جامعة محمد بوضياف بالمسيلة

كلية العلوم الإنسانية والاجتماعية

قسم علوم الاعلام والاتصال

دور الدرك الوطني في محاربة الجريمة الالكترونية

المجموعة الاقليمية للدرك الوطني بالمسيلة أنموذجا

مذكرة مكملة لنيل شهادة الماستر في علوم الاعلام والاتصال

تخصص: اتصال وعلاقات عامة

إعداد الطالبة:

سليمة نواوي

إشراف الأستاذة:

د:هدى عكوشي

الأستاذ	الجامعة	الصفة
هدى عكوشي	جامعة المسيلة	مشرفا ومقرر
حجاب عبد الله	جامعة المسيلة	ممتحننا ومناقشا
يوسفي عبد العالي	جامعة المسيلة	رئيسا

السنة الجامعية: 2018/ 2019

إهداء

إلى من قال فيهما الرحمان:{فَلَاتَقُلْلَّهُمَاأُفٍّوَلَاتَنْهَرْهُمَاوَقُللَّهُمَاقَوْلًاكَرِيمًا}

الآية 23من سورة الإسراء

إلى رمز العطاء التي غرست بداخلنا الأخلاق والتي لازمتني ملازمة شعاع الشمس وشجعتني وكانت لي أعذب من الماء وأرفع من السماء وأزكى ومن الورد

أمي الغاليةأطال الله عمرها

إلى الذي فارقني وكانت روحه بداخلي وشعاع شمسه لا يفارقني وإحساسه ونبع حنانه بداخلي والذي كان سر وجودي إلى من أخذه الله إلى جواره دون أن يسعد بثمرة جهدي

أبي رحمه الله وأسكنه فسيح جنانه

إلى من يسري في عروقهم دمي إخوتي:

نور الدين فيصل رفيق شاكرالطاهر وافية ياسمينةسارة

إلى زوجاتهم وأزواجهم وأولادهم كل باسمه

سليمة

شكر وتقدير

الحمد والشكر لله العلي القدير الذي أمدنا بالعون الكافي في انجازنا لهذه المذكرة

سبحانه وتعالىنحمده ونشكره على نعمه وحسن عونه

أشكر الأستاذة **" هدى عكوشي "**

على قبولها الإشراف لهذا العمل ولما قدمته من توجيهات وإرشادات

أشكر لجنة المناقشة على قبولها مناقشة هذا العمل

أشكر كل أساتذتي الذين واكبوا مختلف أطوار دراستي

كما اشكر قيادةالدرك الوطني بالمسيلة لقبولها لطلبنا وتزويدنا بالمعلومات حول موضوع دراستنا

الملخص :

يهدف هذا البحث إلى الوقوف على ماهية الجريمة الإلكترونية مميزاتها و خصائصها و إبراز دور الدرك الوطني في مجال الوقاية من الجريمة الإلكترونية ، بالإضافة إلى معرفة أهم الأساليب و الاجراءات التي تقوم بها الفرقة لمجابهة الجريمة وكشف النقاب عنها. ومن هدا المنطلق جاءت دراستنا للكشف عن دور الدرك الوطني في محاربة الجريمة الالكترونية ؟

وللإجابة عن التساؤل المطروح اعتمدنا في دراستنا على المنهج الوصفي التحليلي الدي ينتمي إلى الدراسات الوصفية ،والدي ساعدنا في وصف هده الظاهرة وتصوير النتائج ،كما استعنا على أدوات جمع البيانات والمعلومات التالية: الملاحظة والمقابلة التي تخدم موضوع دراستنا ،والتي من خلالها توصلنا الى النتائج التالية :

-ادراك ماهية الجرائم الالكترونية باستظهار موضوعها وخصائصها وسندها القانوني ،يتخذ أهمية سلامة التعامل مع هذه الظاهرة مما يسهل عملية التحقيق في حالة وقوع الجريمة .

-توفر جهات وكوادر وأجهزة متخصصة تعنى بعملية البحث والتحري عن الجرائم الالكترونية واثباتها والوصول الى الحقائق والاهداف المرجوة.

-تواجه طرق التحقيق في الجريمة الالكترونية عراقيل وصعوبات متعددة يتعرض لها المحققون خاصة وأنها ترتكب في العالم الافتراضي ولا تترك أي اثر باعتبارها جريمة عالمية يرتكبها اشخاص خارج التراب الوطني والضحية داخل التراب الوطني مما يصعب توقيفه.

الكلمات المفتاحية: الجريمة الالكترونية ،الدرك الوطني ، التحقيق ، البحث ، التحري.

Summary :

The aim of this research is to identify the characteristics of the e-Jizmeh and its characteristics and to highlight the role of the national gendarmerie in the field of cybercrime prevention, in addition to the knowledge of the most important methods and procedures of the group to confront and expose the crime. From this point came our study to reveal the role of the gendarmerie in the fight against electronic crime?
In order to answer this question, we adopted the descriptive descriptive approach that belongs to the descriptive studies. My father helped us describe this phenomenon and the results. We also used the following data and information tools: observation and interview that serve the subject of our study, :
- Recognizing the nature of cybercrime by invoking its subject matter, characteristics and legal authority, the importance of the safety of dealing with this phenomenon is facilitated, thus facilitating the investigation process in case of crime.
- Provide specialized bodies and cadres specialized in the process of research and investigation of electronic crimes and proof and access to the facts and objectives desired.
- The methods of investigating cybercrime face many obstacles and difficulties to the investigators, especially in the virtual world, and leave no trace as a global crime committed by people outside the national territory and the victim within the national territory, making it difficult to arrest him.
Keywords: cyber crime, national gendarmerie, investigation, search, investigation.

مقدمة

مقدمة :

يعيش العالم اليوم أزهى عصوره العلمية والتكنولوجية، والتي يعود الفضل فيها للثورة المعلوماتية، التي حققت طفرة ملحوظة في مستويات التقدم التقني والعلمي شملت نواحي الحياة، خاصة التطور الهائل في مجال الاتصالات وأنظمة المعلومات، المتمثل في ظهور شبكة الانترنت وما وفرته من سهولة الاتصالات داخليا وخارجيا بتبادل المعلومات بشكل فعال، ما جعل هذا العصر يسمى بعصر المعلومات .

