذه الجرائم. وهذا يهدف إلى توفير حماية قانونية للأنظمة المعلوماتية وطرق معالجة البيانات. ولذلك، قام المشرع الجزائري بتعديل قانون العقوبات لسد الثغرات القانونية في هذا المجال و كان ذلك بموجب قانون 15/04 المؤرخ في 2004/11/10 المتمم و المعدل للأمر 66/165 المتضمن قانون العقوبات والذي أقر له القسم السابع مكرر منه تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ، فقد أثار المشرع الجزائري استخدامه لمصطلح للدلالة على كلمة المعلومات و النظام الذي يحتوي عليها و يخرج بذلك من نطاق تجريم تلك الجرائم التي يكون النظام المعلوماتي وسيلة ارتكابها و حصرها فقط في صور الأفعال التي تشكل اعتداء على النظام المعلوماتي ، أي الجرائم التي يكون النظام المعلوماتي محلا لها.[3]

---

[1] – عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري و المقارن ، دار الجامعة الجديدة ، كلية الحقوق ، جامعة الإسكندرية ، 2006 صفحة 27

[2] – نشناش منية ، مرجع سابق ، صفحة 4

[3] – سعيد نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة ماجيستر في العلوم القانونية، جامعة الحاج لخضر،باتنة، 2013/2012 ، صفحة 41

اعتبر المشرع في تدخله أن جوهر المعلوماتية يتعلق بالمعطيات التي تُدخل إلى الحاسب الآلي، حيث يتم تحويلها إلى معلومات بعد معالجتها وتخزينها. لذلك، قام بحماية هذه المعطيات من عدة جوانب. في مرحلة لاحقة، اختار المشرع الجزائري استخدام مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال لتوصيف الجريمة المعلوماتية، وذلك بموجب القانون رقم 04/09 المتعلق بالجرائم المرتبطة بتكنولوجيا الإعلام والاتصال ومكافحتها.[1]

الفرع الثاني: الطبيعة القانونية للجريمة الإلكترونية

بالنظر إلى مجمل التعاريف التي تختص بها الجريمة المعلوماتية فإنه وبدون شك ستتبادر في أذهاننا فكرة التساؤل حول طبيعتها القانونية فهي في ظاهرها تبدو هذه الجريمة كأنها غير مادية، لأنها تحدث في الفضاء الإلكتروني ولا تترك آثاراً مادية واضحة. وهذا يجعلها تختلف تماماً عن الجرائم الأخرى التي تعتبرها القوانين تهديداً لمصالح الآخرين، وقد اختلف الخبراء في كيفية تصنيف هذه الجريمة، سواء بوصفها خاصة أو عامة.

أولا:الاتجاه الفقهي الذي يرى بان الجريمة المعلوماتية جريمة من نوع خاص

يستند هذا الاتجاه على فكرة أن مجال الحماية القانونية هو المعلومة في حد ذاتها باعتبارها السند الأساسي للنظم المعلوماتية وانطلاقا من أن وصفا "التسمية" يضفي على الأشياء المادية القابلة للاستحواذ دون تلك المعنوية التي لا يمكن الاستحواذ عليها، فإن مجال الحماية المقررة لها هو في ضوء حقوق الملكية الفكرية فقط، ولعل أن فكر هذا الاتجاه الفقهي يتعارض مع المفاهيم الحديثة للقانون الجنائي الذي يقر بأحقية توفير الحماية القانونية للمعلومة باعتبارها تكتسب صفة المال وهو ما تبناه أنصار المذهب الثاني.[2]

ثانيا: الاتجاه الفقهي الذي يرى بان الجريمة المعلوماتية جريمة مستحدثة

يتخذ هذا الاتجاه موقفا صريحا مفاده أن الجريمة المعلوماتية وباعتبارها جريمة تستهدف المعلومات وباعتبار هذه الأخيرة مجموعة مستحدثة من القيم باعتبارها قابلة للاستحواذ عليها داعمتها المادية، كما أنها قابلة للتقويم بحسب سعر السوق متى كانت غير محظورة تجاريا بعيدا عن أنها نتاج

[1] – سعيد نعيم، مرجع سابق، صفحة 41

[2]– مخلوف عكاشة، دور الشرطة القضائية في مكافحة الجريمة الإلكترونية، رسالة نيل شهادة ماستر جامعة سعيدة، السنة الجامعية 2016–2017، صفحة 22

مؤلفها وتجمع بينها علاقة وهو الرأي الذي جاء به الأستاذ فيفانتي (vivanti) بقوله إن «فكرة الشيء أو القيمة لها صورة معنوية وأن نوع الحق يمكن أن ينتمي إلى قيمة معنوية ذات طابع اقتصادي وان تكون جديرة بحماية القانون ومتى كانت المعلومات والبرامج المعالجة آليا ذات قيمة اقتصادية فإنه يجب معاملتها معاملة المال."[1]

إذا فالبيانات والمعلومات الموجودة داخل ذاكرة الحاسوب تعتبر من الأموال ولها قيمة مادية، قابلة للنقل من حاسوب لآخر أو القرص المضغوط أو البريد الإلكتروني فهي بالتالي مال منقول وإذا نقلت من دون رضا صاحبها فيطبق عليها قانون العقوبات.

ولقد استقر الرأي الراجح حتى الفقه على أن البرامج والمعلومات تخضع لمبدأ الحماية الجنائية والبرامج والمعلومات ملك لصاحبها إذا سرق محتواها من شخص آخر فإن ذلك يعتبر سرقة للمعلومات في حد ذاتها لأنه لا يمكن الفصل بين الدعامة والمعلومة محل السرقة.[2]

الفرع الثالث: أهداف الجريمة الإلكترونية

وتتمثل أهداف الجريمة الإلكترونية في الوصول إلى المعلومات بطريقة غير قانونية، مثل سرقة المعلومات أو الاطلاع عليها أو حذفها أو تغييرها لتحقيق أهداف المجرم. كما تشمل هذه الجرائم الوصول إلى الخوادم التي تحتوي على المعلومات عبر الإنترنت وتعطيلها أو تغيير محتواها. يحصل المجرمون أيضًا على معلومات سرية من المؤسسات والبنوك والجهات الحكومية والأفراد، ويقومون بابتزازهم من أجل المال أو لأسباب سياسية. كما يسعون لتحقيق مكاسب مادية أو معنوية باستخدام تقنيات المعلومات، مثل اختراق المواقع الإلكترونية وسرقة الحسابات البنكية.[3]

المطلب الثاني:خصائص وأنواع الجريمة الالكترونية

بعد التعريف بمفهوم الجريمة الإلكترونية وشرح طبيعتها القانونية سنقوم في هذا المطلب بتوضيح خصائص هذه الجريمة من خلال استعراض السمات الخاصة بالجريمة الالكترونية والسمات الخاصة بالمجرم الاليكتروني وتنوع هذه الجريمة.

[1]– محمد علي العريان، مرجع سابق ، صفحة 51

[2] – خالد عباد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع،عمان، الأردن،2001، صفحة 57

[3] – حشمان عمار، الجريمة الإلكترونية في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات شهادة ماستر مهني، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرباح،ورقلة، 2019/2018، صفحة 09

الفرع الأول: خصائص الجريمة الالكترونية

تتميز الجريمة الالكترونية عن غيرها من الجرائم بعدة خصائص وهي كالتالي: السمات الخاصة بالجريمة الالكترونية والسمات الخاصة بالمجرم الالكتروني.

أولا: السمات الخاصة بالجريمة الالكترونية

1. الجريمة الالكترونية جريمة عابرة للحدود:

تتميز الجريمة الالكترونية بأنها غالبا ما تحمل طابعا دوليا، ذلك بسبب الطبيعة العالمية لشبكة الانترنت التي تتيح الاتصال المستمر بين معظم دول العالم، مما يسهل من ارتكاب الجرائم عبر الحدود الوطنية حيث لا تعترف الجريمة الالكترونية بالفواصل الجغرافية بين الدول والقارات، وبالتالي فهي جريمة عابرة للقارات، حيث يمكن تنفيذ العديد من الجرائم كالتلاعب بقواعد البيانات وتزوير وإتلاف المستندات الالكترونية، إضافة إلى الاحتيال المعلوماتي والقرصنة. [1]

تتميز بها الجريمة الالكترونية بكونها جريمة عابرة للحدود، وهذا يخلق مشاكل في تحديد الدولة صاحبة الاختصاص القضائي، وتحديد القانون الواجب تطبيقه، بالإضافة إلى مشاكل تتعلق بإجراءات الملاحقة القضائية.

2. صعوبة اكتشاف الجريمة الالكترونية:

تتميز الجرائم المرتبطة باستخدام الانترنت بانها غالبا ما تكون خفية وصعبة الكشف، حيث لا يلاحظ الضحية وقوعها رغم انها قد تحدث اثناء تواجده على الشبكة، وذلك لان الجاني يمتلك مهارات فنية تسمح له بتنفيذ جريمته بدقة عالية مثل ارسال الفيروسات وسرقة الأموال والبيانات الشخصية وتدميرها بالإضافة الى التجسس وسرقة المكالمات وغيرها من الجرائم. [2]

[1]– خالد محمود إبراهيم، مرجع سابق، ص 77

[2]– محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، ص 32

كما تتميز وسائل هذه الجرائم في معظم الأحيان بالطابع التقني المعقد، كما انه يتردد الضحايا في الإبلاغ عنها في حال اكتشافها خوفا من فقدان عملائهم فضلا عن إمكانية تدمير المعلومات التي قد تستخدم كأدلة إثبات في زمن قصير جدا قد لا يتجاوز الثانية. [1]

3. صعوبة إثبات الجريمة الالكترونية:

الجريمة الالكترونية تحدث في بيئة غير تقليدية إذ تتم خارج نطاق الواقع المادي الملموس، لتقوم أركانها في فضاء الحاسوب والانترنت مما يجعل الأمور تزداد تعقيدا أمام الجهات الأمنية و أجهزة التحقيق و الملاحقة ،ونظرا للطبيعة التقنية التي تتسم بها هذه الجرائم فان اكتشافها والبحث عنها يتطلبان تقنيات متقدمة وأساليب خاصة في التحقيق و التعامل، إلا أن هذه الإجراءات لم تتحقق بشكل كافي في الأجهزة الأمنية والقضائية لدينا، نتيجتا لنقص المعرف وهو ما يتطلب تخصص في التقنية لتحصين الجهاز الأمني و القضائي ضد هذه الظاهرة، حيث أن القوانين التقليدية لم تعد قادرة على مواكبة تطور الجريمة المعلوماتية في ظل التسرع المستمر للتقدم التكنولوجي. [2]

4. أسلوب ارتكاب الجريمة الالكترونية:

من خصائص الجريمة الالكترونية إنها تتجلى بشكل أكثر وضوحا في الطريقة التي ترتكب بها وأسلوبها، فالجرائم المعلوماتية تتميز بالهدوء بطبيعتها، لا تتطلب العنف بل تقتصر على القدرة على التعامل على جهاز الكمبيوتر بشكل تقني يسمح باستخدامه في تنفيذ الأفعال الغير قانونية.[3]

كما تحتاج كذلك إلى توافر شبكة الانترنت ومجرم قادر على استغلال مهاراته وقدراته للتعامل مع هذه الشبكة وتنفيذ جرائم متنوعة مثل اختراق خصوصيات الآخرين أو التجسس، وذلك دون الحاجة إلى اللجوء إلى العنف أو سفك الدماء على عكس الجرائم التقليدية التي قد تستلزم بدل جهد جسدي مثل ممارسة العنف أو الإيذاء كما في جريمة القتل أو السرقة والكسر. [4]

---

[1]– نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2، دار الثقافة للنشر والتوزيع، ص56

[2]– محمد عبيد الكعبي، مرجع سابق، ص 40

[3] –نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان ،2008، ص55

[4] –نفس المرجع السابق، ص55

5. الجريمة المعلوماتية تتم عادة بتعاون أكثر من شخص:

تتميز الجريمة الاليكترونية عادة بتعاون عدة أفراد على ارتكابها بهدف الإضرار بالجهة المجني عليها، وغالبا ما يشترك في تنفيذ هذه الجريمة شخص متخصص في تقنيات الحاسوب والانترنت، الذي يتولى الجانب الفني من المشروع الإجرامي، بالإضافة إلى شخص اخرمن داخل المؤسسة المجني عليها او خارجها الذي يساعد في تغطية عملية التلاعب وتحويل الأرباح إليه. [1]

6. الجرائم التي تدفع على المعطيات:

بسبب ما تشهده الدول بشكل عام، بما في ذلك الجزائر، من تحول رقمي في المعلومات التي تستخدم لأغراض متنوعة، سواء كانت عامة أو خاصة، ومهما كانت قيمتها، فمن المهم حماية هذه المعلومات من الاعتداءات. لذلك، تدخل المشرع لوضع قوانين تحمي هذه المعلومات، مما يوفر نوعاً من الأمان القانوني للمالكين. هذه الحماية تكون ضرورية بشكل خاص للمعلومات الشخصية لأنها تعتبر أكثر حساسية، هذا النص يرتبط بحماية الحياة الخاصة للأفراد. رغم وجود العديد من القوانين المتعلقة بالمعلومات وخصوصية الحياة، إلا أنها لم تعترف بالبيانات الشخصية كحق يستحق الحماية. استمر هذا النقص في القوانين حتى صدور القانون رقم 07/18 في 10 يونيو 2018، الذي يعنى بحماية الأشخاص في مجال معالجة البيانات الشخصية. يحتوي هذا القانون على فصول تتعلق بالعقوبات، وسنركز في دراستنا على الجرائم المتعلقة بالبيانات الشخصية، حيث سنستعرض أنواع هذه الجرائم ونحلل عناصرها والعقوبات المترتبة عليها.[2]

7. جرائم متطورة ومتعددة الأشكال:

مجرم المعطيات يختلف كثيرًا عن المجرم في الجرائم التقليدية. له خصائص خاصة لا توجد عند الآخرين، كما أن لديه أنواعًا وأشكالًا مختلفة، العوامل التي تدفعه لارتكاب الجريمة أيضًا مختلفة، بالنسبة لخصائصه فهو شخص اجتماعي، مما يعني أنه يتكيف مع مجتمعه وغالبًا ما يكون له مكانة مهمة ويحظى بالاحترام، كما أنه يمتلك المعرفة والمهارة اللازمة للجريمة، والتي يكتسبها من خلال الدراسة أو من خلال التجربة والتعامل مع الآخرين، بالإضافة إلى ذلك هو شخص ذكي حيث يستخدم ذكاءه في

[1]– محمد عبيد الكعبي، مرجع سابق ص42

[2]– ملياني عبد الوهاب، جرائم المساس بالمعطيات الشخصية على ضوء القانون رقم 18/07، مجلة البحوث القانونية والاقتصادية، الطبعة 6، العدد 1، بتاريخ 2023/01/28، الصفحة 272.

تنفيذ جريمته، ولا يحتاج إلى استخدام القوة الجسدية إلا في حالات قليلة وغالبًا ما يكون من ذوي المستويات العلمية العالية، مجرم المعطيات يتميز بدوافع مختلفة تدفعه للقيام بجرائمه هذه الدوافع قد تكون الرغبة في الربح، الانتقام من شخص ما، أو حتى الرغبة في تجاوز الأنظمة والتقنيات أحيانًا، تكون هذه الدوافع مرتبطة بحب التعلم أو بالسياسة. مجرم المعطيات ينقسم إلى نوعين رئيسيين:

-**الأول:** هم الهواة الذين يحبون المعلوماتية.

-**الثاني:** هم المحترفون في الجرائم المعلوماتية الفرق بين النوعين هو سبب ارتكاب الجريمة، حيث يكون الدافع لدى الهواة بسيطًا مثل الفضول، بينما يكون لدى المحترفين دوافع أكثر تعقيدًا مثل الرغبة في المال أو السياسة. [1]

8. قلة الإبلاغ عن الجرائم الإلكترونية:

ترجع إلى أن معظم هذه الجرائم تُكتشف بشكل غير مقصود، لأنها تبقى غالبًا مخفية. وهذا ما يُعرفه علماء الإجرام بالرقم الأسود أو الرقم الخفي.

من أسباب اختفاء هذه الجرائم هو عدم إبلاغ المجني عليهم عنها، نجد أن معظم المؤسسات التي تتعرض للاختراقات المعلوماتية تكتفي باتخاذ تدابير داخلية ولا تبلغ السلطات المختصة، وذلك خوفاً من التأثير على سمعتها، خاصة إذا كانت هذه المؤسسات مالية مثل البنوك، تخشى هذه المؤسسات أن تؤدي الإجراءات القانونية إلى تقليل ثقة العملاء بها وبالتالي ابتعادهم عنها.[2]

من ناحية أخرى، يتم الإبلاغ عن الجرائم التقليدية بشكل كبير لأنها سهلة الاكتشاف. كما أن الشخص الذي يتعرض للجريمة يجب عليه الإبلاغ عنها، وإلا سيتعرض لمشكلة عدم الإبلاغ.[3]

9. نقص الخبرة في الشرطة والقضاء:

نقص الخبرة في الشرطة والقضاء يجعل من الصعب كشف جرائم الإنترنت والقبض على مرتكبيها، يتطلب الأمر استراتيجيات تحقيق وتدريب خاصة تناسب طبيعة هؤلاء المجرمين، مما يساعد على فهم الأساليب التي يستخدمونها.

---

[1]– د. عبد الله حسين محمود، شرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، ط2، القاهرة، 2002، ص36.