فنتيجة لهذا التطور الحاصل وباعتبار الانترنت فضاء مفتوح لا حدود له مقارنة بالحدود الإقليمية للدول،ولكون الكثير من المنظمات والمؤسسات وخاصة المالية منها مرتبطة بهذه الشبكة من أجل التسيير وتقديم مختلف الخدمات لزبائنها،الأمر الذي جعل أصحاب النوايا الإجرامية يتجهون إلى استغلال هذه المنظومات المعلوماتية من أجل ارتكابهم جرائمهم المختلفة نتيجة لما توفره من ميزات خاصة تساعدهم على ذلك، وكذلك من أجل التهرب من المتابعة الجزائية، وأمام هذا الاستعمال المتزايد لهذه المنظومات برز شكل جديد من الإجرام المستحدث خاص بهذه البيئة وهو ما يسمى بالجرائم الإلكترونية CYBER (CRIME).

إن بروز هذا النوع من الجرائم حتم على المجتمع الدولي إيجاد آليات وتقنيات فعالة للحد من انتشارها وتأثيرها، عن طريق سن قوانين وإجراء تعديلات على القوانين السارية بما يمكن وضع إطار قانوني لمكافحة هذا النوع من الجرائم محليا ودوليا.

باعتبار الجزائر واحدة من الدول التي مسها هذا التطور التكنولوجي إيجابا وسلبا، فهي معنية أيضا بمكافحة هذا النوع من الجرائم على غرار الدول المتقدمة، وكان لابد لها من وجود الإطار القانوني المناسب للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أين تم تعديل قانون العقوبات وإصدار قانون خاص لمكافحة الجرائم الإلكترونية .

قيادة الدرك الوطني على غرار مؤسسات الجمهورية شهدت تطورا في استعمال المنظومات المعلوماتية في التسيير وأداء الخدمات ما قد يجعلها عرضة للتهديدات المعلوماتية، وعلى هذا الأساس قامت قيادة الدرك الوطني بوضع آليات تضمن الحماية من هذه التهديدات وذلك باتخاذ العديد من الإجراءات المادية و المعلوماتية والتقنية.

وبما أن الدرك الوطني قوة أنشئت للسهر على الأمن العمومي وحفظ النظام وتنفيذ القوانين والأنظمة، فقد سايرت التطور الإجرامي الذي شهده المجتمع عن طريق توفير الوسائل، تطوير المنظومات وتأهيل الأفراد

المختصين في مكافحة هذا النوع من الإجرام، وذلك بإنشاء العديد من الهياكل المتخصصة في الإسناد القضائي التقني والعلمي، ومن بين هذه الهياكل المتخصصة بهذا النوع من الجرائم مشروع مركز الوقاية من جرائم الإعلام الآلي والجرائم الإلكترونية ومكافحتها.

ولذلك سنتناول في هذه الدراسة **"دور الدرك الوطني في محاربة الجريمة الإلكترونية "** دراسة ميدانية للمجموعة الاقليميةللدرك الوطني بالمسيلة، وقد قسمنا الدراسة إلى إطار منهجي وإطار نظري وإطار تطبيقي .

الإطار المنهجي:وقد اختص بتناول الإشكالية والتساؤلات ثم أهمية الدراسة وأسبابها وأهدافها وبعد ذلك انتقلنا إلى تحديد مفاهيم الدراسة ثم الدراسات السابقة، بالإضافة غلى ذلك إلى منهج الدراسة و أدوات جمع البيانات ومجالات الدراسة والنظرية الوظيفية كنموذج إرشادي في موضوع دراستنا .

أما الإطار النظري فقد قسمناه إلى ثلاثة مباحث:

المبحث الأول:ماهية الجريمة الالكترونية

المبحث الثاني:تصنيف الجريمة الالكترونية

المبحث الثالث: إستراتيجية الدرك الوطني في محاربة الجريمة الالكترونية

أما الإطار التطبيقي:تناولنا فيه تفسير وتحليل البيانات وعرض النتائج وخاتمة الدراسة والملخص إضافة إلى بعض التوصيات.

الفصل الأول

الإطار المنهجي للدراسة

1- الإشكالية :

إن التطور التقني الذي تعيشه اليوم كافة مناطق العالم وبلدانه والمتمثل في استخدام الكمبيوتر والشبكات، أدى إلى استحداث جرائم لم تكن معروفة من قبل، وكثيرا ما تدعى بالجرائم المستحدثة، وهي دون شك جرائم من نوع فريد يحتاج إلى تشريعات خاصة، والى وسائل إثبات مختلفة عن ما كان سابقا.

انتشرت الجرائم الالكترونية خلال السنوات الأخيرة في الدول الصناعية، ولم تكن بلادنا بمنأى عنها نتيجة التطور الكبير الذي تشهده في شتى الميادين إلى جانب استخدام الانترنت إلى نحو متسارع، ولذلك لم يعد من الغريب أن يصبح امن المعلومات هاجس الجميع من منظمات وشركات، لاسيما أن الجريمة الالكترونية تطورت تطورا أدى إلى انتهاك حرمة المعلومات وتعريض أمنها إلى الخطر، ومواكبة للتطور الحاصل على جميع الأصعدة خاصة في مجال المعلوماتية ، باشرت قيادة الدرك الوطني بتنصيب مكتب على المستوى المركزي كمرحلة أولى ممثل في المكتب المركزي لمكافحة جرائم الإعلام الآلي والانترنت التابع للمصلحة المركزية للتحريات الجنائية والذي سيساهم في بلورة نظرة على واقع الجريمة الالكترونية في الجزائر ، وإعطاء وتقييم وتشخيص لواقعها حيث سمح ذلك للدرك الوطني في توفير كامل المعطيات التي جعلته ينطلق في إنشاء المركز الوطني لمكافحة جرائم الإعلام الآلي والانترنت .

وبهذا نطرح الإشكالية التالية :

ماهو دور الدرك الوطني في محاربة الجريمة الالكترونية بالمسيلة ؟

2- تساؤلات الدراسة

1- ماهي الجريمة الالكترونية؟وما أهم خصائصها ؟

2- ماهو دور الدرك الوطني في مواجهة الجريمة في خضم الأساليب والإجراءات الخاصة للبحث والتحري عنها؟

3- ماهي المعوقات التي تواجه إثبات الجريمة الالكترونية؟

4- ما طبيعة الوسائل والتقنيات التي تستخدم في الكشف عن الجرائم الالكترونية؟

3- أهمية البحث

تكمن أهمية البحث أساسا فيكون الجريمة الالكترونية حديثة النشأة، يمتد تأثيرها لجميع الأصعدة لارتباطها بتطور تكنولوجيات الإعلام والاتصال الضرورية واستخداماتها في الحياة اليومية، الأفراد والمؤسسات، خصائصها المتميزة تجعل التعامل معها صعبا ومعقدا،مايحتم إيجاد طرق جديدة وناجعة لمكافحتها .

4- أهداف البحث

نظرا للأهمية البالغة التي تكتسبها مكافحة الجريمة الالكترونية ومافرضته من تحديات خاصة فيعصرنا الحالي، الذي يعرف تطورا متسارعا لتكنولوجيات الإعلام والاتصال ، التي أصبحت ركيزة لمختلف القطاعات العامة والخاصة منها، لذا سنقوم في دراستنا هذه بمحاولة الوصول إلى تحقيق الأهداف التالية :

- الوقوف على ماهية الجريمة الالكترونية، ومميزاتها وخصائصها .
- تحديد مدى تأثير الجريمة الالكترونية على الأمن العام الأشخاص والمؤسسات .
- إبراز دور الدرك الوطني في مجال الوقاية من الجريمة الالكترونية.
- إبراز دور مختلف المتدخلين من الدرك الوطني في ميدان مكافحة الجريمة الالكترونية، ودور مركز الوقاية من جرائم الإعلام الآلي والجرائم الالكترونية ومحاربتها .

5- أسباب اختيار الموضوع

الأسباب الموضوعية

الجرائم الالكترونية جرائم حديثة ذات خصائص متميزة تستعمل التقنيات المتطورة ما جعلها تختلف عن باقي الجرائم التقليدية فرغم تعدد الدراسات والبحوث حول هذه الجريمة من اجل تشخيص خطورتها إلا إنها تفاقمت وتضاعفت مخاطرها ومافتئت تزداد مما اوجب وضع إستراتيجية فعالة للوقاية والتصدي لهذه الظاهرة والوقوف على ضرورة وضع آليات جديدة لأجل مكافحتها.

الأسباب الشخصية

نظرا لما أحدثتها لجريمة الالكترونية من ضجة في العالم،والتهديدات والمخاطر التي مست مصالح المجتمع،اخترنا الخوض في هذا الموضوع أملا منا أن نبين كيفية إثبات الجريمة الإلكترونية وكيفية محاربتها والقضاء عليها من قبل مصالح الدرك الوطني.

6- المدخل النظري للدراسة

النظرية البنائية الوظيفية:

يعد المنظور البنائي الوظيفي من أهم المنظورات وأكثرها واقعية حيث ينظر للمؤسسة باعتبارها شبكة العلاقات الاجتماعية، بحيث أن استمرار التنظيم و وجوده يعتمد على مدى التوافق والانسجام في شبكة العلاقات، ويمثل المنظور البنائي في إطار للعمل يشمل وتمتد الأصول النظرية لذلك المنظور في النموذج العلمي الوضعي في كتابات اميل دور كايم، تالكوتبارسونز، وروبرت ميرتون

وترى تلك النظرية أن الظاهرة الاجتماعية توجد كنتيجة للتفاعل داخل الأبنية الاجتماعية وتكون الوظيفة هي تعزيز ذلك البناء ،تنظر للتنظيم باعتباره رمزا للتفاعل داخل الأبنية الاجتماعية أو نتاجا للتبادل الاجتماعي بحيث يحدث نوع من التوازن بين العلاقات(**الجبوري، 2016، ص124-125**)

افتراضات النظرية:

- تفترض النظرية أن التنظيم وعلاقاته يعد جزءا من نسق أكبر والعمليات التي تؤدي إلى وجود تلك التنظيمات، مثل التعاون والصراع والاتصال، تحدث كنتيجة للتفاعل في أجزاء معينة في النسق تتأثر وتتكيف مع بعضها البعض من اجل حماية البناء ككل، ويعد النموذج البنائي الوظيفي نموذجا ذاتيا إذ يهتم السلوك في إنطاق معناه الذاتي عند الفاعل، فالأفراد من وجهة النظر البنائية الوظيفية يمارسون وأنواعا شتى من الأفعال وأثناء تلك العملية، يتبادلون العلاقات فيما بينهم وإذا رؤى أنه من الضروري المحافظة على العلاقات الاجتماعية، فلا بد من وجود أنواع أخرى من نشاطات جزئية التي تهدف إلى الحفاظ على الكل، وهذا هو المعنى التقريبي للوظيفة.

حيث هي الدور الذي تؤديه الجزء في الحياة الاجتماعية وفي الكل الاجتماعي المتمثل في البناء الذي يتكون من انساق اجتماعية تتوافق فيما بينها، ويقصد بالبناء الاجتماعي مجموعة العلاقات الاجتماعية التي

تتكامل وتنسق الكل الاجتماعي وتحدد بالأشخاص والاجتماعات وما ينتج بينهم من علاقات، وفقا للدور الاجتماعي الذي تمارس في ضوء الكل وهو البناء الاجتماعي .

وترى أن المجتمع يمثل بناءا معقدا، كما لو كان تنظيما معقدا ، وبهذا فان الظاهرة الاجتماعية تعد أكثر من مجرد تجمع من الأفراد ككيان، و بهذا فإنها في حين تنظر التفاعلية الرمزية للجزء حتى تفهم الكل، فان النظرية البنائية الوظيفية تنظر للكل حتى تفهم الجزء، ويرى "ويلسون "أن المنظور للبناء الاجتماعي كما لو كان بناءا تنظيميا يوجد كنتيجة للوظيفة، ومن منظور البنائية الوظيفية فانه يفيد أبحاث الظواهر الاجتماعية وطبيعة موضوع دراستنا تتبنى النظرية البنائية الوظيفية لكون الجريمة الالكترونية ظاهرة عويصة تهدد المجتمع والدرك الوطني بدوره يقوم بالتصدي لهذه الظاهرة .

انتقادات النظرية:

إن تدعيم النسق أو الوضع القائم والتركيز على الجانب الاستاتسكي، وإهمال الصراع مع المبالغة في التأكيد على الانسجام والتوافق في المجتمع والتقليل من أهمية التغير الاجتماعي الذي يعد جزء من طبيعة أي مجتمع هو ما يعاب على ما نادت به النظرية الوظيفية ما تعرض المنظور الوظيفي للنقد من خلال تركيزه على مسألة الاتفاق حول القيم والمعتقدات، وقد لا يوافق بعض أعضاء المجتمع على بعض القيم والمعتقدات، ولكنهم غالبا ما يمثلون للقواعد الأساسية في المجتمع حتى يتسنى لهم إشباع حاجاتهم الضرورية اليومية .