[2]– هشام فريد رستم،الجوانب الإجرامية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الانترنت الحديثة، أسيوط، مصر، 1994، ص25

[3]–بوديسة بجاد عبد الرؤوف، آليات التحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر مهني في الحقوق، تخصص قانون الإعلام الآلي و الانترنت، كلية الحقوق و العلوم السياسية، جامعة محمد البشير الإبراهيمي بورج بوعريريج، 2022/2021،

لذلك تجد أجهزة العدالة نفسها غير قادرة على التعامل مع هذه الجرائم بوسائل التحقيق والإجراءات التقليدية، فهي تختلف عن الجرائم التقليدية حيث يكون رجال الشرطة والقضاء مدربين وذوي خبرة في تلك الحالات.[1]

ثانيا: السمات الخاصة بالمجرم المعلوماتي:

من المعروف أن شخصية المجرم الذي يقوم بارتكاب الجرائم الالكترونية لا تتشابه مع شخصية المجرم الذي يقوم بارتكاب الجرائم التقليدية، حيث أن الجرائم الالكترونية تحتاج إلى شخص عبقري له درجة عالية من العلم والثقافة، إما الجرائم التقليدية ترتكب من طرف شخص عادي، وغالبا ما يتميز المجرم العادي بالقوة العقلية ونادرا ما يتميز بعضهم بالذكاء، ومنه سنتطرق إلى السمات التي يتميز بها المجرم الالكتروني وهي كالأتي:

1. الذكاء Intelligence:

يعد الذكاء من أهم صفات المجرم الالكتروني لان ذلك يحتاج إلى المعرفة التقنية للوصول إلى أنظمة الحاسوب وتعديل البرامج، بالإضافة إلى القدرة على ارتكاب جرائم السرقة والاحتيال التي تتطلب أن يكون الجاني على درجة عالية من المعرفة، لكي يستطيع تنفيذ هذه الجرائم.[2]

ولهذا السبب تعتبر الجريمة الاليكترونية من جرائم الأذكياء، على عكس الجريمة التقليدية التي تعتمد على القوة والعنف [3]، وبالتالي لا يمكن أن ينتمي المجرم الالكتروني إلى فئة المجرمين منخفضي الذكاء، باعتباره يستعين بالكومبيوتر في السرقة تجنبا لعدة عواقب وهذا مستوى مرتفع من الذكاء، فهو بهذا أقرب إلى النصب منه إلى السرقة .[4]

2. الاحتراف:

[1]– هبة هروال، مرجع سابق، ص50

[2] –ايمن عبد الحفيظ، "استراتيجية مكافحة جرائم استخدام الحاسب الالي "، بدون دار النشر، ص243

[3]– جميل عبد الباقي الصغير، "القانون الجنائي والتكنولوجيا الحديثة "، الكتاب الأول: "الجرائم الناشئة عن استخدام الحاسب الالي "، دار النهضة العربية، القاهرة، ط1، 1992، ص15

[4]– سليمان احمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدوليةَ (الانترنت)، دار النهضة العربية، القاهرة، 1428هـ/2007م، ص 12.11

المجرم الالكتروني مجرم محترف يمتلك مهارات تقنية وقدرات فنية عالية، مما يسمح له باستغلال مهاراته في ارتكاب جرائم الكترونية متعددة، كالاختراق والسرقة والنصب والاعتداء على حقوق الملكية الفكرية، للحصول على مكاسب مالية. [1]

لذلك لا يمكن للشخص الهاوي ارتكاب جرائم الكترونية بسهولة إلا في حالات نادرة، حيث يتطلب الأمر الدقة والتخصص في مجال الأمن السيبراني للتمكن من التغلب على العقبات التي وضعها الخبراء بهدف حماية أنظمة الكمبيوتر مثل ما يحدث في البنوك وغيرها من المؤسسات المالية الأخرى. [2]

3. الخبرة والمهارة:

إن المجرم الالكتروني يتصف بأنه على درجة عالية من الخبرة والمهارة في استخدام التقنية المعلوماتية، وذلك لان مستوى الخبرة التي يكون عليها هي التي تحدد الأسلوب الذي يرتكب به تلك الجرائم، حيث إذا كان مرتكب الجريمة ذو خبرة ضعيفة، نجد ان الجرائم التي يرتكبها لا تتعدى الإتلاف المعلوماتي، إما إذا كان ذو خبرة عالية يختلف أسلوب ارتكابه للجرائم حيث يقوم بجرائم تتطلب مهارة عالية مثل النصب وسرقة الأموال آليا. [3]

4. الميل إلى ارتكاب الجرائم:

يتميز مرتكبو الجرائم في مجال الحاسب الآلي بالنزعة الإجرامية، حيث يتعلمون و يتقنون المهارات التكنولوجية التي تساعدهم على ارتكاب الجرائم.[4]

وهذه النزعة الإجرامية تتكون نتيجة عوامل عضوية ونفسية في محيط الشخص، ومع اقتران هذه العوامل باكتساب المهارات العلمية والتكنولوجية تزيد قدرة عوامل الإجرام وتظل تلك العوامل بمثابة طاقة كامنة، ويمكن إجمال هذه الحالة الإجرامية طبقا للنظرية التالية: (حالة إجرامية كامنةَ + موقف إجرامي + قرار الحسم الإداري = سلوك إجرامي). [5]

---

[1]– محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركو الإعلام الأمني، مملكة البحرين، ص12

[2]– سليمان احمد فضل، مرجع سابق، ص 22

[3]– ايمن عبد الحفيظ، مرجع سابق، ص244

[4]– ايمن عبد الحفيظ، الاتجاهات الفنية و الأمنية لمواجهة الجرائم المعلوماتية، مطابع الشرطة، 2005،ص15

[5]– ايمن عبد الحفيظ، مرجع سابق، ص245

5. المجرم الالكتروني مجرم غير عنيف:

يتميز المجرم الالكتروني بعدم استخدامه للعنف، حيث يعتمد على الذكاء والحيلة لان هذا النوع من الجرائم لا يتطلب استخدام القوة والعنف لتنفيذه. [1]

6. الوسيلة:

يقصد بها الإمكانيات التي يستعين بها الفاعل لتنفيذ جريمته، وفيما يتعلق بالمحرم المعلوماتي فان الأدوات اللازمة للتلاعب بأنظمة الحواسيب غالبا ما تتسم بالبساطة و سهولة التوفر.[2]

7. السلطة:

أما السلطة فقصد بها الصلاحيات أو الامتيازات التي يمتلكها المجرم المعلوماتي والتي تمكنه من تنفيذ جريمته، وقد تتخذ هذه السلطة أشكالا كثيرة، كامتلاكه لرمز الدخول إلى النظام المعلوماتي، حيث تمنح الفاعل مزايا متعددة مثل فتح الملفات أو حذفها أو تعديلها أو مجرد قراءتها أو كتابتها ، وقد تتمثل هذه السلطة في الحق في استكمال الحاسب الآلي أو إجراء بعض التعاملات وقد تكون هذه السلطة في بعض الحالات مزيفة، كما في حالة استخدام الجاني بيانات دخول خاصة بشخص آخر دون علمه.[3]

8. الباعث:

في النهاية، الدافع لارتكاب الجريمة غالبًا لا يختلف كثيرًا عن دوافع ارتكاب جرائم أخرى، الرغبة في الحصول على المال بطريقة غير قانونية تظل هي الدافع الرئيسي وراء ارتكاب الجرائم المعلوماتية، بعد ذلك تأتي الرغبة في اختراق نظام الكمبيوتر وتجاوز الحواجز الأمنية، وأخيرًا، يمكن أن يكون الانتقام من صاحب العمل أو أحد الزملاء دافعًا أيضًا.[4]

---

[1]– غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم الى مؤتمر القانون و الكمبيوتر و الانترنت الذي نظمته كلية الشريعة والقانون في الفترة من 3.1مايو2000، جامعة الامارات العربية المتحدة 2000،ص5

[2]– خالد داودي، الجريمة المعلوماتية، الطبعة الأولى، دار الاعصار العلمي للنشر والتوزيع، عمان، الأردن، 2008، ص84

[3]– نور الدين فليح، الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة د. مولاي الطاهر، سعيدة، 2019/2018، ص19

[4]– خالد داودي، مرجع سابق، ص74

الفرع الثاني: أنواع الجريمة الالكترونية:

أولا: الجرائم التي تقع على الأشخاص:

هي الجرائم التي تهدد الحقوق الشخصية للفرد، حيث تعتبر هذه الحقوق أساسية للشخصية الإنسانية والتي تقع خارج مجال التعاملات الاقتصادية ومن بين هذه الحقوق الحق في الحياة والسلامة الجسدية والحرية والشرف. [1]

1-جريمة انتحال الشخصية:

هي جريمة قديمة جدا لكنها أخذت شكلا جديدا بعد انتشار شبكة الانترنت، وهي انتحال شخصية الفرد على الانترنت واستغلالها بشكل غير مشروع، حيث يتم أخذ المعلومات الشخصية مثل العنوان وتاريخ الميلاد ورقم الضمان الاجتماعي وغيرها، يتم استغلال هذه البيانات من اجل تحقيق مكاسب مشروعة كالحصول على بطاقات الائتمان، حيث يستطيع المنتحل إخفاء شخصيته والتصرف بحرية تحت اسم مستعار. [2]

2-جريمة المضايقة و الملاحقة:

هي نوع من الجرائم التي تزداد انتشارا مع كل تطور وتحديث برامج الدردشة والمحادثات المتبادلة، وهي عبارة عن مساحات في الفضاء الالكتروني تسمح لمستخدميها الدخول في محادثات بين بعضهم البعض، كما أن هذه الجرائم تشمل رسائل تهديد وتخويف ومضايقة حيث شبهها القضاة بجرائم التهديد العلني التي تتم خارج الشبكات، ولا تتطلب هذه الجريمة أي اتصال مادي بين المجرم والضحية لما لها من تأثيرات سلبية نفسية، فهي لا تؤدي إلى أي تصرفات عنف مادية. [3]

3-جرائم التغرير والاستدراج:

تعتبر من أشهر جرائم الانترنت التي تتميز بانتشار واسع، خاصة بين الشباب ومستخدمي الشبكة، تعتمد هذه الجرائم على الخداع حيث يقوم المجرمون بخداع الضحايا وإيهامهم بتكوين علاقة

---

[1]- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مرجع سابق، ص 5

[2]-- منير محمد الجنيهي ممدوح محمد الجنيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005، ص42-43

[3]- محمد أمين احمد الشوابكة، جرائم الحاسوب الأولى والانترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2004، ص 45

صداقة أو زواج عبر الانترنت، وقد تتحول هذه الجريمة إلى لقاء مادي بين الطرفين، وتتميز هذه الجرائم بعدم وجود حدود لها، حيث يستطيع كل مراسل على الشبكة ارتكابها بسهولة، كما يمكن لأي مستخدم بريئ أن يقع ضحيتها.[1]

4-جرائم التشهير وتشويه السمعة:

لنشر هذه الشائعات والأخبار الزائفة، وكذلك لتشويه أفكار الناس أو محاولة ابتزاز الأفراد من خلال نشر الشائعات عنهم.

مع تفشي ظاهرة الشائعات والإخبار الكاذبة التي تهدف إلى تشهير وتشويه سمعة رموز الشعوب سواء كانت رموز فكرية أو سياسية أو دينية، ظهرت على شبكة الانترنت بعض المواقع التي خصصت نفسها

و أبرز الطرق التي تستخدم لارتكاب هذه الجريمة إنشاء مواقع على الشبكة تحتوي على المعلومات المراد نشرها أو إرسالها عبر المواقع الاليكترونية، مثل إرسال صور غير لائقة أو معلومات غير صحيحة.[2]

5-الجرائم المخلة بالأخلاق والآداب العامة:

بما أن شبكة الانترنت تتمتع بالعالمية ولا تقتصر على مستخدم دون الآخر، فان المواد التي تعرض تعد مخلة بالآداب و الأخلاق العامة في بلد معين قد تعتبر جريمة يعاقب عليها القانون في حين أنها لا تعتبر كذلك في بلد آخر، وتشمل هذه الجرائم تحريض القاصرين على أنشطة جنسية غير قانونية عبر الوسائل الالكترونية أو محاولة إغوائهم للقيام بهذه الأنشطة، كما تتضمن نشر معلومات عنهم عبر الانترنت ودعوتهم للقيام بالأفعال الفاحشة، بالإضافة إلى تصوير القاصرين ضمن أنشطة جنسية.

تعد الأعمال الإباحية من أكثر الأنشطة انتشارا ورواجا في الوقت الحالي، خاصة في الدول العربية والأوروبية والآسيوية، وتشمل الجرائم المخلة بالأخلاق والآداب العامة على الانترنت جميع

[1]- عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة د. الطاهر مولاي، سعيدة، سنة 2016/2015، ص19

[2]- منير محمد الجنيهي ممدوح محمد الجنيهي، مرجع سابق، ص 34

الأشكال سواء كانت صورا أو مقاطع فيديو أو محادثات أو أرقام هاتفية مما خول هذه الشبكة ان تكون متاحة للجميع دون قيود أو حواجز.[1]

ثانيا: الجرائم التي تقع على الأموال:

هي الجرائم التي تستهدف الاعتداء على الأموال والتي تهدد الحقوق ذات القيمة المالية، وتشمل هذه الجرائم الحقوق ذات القيمة الاقتصادية.

فإذا كان موضوع الاعتداء على الأموال يتعلق بالحاسوب نفسه وما يرتبط به من ملحقات فانه لا يواجه أي صعوبات أو عراقيل في تطبيق النصوص الجزائية التقليدية لكون الأمر يتعلق بأموال وممتلكات عادية منقولة، إما إذا كان الاعتداء يتعلق بفن الحاسوب من برمجيات وأنظمة، حيث أن النصوص التشريعية التقليدية غير قادرة على توفير الحماية نظرا للطابع الخاص وغير التقليدي لهذا المجال.[2]

1-جرائم صناعة ونشر الفيروسات:

الفيروس هو برنامج كأي برنامج آخر موجود على جهاز الحاسوب، لكنه مصمم بطريقة تسمح له بالتأثير على البرامج الأخرى الموجودة على الجهاز بأن تجعل تلك البرامج نسخة منها أو أن تعمل على مسح كافة البرامج الأخرى، مما يؤدي إلى تعطيلها عن العمل.

أما بالنسبة لمبدأ عملها فيعتمد على أسلوب تصميمها فقد تبدأ الفيروسات بالعمل مباشرة عند فتح الرسالة الموجودة بها، أو بعد تشغيل البرامج الموجودة عليها، وتعد هذه الفيروسات من أبرز جرائم الانترنت و أكثرها انتشارا، وقد ظهرت الفيروسات لأول مرة في أربعينيات القرن الماضي عندما تحدث عنها العالم الرياضي "فون نيو مان" فيما يتعلق بالحواسيب دون الانترنت، ومن أشهر الفيروسات فيروس "رسائل الحب" وفيروس "الدودة الحمراء"، حيث تسبب هذا الأخير في تعطيل أكثر من ربع مليون جهاز كمبيوتر في اقل من 9 ساعات عام 2001. [3]

2-جرائم الاختراقات:

يعرف الاختراق بأنه الدخول غير المصرح به إلى أجهزة الغير والشبكات الالكترونية، ويتم هذا الاختراق باستخدام برامج حديثة ومتطورة من قبل أشخاص لهم القدرة والخبرة الكافية لتجاوز أي إجراءات أو أنظمة حماية من اجل حماية تلك الشبكات أو الحاسبات.

---

[1]- محمد أمين احمد الشوابكة، مرجع سابق، ص114

[2]- محمد أمين احمد الشوابكة، مرجع سابق، ص136

[3]- منير محمد الجمبيهي ممدوح محمد الجمبيهي، مرجع سابق، ص 36

تختلف دوافع الاختراق باختلاف نوايا المخترقين، فالبعض منهم يقوم باختراق أجهزة الآخرين ومواقعهم بدافع الفضول فقط بينما هناك من يسعى إلى سرقتها، وهذا هو الدافع الأساسي الذي يدفع المخترقين للوصول إلى حواسيب الآخرين والاستيلاء على معلومات قد تكون عرضت مقابل مبلغ مالي للاطلاع عليها.

وقد يكون الدافع هو التلاعب بالمعلومات أو تعديلها أو تعطيلها على أجهزة الآخرين، وهو من أخطر أشكال الاختراق، حيث تعد مواقع الانترنت من أبرز ضحايا الاختراق التي يقوم المحترفون بتغيير شكلها أو محتواها. [1]

3-جريمة تعطيل الأجهزة والشبكات:

هي إيقاف أو تعطيل عمل أجهزة الحاسب الآلي عبر برامج، مما قد يسبب تعطيلات تقنية قد تؤثر على المكونات الاليكترونية للجهاز والغاية من هذا النوع من الجرائم هو إيقاف الحواسيب والشبكات من أداء وظائفها دون الحاجة إلى تنفيذ اختراق مباشر لتلك الأجهزة، حيث يتم هذا التعطيل من خلال إرسال كميات كبيرة من الرسائل بشكل مدروس ومنظم إلى الأجهزة المستهدفة، وهذا ما يؤدي إلى إيقافها عن تنفيذ عملها.[2]

4-جريمة النصب والاحتيال:

أصبح التعاقد الاليكتروني ضرورة حتمية في وقتنا هذا، وذلك نظرا لسهولة وسرعة التعامل عبر الانترنت، ومع كل هذا فقد ظهرت العديد من السلبيات وهي عبارة عن أفعال إجرامية تعرف النصب والاحتيال من أبرزها:

استخدام طرق احتيالية جديدة لخرق التعاملات الالكترونية وهذا ما أدى إلى زيادة جرائم النصب التي لا يزال العديد من مستخدمي الانترنت يقعون فيها.

من أهم مظاهر الاحتيال سرقة معلومات البطاقات الائتمانية واستخدامها لسرقة أموال الضحايا الموجودة داخل حساباتهم، ويسهل على مرتكبي هذه الجرائم الفرار وتواريهم مما يصعب ملاحقتهم والقبض عليهم.[3]

[1]– منير محمد الجمبيهي ممدوح محمد الجمبيهي، نفس المرجع السابق، ص37

[2]– المرجع نفسه، ص38

[3] –عبد الكريم شيباني، مرجع سابق، ص 23

ثالثا: الجرائم الواقعة على امن الدولة

تتمثل في جريمتي المساس بأمن الدولة وكذلك الإرهاب الالكتروني:

1-الإرهاب الإلكتروني:

يعد الإرهاب الالكتروني من اخطر الجرائم الإلكترونية ، حيث أصبحت الإنترنت وسيلة لنشر وترويج أفكار المنظمات الإرهابية والتعبير عن معتقداتها، مما يؤدي إلى محاولة التأثير على العقائد الدينية لأفراد المجتمع وتقاليده مما يخلق الفوضى ويزعزع الاستقرار ويمس بأمن الدولة ، و يمكن أن يتم هذا النوع من الجرائم من خلال تعاون عدة أفراد بهدف الإضرار بالبلد، وقد تكون بالإشادة بالأفعال الإرهابية المرتكبة ضد الدولة أو من خلال استهداف المؤسسات العسكرية وإلحاق الأذى بهم، عن طريق استخدام فيروسات مدمرة أو تعطيل الأنظمة الإلكترونية، واستغلال المؤيدين للفكر المتطرف في تنفيذ هذه الأنشطة.[1]

2-جريمة التجسس على الدولة:

تعتبر من اخطر التهديدات التي تمس بأمن الدولة، سواء في المجال الأمني أو الاقتصادي من طرف الدول المعادية بتجميع الأسرار وتموين بالأخبار فيستهدف التجسس الأسرار العسكرية، عن طريق قرصنة المواقع الحكومية والرئاسية أو اختراقها وبالتالي الاطلاع على أسرار الدولة العسكرية والاقتصادية حيث أن استهداف الدفاع الوطني للدولة والهيئات العسكرية يتم بواسطة أشخاص أو منظمات يتواجدون خارج البلاد والتجسس يكون على المواقع و المنظمات والشخصيات العسكرية، إما في الجانب الاقتصادي يتم على اقتصاد والمؤسسات الاقتصادية التابعة للدولة تكون من قبل عملاء من دولة معادية أو حتى صديقة لكشف الأسرار الاقتصادية، أو من شركة على شركة منافسة في نفس المجال فهي معلومات سرية مؤمنة لا يسمح بالاطلاع عليها لأنها أسرار دولة، لكن الاختراق يكشف عن الحماية وخاصة إذا كانت أنظمة الحماية ضعيفة.[2]

[1]– مصطفى يوسف كافي، جرائم الفساد غسيل الأموال السياحة الإرهاب الالكتروني المعلوماتية، مكتبة المجتمع العربي للنشر والتوزيع، الأردن، ط1، 2015، ص143

[2] –خالد حسن احمد لطفي، جرائم الانترنت بين القرصنة الالكترونية وجرائم الابتزاز الالكتروني، دار الفنر الجامعي، الإسكندرية، د ذ ط، 2019، ص38

المبحث الثاني: أركان الجريمة الإلكترونية ودوافع ارتكابها

بعد أن تطرقنا في بداية بحثنا إلى ماهية الجريمة الالكترونية، سنناقش في هذا المبحث أركان الجريمة الالكترونية في المطلب الأول، ودوافع ارتكابها في المطلب الثاني.