إن هذه الانتقادات المقدمة أو غيرها لم تثن على الدور المهم الذي لعبته النظرية الوظيفية لوضع النظرية السيولوسوجية المتميزة تساهم بشكل فعال في دراسة المشاكل و القضايا الاجتماعية الخاصة بالمجتمع الحديث والتي ظهرت خلال القرنين التاسع عشر والعشرين ، وبذلك فهي أثرت على علم الاجتماع بكل مجالاته وتخصصاته بالكثير من الإسهامات النظرية والأطر التصويرية المساعدة في توجيه البحوث والدراسات التجريبية حتى وقتنا هذا ، هذه الخلاصة من الإسهامات الوظيفية أصبحت جزءا مهما من التراث العلمي الأكاديمي الذي هو مرجعية الكثير من المتخصصين في فروع علم الاجتماع، وغيره من العلوم الاجتماعية الأخرى، مثل علوم الإعلام والاتصال، والأخذ بهذا المنظور كبراديغم للدراسة دليل على ذلك وغيرها من الدراسات الأكاديمية والعلمية الأخرى للنظرية الوظيفية المعاصرة مكانة علية متميزة نظرا لمحاولتها في وضع نظرية سوسيولوجية عامة أو موحدة يمكن عن طريقها الاعتماد في دراسة المشكلات و القضايا المجتمع، كما يمكن اعتبارها بمثابة الإطار المرجعي لتوجيه الباحثين والمتخصصين بصورة علمية لدراسة الواقع الذي يعيشون فيه ولاسيما أن غياب النظرية العلمية السوسيولوجية كان من أهم العوامل التي تأخذ علم الاجتماع كغيره من

العلوم الاجتماعية الأخرى التي لم تتبلور لها نظريات علمية على غرار العلوم الطبيعية التي قطعت شوطا كبيرا من التقدم نتيجة إلى توصلها لعديد النظريات التي خضعت إلى البحث والتجريب والتطور المستمر إلى جانب هذا حرصت الوظيفة على إلزامية تطوير المداخل التحليلية والبحثية المستعان بهما في النظرية الميدانية في نفس الوقت ، إذ لجأ كثير من رواد النظرية الوظيفية التقليدية أمثال" روبرت سبنسر" ، "إميل دوركايم" إلى العديد من المداخل البيولوجية والطبيعية والرياضية وذلك لإثراء البحث الميداني، ومختلف عمليات جمع البيانات واقعية ، وتحليلها وفق طرق علية سليمة وتطور هذا الاهتمام فيما بعد مع المتزعمين الجدد لهذه النظرية "بارسونز" في تحليلاته المركزة على المدخل النسقي وغيرها من المداخل التحليلية المعتمدة على تقديم الكثير من النماذج التصويرية ، والتي يمكن الرجوع إليها كأنساق بنائية فكرية تساهم في تطوير النظرية الوظيفية على المستويين النظري والميداني .

7- تحديد مفاهيم الدراسة

- **الجريمة:**

لغة :من الفعل جرم؛بمعنى تعدى، والمصدر :الجرم هو التعدي والذنب

يقال :جرم يجرم جرما،وأجرم وإجترم فهو مجرم .

اصطلاحا:تعرف الجريمة في القانون"كل عمل أو امتناع يعاقب عليه القانون بعقوبة جزائية" **(الحوامدة،2016، ص5)**

التعريف الإجرائي:هي فعل غير مشروع ،صادر عن أدلة جنائية يقرر لها النظام عقوبة.

- **الجريمة الالكترونية :**

اصطلاحا :هي نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغيرها أو حذفها(**المومني، 2010، ص48**)

إجرائيا:هي الجريمة التي يمكن أن يرتكبها أو يقوم بها شخص يملك جهاز الحاسوب، ويكون متصل بشبكة الانترنت ويكون هدفه إلحاق الضرر بالمجني عليه في سمعته أو مكانته.

➢ **شبكة الانترنت :**

اصطلاحا:هي مجموعة ضخمة من شبكات الاتصال المرتبطة ببعضها البعض ، وهذه المجموعة تنمو ذاتيا بقدر ما يضاف إليه من شبكات وحاسبات ، وقد أدى تغلغلها واتساع مداها إلى وصفها بشبكة الشبكات. (**دليو، بصلي ، 2011، ص49**)

إجرائيا: هي شبكة عالمية تربط أجهزة كومبيوتر عديدة ببعضها البعض في شتى أنحاء العالم ، وهي وسيلة للتواصل السريع وتبادل مختلف المعلومات للأفراد والمؤسسات .

➢ **الحاسب الآلي :**

اصطلاحا:هو مجموعة من الأجهزة المتكاملة تعمل مع بعضها البعض ،بهدف تشغيل مجوعة من البيانات المتداخلة وفقا لبرنامج موضوع مسبقا للحصول على نتائج معينة (**قشقوش، 1992، ص195**)

كما عرف أيضا:بأنه مجموعة متداخلة من الأجزاء لديها هدف مشترك من خلال أداء التعليمات المخزنة، وهو حاسبة إلكترونية ذات سرعة عالية ودقة كبيرة، يمكنها قبول البيانات وتخزينها ومعالجتها للحصول على النتائج المطلوبة (**هلالي ، 1997، ص165**)

إجرائيا:هو مجموعة الأجهزة ذات السرعة العالية والدقة الكبيرة ، التي تشكل نظاما تقنيا وظيفته حل المسائل المختلفة ومعالجتها.

➢ **نظام المعلوماتية:**

اصطلاحا:هو ذلك النظام الذي يستخدم لإنشاء رسائل بيانات وإرسالها أو استلامها أو تخزينها أو تجهيزها على أي وجه آخر.(**ممدوح إبراهيم ، 2008، ص14**)

إجرائيا:هو مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونيا أو إرسالها أو تسلمها أو معالجتها أو تخزينها.

➢ **الهاتف النقال:**

اصطلاحا: عبارة عن جهاز اتصال صغير الحجم، مربوط بشبكة للاتصالات اللاسلكية والرقمية ، حيث تسمح ببث واستقبال الرسائل الصوتية والنصية والصور عن بعد وبسرعة فائقة، ونظرا لمكوناته الإلكترونية العملية فقد يوصف بالخلوي أو بالهاتف النقال (**دليو ، 2003، ص128**)

إجرائيا:هو جهاز اتصال واستقبال يقوم بنقل الرسائل الصوتية واستقبالها بسرعة فائقة.

➢ **الدرك الوطني:**

هو قوة عمومية ذات طابع عسكري، له علاقة خدمات وطيدة مع أجهزة الأمن الأخرى ومع الأجهزة الوطنية، له مشاركة في الدفاع الوطني طبقا للخطط المقررة من قبل وزير الدفاع الوطني وفي محاربة الإرهاب ويتولى مهام الشرطة الإدارية والشرطة العسكرية. تأسس رسميا الدرك الوطني بموجب الأمر 62-19 المؤرخ في 23أوت 1962 بكونه جزء لا يتجزأ من الجيش الوطني الشعبي الجزائري (Https://ar.wikipedia .org.wiki).

إجرائيا: هو قوة عسكرية تمارس مهامها من خلال المراقبة العامة والمتواصلة وإعلام السلطات العمومية وممارسة العمل الوقائي والردعي

8- منهج الدراسة:

لإجراء أي دراسة علمية أو بحث علمي من أجل الوصول إلى حقيقة أو البرهنة على حقيقة ما، وجب إتباع منهج واضح يساعد على دراسة المشكلة وتشخيصها، وذلك بإتباع مجموعة من القواعد والأنظمة العامة التي يتموضعها بغية الوصول إلى حقائق حول الظاهرة موضوع الدراسة والبحث ويعرف المنهج على أنه:أسلوب للتفكير والعمل يعتمده الباحث لتنظيم أفكاره وتحليلها وعرضها وبالتالي الوصول إلى نتائج وحقائق معقولة حول الظاهرة موضوع الدراسة(**ربحي، وآخرون، 2008، ص35**)

كما يمكن تعريفه على أنه:عبارة عن أسلوب من أساليب التنظيم الفعالة لمجموعة من الأفكار المتسارعة والهادفة للكشف عن حقيقة تشكيل هذه الظاهرة او تلك(**عبيدات، وآخرون، 1989، ص33**)

وفي دراستنا هذه المندرجة تحت عنوان "دور الدرك الوطني في محاربة الجريمة الإلكترونية" ارتأينا الاعتماد على المنهج الوصفي التحليلي، بحيث أننا وجدناه المناسب لدراستنا هذه، علما أن طبيعة البحث هي التي

تفرض على الباحث نوع المنهج الذي سيتبعه، فالمنهج الوصفي هو: أسلوب من أساليب التحليل المرتكز على معلومة كافية ودقيقة عن ظاهرة أو موضوع محدد خلال فترة أو فترات زمنية معلومة، وذلك من أجل الحصول على نتائج علمية تم تفسيرها بطريقة موضوعية وبما ينسجم مع المعطيات الفعلية الظاهرة .في حين يرى آخرون بأن المنهج الوصفي هو:عبارة عن طريقة لوصف الموضوع المراد دراسته من خلال منهجية علمية صحيحة وتصوير النتائج التي يتم التوصل إليها على أشكال رقمية معبرة يمكن تفسيرها.

9- أدوات جمع البيانات

أدوات جمع البيانات هي الوسائل والتقنيات التي يستخدمها الباحث قصد الحصول على البيانات والمعلومة المتعلقة بموضوع الدراسة، وعلى الباحث أن يتأكد من أدوات التي اختارها لتمكنه من الحصول على البيانات المطلوبة، وعلى ضوء إشكالية البحث وأهدافه اتضح لنا أن أسلوب الملاحظة والمقابلة هو انسب أدوات البحث وأكثرها ملائمة لجمع المعلومات المتعلقة ببحث موضوع الدراسة.

1- **الملاحظة**: هي أسلوب من الأساليب الجيدة لكشف وحل المشاكل وهذا يتطلب الموضوعية والدقة وأن يكون الباحث بعيدا عن التحيز والأهواء الشخصية وقد تكون مباشرة بالأشياء المادية والنماذج المهمة وهذا الشيء سهل لأنها تعتمد على العدد والقياس(**محجوب، 2014، ص177**).

وتعرف أيضا بأنها توجيه الحواس والانتباه إلى الظاهرة أو مجموعة من الظواهر رغبة في الكشف عن صفاتها وخصائصها، بهدف الوصول إلى كسب معرفة جديدة عن تلك الظاهرة أو الظواهر(**زيدان، 1980، ص46**).

وقد اجمع الباحثون على أن الملاحظة كأداة هي من أهم الأدوات التي تستخدم في البحث العلمي، ومصدرا أساسيا للحصول على البيانات والمعلومات اللازمة لموضوع الدراسة، خاصة إذا استخدمت بطريقة مخططة ومصممة للجوانب التي ستتم ملاحظتها وتسجيل البيانات عنها(**بن مرسلي، 2005، ص203**)

أنواعها:

- **الملاحظة البسيطة**: هي عبارة عن ملاحظة يستخدمها الباحث عشوائيا ولا تخضع للضبط العلمي الدقيق لأن الباحث يقوم بها دون تخطيط مسبق .

- **الملاحظة المنتظمة**:وهي الملاحظة التي يقوم بها الباحث يكون خطط وحدد نوع السلوك المراد ملاحظته بصورة إجرائية وأعد الأداة المناسبة للملاحظة طبقا للهدف الذي يسعى إلى تحقيقه.

- **الملاحظة المباشرة:**قد يلجأ الباحث إلى المشاهدة المباشرة التي تتم عن طريق الاتصال المباشر بالظاهرة المطلوب ملاحظتها ومراقبة سلوكها بكل دقة والتعايش بغرض المعلومات المتعلقة بها.

- **الملاحظة بالمشاركة:**هنا يقوم الباحث بدور ايجابي كواحد من أفراد العينة المبحوثة، فيعيش معهم حياتهم بكل جوانبها، ومن المهم في هذا النوع إلا يكشف الباحث عن هويته حتى يبقى سلوك عينة البحث طبيعيا وعفويا بدون تكلف حيث تتيح للباحث الملاحظة السلوك بصورة عفوية وطبيعية دون تكلف أو تصنع.