المطلب الأول: أركان الجريمة الالكترونية

لا تختلف الجريمة الالكترونية عن الجريمة العادية في اشتراط توفر أركان لقيامها على الرغم من ارتكابها في الفضاء الافتراضي، فهناك ركن شرعي وركن مادي وركن معنوي، وكل نوع من هذه الأركان يختص بميزة عن جريمة أخرى. تتميز هذه الأركان بالافتراض لكونها ترتكب في العالم الافتراضي ونلخصها كما يلي:

الفرع الأول: الركن الشرعي:

يقصد به أن هناك نص قانوني يجرم الفعل ويحدد العقاب المترتب عليه وقت وقوع هذا الفعل، وبناء على هذا لا يجوز معاقبة الشخص عن فعل ارتكبه قبل صدور نص تشريعي يجرم الفعل الذي قام به، أو بعد إلغاء نص التجريم كما لا يجوز قياس أفعال لم يرد نص على تجريمها و افعال نص المشرع على تجريمها مهما كان هناك تشابه بينهما من حيث الدوافع أو النتائج أو الفاعلية أو العناصر، وأيضا لا يجوز التوسع في تفسير النصوص الجزائية، وعلى القضاة التقيد بمدلول النص والالتزام بمضامينه.[1]

عند إهمال قاعدة شرعية الجرائم والعقوبة يؤدي إلى نتيجة مهمة، وهي عدم رجعية القاعدة الجنائية، وهذا يعني أن القواعد الجنائية تطبق بأثر فوري ولا يمكن إهمالها بأثر رجعي، إلا إذا نص عليها القانون صراحة أو إذا ما تم تطبيق القانون الأصلح للمتهم.[2]

يتطلب الركن الشرعي للجريمة ركنين أساسيين هما:

-مطابقة الفعل لنص التجريم.

---

[1]- أسامة احمد المناعة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الالكترونية، الطبعة الثالثة، دار النشر والتوزيع، عمان2014، ص45

[2]- حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، ب يروت2014، ص57

– إلا يخضع الفعل المرتكب لسبب من أسباب الإباحة.

مطابقة الفعل لنص التجريم تعني تطابق الأفعال التي يجرمها القانون مع النصوص التشريعية الموجودة، وفيما يتعلق بخضوع الفعل لسبب من أسباب الإباحة، فقد ذهب اجتهاد المحكمة العليا إلى انه لتطبيق نظرية العقوبة المبررة، يجب أن يكون النص الواجب التطبيق يقرر نفس العقوبة.[1]

الفرع الثاني: الركن المادي

يشمل الركن المادي للجريمة كل فعل أو سلوك إجرامي صادر عن شخص سليم الإدراك، سواء كان هذا التصرف إيجابي أو سلبي، حيث يترتب عليه أثر يعتدي على أحد الحقوق التي يحميها الدستور والقانون. وقد قسم الدكتور رضا فرح الركن المادي إلى ثلاث عناصر:

–السلوك الإجرامي.

–النتيجة الإجرامية.

–العلاقة السببية بين الفعل والنتيجة.

أ–السلوك الإجرامي:

يتخذ السلوك الإجرامي شكلين أساسيين، فقد يتمثل في فعل إيجابي يصدر عن الجاني بصورة إرادية بهدف إحداث نتيجة معينة، وقد يكون الفعل سلبي من خلال الامتناع عن القيام بفعل يفرضه القانون، وفي إطار الجرائم المعلوماتية يمكن إن نجد كلا الطرفين السلوك الإيجابي والسلوك السلبي.

كما انه يوجد تطور هائل في طبيعة ومضمون هذا السلوك الإجرامي، ذلك نتيجة لتطور الأدوات والوسائل التكنولوجية المتاحة للجاني، وقد ساهم ذكاء الفاعل في تجاوز الأساليب التقليدية للجريمة والانتقال إلى مستويات أكثر تعقيدا مما خلقت دون شك صعوبات وتحديات كثيرة. [2]

ب–النتيجة الإجرامية:

[1]– إبراهيم بلعليات، اركان الجريمة وطرق اثباتها في قانون العقوبات الجزائري، الطبعة الأولى، دار الخلدونية، الجزائر، 2007، ص94–95

[2] – أسامة احمد المناعة، جلال محمد الزغبي، المرجع السابق، ص 51–52

يقصد بها الأثر المادي الملموس الناتج عن السلوك الإجرامي، حيث يحدث هذا السلوك تغييرا ظاهرا، كما أن مفهوم النتيجة يقوم على أساس ما يعتد به المشرع وما يترتب عليه من نتائج، بغض النظر عن النتائج الأخرى التي يحدثها السلوك الإجرامي.[1]

ج-العلاقة السببية بين الفعل والنتيجة:

تتمثل في العلاقة التي تربط بين السلوك الإجرامي والنتيجة المترتبة عليها، حيث تثبت أن الفعل المرتكب هو السبب الأساسي في وقوع النتيجة، كما أن أهمية هذه الرابطة السببية تكمن في إسناد النتيجة إلى الفعل، وتعد هذه العلاقة شرطا جوهريا لتحميل الفاعل المسؤولية عن النتيجة، وتحقيق العلاقة السببية يقتضي وجود ارتباط مادي مباشر بين الفعل والنتيجة، فإذا لم يتوافر هذا الترابط فان مسؤولية الجاني تقف عند حد الشروع، ولا يسأل عن النتيجة التي حدثت فعلا، إما في الجرائم الغير عمدية فان غياب الرابطة السببية يؤدي إلى انعدام المسؤولية الجنائية كليا، لأنه لا شروع في الجرائم الغير عمدية[2]

الفرع الثالث: الركن المعنوي:تعتبر الجرائم المعلوماتية مثل باقي الجرائم، حيث تتطلب وجود نية واضحة وإرادة لتحديد المسؤولية القانونية،كما لا يمكن أن كون هناك نية خاصة للجريمة بدون وجود نية عامة، أما بالنسبة للنية الخاصة في الجرائم المعلوماتية فهي تعتمد بشكل أساسي على نوع الجريمة المرتكبة والهدف الذي يسعى له الجاني عند القيام بالفعل الغير قانوني، يتكون الجانب المعنوي للجريمة الإلكترونية من عنصرين: العلم والإرادة

-العلم: يعني فهم الشخص لما يحدث.

-إما الإرادة: فهي توجه الشخص نحو القيام بفعل غير قانوني لتحقيق نتيجة معينة.

وفقًا للقوانين العامة في قانون العقوبات، يمكن أن يكون القصد الجنائي عامًا أو خاصًا:

-فالقصد الجنائي العام: هو الهدف المباشر من الفعل الإجرامي ويقتصر على القيام بالفعل.

-أما القصد الجنائي الخاص يحتاج إلى شروط معينة في بعض الجرائم، حيث لا يكتفي الجاني بمجرد ارتكاب الجريمة، بل يسعى للتأكد من حدوث النتيجة.

[1]- بلعليات إبراهيم، المرجع السابق، ص18

[2]- أسامة احمد المناعة، جلال محمد الزغبي، المرجع السابق، ص 58-59

على سبيل المثال: في جريمة القتل، لا يكتفي القاتل بفعل القتل فقط، بل يتأكد من وفاة الضحية وبالتالي، ما هو القصد الجنائي المطلوب في الجريمة الإلكترونية؟

الفاعل في الجريمة الإلكترونية يقوم بتصرف غير قانوني وهو يعرف ذلك ويقصده. و بالتالي، فإن القصد الجنائي العام موجود في جميع الجرائم الإلكترونية دون استثناء، لكن بعض الجرائم الإلكترونية قد تحتوي أيضًا على قصد جنائي خاص، مثل تشويه السمعة عبر الإنترنت أو نشر الفيروسات. في النهاية، يعود الأمر للقاضي لتقدير الحالة.[1]

أما بالنسبة لإثبات وجود القصد في الجرائم المعلوماتية، فإن ذلك يكون مسؤولية النيابة العامة والمحكمة المختصة، المحكمة هي التي تقرر ما إذا كان هناك سوء نية أو لا، وهي الوحيدة التي تملك القرار النهائي في القضايا المقدمة أمامها.[2]

المطلب الثاني: دوافع ارتكاب الجريمة الإلكترونية

على الرغم من التقدم الذي أحرزته الأبحاث في مجال علم الجريمة، إلا أن إحدى الصعوبات التي يواجهها الباحثون في هذا المجال هي تحديد العوامل والدوافع الكامنة وراء الجريمة بشكل عام والجريمة الإلكترونية بشكل خاص، وإن إقدام شخص على ارتكاب جريمة إلكترونية لا يكون بدون سبب معين بل هناك العديد من الدوافع التي تتحكم فيه وتحثه على ارتكاب هذا الفعل.

ويمكن تصنيف هذه الدوافع إلى فرعين دوافع شخصية في الفرع الأول ودوافع خارجية في الفرع الثاني.

الفرع الأول: دوافع شخصية

يمكن تصنيف الدوافع الشخصية لدى مرتكب الجريمة الإلكترونية إلى دوافع مالية ودوافع ذهنية وذلك من حيث تأثير الدافع المادي في تحقيق الربح كعامل محفز لارتكاب الجريمة الإلكترونية، أو تأثير العوامل الذهنية على المجرم الإلكتروني وحثه لارتكاب هذه الأخيرة.

---

[1]– فضيلة عاقلي، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر"الجرائم الالكترونية"، طرابلس، بتاريخ 25–24، مارس 2017، ص120

[2]– لورنس سعيد الحوامدة، "الجرائم المعلوماتية أركانها و آليات مكافحتها" دراسة تحليلية مقارنة، مجلة ديوان للجلسات القانونية والشرعية، الأردن، 2016/08/13، ص24

أولا: دوافع مادية:

يعتبر الدافع المالي من أهم دوافع التي تدفع المجرم لارتكاب الجريمة الإلكترونية، لأن الأرباح الضخمة التي تنتج من خلالها تدفع بالمجرم الإلكتروني إلى تطوير نفسه كي يواكب مستجدات تكنولوجيا المعلومات، ويستغل كل الفرص ساعيا للاحتراف كي يحقق أعلى مكسب بجهد قليل دون ترك أي أثر ومن أجل تحقيق الربح يتلاعب الجاني بأنظمة المعالجة الآلية للبنوك و المؤسسات المالية إذا كان أحد موظفيها أو من خلال اختراق أنظمة المعالجة الآلية الخاصة بها من خلال اكتشاف ثغراتها الأمنية، ثم العمل على استغلال هذه الأنظمة وبرمجتها لتحويل مبالغ مالية كبيرة إلى حسابه أو حسابات شركائه أو حساب من يعمل لصالحهم إذا كان خارج المؤسسة ويمكن أيضا الحصول على مكاسب مالية عن طريق المساومة على البرامج أو على المعلومات المتحصل عليها نتيجة السرقة من جهاز الحاسوب وتشير المجلة المتخصصة في الأمن المعلوماتي securité informatique أن 43٪ من حالات الغش المعلن عنها قد تمت لغرض اختلاس الأموال و23٪سرقة المعلوماتو19٪ أفعال الأخلاق و15٪ الاستعمال الغير قانوني للحاسوب من أجل تحقيق مكاسب شخصية و في حال نجاح الجاني الإلكتروني في ارتكاب جريمته فسوف يحقق أرباح ضخمة في وقت صغير ويمكن توضيح الأرباح المالية التي يحققها من هذا الفعل من خلال أحدث خلاصة لإحدى الدراسات الواردة عن التقرير السادس لمعهد أمن المعلومات حول جرائم الكمبيوتر أين أجريت هذه الدراسة بمشاركة 538 مؤسسة أمريكية تجمع وكالات حكومية وبنوك ومؤسسات صحية و جامعات أين أظهرت حجم الخسائر التي خلفتها الجريمة المعلوماتية حيث تبين أن 85٪ من المشاركين في هذه الدراسة تعرضوا لاختراقات لأنظمة المعلوماتية و64٪ أصابتهم خسائر مادية نتيجة هذه الاعتداءات. [1]

ثانيا: دوافع ذهنية:

هي المتعة والتسلية والتحدي والرغبة في فهم الأنظمة المعلوماتية ومحاولة إبراز الذات، في غالب الأوقات ما يكون الباعث لدى مرتكبي الجرائم الالكترونية السعي لإبراز الذات،وتحقيق الفوز على أنظمة المعلوماتية، دون أي نوايا مجرمة فيعملون لخرق هذه الأنظمة وإبراز تفوقهم وفوزهم عليها،ويعتبر دافع

[1]– سعيدان نعيم، آليات البحث و التحري عن الجرائم المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجيستر في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة ،2012–2013 ص 60 ص 61و نقلا عن نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة 2،2010، ص90 نقلا عن ضاح محمود الحمود و نشأت مفقي المجالي ، جرائم الأنترنت ، دار المنار لنشر و التوزيع ،2005 ص 31

المزاح والترفيه من الدوافع و الأسباب التي تحمل الفرد للقيام بهذه التصرفات حتى وإن كان غير قاصدا القيام بجريمة لكن قد يترتب عليها نتائج ترتقي لدرجة الجريمة.[1]

الفرع الثاني: دوافع خارجية:

يتأثر المجرم الإلكتروني ببعض العوامل من الممكن أن تكون سببا لاقترافه جريمة معلوماتية ولا يسعى فيها لا للتسلية ولا لإظهار وإبراز ذاته ولا حتى لكسب المال ويمكن إبراز هذه الدوافع من خلال هذا الفرع.

أولا: دافع الانتقام و إلحاق الضرر برب العمل:

يعتبر هذا الدافع من أخطر الدوافع لارتكاب الشخص للجريمة الإلكترونية، فلانتقام غريزة متأصلة في النفس البشرية فالعديد من الأفراد الموظفين يفصلون تعسفيا من دون حق من وظائفهم، بالرغم من أنهم يملكون ويحملون معلومات كافية بخفايا تلك الجهة المفصلون منها، لذلك يرتكب الجاني الإلكتروني هذه الجريمة بهدف الانتقام، وجعل تلك المؤسسة المطرود منها تعاني وتتكبد خسائر مالية ضخمة تتطلب وقت معين لإصلاح ما حل بها.[2]

كذلك يكون هذا الدافع نتيجة تخطي الموظف في الحوافز أو الترقيات الممنوحة في بيئة عمله فكل هذه الأمور تجعله يقدم على القيام بالجريمة. [3]

ثانيا: دافع التعاون والتواطؤ:

يعتبر هذا النوع كثير التكرار والحدوث في الجرائم الإلكترونية وفي أغلب الأوقات يصدر من متخصص في النظم المعلوماتية، والكثير من مجرمي هذه الجرائم يشكلون جماعات في هذا المجال للقيام بتلك الجريمة ويسعون للتعاون على ممارستها بدقة لغرض تحقيق أهداف مشتركة بينهم، أين يقوم بالجانب الفني من المشروع الإجرامي متخصص في الأنظمة المعلوماتية وشخص آخر من خارج المؤسسة

[1]– يوسف صغير، الجريمة المرتكبة عبر الأنترنت، مذكرة ماجيستير منشورة، تخصص قانون دولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو،2013، ص 40–41

[2]– بن مكي نجاة، السياسة الجنائية لمكافحة الجرائم المعلوماتية، منشورات دار الخلدونية، 2017 ص 43/42

[3]– صغير يوسف، رسالة ماجيستير، مرجع سابق، ص 42

المرتكب ضدها الجريمة حيث يقوم بتغطية عمليات التحويل وتغير المكاسب المالية، وفي الكثير من الأحيان تكون أنشطتهم بصورة منظمة. [1]

ثالثا: دافع جنون العظمة أو الطبيعة التنافسية:

هذه الطبيعة قد تدفع العاملين والموظفين داخل المنشأة لإبراز مهارتهم في إدارة المنشأة، فيؤذي هذا لارتكاب مثل هذه الجرائم حتى يتنافس مع باقي العاملين في بلوغ مناصب مرموقة. [2]

رابعا: دافع الضغوطات العامة:

وهي الضغوط التي يواجهها المجتمع كالبطالة والفقر والظروف الاقتصادية الصعبة، والتي تعتبر من الضغوطات على المجتمع بشكل عام وعلى مجتمع الشيباني بشكل خاص، والتي تجعل لدى قسم كبير من السكان مشاعر سلبية تجاه المجتمع، مما يجعلهم يتكيفون بشكل سلبي مع هذه المواقف الصعبة. [3]

كانت هذه أبرز الدوافع لارتكاب الجرائم الإلكترونية بالرغم من أنها ليست ثابتة ومعتمدة لدى الفقهاء والباحثين لأن ببساطة السلوك الإجرامي يتغير وتتغير معه أسباب الارتكاب.

خامسا: دافع الرغبة في قهر النظام والتفوق على تعقيد الرسائل التقنية:

يميل مرتكبو هذا النوع الجرائم إلى إبراز تفوقهم و مهاراتهم المتقدمة و براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة و يحاولون إيجاد و غالبا ما يوجدون الوسيلة التي تحيطها، و مع تزايد شيوع هذا الدافع لدى فئة الشباب من مرتكبي الجرائم الإلكترونية الذين يمضون وقتا طويلا أمام حواسيبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الحواسيب و شبكة المعلومات لإظهار تفوقهم على رسائل تقنية، وإن هذا الدافع هو أكثر المحفزات التي تستغلها منظمات

[1]– سعيداني نعيم، آليات البحث والتحري عن الجرائم المعلوماتية في القانون الجزائري، مرجع سابق، ص 62/61

[2]– لغويلي ليلى، الجريمة الإلكترونية، مذكرة لنيل شهادة ماستر في القانون، تخصص قانون العقوبات والعلوم الجنائية،كلية الحقوق، جامعة قسنطينة 1، 2013/2012 ص 33

[3]– ذياب موسى، الجرائم الإلكترونية، المفهوم والأسباب الملتقى العلمي للجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية، كلية العلوم الإستراتيجية،الأردن، 2014 ص 15

الجريمة ، لأجل استرجاع محترفي الاختراق إلى قبول المشاركة في أنشطة إعتداء معقدة أو إستجارهم للقيام بالجريمة و هذا وإن كان الحل الواحد.[1]

سادسا: الولع في جمع المعلومات وتعلمها:

يرى قراصنة الحاسوب أن المعلومات يجب أن تكون متاحة دون قيود، ولذلك يكرّسون جهودهم لتعلم طرق اختراق المواقع المحظورة، وغالبًا ما يعمل هؤلاء القراصنة ضمن مجموعات، يكون هدفها الأساسي تبادل المعلومات، ومشاركة البرامج والأخبار التقنية، كما يحرص القراصنة على الحفاظ على هويتهم مجهولة لتمكينهم من البقاء داخل الأنظمة المستهدفة لأطول فترة ممكنة دون انكشاف.[2]

[1]– بوديسة بجاد عبد الرؤوف، آليات التحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر مهني في القانون، كلية الحقوق، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2022/2021، الصفحة 25

[2]– بن مكي نجاة مرجع سابق صفحة 43

ملخص الفصل الأول:

تعتبر الجريمة الإلكترونية من أبرز مظاهر الإجرام المستحدث في العصر الرقمي، اذ تحدث إما على التعدي على البيانات والمعلومات بمختلف أشكالها التقنية أو لارتكاب جرائم أخرى في بيئة رقمية افتراضية، وفي هذا الفصل تم التطرق إلى تعريفها من خلال استعراض العديد من الاتجاهات التي تناولت تعريفها، ثم بعد ذلك تم تحديد طبيعتها القانونية كما تم الوقوف على أهم الخصائص التي تميز هذه الجريمة.