- **الملاحظة بدون مشاركة:** يقوم الباحث هنا بدور المراقب للعينة المبحوثة دون أن ينخرط مع المبحوثين ولكن المعلومات التي تتجمع بهذه الطريقة قد يعتريها التشويه الذي يتكلف ويتصنع أومن قبل الباحث نتيجة للذاتية والتحيز.

والملاحظة أول أداة استعملناها وبدأنا ممارستها من اختيار الموضوع بحيث لاحظنا التطور التكنولوجي الهائل وما صاحبه من تطورات وكذلك تفاقم الجريمة الالكترونية وتطورها بشكل واسع في الآونة الأخيرة وملفت للنظر.

كما قمنا بأخذ العديد من الملاحظات من خلال الزيارات الميدانية المتعددة لمقر المجموعة الإقليمية للدرك الوطني بالمسيلة محل الدراسة، فيما يخص طرق الاستقبال وكيفية تقديم المعلومات حول الجريمة الإلكترونية ومدى انتشارها وكيفية ردعها من خلال الطرق المقدمة لنا في محاربتها .

2- المقابلة:

تعرف على أنها تفاعل لفظي يتم بين فردين في موقف المواجهة يحاول أحدهما أن يعرف بعض المعلومات لدى الأخر، والتي تدور حول خبرته وأرائه ومعتقداته وتكون ذات صلة بالظاهرة قيد الدراسة(**علي، 2006، ص119**).

هي لقاء بين شخصين فأكثر لتحقيق هدف ما، من خلال طرح الأسئلة الهادفة من قبل المقابل على شخص تجري معه مقابلة ، والتي يصاحبها عادة الكثير من الانفعالات الناجمة عن سؤال ورد فعل على هذا السؤال وكل هذه العملية تهدف إلى جمع أكبر قدر من المعلومات والبيانات المقصودة من الباحث ليستفيد منها في تحقيق هدفه من المقابلة.

أهمية المقابلة:

تبرز أهمية المقابلة فيما يلي :

- تعتبر عملية تتيح الفرصة للمستجيب للتعبير الحر عن الآراء والأفكار والمعلومات.
- تتحول من أداة اتصال ووسيلة التقاء غلى تجربة عملية.
- تعتبر المقابلة مصدرا كبيرا لبيانات والمعلومات عن كونها أداة للتعبير والتوعية والتفاعل الديناميكي.
- تختلف أهداف المقابلة باختلاف الغاية التي تستهدف المقابلة إلى تحقيقها في نهاية المطاف ويتضح ذلك من الأنواع المختلفة للمقابلة، فلكل نوع هدفه وغرضه المحدد وغايات يحاول المقابلون الوصول إليها(**العكش ، 1986، ص 55**).

وقد استعنا بالمقابلة غير المقننة المفتوحة لطرح الأسئلة بطريقة حرة موجهة في شكل إثارة للعديد من النقاط والأبعاد والخلفيات المختلفة للنقطة المبحوثة قصد استكشاف مختلف جوانبها، وهذا النوع من الأسئلة هو المناسب لجعل المبحوث يسترسل في الكلام لإعطاء المزيد من المعلومات والبيانات .

حيث عملنا على مقابلة الرائد والنقيب المكلفين بالإعلام والاتصال على مستوى المجموعة ا لإقليمية للدرك الوطني بالمسيلة محل الدراسة، بقصد إعطائنا المعلومات المراد الحصول عليها والبيانات الكافية حول موضوع دراستنا وإفادتنا بآرائهم لإتمام هذه الدراسة.

ولقد صيغت أسئلة المقابلة محورين أساسين جاءا كالتالي :

المحور الأول:المبادئ الأساسية للتحقيق في الجرائم الالكترونية

المحور الثاني:دور مختلف مصالح الدرك الوطني في مجال الوقاية من الجريمة الإلكترونية ومحاربتها.

10- التعريف بمجتمع البحث وعينة الدراسة :

مما لاشك أن لكل بحث أو دراسة مجتمع تدور حوله الدراسة، وعادة ما يواجه الباحثون مشكلة الأعداد الكبيرة لمجتمع بحث الدراسة وهو ما يصعب دراسة خاصة من ناحية الجهد والمال والوقت،إضافة إلى الصعوبات التي تواجه الباحث أثناء جمع البيانات مع جميع أفراد مجتمع البحث وهو ما يجعل البحث يقلص في مجتمع بحثه إلى عدد صغير يسهل عليه جمع البيانات القدرة على التحكم فيها .

حيث اعتمدنا في دراستنا على العينة القصدية: وتعرف تحت أسماء متعددة مثل العينة العرضية أو النمطية، يقوم الباحث باختيار مفرداتها بطريقة تحكمية لامجال فيها للصدفة،بل يقوم شخصيا باقتناء المفردات لإدراكها لمسبق ومعرفتها لجيدة لمجتمع البحث والعناصر الهامة.

وقدتماختيارناالهذاالنوعمنالعينةباعتبارهاتتناسبمعموضوعالدراسة،وأيضـالأننااعتمدناااختيارالمبحوثين،وعليهفقد اخترناعينةتتكونمنضابطينبالمجوعةالإقليميةللدركالوطنيبالمسيلةالمكلفينبالإعلاموالاتصالوكانترتبتهمرائدونقيب.

11- مجال الدراسة

المجال المكاني:

أجريت الدراسة بالمجموعة الإقليمية للدرك الوطني بالمسيلة التابعة لوزارة الدفاع الوطني، التي تقع في وسط مدينة المسيلة، المتواجدة بالتحديد في شارع الحاج عيسى مقابل الدائرة في الجهة الغربية، تعتبر قوة عسكرية منوطة بها مهام الأمن العمومي تمارس مهامها من خلال المراقبة العامة والمتواصلة ، والاستعلام وإعلام السلطات العمومية وممارسة العمل الوقائي والردعي.

المجال الزمني:

يقصد بها المدة الزمنية المستغرقة في إجراء الدراسة الاستطلاعية إلى نهاية البحث العلمي ، وعليه فقد استغرقت دراستنا الميدانية لموضوع بحثنا مدة شهر من9 افريل إلى 9 ماي ، وقسمت الفترة إلى 3مراحل :

- **المرحلة الأولى**: في هذه المرحلة قمنا بزيارة المؤسسة موضوع الدراسة، حيث تم إعطائنا وتزويدنا بالمعلومات الكافية حول موضوع الدراسة وأملاكن انتشارها وتوسعها، وكان ذلك يوم 9أفريل 2019.

-**المرحلة الثانية**:بدأنا بالتعمق بالدراسة، وعقدنا مرة أحرى مقابلة مع الرائد والنقيب واتضح من خلال هذه المرحلة وقوفنا على المحاور الأساسية لموضوع بحثنا.

-**المرحلة الثالثة**:حيث تم مرة أخرى مقابلة مع الرائد للوقوف على بيانات ومعلومات إضافية تخص الدراسة وقد قام بتزويدنا بكل النقائص في موضوع الدراسة.

12- الدراسات السابقة

➢ **الدراسة الأولى**

"آليات البحث عن الجريمة المعلوماتية في القانون الجزائري "، *مذكرة لنيل* شهادة الماجستير في العلوم الجنائية لنعيم سعيداني، جامعة الحاج لخضر باتنة 2013/2012. كان الهدف من هذه الدراسة محاولة المساهمة في وضع الخطوط العريضة للتعرف على طرق التحقيق في الجريمة المعلوماتية.

انحصرت إشكالية الدراسة فيما يلي: هل استجاب المشرع الجزائري لهذه المبررات واستحدث في سبيل ذلك تشريعات جديدة لمعالجة آثار وانعكاسات التقنية المعلوماتية على إجراءات البحث والتحري؟وإلى أي مدى وفق المشرع في استحداث طرق إجرائية في سبيل البحث والتحري عن الجريمة والمجرم المعلوماتي؟

ويتفرع عن سؤال الدراسة الرئيسي، الأسئلة الفرعية التالية:

- ما هي خصائص الجريمة المعلوماتية وكذا خصائص المجرم المعلوماتي، وما مدى تأثيرها على إثبات الجريمة وإسنادها للمتهم؟
- ما طبيعة الدليل المناسب لإثبات الجريمة المعلوماتية، وما هي خصائصها؟
- كيف يمكن استخلاص الدليل الرقمي من البيئة الإلكترونية التي يتواجد بها ؟
- ما هي الصعوبات والمعوقات التي تواجه جهات البحث والتحري في استخلاص الدليل الرقمي ؟
- كيف تعامل المشرع مع هذا الدليل الرقمي في مجال الإثبات الجزائي من حيث كونه دليلا علميا وأثر هذه الخاصية على مبدأ الاقتناع الشخصي للقاضي الجزائي؟
- ما مدى حجية المخرجات الإلكترونية في الإثبات نظرا لطبيعتها الخاصة بالمقارنة بوسائل الإثبات التقليدية؟

لتحليل هذه الدراسة استخدم الباحث المنهج الوصفي، للقيام بوصف ظاهرة الجريمة الإلكترونية وتحديد بعض المفاهيم التي تقوم عليها الدراسة، بالإضافة إلى مناهج أخرى كتكميلية تتمثل في المنهج المقارن والتحليلي والتأصيلي للجوء إليهم كلما تطلب البحث ذلك.

وقد قسم الباحث بحثه إلى فصلين، الفصل الأول كان لتحليل الجوانب القانونية للجريمة المعلوماتية، أما الفصل الثاني فتناول فيه الجوانب القانونية للتحقيق وإجراءات جمع الدليل في الجريمة المعلوماتية.

وقد لخصت الدراسة في النتائج التالية:

- إن من أهم مميزات جرائم الاعتداء على نظم المعالجة الآلية للمعطيات أنها تنصب على محل من نوع خاص، يختلف تماما على محل الجرائم التقليدية على هيئة إشارات ونبضات غير مرئية تنساب عبر أجزاء النظام المعلوماتي وشبكات الاتصال العالمية.

- إن الدليل الرقمي على ضوء ما أسفرت عليه التطورات التقنية في مجال المعلوماتية لا يغني عنه أن يتم الحصول عليها بالطرق القانونية، وأن يقدم للمحكمة على نفس الهيئة التي تم جمعه عليها، بأن لا يطرأ عليه أي تغيير أو تحريف خلال فترة حفضه.

- أن القاضي الجزائري يتمتع بدور إيجابي من حيث تقدير القيمة القانونية للدليل الرقمي وخضوعه للسلطة التقديرية، شانه في ذلك شأن باقي الأدلة.

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

جوانب الاستفادة والاختلاف :

جوانب الاستفادة: محاولة التعرف على طرق التحقيق وإثبات الجريمة الإلكترونية.

نقاط الاختلاف: اختلف الباحث نعيم سعيداني في إشكالية الدراسة، وكذلك عنوان ومجالها الزماني والمكاني .

- **الدراسة الثانية**

"الجرائم الإلكترونية في *التشريع الفلسطيني* " دراسة تحليلة مقارنة، مذكرة لنيل شهادة الماجستير في القانون العام ،كلية الشريعة والقانون ، من إعداد "يوسف خليل يوسف العفيفي"، الجامعة الإسلامية غزة ، 2013 .

تهدف هذه الدراسة غلى تقديم رؤية قانونية متكاملة حول الجرائم الإلكترونية ،أنواعها وأركانها والأحكام الموضوعية والإجرائية فيها، بيان مدى فاعلية نصوص التجريم للجرائم الإلكترونية في التشريع الفلسطيني مقارنة مع التشريع الأردني والقوانين العربية الأخرى، وكذلك معرفة سلطات الضبط القضائي والنيابة العامة والتمييز بينهما في التحقيق في الجرائم الإلكترونية ، وكذلك المحكمة المختصة بالنظر فيها.

وقد تمحورت أسئلة هذه الدراسة فيما يلي :

- ما هي الجريمة الإلكترونية ؟
- ما هي خصائص الجريمة الإلكترونية؟
- ما هي إجراءات التحقيق في الجريمة الإلكترونية ؟
- ما هو موقف المشرع والقضاء الفلسطيني من الجريمة الإلكترونية؟
- هل يتناسب الجزاء الجنائي المقرر على مرتكب الجرائم الإلكترونية مع جسامة السلوك المرتكب؟

ولتحليل هذه الدراسة اعتمد الباحث على المنهج المقارن للمقارنة بين القانون الفلسطيني والقانون الأردني ،بالإضافة إلى المنهج الوصفي التحليلي لجملة من النصوص القانونية للوقوف على معرفة الجريمة الإلكترونية منحيث ماهيتها وخصائصها وأركانها ، والجزاء الجنائي المترتب على ارتكابها.