وضمن نفس السياق تم عرض أبرز التصنيفات المعتمدة لأنواع الجرائم الإلكترونية، و في الأخير لم يغفل الفصل أيضا الحديث عن الأركان القانونية اللازمة لقيام الجريمة الإلكترونية، إضافة إلى الدوافع المختلفة لارتكاب هذا النوع من الجرائم.

الفصل الثاني

طرق و آليات مكافحة الجريمة الإلكترونية

تمهيد:

في ظل التطورات الواسعة الحاصلة في مجال العلوم الرقمية والتكنولوجية واستحداثها، تنوعت وتعددت سبل الجريمة الإلكترونية وأصبحت أشد ضررا، حيث أصبح من اللازم وضع طرق وآليات فعالة لمعالجة هذه الظاهرة والحد من انتشارها و تفشيها.

لذلك سوف نستعرض في هذا الفصل مبحثين، المبحث الأول يتضمن الأجهزة المختصة بالمكافحة والمبحث الثاني إجراءات المتابعة.

المبحث الأول: الأجهزة المختصة بالمكافحة

تسهم الأجهزة المختصة بمكافحة الجريمة الإلكترونية بشكل كبير ومباشر على مواجهة التهديدات والهجومات السيبيرانية على البنى الرقمية وتأمينها، كما أنها تعزز مستوى الحماية للمؤسسات ومستخدمي وسائل التكنولوجيا الحديثة، كما تلعب دورا بارزا في تقوية وتدعيم التعاون الدولي للحد من هذه الظاهرة.

المطلب الأول:الأجهزة الوطنية

وجد المشرع الجزائري نفسه أمام ضرورة ملحة للتصدي لظاهرة الإجرام الإلكتروني وما يصاحبها من أضرار معتبرة على الأفراد والمؤسسات، فاستحدث أجهزة خاصة بالمكافحة مهمتها الوقاية ومحاربة هذه الجريمة.

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

تعود فكرة إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال إلى سنة 2009 بتاريخ 05اوت 2009، وتعتبر الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي ومقرها الجزائر العاصمة.

أولا:اختصاصات الهيئة

بينت الفقرة 02 من المادة 04 من المرسوم الرئاسي 15/261 المهام الأساسية التي تقوم بها الهيئة الغرض منها الوقاية من الجرائم المعلوماتية والتصدي لها، أبرز مهام هذه الهيئة هي:

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

-تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مكافحتها.

-مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدها بالمعلومات والخبرات القضائية.

-تنفيذ الطلبات الصادرة عن الدول الأجنبية وتطوير سبل التبادل معها.

-تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المعلوماتية.[1]

ثانيا: تشكيلة الهيئة وطبيعة عملها

1-تشكيلة الهيئة الإدارية:

تتشكل من اللجنة التي تدير إضافة إلى مديرية عامة، اللجنة التي تدير تتكون من الوزير المكلف بالعدل رئيسا إضافة إلى الوزير المكلف بالداخلية والوزير المكلف بتكنولوجيات الإعلام والاتصال وقائد الدرك الوطني والمدير العام للأمن الوطني وممثلين أحدهما عن رئاسة جمهورية وآخر عن وزارة الدفاع وقاضيان من المحكمة العليا، أما المديرية العامة يترأسها مدير عام معين بموجب مرسوم رئاسي.[2]

2-تشكيلة الهيئة التقنية:

تضم الهيئة مديريات مهمتها إنجاز المهام التقنية المتعلقة بالوقاية وبمكافحة الجرائم المعلوماتية وهذه المديريات هي:

-**مديرية المراقبة الوقائية واليقظة الإلكترونية:**لم يشر المرسوم الرئاسي 261 /15 إلى تشكيلة هذه المديرية، تعمل هذه المديرية على إنجاز المهام التالية:

-تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية.

-إرسال المعلومات المتحصل عليها إلى السلطات القضائية ومصالح الشرطة القضائية.

-جمع كل المعلومات واستغلالها من أجل الكشف عن الجرائم المعلوماتية.

-المشاركة في حملات توعوية حول مخاطر تكنولوجيا الإعلام والاتصال.

[1]- عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات شهادة ماستر مهني، جامعة قاصدي مرباح، ورقلة 2019/2018، صفحة34

[2]- المواد 06 إلى 10 من المرسوم الرئاسي 15/261 الذي يحدد تشكيلة وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

من خلال مهامها يمكن إطلاق وصف على هذه المديرية بأنها المركز العمليات للهيئة.[1]

-**مديرية التنسيق التقني:** لم ينص المرسوم الرئاسي 15/261 على تشكيلة هذه المديرية، حيث تختلف عن مديرية المراقبة الوقائية واليقظة الإلكترونية من حيث المهام ولعل مهامها تتمثل في:

-انجاز الخبرات القضائية في مجال اختصاص الهيئة.

-تكوين قاعدة معطيات تحليلية للإجرام المعلوماتي.

-إعداد الإحصائيات الوطنية للإجرام المعلوماتي.

-تسيير المنظومة المعلوماتية وإدارتها.[2]

الفرع الثاني: الأجهزة الأمنية

أولا: جهاز الأمن الوطني

الوحدات التابعة لهذا الجهاز هي:

1-على المستوى المركزي:تعمل هذه الوحدات على مكافحة نوع معين من الجرائم دون غيرها، حيث استحدث مصلحة مختصة في مكافحة الجريمة الإلكترونية أطلقت عليها تسمية نيابة مديرية مكافحة الجرائم

المتصلة بتكنولوجيات الإعلام والاتصال زيادة إلى ذلك نيابة مديرية الشرطة العلمية والتقنية مهمتها البحث والتحري عن الجرائم المعلوماتية والمخبر المركزي للشرطة العلمية المتمركز في الجزائر العاصمة، حيث يتولى القيام بمهمة البحث والتحقيق وتحليل الأدلة الجنائية المختلفة.[3]

[1]- المواد 11.13.14.18.21 من المرسوم 15/261 مرجع سابق

[2]- المادة 12 من المرسوم الرئاسي 15/261 مرجع سابق

[3]- مساهمة المخبر الجهوي للشرطة العلمية في كل من قسنطينة ووهران في إدارة الدليل ضمن التقنيات الخاصة للتحقيق – وثيقة خاصة صادرة عن نيابة مديرية الشرطة العلمية والتقنية، مديرية الشرطة القضائية، المديرية العامة للأمن الوطني صفحة 02،03

2-على المستوى الجهوي: تم انشار مخابر جهوية للشرطة العلمية في كل من ولاية قسنطينة و وهران بالإضافة إلى03 قيد الإنجاز.[1]

يوجد على مستوى كل مخبر مصلحة تدعى بدائرة الأدلة الرقمية والآثار التكنولوجية و تضم هذه الدائرة 03 أقسام وهي:

-قسم استغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات.

-قسم استغلال الأدلة الناتجة عن الهواتف النقالة.

-قسم تحليل الأصوات.

وتتكون الدائرة من 08 أعضاء محققين 04 منهم يتمتعون بصفة ضابط شرطة قضائية.[2]

وتعلب الدائرة دورا مهما للغاية في الكشف عن خفايا الجرائم المعلوماتية من خلال مختلف الإجراءات المباشرة سواء في مرحلة البحث والاستدلال من خلال الاستجابة لطلبات المقدمة لهم أو أثناء مرحلة التحقيق القضائي.

ثانيا: جهاز الدرك الوطني:

الوحدات التابعة لهذا الجهاز هي:

1-على المستوى المركزي: تعمل مصالح الدرك الوطني على مكافحة الجرائم الإلكترونية من خلال الهيئات التالية:

أ-مديرية الأمن العمومي والاستغلال.

ب-المصلحة المركزية للتحريات الجنائية.

[1]- حشمان عمار، الجريمة المعلوماتية، مرجع سابق، صفحة 38

[2]- حسن سعيداني آليات تحقيق في الجرائم المعلوماتية مرجع سابق صفحة 180

ج–مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية: أنشأ هذا المركز حديثا ويعتبر بمثابة نقطة وصل وطنية في مجال دعم أعمال البحث والتحري في الجرائم الإلكترونية.[1]

من أبرز مهامه:

–ضمان المراقبة الدائمة والمستمرة على شبكة الإنترنت.

–المشاركة في قمع الجرائم المعلوماتية من خلال التعاون مع مختلف مصالح الأمن والهيئات الوطنية.

–المشاركة في عمليات التحري والتسرب عبر شبكة الإنترنت لفائدة وحدات الدرك الوطني والسلطات القضائية.

د–المعهد الوطني للأدلة الجنائية وعلم الإجرام: يتكون هذا المعهد من إحدى عشر دائرة متخصصة في مجالات مختلفة جميعها تضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية ودائرة الإعلام الآلي الإلكتروني المكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة، كما تقدم مساعدات تقنية للمحققين في المعاينات.[2]

الفرع الثالث: المكافحة على ضوء قانون 04/09

كخطوة مستحدثة قام المشرع الجزائري بسن قانون 04/09 المتعلق بالوقاية من تكنولوجيات الإعلام و الاتصال و مكافحتها ، نتيجة لتفاقم الاعتداءات و الهجومات المعلوماتية على معطيات الحاسب الآلي يحتوي هذا القانون على 19 مادة و 6 فصول ، حيث الفصل الأول منه و الثاني يتضمنون أهداف القانون ومفهوم المصطلحات التقنية و التأكيد على احترام مبدأ المحافظة على سرية الاتصالات الإلكترونية ، و مراقبة الاتصالات الإلكترونية في مجال العمليات الاتصالية المنطوية على خطورة التهديدات ، ثم التأكيد على إلزامية عدم جواز إجراء عملية المراقبة إلا بإذن السلطة المختصة ، والفصل الثالث يتضمن القواعد الإجرائية المتعلقة بتفتيش المنظومة المعلوماتية ، و الفصل الرابع يحدد الالتزامات التي تقع على عاتق المتعاملين في مجال الاتصالات الإلكترونية و الفصل الخامس يتضمن إنشاء هيئة

[1]– بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة ،17/16 نوفمبر،2015، كلية الحقوق، جامعة بسكرة، صفحة 29

[2]– فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر، الجرائم الإلكترونية،طرابلس، 25/24 مارس 2017 صفحة 133

وطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال والأخير يتضمن المساعدة و التعاون القضائي الدولي.[1]

حيث أن هذا القانون وضع مجموعة تدابير وقائية وإجرائية للوقاية من هذه الظاهرة وطمسها أهمها:

أولا: المراقبة الإلكترونية:

سمح باللجوء لهذا الإجراء في حالات محددة على سبيل الحصر في المادة 04 من قانون09/04وتكون بموجب إذن صريح مكتوب من السلطات القضائية المعنية.[2]

ثانيا:الاستعانة بمزودي الخدمات للوقاية من الجرائم السيبيرانية:

يمكن الاستعانة بمزودي الخدمات للوقاية من الجرائم السيبيرانية من خلال تقديم المساعدة اللازمة لسلطات المكلفة بالتحقيقات القضائية لجمع وتوثيق البيانات ذات الصلة تاريخ ووقت ومدة الاتصال،وكذا المعطيات التي تسمح بالتعرف على المرسل والمرسل إليه أو المرسل إليهم بمحتوى الاتصالات في حينها، ومنها المعطيات التي تسمح بالتعرف على مستعملي الخدمة، خصائصها التقنية وكذا الإتصال.[3]

الفرع الرابع: التفتيش والحجز الوقائيين في المنظومات المعلوماتية

أولا: التفتيش الوقائي:

إذ يعد من الصلاحيات التي تدعم ضباط الشرطة والسلطات القضائيين على القيام بمهامهم في الوقاية من الجرائم، وهذا من خلال التفتيش في المنظومة المعلوماتية من خلال معطياتها بهدف نسخ المعطيات محل البحث، هذه المعلومات من شأنها المساعدة والإفادة في الكشف عن الجرائم ومرتكبيها، شرط ألا تمس بسلامة المنظومة المعلوماتية.[4]

---

[1] – بن مكي نجاة، السياسة الجنائية لمكافحة الجرائم المعلوماتية، مرجع سابق، ص 228، 229، 230

[2] – مهدي رضا، الجرائم السيبيرانية وآليات المكافحة في التشريع الجزائري، مجلة إليزا للبحوث والدراسات، المجلد 06، العدد 02،2021، صفحة 118

[3]– مهدي رضا،نفس المرجع صفحة 119

[4]– عقباش بريزة ومبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2022/2021، صفحة 41

ثانيا: الحجز الوقائي:

ويأتي هذا الحجز في إحدى الصورتين:

1-حجز عادي: يكون فيه الحجز كامل و شامل للمنظومة المعلوماتية التي تحتوي على كل المعطيات اللازمة للجريمة أو جزئها، و يتم تغيير الدلائل من آثار معنوية غير ملموسة إلى أدلة عادية ملموسة ، يمكن أن يكون التعامل معها عن طريق نسخها على دعائم تخزين إلكترونية مع نسخ المعطيات اللازمة لفهمها ، بعد ذلك يقوم المسؤول عن عملية التفتيش بوضع إحراز و يختم عليها و يحرر محضر بذلك مع ضمان سلامة المعطيات من التلف أو التخريب. [1]

2-حجز عن طريق منع الوصول إلى المعطيات:إذا أصبح من الصعب على مسؤول التفتيش حجز المعطيات وجب عليه استعمال كل الطرق الممكنة لجعل الدليل آمنا من التلف أو التخريب أو حتى التغيير وذلك عن طريق المنع من الدخول إليه من قبل أي شخص حتى يتم اتخاذ كافة التدابير الممكنة للولوج إلى هذا النظام للحصول على الأدلة وفي حالة ما إذا تبين أن هذه المعطيات تشكل جريمة يمكن لسلطات المعنية بمباشرة التفتيش الأمر بالأخذ بالإجراءات اللازمة لمنع الاطلاع عليها. [2]

المطلب الثاني: الأجهزة الدولية

لم تعد الجهود الوطنية كافية لمواجهة الجرائم الإلكترونية والحد منها، وهذا ما استدعى تدخل المجتمع الدولي بمختلف الهيئات والمنظمات المتخصصة، فأصبح من المهم تنسيق الجهود على الصعيد الدولي من اجل وضع إطار قانوني مشترك وتعزيز التعاون الولي، سواء كان ذلك من خلال الدعم التدريبي أو التقني أو من خلال تبادل المعلومات، أو عبر آليات قانونية تنبثق عن معاهدات ومؤتمرات دولية بهدف مجابهة التهديدات التي تواجه الأمن العالمي.

الفرع الأول: المعاهدات والمؤتمرات الدولية

تعتبر المعاهدات الدولية الأساس الذي يرتكز عليه التعاون الدولي في مجال مكافحة الجرائم الالكترونية، وقد تم عقد العديد من المعاهدات التي تعمل على تعزيز التعاون الدولي في هذا المجال.

[1]- عقباش بريزة ومبارك حنان، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مرجع سابق، صفحة42

[2]- حابت أمال، دور الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجلة درية للبحوث القانونية والسياسية صفحة 437

أولا: اتفاقية برن

تم التوقيع عليها سنة 1971 في سويسرا، حيث تعتبر الحجر الأساسي في مجال الحماية الدولية لحق المؤلف، حيث وقعت على هذه الاتفاقية 120 دولة من بينها مصر.[1]

نصت المادة تسعة من اتفاقية برن على منح أصحاب حقوق المؤلف حق استئثاري في التصريح بعمل نسخ من هذه المصنفات بأي طريقة كانت، وتم تعديل هذه الاتفاقية سنة 1979، وفي عام 1999 أصبح عدد الدول فيها 140 دولة. [2]

كما انه تمنح اتفاقية برن صاحب حق المؤلف الحق في أن يرخص أو يمنح أي ترجمة أو اقتباس أو بث إذاعي أو أي توصيل إلى الجمهور، كما تلزم الاتفاقية بتوقيع الجزاءات بغض النظر إذا كان المؤلف المعتدى عليه وطنيا أو أجنبيا. [3]

وبموجب هذه الاتفاقية تتمتع برامج الحاسب الآلي بالحماية وذلك باعتبارها أعمالا أدبية وفقا لما جاء فيها، تتيح اتفاقية برن لدول العالم الثالث بعض الحقوق مثل حق الترجمة المجانية للجامعات والاستفادة العلمية منها والغاية من هذه الاتفاقية هو حماية حقوق المؤلفين على مصنفاتهم الأدبية والفنية وهذا ما ميزها.[4]

تضمنت الاتفاقية أحكاما محددة بشأن المصنفات الأدبية والفنية المشمولة بالحماية، بالإضافة إلى الشروط المطلوبة للاستفادة من الحماية ومبدأ المعاملة بالمثل.[5]

كما تتضمن الاتفاقية الدولية مبادئ أساسية تحدد نطاق الحماية آلية تطبيقها، وهذه المبادئ تبقى ثابتة رغم حدوث أي تعديلات أو بروتوكولات تدخل على الاتفاقية، حيث يجب إن تكون هذه التعديلات متفقة مع هذه المبادئ والأسس.

---

[1]– المرسوم الرئاسي رقم 341/97 المؤرخ في 1997/09/13 المتضمن انضمام الجزائر مع التحفظ إلى اتفاقية برن المؤرخة في 09/09/ 1869 المتممة في باريس 1909/05/04 والمعدلة في 1997/09/28، ج.ر رقم 01 المؤرخة في 1997/09/14.

[2]– بن الأخضر محمد، جرائم الكمبيوتر والانترنت، مذكرة لنيل رتبة ضباط المدرسة العليا للشرطة، بن عكنون، 2007–2008، ص49

[3]– منير محمد الجنيهي وممدوح الجنيهي، مرجع سابق، ص201

[4]– شرابشة ليندة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية، القي في الملتقى الدولي حول التنظيم القانوني للأنترنت والجريمة الالكترونية، جامعة زيان عاشور الجلفة، 28/27 افريل 2009، ص7

[5]– عبد الله عبد الكريم، جرائم المعلوماتية والانترنت، منشورات الحلبي الحقوقية، بيروت، 2007، ص49

ويمكن حصر هذه المبادئ فيما يلي:

1-مبدأ المعاملة الوطنية:

يقصد به أن المصنفات الخاضعة لحماية الاتفاقية في إقليم دولة عضو تتمتع بنفس الحماية التي تتمتع بها المصنفات الوطنية في تلك الدولة،ويترتب على ذلك ان الدول الأعضاء في الاتفاقية تعتبر كأنها تشكل إقليما واحدا، بحيث يحظى اي مصنف تم نشره لأول مرة في اي جزء من هذا الإقليم، بنفس مستوى الحماية التي يتمتع بها أي مصنف آخر في جزء منه، وقد يحدث تفاوت ملحوظ بين معايير الحماية ومستوياتها وذلك من دولة إلى أخرى.

ومن نظام قانوني إلى آخر، حيث سعت اتفاقية برن الى وضع حد أدنى للحماية لضمان ألا يقل مستوى حماية المصنفات وفقا للاتفاقية عن مستوى معين نصت عليه أحكامها. [1]

2-مبدأ الحد الأدنى للحماية:

يعد هذا المبدأ محاولة من واضعي قواعد اتفاقية برن لمواجهة التفاوت التشريعي بين مستويات الحماية في الأنظمة القانونية المختلفة.[2]

وقد نصت الاتفاقية على تمتع المؤلفين بمجموعة من الحقوق التي تضمنها نصها، حيث تضمنت عدة قواعد موضوعية خاصة بحماية المصنفات الأدبية ومن بينها برامج الحاسوب إعمالا لاتفاقية تريبس التي صنفت البرمجيات ضمن المصنفات الأدبية.

كما نظمت اتفاقية برن الحد الأدنى من الحماية وألزمت الدول الأعضاء بعدم تقديم حماية تقل عن هذا المستوى الذي تم تحديده في الاتفاقية.

يتضح مما سبق أن مبرمج ومصمم البرامج يمنح نفس الحقوق التي يحصل عليها مؤلفو المصنفات التي

تدخل ضمن نطاق الاتفاقية، والتي يتمتع بمقتضاها المؤلفون بحقوق مادية وأدبية.

---

[1]- رشا علي الدين، النظام القانوني لحماية البرمجيات، دار الجامعة الجديدة، الإسكندرية، 2007، ص241

[2]- طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر، 2011-2012، ص11

كما انه اختلفت النظم القانونية والفقهية في تطبيق هذه الحقوق على البرمجيات، فمن المعروف أن بعض أنواع البرامج لا يمكن تحليلها أو إدراكها بحواس الإنسان كالأذن والعين، ويلزم لفهمها الاستعانة بأدوات تقنية خاصة مثل برمجيات الهدف التي يتم معالجتها بلغة الكمبيوتر وتحويرها في صورة غير صورة الأصل وفك شفرتها أيضا.

وبسبب هذه المشكلة اعتبر البعض أن القيام بعملية فك التشفير لبرنامج الكمبيوتر يعد بمثابة تعديل وتغيير فيها مما يتطلب موافقة مسبقة من مؤلفها.[1]

وقد أثيرت العديد من الإشكالات حول حماية هذه البرمجيات في ظل اتفاقية برن التي حسمت فيها اتفاقية تريبس هذا الخلاف مقررة اعتبار البرمجيات مصنفات أدبية تحمي وفقا للأحكام المنصوص عليها في اتفاقية برن الخاصة لحماية المصنفات الأدبية والفنية، وهذه الحماية تكون على أساس معيارين رئيسيين:

أ-المعيار الشخصي:

يستند إلى شخصية مؤلف البرنامج من حيث جنسيته أو محل إقامته، فاتفاقية برن تقرر اشتمال الحماية للمصنفات التي يعتبر مؤلفوها من رعايا إحدى دول اتحاد برن سواء كانت هذه المصنفات منشورة أو لا.

ب-المعيار الإقليمي:

يعتمد على مكان النشر الأول للمصنف، وفقا لهذا المعيار تمنح الحماية للبرمجيات إذا ما نشرت في إحدى دول الأعضاء بغض النظر عن جنسية المؤلف أو محل إقامته المعتاد.[2]

وتقوم اتفاقية برن على مبدأين أساسيين يتمثلان في المساواة بين المؤلفين الوطنيين والأجانب، ووضع حد أدنى يجب ألا تقل عنه الحماية التي تلقاها أي من المصنفات المتمتعة بحمايتها، ويجري تطبيق هذان المبدآن على جميع أقاليم الدول الأعضاء في معاهدة برن، باستثناء دولة أصل المصنف، فالاتفاقية تستبعد أحكامها الخاصة بالحماية في دولة الأصل.

---

[1]- الحاج الطاهر زهير، آليات الوقاية من الجريمة المعلوماتية ومكافحتها، مذكرة الحصول على شهادة الماجستير في فرع القانون الجنائي، كلية الحقوق، جامعة الجزائر، 2012-2013، ص11

[2]- رشا علي الدين، مرجع سابق، ص24

إن اتفاقية برن لم تعالج النشر الإلكتروني عبر شبكة الإنترنت، وذلك لأن آخر تعديل لها كان عام 1971 أي قبل ظهور عصر الاتصالات والمعلومات وانتشار الإنترنت، لذا فإن الاتفاقية تبدو غير كافية لمعالجة الإشكاليات القانونية الناتجة عن المصنفات المنشورة على شبكة الإنترنت،حيث يمكن القول بان استكمال الحديث عن البرمجيات لا يكتمل دون التطرق التفصيلي لاتفاقية برن حتى نكون أمام صورة واضحة لحماية البرمجيات في ظل أحكام القانون الدولي الإتفاقي.[1]

ثانيا: معاهدة الويبو

تنقسم معاهدة الويبو إلى ثلاث معاهدات وهي كالتالي:

1-معاهدة الويبو بشأن حق المؤلف:

تم التوقيع على هذه المعاهدة في 20 ديسمبر 1996، وتتضمن ثمانية عشر مادة، وقد بنيت على مجموعة من الأسس والمبادئ.

تبدأ المعاهدة بديباجة ثم تبين علاقتها بمعاهدة برن، ثم تتعرض لنطاق تطبيق حماية حق المؤلف مثل حق التوزيع والتأجير ونقل المصنف إلى الجمهور والالتزامات المترتبة على المعاهدة ودخول المعاهدة حيز التنفيذ الفعلي، وتجدر الإشارة إلى أن المعاهدة قد واجهت في السنوات الأخيرة بعض التحفظات والانتقادات، سواء من أحد أفرادها الموقعين عليها أو من إحدى الدول غير الموقعة عليها.[2]

2-معاهدة الويبو بشأن الأداء والتسجيل الصوتي

تم التوقيع عليها في 20 ديسمبر 1996 حيث تتكون هذه المعاهدة من أربعة فصول، يختص الفصل الأول منها بالأحكام العامة،ويبين علاقة المعاهدة بالاتفاقيات الدولية الأخرى، إضافة إلى وضع تعريفات وتحديد المستفيدون من الحماية وفقا لما نصت عليه المعاهدة.

أما الفصل الثاني فيتناول حقوق فناني الأداء سواء من الجانب المعنوي أو المالي، ومن بين هذه الحقوق حق الاستنساخ، وحق التوزيع، وحق التأجير، وحق إتاحة الأداء المثبت، ويتناول الفصل الثالث حقوق المنتجين كحق إتاحة التسجيلات الصوتية وحق الاستنساخ والتأخير والتوزيع.

---

[1]- رشا علي الدين، مرجع سابق، ص253

[2]- محمود احمد عبابنة، جرائم الحاسوب و ابعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2009، ص160

إما الفصل الرابع فيتضمن الأحكام المشتركة كالحق في مكافأة مالية مقابل الإذاعة أو التنقل إلى الجمهور والاستثناءات على هذا الحق كمدة الحماية مثل الالتزامات المتعلقة بالتدابير التكنولوجية وأخيرا التعرض للإجراءات الشكلية.[1]

3-معاهدة الويبو بشأن الحماية الدولية لحق المؤلف والحقوق المجاورة

تتضمن هذه الاتفاقية مقدمة تسلط الضوء على الطبيعة القانونية للمعاهدتين الجديدتين، وتوضح علاقتهما بالاتفاقيات الدولية الأخرى، مع الإشارة إلى جدول الأعمال الرقمي كالمعاهدات الجديدة، كما تتعرض الاتفاقية إلى أحكام أخرى عن المعاهدتين الجديدتين.

وفي ختامها تركز على المتابعة بعد المؤتمر الديبلوماسي، حيث تهدف المنظمة العالمية للملكية الفكرية الويبو إلى:

-تدعيم اتخاذ الإجراءات التي تهدف إلى تسيير الحماية الفاعلة للملكية الفكرية في كافة أنحاء العالم.[2]

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

-تقديم الدعم الفني والقانوني والتدريبي في مجال العمل على الحماية الدولية للملكية الفكرية.

-منح الخدمات الفنية والقانونية والتدريبية في إطار العمل على الحماية الدولية للملكية الفكرية.

-تحمل مسؤوليات التسجيل في مجال الحماية الدولية للملكية الفكرية، مع نشر المعلومات والبيانات المتعلقة

بالتسجيلات كلما كان ذلك مناسبا وملائما.

[1]- منير محمد الجنيهي وممدوح محمد الجنيهي، مرجع سابق، ص204

[2]- نفس المرجع، ص206

لهذا نجد المنظمة منذ تأسيسها أنها قد سخرت إمكاناتها لتنفيذ رسالتها، وتحقيق أهداف نشأتها من خلال النهوض بحماية الملكية الفكرية على الصعيد الدولي، في ضوء التعاون الدولي والسهر على حماية حقوق المبتكرين كأصحاب حقوق الملكية الفكرية.[1]

تتسم معاهدة الويبو المتعلقة بحماية حقوق المؤلفين بدورها الهام في:

أ-حماية البرمجيات حيث نصت المادة 4 منها على أن برامج الحاسوب تتمتع بالحماية حيث تعتبر مصنفات أدبية، وفقا لما وارد في المادة 2 من اتفاقية برن.

ب-حماية الملكية الفكرية في إطار معاهداتها، كما تعمل معاهدة الويبو على إقامة توازن عادل بين مصالح الدول المتقدمة والدول النامية.[2]

كما أن الاتفاقية لم تقتصر على إبرام المعاهدات والعمل على تنفيذها، بل يتعدى ذلك إلى ميادين التكوين والتدريب من خلال تنظيم دورات وبرامج تهدف إلى إعداد كوادر بشرية قادرة على تطبيق

متطلبات الاتفاقيات التي المعاهدات التي تم توقيعها والمصادقة عليها من قبل الدول.

ومما سبق يتضح أن المنظمة العالمية للملكية الفكرية لها دور كبير في حماية حقوق الملكية الفكرية.

ثالثا: اتفاقية تريبس

تحتوي اتفاقية تريبس[3]على العديد من المواد التي تهدف إلى حماية الملكية الفكرية وخصوصاً من السرقة الإلكترونية التي تستهدف الأعمال الفنية، دون تعويض لأصحابها.

وقد تم التوقيع على الاتفاقية سنة1994 من قبل الدول الأعضاء، حيث عالج موقعوا الاتفاقية العامة للتعريفات والتجارة حقوق الملكية الفكرية بتوقيع اتفاق الجوانب المتصلة بالتجارة وحقوق الملكية الفكرية، فربطوا بذلك بين المعايير الدولية والمعايير المحلية.[4]

[1]- منير محمد الجنيهي وممدوح محمد الجنيهي، مرجع سابق، ص206

[2]- رشا علي الدين، مرجع سابق، ص

[3]- وقعت بمدينة مراكش بالمغرب بتاريخ 15-04-1994

[4]- منير محمد الجنيهي وممدوح محمد الجنيهي، مرجع سابق، ص201

كما نصت اتفاقية تريبس على ضرورة تحرير التجارة العالمية من مختلف القيود المرتبطة بأنشطة التجارة الدولية، ونظرا لأهمية حماية الملكية الفكرية في ظل النظام التجاري العالمي الجديد، فقد جاءت هذه الاتفاقية ثمرة مفاوضات متعددة دامت لعدة سنوات لتكون واحدة من أبرز أدوات تحرير التجارة العالمية، وقد أثارت جدلا واسعا أثناء المفاوضات بين الدول الصناعية المتقدمة والدول النامية.[1]

وقد تميزت اتفاقية تريبس بتركيزها على الأوجه التجارية المتعلقة بحقوق الملكية الفكرية على مكافحة الجريمة المعلوماتية، حيث نصت المادة 10على ان برامج الحاسوب سواء كانت بلغة المصدر أو بلغة الآلة تتمتع بالحماية باعتبارها أعمالا أدبية، وذلك وفقا لأحكام معاهدة برن لعام 1971، ونصت الفقرة الثانية من نفس المادة على حماية البيانات المجمعة أو المواد الأخرى بشروط معينة، كشرط الأصالة سواء أكانت مقروءة آليا أو بشكل آخر، وإذا كانت تشكل خلقا فكريا نتيجة انتقاء أو ترتيب محتوياتها.

ولضمان فعالية هذه المكافحة ألزمت الاتفاقية على الدول الأعضاء اتخاذ تدابير لحماية حقوق الملكية الفكرية المنصوص عليها فيها، وبهدف تسهيل اتخاذ تدابير فعالة ضد أي تعد على حقوق الملكية الفكرية التي تناولتها الاتفاقية، يجب اتخاذ إجراءات سريعة لمنع التعديات والانتهاكات الواردة في المادة 41 من الاتفاقية.

وتضمنت اتفاقية تريبس الكثير من المواد التي تنص على ضرورة توافر إجراءات قضائية ومدنية إلى جانب إجراءات إدارية أخرى في المادة 42 منها، وأيضا فقد نصت المادة التاسعة من الاتفاقية على أنه على الدول الأعضاء فيها الالتزام بأحكام المواد من 1إلى 21 من معاهدة برن لعام 1971، مع التأكيد على أن الحماية تسري على المنتوج وليس على مجرد الأفكار أو الإجراءات أو أساليب العمل أو المفاهيم الرياضية

كما تناولت الاتفاقية مسألة الحماية الزمنية لهذه المصنفات وقررت ان مدة الحماية تمتد طوال حياة المؤلف، واستمر لمدة خمسين سنة بعد وفاته.[2]

إضافة إلى الاتفاقيات السابقة يجب التنويه أيضا لدور المنظمات العالمية في مكافحة الجريمة المعلوماتية مثل منظمة الأمم المتحدة، حيث أنها في تقرير لها تحت عنوان " اقتراحات المواجهة الدولية اتجاه صور

[1]– رشا علي الدين، مرجع سابق، ص74

[2]– طرشي نورة، مرجع سابق، ص74

تطور الجريمة" عام 1987، وفي اجتماع آخر لها عام 1990، تم التطرق إلى مشروع لحلول مشكلة الجرائم المرتبطة بالحاسوب،[1] حيث تم التأكيد على أهمية جهود الدول الأعضاء لضبط جرائم المعلوماتية نظرا لآثارها السلبية والوخيمة على الأمن المعلوماتي والاستقرار الاجتماعي والاقتصادي.

وفي سياق الاهتمام الدولي لمكافحة الجريمة المعلوماتية أرسل مؤتمر ريو دي جانيرو الدولي الخامس عشر للجمعية الدولية لقانون العقوبات في 4-09-1994 جانبا مهما من المبادئ العامة المتعلقة بالقانون الإجرائي المتعلق بالجرائم المعلوماتية.

وامتدادا لاتفاقية بودابست لمكافحة الجريمة المعلوماتية ابرم المجلس الأوروبي اتفاقية أخرى عام 2003 تضمنت جرائم معلوماتية جديدة، من أبرزها "جرائم التمييز العنصري المعلوماتي" و "جريمة كره الأجانب المعلوماتية". وقد تم اعتماد برتوكول إضافي لاتفاقية بودابست في 7 نوفمبر 2002 من قبل دول المجلس الأوروبي، وتم التوقيع عليه في ستراسبورغ ب 28 يناير 2003 بمناسبة الاجتماع البرلماني لدول المجلس الأوروبي، ويعد هذا البرتوكول مكملا لاتفاقية بودابست 2001، وقد تم اعتماد هذا البرتوكول لتحقيق شرطين أساسيين:

-**أول شرط:** من أجل تكييف قانون العقوبات الموضوعي للدول الأعضاء، وذلك من خلال تجريم أفعال التمييز العنصري وكره الأجانب التي ترتكب عبر الوسائط المعلوماتية، لا سيما شبكة الإنترنت.

-**ثاني شرط:** يختص بتعزيز التعاون الدولي في مجال مكافحة هذه الجرائم، سواء على صعيد القانون الداخلي للدول أو على المستوى الدولي بتنظيم إجراء تسليم المجرمين.

وقد تضمن هذا البرتوكول الإضافي لاتفاقية بودابست تعريفا دقيقا لجرائم التمييز العنصري وكره الأجانب باعتبارها كل مادة مكتوبة أو صورة أو أي شكل من أشكال تشغيل الأفكار التي تحث على الكراهية، أو التي تتضمن إنكارا أو تبريرا لأي انتهاك موجه ضد شخص أو مجموعة من الأشخاص بسبب عرفهم أو لونهم أو أصلهم أو جذورهم الوطنية أو الدينية، كما انه ولأول مرة عالميا صنف هذا البرتوكول الأفعال التالية ضمن صور جرائم التمييز العنصري وكره الأجانب عبر الشبكات المعلوماتية:

[1]- كحكد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة الإسكندرية، 2004، ص33

-نشر أو وضع مواد عنصرية أو تنطوي على كراهية الأجانب بأي وسيلة كانت عبر الشبكات الالكترونية.

-السب أو الشتم لعرق معين باستخدام الوسائل المعلوماتية.

-تبرير أو تشجيع الجرائم ضد الإنسانية.[1]

تقوم اتفاقية تريبس كغيرها من الاتفاقيات على مجموعة من المبادئ هي:

1-المعاملة الوطنية والمساواة في الدولة:

عملت اتفاقية تريبس بقاعدة أساسية تقوم على مبدأ المساواة في الدولة العضو بين الأجانب المنتمين إلى إحدى الدول الأعضاء والوطنيين المنتمين إليه، فقد نصت المادة الثالثة من الاتفاقية على التزام كل دولة عضو بمنح رعايا الدول الأعضاء الأخرى نفس الحماية والمعاملة التي تمنحها لرعاياها في شأن حماية الملكية الفكرية وتشمل المساواة في الحماية هنا تحديد المستفيدين من الحماية، آليات اكتساب الحقوق، نطاقها، مدة سريانها، طريقة انفاذها، وانقضائها، وسائر المسائل ذات الصلة باستخدام الحقوق التي وردت في هذه الاتفاقية.[2]

2-الدولة الأولى بالرعاية:

فرضت المادة الرابعة من اتفاقية تريبس على الدول الأعضاء أن تمنح كل أعضاء منظمة التجارة العلمية الدول ذات المزايا أو الحصانات أو المعاملة التفضيلية التي تمنحها للمنتمين إلى أي دولة أخرى متعلقة بحماية حقوق الملكية الفكرية، دون الحاجة إلى شروط إضافية أو إجراءات خاصة.[3]

ويترتب على هذا أن كل دولة عضو في منظمة التجارة العالمية إذا قامت بمنحاي امتياز إلى دولة أخرى عضو يجب عليها أن تمنح جميع الدول الأعضاء الأخرى نفس الميزة، غير أن هذا المبدأ لا يمنع

[1] -http://www.conventions.coe.int/treaty/fr/treaties/html/189.htm

[2]- رشا علي الدين، مرجع سابق، ص178

[3]- أمجد عبد الفتاح احمد حسان، مدى الحماية القانونية لحق المؤلف، دراسة مقارنة، رسالة دكتوراه، جامعة تلمسان، 2008، ص416

الدول الأعضاء من فرض قيود لتنظيم التجارة الدولية، شريطة أن تكون هذه القيود ذات طابع عام وموضوعي ومجرد دون أن تحمل مزايا للبعض دون الأخر.[1]

3-مبدأ الحد الأدنى من الحماية القانون:

حرصت اتفاقية تريبس عند إبرامها على وضع حد أدنى من الحماية القانونية في كل مجال من مجالات حماية الملكية الفكرية، حيث نجد أن الدولة العضو تستطيع تقديم حماية قانونية تفوق الحماية المنصوص عليها في اتفاقية تريبس، غير أن الدول الأعضاء لا يجوز لها النزول عن هذا الحد الأدنى أو اعتماد معايير حماية أدنى مما تنص عليه أحكام الاتفاقية، ولا يوجد ما يمنع من منح حماية أكثر سعة مما قدمته الاتفاقية مثل منح الدول الأعضاء امتيازات تفوق ما قررته أحكامها، ويتعين على التشريعات الوطنية للدول الأعضاء أن تنسجم مع أحكام الاتفاقية. [2]

4-وقت إنفاذ اتفاقية تريبس:

حرصت الدول الصناعية المتقدمة، وعلى رأسها الولايات المتحدة الأمريكية على الاتفاق على قواعد اتفاقية تريبس مند لحظة توقيعها، ويكفي أن نسوق هذا دليلا على قولنا وهو إحصائية الاتحاد الدولي للملكية الفكرية(IIPA)، التي قدرت خسائر الملكية الفكرية في الدول الصناعية المتقدمة بحوالي 12.5 مليار دولار أمريكي في عام 1998 مما دعا الدول الصناعية الكبرى للعمل على دفع عجلة القانون الدولي الاتفاقي نحو وضع قواعد دولية لحماية حقوق الملكية الفكرية.

حيث تعتبر الدول الصناعية المتقدمة المتضرر الأول من ظاهرة القرصنة، حيث حاولت هذه الدول إلزام العديد من الدول النامية للانصياع للاتفاقيات والحد من القرصنة والتقليد والتزوير.

ومع ذلك لم تتمكن هذه الدول من التوصل إلى عقد اتفاقية تريبس ما لم يكن لديها قدر من المرونة التي من مظاهرها الرضا بالفترات الانتقالية التي تم إقرارها وهي فترات سماح لا تلزم الدول خلالها بتنفيذ

[1]- مليكة عطوي، الحماية القانونية لحقوق الملكية الفكرية على شبكة الانترنت، المؤلف، رسالة دكتوراه، جامعة الجوائر، 2010، ص270

[2]- أمجد عبد الفتاح احمد حسان، مرجع سابق، ص286

الالتزامات المفروضة بموجب الاتفاقية.[1]

5-المعاملة التفضيلية للدول النامية:

إن مراعاة احتياجات الدول الأعضاء الأقل نموا، من المبادئ الأساسية التي ترتكز عليها اتفاقية تريبس، حيث حرصت الاتفاقية على توفير المرونة في تطبيق أحكامها وبالأخص على المستوى الداخلي لهذه الدول الأعضاء، حيث أن الهدف من الاتفاقية إعطاء الأفضلية للدول النامية، وهذا قصد بناء قاعدة تكنولوجية قوية ومتطورة تخدم مصالحها الاقتصادية، وتمكنها من اللحاق بعجلة التجارة الدولية.[2]

كما أن الاتفاقيات الدولية لعبت دورا مهما في مكافحة الجرائم الإلكترونية على الصعيد الدولي، كذلك يجب تسليط الضوء على جهود المنظمات العالمية في مكافحة الجرائم الإلكترونية مثل منظمة الأمم المتحدة وجهودها المبذولة للإحاطة بالإجرام المعلوماتي، بحيث أصدرت تقريرا بعنوان "اقتراحات المواجهة الدولية تجاه صور تطور الجريمة "سنة 1987، كما ناقشت في اجتماع آخر سنة 1990 مشروع يسعى إلى إيجاد حلول للجرائم المرتبطة بالحاسوب، وقد ركزت على أهمية جهود الدول الأعضاء لمكافحة الجرائم الإلكترونية نظرا لما تسببه من آثار سلبية على الأفراد والمجتمعات.

وفي سياق اهتمام المجموعة الدولية لمكافحة الجرائم الإلكترونية، عقد المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات في ريو دي جانيرو بتاريخ 4 سبتمبر 1994، والذي أضاف مجموعة من المبادئ العامة المتعلقة بالقانون الإجرائي للجرائم المعلوماتية.[3]

ومنه فإن المعاهدات والاتفاقيات الدولية بالإضافة إلى المنظمات الدولية تعتبر الأساس الذي يعتمد عليه التعارف الدولي في مجال مكافحة الجرائم الإلكترونية.

[1]- محمد حسام محمود لطفي، تأثير اتفاقية تريبس على نظام حماية حق المؤلف، حقوق المؤلف في الوطن العربي، في إطار التشريعات العربية والدولية، المنظمة العربية للتربية والثقافة والعلوم، تونس، 1999، ص42

[2]- رشا علي الدين، مرجع سابق، ص182

[3]- طرشي نورة، مرجع سابق، ص74

الفرع الثاني: جهود المنظمات الدولية في مواجهة الجرائم الالكترونية

أولا: جهود منظمة الأمم المتحدة

عملت منظمة الأمم المتحدة بشكل كبيرة ومستمر على مكافحة جرائم الإنترنت، وهذا لما تسببه هذه الجرائم من أضرار جسيمة وخسائر فادحة بالإنسانية جمعاء، واقتناعها بأن منع هذا النوع من الجرائم يتطلب استجابة دولية في ضوء الطابع والأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم المتعلقة به.

ومع تصاعد الجرائم المرتكبة عبر الإنترنت، قامت منظمة الأمم المتحدة سنة 2000 بإبرام اتفاقية خاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية، وقد أكدت على ضرورة تعزيز التنسيق والتعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، مع الإشارة إلى الدور المهم الذي يمكن أن تقوم به كل من منظمة الأمم المتحدة والمنظمة الإقليمية.[1]

أكملت الأمم المتحدة جهودها المبذولة لمكافحة جرائم الإنترنت، من خلال إبرام عقد عدة مؤتمرات وورش عمل تضمنت مشاورات مع الخبراء، بهدف التصدي للأشكال الحديثة من الجريمة الالكترونية، بالإضافة إلى مجهودات لجنة حقوق الطفل التابعة لمنظمة الأمم المتحدة التي عقدت اتفاقات خاصة بحقوق الطفل وذلك من أجل النظر في الجرائم التي ترتكب في حق الطفولة من أبرزها استغلالهم عبر الإنترنت في إنتاج وترويج المواد الإباحية.

ثانيا: منظمة التعاون الاقتصادي والتنمية

بدأ اهتمام هذه المنظمة بالجرائم المرتكبة عبر الإنترنت منذ عام 1978، حيث قامت بوضع مجموعة من المبادئ والقواعد التوجيهية التي ترتبط بتقنية استغلال المعلومات، ويعد الدليل الخاص بحماية الخصوصية وقواعد نقل البيانات من أول الأدلة التي اعتمدها مجلس المنظمة في عام 1980، مع توصية الأعضاء بالالتزام بها.

وفي سنة 1992 وأصدرت المنظمة توصيات توجيهية تتعلق بأمن أنظمة المعلومات، وقد تمخضت جهود منظمة من أجل معالجة الجرائم المرتكبة عبر الإنترنت بالتوصية بضرورة أن تمنح التشريعات الجنائية للدول الأعضاء الأفعال التالية: التلاعب بالبيانات المعالجة إلكترونيا، محو المعطيات، التجسس

[1]– محمود حسام ومحدود لطفي، الحماية القانونية لبرامج الحاسب الالكتروني، دار الثقافة للطباعة والنشر، القاهرة، ط1، 2014

المعلوماتي، ويندرج تحته الحصول أو استخدام البيانات بطرق غير قانوني والتخريب المعلوماتي وغيرها، وتنظم المنظمة سنويا عددا من الملتقيات وورش العمل المتخصصة للقطاعات ذات العلاقات في هذا المجال، حيث ترتكز فيها على معايير و مستويات الأمن ، بالإضافة إلى تنفيذ القانون وتطبيقه بهدف مواكبة التطورات في مجال جرائم الإنترنت.[1]

ثالثا: المنظمة العالمية للملكية الفكرية

تعد المنظمة العالمية للملكية الفكرية إحدى الهيئات المختصة التابعة للأمم المتحدة، حيث اهتمت هذه المنظمة في دعم الملكية الفكرية على مستوى العالم، والغاية من ذلك تشجيع الابتكار و الإبداع وحماية المصنفات الأدبية والفنية والفكرية وتطوير الاتحادات المنشأة في مجالات الحماية الصناعية.

كما أولت هذه المنظمة اهتماما كبيرا في المجال المعلوماتي، حيث سعت إلى توفير الحماية القانونية للبرامج المعلوماتية وقواعد البيانات، فبعد أن استقر الرأي لديها بعدم إمكانية توفير الحماية لها في تشريعات براءات الاختراع، كما عملت المنظمة على فرض عقوبات على جميع أعمال التزوير في العلامات التجارية والقرصنة التي تتم لأغراض تجارية، وبالطبع تعتبر شبكة الإنترنت من الأماكن الخصبة لهذا النوع لهذه الانتهاكات، والتي وفرت بموجبها الحماية القانونية للبرامج وقواعد البيانات المعلوماتية.[2]

رابعا: دور المنظمة الدولية للشرطة الجنائية في مواجهة الجريمة الإلكترونية (الانتربول)

تسعى المنظمة الدولية للشرطة الجنائية الإنتربول [3] إلى تعزيز التعاون بين أجهزة الشرطة في الدول الأعضاء، ومكافحة الجريمة وكذا مساهمتها في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول

---

[1]– محمود الرشيدي، العنف في جرائم الانترنت، الدار المصرية اللبنانية، 2011

[2]– مليكة بقاح، إشكالية الجرائم الالكترونية في التشريع الجزائري، أطروحة مقدمة لنيل شهادة الدكتوراه في علوم الإعلام والاتصال، كلية علوم الاعلام والاتصال، جامعة الجزائر3 ، 2018–2019، ص 130–131

[3]–هي أكبر منظمة للشرطة الدولية،أنشأت عام 1923، مكونة من قوات الشرطة Interpolمنظمة الشرطة الجنائية الدولية، لـ 192 دولة، وللمنظمة أربعة لغات رسمية هي الفرنسية،الإنجليزية، العربية، الاسبانية، مقرها في مدينة ليون في فرنسا، توجد مكاتب وطنية للمنظمة في الدول الأعضاء، وهي منظمة رسمية بين الحكومات تقوم بعدة مهام خاصة في مجال تبادل المعلومات التعاون الدولي للتصدي للجريمة، أنظر إلى كتاب شحادة يوسف،الضابطة العدلية، علاقتها بالقضاء ودورها في سير العدالة الجزائية، دراسة مقارنة، ط1، مؤسسة بحسون للنشر والتوزيع، بيروت، ص455

الأطراف حيث ارتكز اهتمام الانتربول في السنوات الأخيرة بصورة أساسية على الجريمة المنظمة والأعمال المرتبطة بها، والدليل على ذلك الدورة 26 لاجتماع الجمعية العامة للشرطة الجنائية الدولية الإنتربول،[1] بالعاصمة الصينية بكين في 29/09/2017 وبمشاركة نحو 1000 شخصية من كبار قادة الشرطة والسياسيين من 156 دولة.

ومن أبرز القضايا التي تم مناقشتها في ذلك الاجتماع هي جرائم الإنترنت والقرصنة الالكترونية والمخاطر الناجمة عنها، و الآليات الدولية للتصدي لهذا النوع من الجرائم على الصعيد الدولي.[2]

يقوم الإنتربول بأداء دور الريادة في مجال مكافحة الجريمة الإلكترونية وذلك من خلال تعزيز التعاون بين أجهزة الشرطة في الدول الأعضاء من اجل مكافحة هذا النوع من الجرائم، كما يزود دول الأطراف بالبيانات والمعلومات المتعلقة بالمجرم والجريمة وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنظمة إليها.

إلى جانب التعاون في ضبط الجناة بمساعدة أجهزة الشرطة في الدول الأعضاء كما يقوم بتتبع مجرمي المعلوماتية من خلال جمع الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود للأنظمة المعلوماتية، وشبكات الاتصال بهدف العثور على الأدلة والبراهين على ارتكاب الجريمة الالكتروني.

إن هذه الجهود تساهم في تنفيذ العمليات الشرطية والأمنية المشتركة، و هي من شأنها متابعة المجرمين الذين يستخدمون التكنولوجيا الحديثة لتحقيق أهدافهم الغير قانونية.

وكما ورد في الفقرة الخامسة من دستور الإنتربول الدولي فهي تتكون من:

الجمعية العامة، اللجنة التنفيذية، الأمانة العامة، المكاتب المركزية الوطنية، المستشارون، لجنة ضبط ملفات الانتربول.[3]

وتنقسم مهام الانتربول إلى أربعة وظائف تتمثل في:

---

[1]– بن عمر الحاج عيسى،الإنتربول كألية دولية شرطية لمكافحة الجريمة المنظمة العابرة للحدود، مجلة الدراسات القانونية، السياسية، كلية الحقوق، جامعة الأغواط، العدد 03، جانفي 2016، ص2

[2]– شبيلي مختار، الجهاز العالمي لمكافحة الجريمة المنظمة، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر،2016، ص266

[3]– دستور الانتربول الدولي من موقعhttp://www.interpol.int

-التنسيق على المستوى الدولي

-تسهيل تبادل المعلومات الجنائية

-تحليل البيانات الجنائية

-تخزين البيانات الجنائية

أما النظام الإداري في الانتربول فيتمثل في:

-الرئيس الأمين العام يتم تعيينه من قبل الجمعية العامة لمدة خمس سنوات

تعقد الجمعية العامة مرة سنويا

-اللجنة التنفيذية تعقد 3 مرات سنويا وتتكون من 13 عضوا.

هذا ويعد الإنتربول، من أبرز الهيئات الدولية الفعالة في أداء مهامها على الصعيد الدولي بحيث ساهمت

تعزيز الأمن والتعاون الدولي بين أجهزة الشرطة في بلدان الأعضاء، كونها منظمة دولية للشرطة الجنائية تختص بمكافحة الجريمة المنظمة بمختلف أشكالها ومن بينها الجرائم الالكترونية، فهي تعد جهاز رئيسي لتحقيق التعاون الدولي في مكافحة الجريمة المنظمة.[1]

[1]- مليكة بقاح، إشكالية الجرائم الالكترونية في التشريع الجزائري، مرجع سابق، ص133

المبحث الثاني: إجراءات المتابعة في الجريمة الالكترونية بين التحري والمحاكمة

تعد الجريمة الإلكترونية من أحدث الجرائم، ولهذا فإن القواعد العامة لمكافحة الجريمة الإلكترونية غير كافية لهذا وضعت قواعد وآليات خاصة بالجريمة الإلكترونية فقط، نظرا لخصوصيتها من الجانب الإجرامي وبالأخص في مجال التحقيق، فيتعين على المحقق في حال وقوع جريمة التأكيد على توافر الأركان الثلاثة للجريمة، وهي: الركن الشرعي، والمادي، والمعنوي.

المطلب الأول: إجراءات البحث والتحري

جهاز الشرطة القضائية له أهمية في الكشف عن الجريمة الالكترونية وضبط المجرم الالكتروني، بالإضافة إلى استعداد المشرع الجزائري لأساليب التحري الخاصة والمناسبة لضبط الوجه الإجرامي الجديد بما يساعد القضاء والشرطة على القيام بمهامها مع الإجرام الجديد تبعا للمواثيق الدولية المصادق عليها من طرف الجزائر، وخاصة المادة 20 من اتفاقية باليرمو لمكافحة الجريمة المنظمة التي اعتبرت الجريمة الإلكترونية جزء من الجريمة المنظمة.[1]

يجب الإشارة إلى أن هذه الإجراءات لا يرخ ضبطها إلا في بعض الإجراءات الجزائية، من طرف المشرع مثل الجريمة الالكترونية بموجب تعديل قانون الإجراءات الجزائية، القانون 06-22 وتمثل في مايلي:

-اعتراض المراسلات عبر الاتصالات السلكية واللاسلكية

-وضع ترتيبات تقنية دون موافقة المعنيين مثل تسجيل كلام من طرف شخص أو عدة أشخاص في أماكن عمومية أو خاصة أو التقاط صور لهم.

-جواز الاختراق للكشف عن الجريمة الالكترونية حسب المادة 65مكرر12 من القانون 06-12 المتضمن قانون الإجراءات الجزائية.

-و لأنه إجراء غريب وخطير في عمل سلطات الضبط القضائي أحاطه المشرع بمجموعة ضوابط منها الإذن القضائي للسرب من وكيل الجمهورية أو قاضي التحقيق المادة 65 مكرر 11، كذلك احترام المدة القانونية للسرب.

[1]- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، الطبعة الثانية، دار الفكر الجامعي، مصر، 2011، ص76

الفرع الأول: جمع الاستدلالات في الجريمة الالكترونية

أولا: تلقي البلاغات والشكاوى

1-تلقي البلاغات في الجريمة الإلكترونية

الأصل أنه يجب على رجال الشرطة قبول البلاغات أو الشكاوى التي تقدم إليهم سواء تم تقديمها شفهيا أو كتابيا، ويتم قيد هذه البلاغات في سجل خاص بتلقي البلاغات بمجرد ورودها إلى مركز الشرطة، كما يجب على المتحري أن يخطر قيادته في حالة الجرائم الإلكترونية، و إبلاغ الجهات المختصة مثل: إدارة مكافحة جرائم المعلوماتية، ومن الأخطار الشائعة في هذا السياق الامتناع عن قبول البلاغ أو الشكوى بحجة عدم الاختصاص النوعي أو المكاني، حيث يفترض اتخاذ الإجراءات المقرة بشأنها، ثم إبلاغ جهة الاختصاص وإحالة المحضر إليه و يقوم المتحري بجمع الأدلة وتحليل البلاغ أو الشكوى وإجراءات معينة تتمثل في المعاينة وجمع الأدلة والتحقيق.[1]

كما يتم الإبلاغ عن الجرائم الإلكترونية عن طريق المسائل الرقمية مثل إرسال رسالة إلكترونية إلى عنوان البريد الإلكتروني للجهات المختصة بالتحقيق، للإبلاغ عن مواقع غير قانونية، كالموقع التي تنشر صورا تتعلق بالاستغلال الجنسي للأطفال.

و المعلومات التي ينبغي على المحقق معرفتها من المبلغ عند تلقي البلاغ يمكن الحصول عليها من خلال طرح أسئلة عن تاريخ ووقت تقديم البلاغ، هوية المبلغ، ونوع الجريمة الإلكترونية المبلغ عنها، وغيرها من الأسئلة التي تتعلق بالجريمة.[2]

2-الشكوى في الجريمة الإلكترونية

قد ينتج على الجريمة الالكترونية ضرر شخصي قد يصيب أحد الأفراد معنويا أو ماديا، فيصبح من حق المتضرر مباشرة الدعوى العمومية عن طريق تقديم شكوى أمام الجهة المختصة بالتحقيق، حيث نص المشرع الجزائري في قانون الإجراءات الجزائية أنه يحق لكل شخص متضرر من جناية أو جنحة أن

[1]- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، الأردن، 2011، ص 79

[2]- محمد بوعمرة، سيد علي بنيال، جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية، تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة اكلي محمد اولحاج، لبويرة، 2019-2020، ص 42

يدعي مدنيا بأن يتقدم بشكواه أمام قاضي التحقيق المختص وقد عرفت الشكوى بأنها البلاغ أو الإخطار الذي يقدمه المجني عليه أو ووكيله الخاص إلى السلطات المختصة طلبا تحريك الدعوى العمومية بشأن جريمة معينة.

ولقد أنشئت الكثير من المؤسسات المختصة بمعالجة هذه الشكاوى من بينها مركز استقبال الشكاوى عن جرائم الاحتيال الالكتروني في فيرجينيا الغربية بالولايات المحتدة الأمريكية الذي أسس من قبل مكتب التحقيقات الفيدرالي والمركز الوطني لجرائم الياقات البيضاء بهدف مكافحة ظاهرة الاحتيال عبر الإنترنت.[1]

ثانيا: الاستجواب وسماع الشهود في الجريمة الإلكترونية

1-الاستجواب

وهو أن يمثل أمام المحقق حتى يتأكد من هويته ومحيطه علما بكل الوقائع المنسوبة إليه، ويجب على المحقق أن يشعر المتهم بأنه حر في الإدلاء بأقواله أو الامتناع عن ذلك، كما يتعين على المحقق إعلام المتهم بحقه في الاستعانة بمحامي وفي حال عدم قدرته على توكيل محامي يجوز للمحقق أن يعين له محام من تلقاء نفسه، كما يجب على المتهم إبلاغ المحقق بأي تغيير يطرأ على محل إقامته. [2]

2-سماع الشهود في الجريمة الإلكترونية

سماع الشهود هو إجراء من إجراءات التحقيق، يساهم في جمع الأدلة المتعلقة بالجريمة، ويستدعي شهود ليست لهم علاقة بالجريمة، لكن شهادتهم قد تكون ضرورية 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]

[1]- محمد بوعمرة، سيد علي بنيال، مرجع سابق، ص 42-43

[2]- خالد عياد الحلبي، المرجع السابق، ص80

[3]- محمد بوعمرة، سيد علي بنيال، مرجع سابق، ص 43

الفرع الثاني: التحقيق في الجريمة الإلكترونية

أولا: التفتيش وضبط الأدلة

1-التفتيش

تعد الجريمة الإلكترونية من الجرائم التي يصعب إثباتها لذلك يسمح المشرع الجزائري بالتفتيش في المنظومة المعلوماتية ضد كل جريمة يحتمل وقوعها وتتقلص معه الضمانات التي يشترطها المشرع عادة في الجرائم التقليدية الأخرى، نظرا لسرعة ارتكابها ومحو آثارها وتجاوزها للحدود الوطنية.

وإذا كان التفتيش يقصد به البحث عن جسم الجريمة والأداة التي استخدمت في ارتكابها وكل ماله عصلة بوقوعها، فإن عالم التقنية قد يتميز عن الجرائم العادية بكونه ينقسم إلى جانبين هما الكيانات المادية والتي تنطبق عليها القواعد العامة للتفتيش من حيث مكان تواجدها بحسب ما إذا كان مكان عام أو خاص.[1]

أما إذ تعلق الأمر بتفتيش الكيانات المعنوية كالبرامج ونظم الشغل وقواعد البيانات، فيختلف الوضع عن تفتيش الأماكن و الأشخاص. وبعيدا عن الآراء الفقهية التي قيلت حولها فقد نص المشرع الجزائري في المادة 47 الفقرة الرابعة من قانون الإجراءات الجزائية الجزائري بإمكانية التفتيش والضبط على المكونات المعنوية للحاسوب بنصه على أنه: " إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم بأي عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو بأمر ضباط الشرطة القضائية للقيام بذلك".[2]

2-ضبط الأدلة

يقصد به ضبط الأدلة أو الأشياء التي تساعد في كشف الحقيقة المتعلقة بالجريمة التي وقعت، فالضبط في اغلب الأحيان هو غرض التفتيش وإن لم يكن له السبب الوحيد، فقد يتم الضبط بناء على أسباب أخرى غير التفتيش مثل المعاينة وما يقدم المتهم أو الشهود لمأموري الضبط القضائي، لهذا يرى بعض الفقهاء أن الضبط ليس من إجراءات التحري بل من إجراءات الاستدلال خصوصا عندما يتم في الأماكن

[1]- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، مصر، 2012، ص74

[2]- محمد بوعمرة، سيد علي بنيال، مرجع سابق، ص 45

التي يجوز لسلطات الضبط دخوله مثل الأشياء التي يتم العثور عليها خارج المساكن أو في الحقول أو في الطريق العام.

والضبط لا يخرج من كونه وضع اليد على شيء يرتبط بجريمة ارتكبت ويساهم في كشف الحقيقة عنها وعن مرتكبيها، سواء كان ذلك الشيء عقارا أو منقولا، بحسب الأصل الضبط لا يراد إلا على أشياء مادية فلا صعوبة بالتالي بضبط الأدلة في الجرائم المتعلقة بالحواسيب، مثل رفع البصمات عن الجهاز، كما انه لا صعوبة في ضبط الدعامة المادية للبرنامج أو الأدوات المستخدمة في نسخها بشكل غير مشروع أو إتلافها بوسائل تقليدية كالحرق أو الكسر، لكن تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في تهريب البرامج مثل الفيروسات أوفي ضبط بيانات الحاسوب الغير مرئي حيث لا تترك هذه الأدلة أثرا ماديا واضحا، ولسهولة تدمير الدليل خلال ثواني معدودة ولعدم معرفة كلمة المرور أو ترميز البيانات.[1]

ثانيا: المعاينة وندب الخبراء في الجريمة الإلكترونية

1-المعانية:

تعد المعاينة وسيلة إثبات لحالة الأماكن والأشياء والأشخاص وكل ما يساعد في كشف الحقيقة فهي بهذا المعنى تتطلب الانتقال إلى مكان وقوع الجريمة أو أي محل آخر توجد به آثار يري المحقق أن لها علاقة بالجريمة، والأصل أن إجراء المعاينة يخضع لتقدير المحقق، لا يقوم بها إلا إذا كان هناك فائدة من ورائها، كما أن هناك حالات يفرض فيها القانون على النيابة الانتقال الفوري إلى مسرح الجريمة كما في حالة

إبلاغها بجناية ملتبس بها، يجب على القائمين بالمعاينة تأمين الأجهزة والمعدات المستخدمة خلال إجراء المعاينة، وبما أن الجريمة الإلكترونية ترتكز على التقنية الحديثة فانه من الضروري تشكيل فريق من الخبراء المختصين في مجال التقنية الحديثة، و ابلاغهم مسبقا حتى يستعد من الناحية الفنية والعملية، ويضع خطة ملائمة للمعاينة مع مراعاة ما ورد في القوانين الجنائية حول المعاينة تحقيقا لمبدأ الشرعية.[2]

[1]- عبج الفتاح بومي حجازي، مكافحة جرائم الانترنت، دار الفكر الجامعي، الإسكندرية، ط1، 2006، ص238

[2]- عبد الفتاح بومبي حجازي، مكافحة جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، مصر، ط1، بدون سنة، ص237

2-ندب الخبراء

تعد الخبرة من الإجراءات الأساسية التي تتخذ لإثبات الأدلة التي تساعد عن الكشف عن الجرائم الإلكترونية، كون الجريمة الإلكترونية ترتكب بوسائل مستحدثة ومعقدة يصعب التعامل معها.[1]

الخبير هو كل شخص يمتلك مهارة في علم أو فن معين سواء كان اسمه مسجلا في جدول الخبراء أو على مستوى المحاكم أم لا، وهو كل شخص له دراية بمسألة من المسائل، وقد يستدعي التحقيق فحص مسألة يتطلب لفحصها كفاءة فنية أو علمية لا تتوفر لدى المحقق، فيمكنه أن يستشير فيها خبراء كما هو الحال في تحليل مادة سامة في جرائم التسمم ، أو تقرير الصفة التشريحية في جرائم القتل، أو فحص لخطوط الكتابة المدعي بتزويرها، ولما كان قاضي التحقيق هو المختص بالتحقيق، قد يواجه في عمله مسائل فنية لا يمكنه البث فيها، حينها يجوز له الاستعانة بأهل الخبرة، لضمان ان يتم التحقيق في صورة موضوعية دقيقة.[2]

المطلب الثاني: إجراءات المحاكمة والصعوبات التي تواجه مكافحة الجريمة الإلكترونية

الفرع الأول: إجراءات المحاكمة

في وقتنا الحالي، أصبحت الجرائم الإلكترونية تمثل خطرًا حقيقيًا يهدد الأفراد والمؤسسات أيضا. لهذا من الضروري اتخاذ إجراءات قانونية قوية لضمان تحقيق العدالة، حيث أن مرحلة المحاكمة تعتبر مرحلة مهمة وأساسية في التعامل مع هذه الجرائم.

أولا: اختصاص المحكمة محليا في الجرائم الإلكترونية

حسب نص المادة 37 من قانون الإجراءات الجزائية يتحدد الاختصاص المحلي للجرائم الإلكترونية في ثلاث ضوابط ألا وهي: مكان إقامة المتهم، مكان ضبطه، أو مكان وقوع الجريمة.

كما نصت أحكام المرسوم التنفيذي رقم 06-348 المؤرخ في 05 أكتوبر 2006 على إمكانية تمديد الاختصاص المحلي لبعض الجرائم ووكلاء الجمهورية و قضاة التحقيق إلى دائرة اختصاص محاكم أخرى.

[1]- ضريفي نادية، سلطات القاضي الجنائي في تقرير الدليل الالكتروني، المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسة القانونية والسياسية، المجلد 04، العدد 02، 2019، ص124

[2]- محمد بوعمرة، سيد علي بنيال، مرجع سابق، ص 47

يمكن أن يحدث سلوك إجرامي في مكان معين، مثل جريمة تدمير المعلومات باستخدام فيروس وتتحقق النتيجة بتدمير وإتلاف المعلومات في مكان آخر، وبالتالي يتم تحديد الاختصاص في هذه الحالة إما في المكان الذي تم فيه الفعل أو في المكان الذي حدثت فيه النتيجة الإجرامية.[1]

ثانيا:اختصاص المحكمة نوعيا في الجرائم الإلكترونية

يتحدد الاختصاص النوعي للمحكمة من أجل الفصل في القضية المعروضة عليها حسب نوع الجريمة محل النظر، حيث تختص محكمة الجنايات في الفصل في قضايا الجنايات والجرائم الموصوفة بأفعال إرهابية أو تخريبية المحالة إليها بقرار نهائي صادر عن غرفة الاتهام حسب نص المادة 248 من قانون الإجراءات الجزائية.

كما تختص المحاكم بالنظر إلى الجنح والمخالفات فيما عدا ما استثنى في قوانين خاصة حسب نص المادة 328 من قانون الإجراءات الجزائية.

نظرًا لتعقيد الجرائم المعلوماتية، خصص المشرع الجزائري متابعتها مع بعض أنواع الجرائم مثل تجارة المخدرات، والجرائم المنظمة عبر الحدود، بالإضافة إلى جرائم الإرهاب وغسيل الأموال، حيث جعل الاختصاص ينعقد إلى دائرة اختصاص أخرى، وهذا ما نصت عليه المواد 37،40،329 من قانون الإجراءات الجزائية.

أثر التعديل الذي جاء به قانون 04-14 المؤرخ في 10 نوفمبر 2004 والذي حددت أحكامه في المرسوم التنفيذي رقم 348/06 المتعلق بالتنظيم القضائي حيث نص على إنشاء أقطاب قضائية متخصصة ذات اختصاص إقليمي واسع لدى المحاكم بكل من الجزائر العاصمة، قسنطينة ،وهران، ورقلة.[2]

ثالثا:سير المحاكمة

تستفتح المحكمة جلستها أولا بالإعلان عن افتتاحها بالقول باسم الشعب الجزائري جلسة مفتوحة، ثم المناداة على أطراف الخصومة بداية مع المتهم والضحية والشهود والمسؤول المدني والتأكد من حضورهم

[1]– بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، دراسة مقارنة ،2016، ص93

[2]– بعرة سعيدة، مرجع سابق صفحة 93

الجلسة أو غيابهم ثم يتم التحقيق من هوية المتهم وتبليغه بالتهم المنسوبة إليه والمادة القانونية المتابع بها، و في حالة إذا كانت القضية غير جاهزة ومهيأة للنظر فيها، تقوم المحكمة بتأجيلها إلى الجلسة القادمة.

وفي هذه الحالة، يمكن للمحكمة اتخاذ أحد الإجراءات التالية: إما أن تترك المتهم حراً، أو أن تفرض عليه تدبيراً من تدابير الرقابة القضائية المنصوص عليهم في المادة 125 مكرر 1 من قانون الإجراءات الجزائية الجزائري، أو أن تقرر وضع المتهم رهن الحبس المؤقت.

وإذا كان المتهم قد سبق حبسه من طرف قاضي التحقيق عن طريق الحبس المؤقت أو إجراءات المثول الفوري فإنه يساق بواسطة القوة العمومية لحضور الجلسة و يعلمه رئيس الجلسة أن له الحق في اختيار محام دفاع، ثم يوجه القاضي للمتهم كل الأدلة القائمة ضده مع مناقشتها تفصيليا، و بعدها سماع الشهود وبعد الإنهاء من التحقيق تعطى الكلمة للطرف المدني، لتقوم بعد ذلك النيابة العامة بالمرافعة و تقديم التماساتها و يكون بعدها للنيابة العامة و المدعى حق الرد على مرافعة محامي المتهم و تعطى الكلمة الأخيرة بعدها للمتهم و محاميه، حيث يعلن رئيس الجلسة إقفال باب المرافعات و يصدر حكمه في نفس الجلسة أو يحدد تاريخ لاحق للنطق بالحكم.[1]

وللمحاكمة قواعد عامة تتقيد بها وهي:

1-علانية الجلسات:جل التشريعات تنص على مبدأ العلنية في الجلسات،وذلك أن العلانية تسمح للجمهور بمراقبة سير عمل المحكمة ومنه الاطمئنان و الشعور بالعدالة، إلا أن مبدأ العلانية لا يسري في كل الجلسات بل للقاضي سلطة تقديرية في إخراج القصر من الجلسة، كما من الممكن أن تكون الجلسة في حد ذاتها سرية إذا كان في علانيتها خطر ومساس في النظام العام والآداب العامة، إلا أن من اللازم صدور الحكم في جلسة علنية.

2-شفوية المرافعات:لأطراف الخصومة كل الحق في مناقشة أي دليل يعرض بالجلسة حتى يسمح للجميع الدفاع عن نفسه.

[1]- بعرة سعيدة، مرجع سابق، صفحة 95

3-حضور أطراف الخصومة:ألزم المشرع الجزائري حضور كل من المتهم والضحية، أما النيابة فهي جزء من التشكيلة.

4-تدوين التحقيق النهائي:من غير الممكن انعقاد جلسة المحاكمة دون أمين ضبط لأن دوره يتجسد في تدوين كل ما يدور في الجلسة.

في النهاية، نقول إن الجرائم الإلكترونية لا تتبع إجراءات خاصة للمتابعة والمحاكمة، بل تخضع لنفس الإجراءات التي تُستخدم في الجرائم التقليدية.[1]

الفرع الثاني: صعوبات مكافحة الجريمة الإلكترونية

يشير المتخصصون في تكنولوجيا المعلومات إلى أن اكتشاف الجرائم الإلكترونية أمر صعب للغاية، وذلك للأسباب التالية:

-يمكن أن تنتهي عدة أشهر أو سنوات قبل اكتشاف.

-صعوبة الوصول إلى الجاني الإلكتروني، فكثيرا ما يقوم الجناة بالدخول إلى شبكة الإنترنت بواسطة مقاهي الإنترنت وباستخدام اسم مستعار ويصعب معرفة الجاني وتحديد موقعه.

-تعارض القوانين الجنائية من حيث نطاق التطبيق المكاني، إذ أن هناك مبادئ تحكم تطبيق القانون الجنائي منها مبدأ إقليمية القانون الجنائي،وتثور مشكلة في حالة ارتكاب الفعل الإجرامي في الخارج فأي من القوانين يخضع لها المجرم؟

-صعوبة تحديد المسؤول جنائيا عن الفعل الإجرامي، كأن يدخل مستخدم للشبكة على موقع فيجد به أفعال مشبوهة فهل يسأل عن هذه الجريمة عامل الاتصال، أم مورد المنافذ، أم مورد المعلومات او غيرهم من العاملين في مجال الإنترنت.

-افتراض العلم بقانون جميع الدول، ففي حالة ارتكاب جريمة في بلد ما وتتحقق النتيجة في بلد آخر، يجد الجاني نفسه يخضع لقانون هذه الدولة،وقد يكون هذا الفعل المرتكب مباح في بلده.

-صعوبة المطالبة بالتعويض المدني، حيث يرجع في ذلك لأحكام القانون الدولي الخاص.

[1]- بعرة سعيدة مرجع سابق، صفحة، 96

-عدم وعي الناس و جهلهم بثقافة الإنترنت يجعلهم يقومون بأفعال لا يعرفون أنها تشكل جريمة معاقب عليها قانونا.[1]

-عدم ظهور دليل مادي وآثار ملموسة للجريمة الإلكترونية.

-عجز الوسائل التقليدية عن ضبط آثار الجريمة المعلوماتية.[2]

-عولمة هذه الجريمة تؤذي إلى تشتيت جهود التحري و التنسيق الدولي لتعقب هذه الجرائم.[3]

[1]- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات (رؤية جديدة للجريمة الإلكترونية)، دار البلدية،عمان،الأردن،2007، طبعة01، صفحة من 220 إلى 223

[2]- عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم كمبيوتر الأنترنت، دار الكتب القانونية، مصر ،2007، صفحة 105

[3]- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية و الأنترنت (جريمة إلكترونية)، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت ،2007، طبعة 01، صفحة 33

ملخص الفصل الثاني:

مما سبق تم التطرق في هذا الفصل إلى الأجهزة المختصة بمكافحة الجريمة الإلكترونية سواء على المستوى الوطني أو الدولي.

ثم عقب ذلك تم التطرق إلى الإجراءات القانونية للمتابعة في الجريمة الإلكترونية بين البحث والتحري إلى غاية إجراءات محاكمة الجاني الإلكتروني، إضافة إلى ذلك تناول هذا الفصل في الختام الصعوبات التي تواجه مكافحة الجرائم المعلوماتية.

الخاتمة

الخاتمة:

تعتبر الجرائم الإلكترونية نوع من الجرائم التي ظهرت نتيجة الاستخدام السيئ لتكنولوجيا المعلومات، إذ تعتبر واحدة من المفرزات السلبية للتقدم التكنولوجي، و لم يعد من الممكن في العصر الرقمي الحالي تجاهل المخاطر المتزايدة الناتجة عن الجرائم الإلكترونية، خاصة مع الاستخدام المتزايد للتكنولوجيا في مختلف المجالات.

وقد أصبح الفضاء السيبيراني مساحة خصبة لممارسات إجرامية جديدة يصعب أحيانا اكتشافها أو ملاحقة مرتكبيها نستخلص فيما سبق دراسته أن موضوع الجرائم السيبيرانية من المواضيع الجد مهمة نظرا لمخاطرها مما يستوجب دراسة معمقة دقيقة حولها فنرى أن المشرع الجزائري حاول جاهدا مواجهة الجرائم الرقمية وسد الثغرات، وقام بإجراء تعديلات هامة على قانون العقوبات وإدراج واستحداث نصوص قانونية تتعلق بهذا المجال لمواكبة التحديات الرقمية، كما توجد أجهزة ومؤسسات تعمل على متابعة هذه الجرائم والتحقيق فيها.

في الختام نؤكد على أن الرصيد التشريعي الجزائري والمنظومة التشريعية الحالية لا تزال غير كافية لمكافحة كل صور الجرائم المعلوماتية مما يستدعي ضرورة تحديثها لتتواكب مع التطورات التكنولوجية السريعة. و عليه إن المكافحة لا تقتصر على الردع القانوني فقط بل تحتاج إلى الوعي من المجتمع و ثقافة رقمية و جهودا متكاملة بين مختلف الفاعلين لضمان بيئة رقمية آمنة.

نتائج الدراسة:

من بين النتائج التي توصلنا إليها:

- ✓ عدم وجود تعريف أو مفهوم موحد و شامل للجريمة الإلكترونية.
- ✓ الجريمة الإلكترونية من بين الجرائم التي يشترط لقيامها توافر القصد الجنائي العام.
- ✓ تعتبر الجريمة الإلكترونية من بين الجرائم الناعمة التي لا تتطلب العنف.
- ✓ هي جريمة مستحدثة وجريمة من الجرائم العالمية العابرة للحدود.
- ✓ قص الخبرة لدى رجال الضبط القضائي وأجهزة العدالة أو الأجهزة الأمنية بصفة عامة فيما يتعلق بثقافة الحاسب الآلي وأنظمة الاتصال.

- ✓ قام المشرع الجزائري بمكافحة هذه الجريمة على غرار باقي الدول بموجب تعديل قانون العقوبات 04/15 وإصدار قانون 09/04 اذ تضمن قواعد إجرائية ووقائية إذ تعتبر خطوة إيجابية في سبيل مكافحة هذه الجرائم.

التوصيات:

من خلال كل العناصر السابقة الذكر خلصنا إلى اقتراح بعض التوصيات التي من شأنها إثراء المنظومة الجزائية للتصدي لهذه الظاهرة و التي تتجلى في:

- ✓ من الضروري تحديث النصوص القانونية باستمرار، مما يعني أنه يجب على التشريع الجزائري متابعة التطورات التقنية السريعة، وهذا يتطلب تعديل القوانين بشكل دوري لسد الثغرات التي قد يستفيد منها المجرمون الإلكترونيون.
- ✓ توفير أدوات تقنية حديثة للتحري تمكن الهيئات المختصة في الكشف عن الجرائم الإلكترونية وتحديد هوية مرتكبيها.
- ✓ إطلاق حملات توعوية لصالح المواطنين والعمل على نشر ثقافة الأمن السيبيراني لدى مختلف شرائح المجتمع.
- ✓ إدراج مادة الأمن السيبيراني في المناهج الجامعية خاصة في كليات الحقوق وكليات الإعلام والمعلوماتية.
- ✓ إعطاء تعريف واحد موحد و شامل للجريمة الإلكترونية.
- ✓ وضع إجراءات قانونية خاصة لهذه الجرائم تختلف عن إجراءات التحقيق في الجرائم التقليدية.
- ✓ تأسيس فرق سريعة لمواجهة الهجمات الإلكترونية، حيث تعمل مجموعات متخصصة على مدار الساعة لمراقبة التهديدات والهجمات الإلكترونية.

في الختام، نود التأكيد على أنه في حال تعرضكم لأي شكل من أشكال التهديد أو الملاحقة من قبل الغير، فإنه يُرجى عدم التردد في التواصل مع الجهات الأمنية والقانونية المختصة لاتخاذ الإجراءات اللازمة وضمان سلامتكم وحماية حقوقكم.

قائمة المصادر والمراجع

قائمة المصادر:

أولا: النصوص القانونية

- **النصوص التشريعية**

-قانون رقم 09/04 المؤرخ في 14 شعبان 1430 سنة 2009، و يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، صادر بتاريخ 2009/08/16 .

- **النصوص التنظيمية**

- المرسوم الرئاسي رقم 341/97 المؤرخ في 1997/09/13 المتضمن انضمام الجزائر مع التحفظ إلى اتفاقية برن المؤرخة في 09/09/ 1869 المتممة في باريس 1909/05/04 والمعدلة في 1997/09/28، ج.ر رقم 01 المؤرخة في 1997/09/14.

- المرسوم الرئاسي 15/261 الذي يحدد تشكيلة وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ثانيا: الكتب

-أسامة احمد المناعة، جلال محمد الزغبي، جرائم تقنية نظم المعلومات الالكترونية، الطبعة الثالثة، دار النشر والتوزيع، عمان2014

-أمير فرج يوسف ، جرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية،الإسكندرية،2009

-أيمن عبد الحفيظ، "إستراتيجية مكافحة جرائم استخدام الحاسب الآلي "، بدون دار النشر

-بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، مصر، 2012

-جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات (رؤية جديدة للجريمة الإلكترونية)، دار البلدية، عمان، الأردن، 2007، طبعة 01

-جميل عبد الباقي الصغير، "القانون الجنائي والتكنولوجيا الحديثة "، الكتاب الأول: "الجرائم الناشئة عن استخدام الحاسب الآلي "، دار النهضة العربية، القاهرة، ط1، 1992،

-خالد حسن احمد لطفي، جرائم الانترنت بين القرصنة الالكترونية وجرائم الابتزاز الالكتروني، دار الفكر الجامعي، الإسكندرية، د ذ ط، 2019

-خالد داودي، الجريمة المعلوماتية، الطبعة الأولى، دار الإعصار العلمي للنشر والتوزيع، عمان، الأردن، 2008

-خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت ، الطبعة الأولى ، دار الثقافة للنشر و التوزيع ، عمان ،الأردن ، 2001

-خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، الأردن، 2011

-د. عبد الله حسين محمود، شرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، ط2، القاهرة، 2002

-رشا علي الدين، النظام القانوني لحماية البرمجيات، دار الجامعة الجديدة، الإسكندرية، 2007

-سامي علي حامد عياد، الجريمة المعلوماتية و إجرام الانترنت ، ماجيستير في القانون ، دار الفكر الجامعي ، 30 شارع سويتر الإسكندرية ، 2008

-سعيدة بعرة ، الجريمة الإلكترونية في التشريع الجزائري ، دراسة مقارنة ،2016

-سليمان احمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدوليةَ (الانترنت)، دار النهضة العربية، القاهرة، 1428هـ/2007م

-ضاح محمود الحمود و نشأت مفقيالمجالي ، جرائم الأنترنت ، دار المنار لنشر و التوزيع ،2005

-عادل محمد فريد نائلة، جرائم الحاسب الآلي الاقتصادية، ط1، منشورات الحلبي الحقوقية، بيروت لبنان 2005

-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري و المقارن ، دار الجامعة الجديدة ، كلية الحقوق ، جامعة الإسكندرية ، 2006

-عبد الفتاح بومبي حجازي، مكافحة جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، مصر، ط1، بدون سنة

-عبد الفتاح بومي حجازي، مكافحة جرائم الانترنت، دار الفكر الجامعي، الإسكندرية، ط1، 2006

-عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم كمبيوتر الانترنت، دار الكتب القانونية، مصر 2007،

-عبد الله عبد الكريم، جرائم المعلوماتية والانترنت، منشورات الحلبي الحقوقية، بيروت، 2007

-كحكد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة الإسكندرية، 2004

-محمد أمين احمد الشوابكة، جرائم الحاسوب الأولى والانترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2004

-محمد حسام محمود لطفي، تأثير اتفاقية تريبس على نظام حماية حق المؤلف، حقوق المؤلف في الوطن العربي، في إطار التشريعات العربية والدولية، المنظمة العربية للتربية والثقافة والعلوم، تونس، 1999

-محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الانترنت، دار النهضة العربية، القاهرة

-محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، مملكة البحرين

-محمود احمد عبابنة، جرائم الحاسوب و أبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2009

-محمود حسام ومحدود لطفي،الحماية القانونية لبرامج الحاسب الالكتروني، دار الثقافة للطباعة والنشر، القاهرة، ط1، 2014

-مختار شبيلي ، الجهاز العالمي لمكافحة الجريمة المنظمة، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2016

-مصطفى يوسف كافي، جرائم الفساد غسيل الأموال السياحة الإرهاب الالكتروني المعلوماتية، مكتبة المجتمع العربي للنشر و التوزيع، الأردن، ط1، 2015

-منير محمد الجنيهي ممدوح محمد الجنيهي، جرائم الانترنت و الحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005

-نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، الطبعة الثانية، دار الفكر الجامعي، مصر، 2011

-نجاة بن مكي، السياسة الجنائية لمكافحة الجرائم المعلوماتية، منشورات دار الخلدونية، 2017

-نهلا عبد القادر المومني، الجرائم المعلوماتية، ماجيستير في القانون الجنائي المعلوماتي، دار الثقافة للنشر والتوزيع 1429هـ/2008م، طبعة الأولى، الإصدار الأول / 2008

-هشام فريد رستم،الجوانب الإجرامية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الانترنت الحديثة، أسيوط، مصر، 1994

هي أكبر منظمة للشرطة الدولية،أنشأت عام 1923، مكونة من قوات الشرطة Interpol- منظمة الشرطة الجنائية الدولية، ل 192 دولة، وللمنظمة أربعة لغات رسمية هي الفرنسية،الإنجليزية، العربية، الاسبانية، مقرها في مدينة ليون في فرنسا، توجد مكاتب وطنية للمنظمة في الدول الأعضاء، وهي منظمة رسمية بين الحكومات تقوم بعدة مهام خاصة في مجال تبادل المعلومات التعاون الدولي للتصدي للجريمة، أنظر إلى كتاب شحادة يوسف،الضابطة العدلية، علاقتها بالقضاء ودورها في سير العدالة الجزائية، دراسة مقارنة، ط1، مؤسسة بحسون للنشر والتوزيع، بيروت

-يوسف، الضابطة العدلية، علاقتها بالقضاء ودورها في سير العدالة الجزائية، دراسة مقارنة، ط1، مؤسسة بحسون للنشر والتوزيع، بيروت.

ثالثا: رسائل جامعية

-أمجد عبد الفتاح احمد حسان، مدى الحماية القانونية لحق المؤلف، دراسة مقارنة، رسالة دكتوراه، جامعة تلمسان، 2008

-بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 17/16 نوفمبر، 2015، كلية الحقوق، جامعة بسكرة

-بريزة عقباش و حنان مبارك ، آليات مواجهة الجريمة الإلكترونية في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2022/2021

- زهير الحاج الطاهر ، آليات الوقاية من الجريمة المعلوماتية ومكافحتها، مذكرة الحصول على شهادة الماجستير في فرع القانون الجنائي، كلية الحقوق، جامعة الجزائر، 2012-2013

-سعيد نعيم ، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ، مذكرة مقدمة لنيل شهادة ماجيستر في العلوم القانونية ، جامعة الحاج لخضر ، باتنة ، 2013/2012

- عبد الرؤوف بوديسة بجاد ، آليات التحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر مهني في الحقوق، تخصص قانون الإعلام الآلي و الانترنت، كلية الحقوق و العلوم السياسية، جامعة محمد البشير الابراهيمي بورج بوعريريج، 2022/2021

-عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة د. الطاهر مولاي، سعيدة، سنة 2016/2015

-عمار حشمان ، الجريمة الإلكترونية في التشريع الجزائري ، مذكرة مقدمة لاستكمال متطلبات شهادة ماستر مهني ، كلية العلوم الاقتصادية و العلوم التجارية و علوم التسيير ، جامعة قاصدي مرياح ، ورقلة ، 2019/2018

-غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم إلى مؤتمر القانون و الكمبيوتر و الانترنت الذي نظمته كلية الشريعة والقانون في الفترة من 3.1مايو2000، جامعة الإمارات العربية المتحدة 2000.

-ليلى لغويلي ، الجريمة الإلكترونية، مذكرة لنيل شهادة ماستر في القانون، تخصص قانون العقوبات والعلوم الجنائية

-محمد بن الأخضر، جرائم الكمبيوتر والانترنت، مذكرة لنيل رتبة ضباط المدرسة العليا للشرطة، بن عكنون، 2008-2007

-محمد بوعمرة، سيد علي بنيال، جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية، تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة اكلي محمد اولحاج، لبويرة، 2019-2020

-مخلوف عكاشة ، دور الشرطة القضائية في مكافحة الجريمة الإلكترونية ، رسالة نيل شهادة ماستر جامعة سعيدة ، السنة الجامعية ،2016-2017

-مليكة بقاح، إشكالية الجرائم الالكترونية في التشريع الجزائري، أطروحة مقدمة لنيل شهادة الدكتوراه في علوم الإعلام والاتصال، كلية علوم الإعلام والاتصال، جامعة الجزائر3 ، 2018-2019

-مليكة عطوي، الحماية القانونية لحقوق الملكية الفكرية على شبكة الانترنت، المؤلف، رسالة دكتوراه، جامعة الجزائر، 2010

-نعيم سعيدان، آليات البحث والتحري عن الجرائم المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجيستر في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة ،2012-2013

-نور الدين فليح، الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة د. مولاي الطاهر، سعيدة، 2019/2018

-هبة نبيلة هروال، جرائم الانترنت، دراسة مقارنة، أطروحة دكتوراه، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة تلمسان الجزائر ،2014/2013

-يوسف صغير، الجريمة المرتكبة عبر الانترنت، مذكرة ماجيستير منشورة، تخصص قانون دولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013

رابعا: المقالات

-أمال حابت، دور الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجلة درية للبحوث القانونية والسياسية

-بن عمر الحاج عيسى، الإنتربول كآلية دولية شرطية لمكافحة الجريمة المنظمة العابرة للحدود، مجلة الدراسات القانونية، السياسية، كلية الحقوق، جامعة الأغواط، العدد 03، جانفي 2016

-حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، ب يروت2014

-سامية عزيز، ما زيا عيساوي، الجريمة من منظور سوسيولوجي، الأسباب الآثار، مجلة دراسات في سيكولوجية الانحراف، السنة 2021، المجلد 6، العدد 1

–لورنس سعيد الحوامدة، "الجرائم المعلوماتية أركاتها ة آليات مكافحتها" دراسة تحليلية مقارنة، مجلة ميوان للدراسات القانونية والشرعية، الأردن، 2016/08/13

–ملياني عبد الوهاب، جرائم المساس بالمعطيات الشخصية على ضوء القانون رقم 18/07، مجلة البحوث القانونية والاقتصادية، الطبعة6، العدد1، بتاريخ 2023/01/28

–مهدي رضا، الجرائم السيبيرانية وآليات المكافحة في التشريع الجزائري، مجلة إليزا للبحوث والدراسات، المجلد 06، العدد 02، 2021

–نادية ضريفي ، سلطات القاضي الجنائي في تقرير الدليل الالكتروني، المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسة القانونية والسياسية، المجلد 04، العدد 02، 2019

خامسا: المداخلات العلمية

–فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر، الجرائم الإلكترونية، طرابلس، 25/24 مارس 2017

–ليندة شرابشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية، القي في الملتقى الدولي حول التنظيم القانوني للأنترنت والجريمة الالكترونية، جامعة زيان عاشور الجلفة، 28/27 افريل 2009

–منية نشناش، مداخلة حول الركن المفترض في الجريمة المعلوماتية، جامعة بسكرة 2015 /2016

–موسى ذياب، الجرائم الإلكترونية، المفهوم والأسباب الملتقى العلمي للجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية، كلية العلوم الإستراتيجية، الأردن، 2014

سادسا: المواقع الالكترونية:

http://www.conventions.coe.int/treaty/fr/treaties/html/189.htm

الانتربول الدولي من موقعhttp://www.interpol.intدستور

قائمة المحتويات

قائمة المحتويات:

العنوان	الصفحة
مقدمة	**أ-د**
الفصل الأول: ماهية الجريمة الإلكترونية	
تمهيد	**02**
المبحث الأول: مفهوم الجريمة الإلكترونية	
المطلب الأول: تعريف الجريمة الإلكترونية وتحديد طبيعتها القانونية	**03**
المطلب الثاني: خصائص وأنواع الجريمة الالكترونية	**08**
المبحث الثاني: أركان الجريمة الإلكترونية ودوافع ارتكابها	
المطلب الأول: أركان الجريمة الالكترونية	**21**
المطلب الثاني: دوافع ارتكاب الجريمة الإلكترونية	**24**
ملخص الفصل الأول	**29**
الفصل الثاني: طرق وآليات مكافحة الجريمة الالكترونية	
تمهيد	**31**
المبحث الأول: الاجهزة المختصة بالمكافحة	
المطلب الأول: الأجهزة الوطنية	**32**
المطلب الثاني: الأجهزة الدولية	**38**
المبحث الثاني: اجراءات المتابعة في الجريمة الالكترونية بين التحري والمحاكمة	
المطلب الأول: إجراءات التحقيق والتحري في الجريمة الالكترونية	**54**
المطلب الثاني: إجراءات المحاكمة والصعوبات التي تواجه مكافحة الجريمة الالكترونية	**59**
ملخص الفصل الثاني	**64**
الخاتمة	**66**
قائمة المصادر و المراجع	**69**
قائمة المحتويات	**II-I**

الملخص

الملخص:

تهدف هذه الدراسة إلى معالجة ظاهرة الجريمة الإلكترونية باعتبارها من أخطر التحديات القانونية المعاصرة، وواحدة من المفرزات السلبية للتقدم التكنولوجي، و قد ركزت الدراسة على دراسة الجريمة الالكترونية و طرق و آليات مكافحتها.

لتحقيق أهداف الدراسة اعتمدنا على المنهج الوصفي و التحليلي لعرض المفاهيم الأساسية للجريمة الالكترونية و أركانها و دوافع ارتكابها، و تم تحليل النصوص القانونية ودراسة الجوانب الإجرائية الخاصة بها، مع رصد أبرز الصعوبات التي تعيق التصدي الفعال لهذا النوع من الجرائم. وخلصت الدراسة إلى ضرورة تعزيز المنظومة القانونية الجزائرية بما يواكب التطور التكنولوجي، وتكثيف الجهود لضمان مواجهة هذه الجريمة.

الكلمات المفتاحية: الجريمة الالكترونية، مكافحة الجريمة الالكترونية، التشريع الجزائري، الأمن السيبيراني.

Abstract:

This study aims to address the phenomenon of cybercrime as one of the most serious contemporary legal challenges and one of the negative outcomes of technological progress. The study focused on studying cybercrime and the methods and mechanisms for combating it.

To achieve the study's objectives, we relied on a descriptive and analytical approach to present the basic concepts of cybercrime, its elements, and the motives for committing it. Legal texts were analyzed, their procedural aspects were studied, and the most prominent difficulties impeding effective response to this type of crime were identified. The study concluded that the Algerian legal system must be strengthened to keep pace with technological developments and that efforts must be intensified to ensure the effective combating of this crime.

Keywords: cybercrime, combating cybercrime, Algerian legislation, cybersecurity.