وقد قسم البحث دراسته إلى ثلاثة فصول ،الفصل الأول كان يشمل الجريمة الإلكترونية، تعريفها، صورها وطبيعتها، والفصل الثاني يشمل القواعد الموضوعية للجرائم الإلكترونية ، والفصل الثالث القواعد الإجرائية للجريمة الإلكترونية.

وقد لخصت نتائج الدراسة في جملة من الاستنتاجات وهي كالآتي:

- الجريمة الإلكترونية هي الجريمة التي تتكون من فعل وامتناع عن فعل باستخدام إحدى الوسائل الإلكترونية بشكل غير مشروع، يوقع ضررا يلحق بالغير يعاقب عليه المشرع الجزائي.
- تتميز الجريمة الإلكترونية بعدة خصائص لا نجدها في الجرائم التقليدية، مثل الطابع التقني لهذه الجريمة وكونها عابرة للحدود.
- الوسائل الإلكترونية الحديثة أصبحت جزءا مهما من حياتنا الشخصية والمهنية .
- إن أكثر الأساليب التي تستخدم في مهاجمة البيانات وإتلافها الفيروسات ، حيث تظهر فيروسات جديدة من حين لآخر، ويكون الفيروس الجديد أقوى من القديم.
- لم يتناول قانون العقوبات الفلسطيني ولا مشروع قانون العقوبات الذي لا يزال تحت أروقة المجلس التشريعي جميع صور الجرائم الإلكترونية.

جوانب الاستفادة ونقاط الاختلاف

جوانب الاستفادة: من خلال تطرق الباحث إلى تقديم رؤية متكاملة حول الجرائم الإلكترونية وخصائصها وأنواعها وحداثتها في المجتمع.

جوانب الاختلاف: كما اختلفت دراستنا مع هذه الدراسة في المجال الزماني والمكاني، والأهداف التي سعت إليها وكذلك في الموضوع الذي تناوله الباحث.

الفصل الثاني

الإطار النظري للدراسة

تمهيد:

رغم المزايا الهائلة التي تحققت بفضل تقنية المعلومات على جميع الأصعدة وفي شتى ميادين الحياة المعاصرة فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة جراء سوء استخدام هذه التقنية المتطورة أو الانحراف عن الأغراض المرجوة منها حيث شكلت أرضا خصبة لكثير من الأنشطة غير المشروعة فأصبحت بذلك الحاسبات الآلية توفر للحياة وسيلة هامة لارتكاب العديد من الجرائم حتى التقليدية منها وساهمت بذلك في تفشي طائفة من الظواهر الإجرامية المستحدثة، ألا وهي ظاهرة الجرائم الالكترونية.

ولما كانت الجريمة الالكترونية ظاهرة إجرامية جديدة ونظرا لارتباطها بالتكنولوجيا الحديثة فقد ترتب على ذلك إحاطة هذه الظاهرة بالكثير من الغموض، لأجل ذلك فقد بدا لنا أنه وقبل الخوض في المسائل الإجرامية التي تنطبق على الجريمة الالكترونية أن ننوه بجانب من المفاهيم الأساسية لهذه الظاهرة الإجرامية إذ يجب الإلمام بماهية الجرائم الالكترونية، تصنيفها، خصائصها، ومختلف أطراف الجريمة.

المبحث الأول: ماهية الجريمة الالكترونية.

سنتطرق في هذا المبحث إلى تعريف الجريمة الالكترونية من المفهوم الضيق والمفهوم الواسع، ثم نتناول التطور التاريخي للجريمة الالكترونية، أنوعها وخصائصها.

المطلب الأول: تعريف الجريمة الالكترونية.

تتكون الجريمة الالكترونية من مقطعين هما: الجريمة والالكترونية ويستخدم مصطلح الالكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات، أما الجريمة وهي السلوكيات والأفعال الخارجة على القانون.

والجرائم الالكترونية هي المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشرا أو غير مباشر باستخدام شبكات الاتصالات مثل الانترنت (غرف الدردشة، البريد الالكتروني، الموبايل)(**البداينة ، 2014، ص2**).

إن مسألة وضع تعريف للجريمة الالكترونية كانت محلا لاجتهادات الفقهاء، لذا ذهب الفقهاء في تعريف الجريمة الالكترونية مذاهب شتى وضغط تعريفات مختلفة ويتراوح تعريف الجريمة الالكترونية بين الجرائم التي ترتكب بواسطة الحاسوب إلى جرائم ترتكب بأي نوع من المعدات الرقمية(**البداينة، نفس المرجع، ص3**).

وتعرف الجرائم الالكترونية باختصار على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال (**البداينة ، نفس المرجع ، ص3**).

وهناك من عرفها على أنها الجرائم ذات الطابع المادي التي تتمثل في كل سلوك غير قانوني من خلال استخدام الأجهزة الالكترونية ينتج عنها حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة، وغالبا ما يكون هدف هذه الجرائم هو القرصنة من أجل السرقة أو إتلاف المعلومات الموجودة في الأجهزة ومن ثم ابتزاز الأشخاص باستخدام تلك المعلومات.

لقد تعددت تعاريف الجريمة الالكترونية وهناك من تناولها من الزاوية التقنية أو من الزاوية القانونية، وهناك من عرفها اعتمادا على وسيلة ارتكاب الجريمة (**طالبي المل، 2017ص9**).

كما وعرفت منظمة التعاون الاقتصادي والتنمية التابعة للأمم المتحدة الجريمة الالكترونية بأنها: "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية الالكترونية" (**المراغي ، 2017، ص27**).

عرفها الأستاذ جون فوستر "John Foster" بأنها " فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية" (**الحلبي ، 2011ص27**).

كما أن هناك جانب من الفقه لا يهتم بالوسيلة أو موضوع الجريمة الالكترونية ويعرفها بوصفها مرتبطة بالمعرفة الفنية أو التقنية باستخدام الحاسب الآلي، ولذلك عرفت هذه الجريمة بأنها: " جريمة يكون متطلبا لاقتراف أن تتوافر لدى فاعلها بتقنية الحاسوب".

وبذلك عرفها الدكتور هشام رسم بأنها " أي جهد فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبيه".

كما عرفت الجريمة الالكترونية بالقول هي "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها"(**الشكري، ص113**).

لم يتفق الفقه على تعريف موحد للجرائم الالكترونية وإنما انعكست هذه الظاهرة الحديثة في نشأتها نسبيا على اتجاهات العديد من الفقهاء الاقتصاديين والجنائيين حول وضع تعريف جامع وموحد لها.

وقد بذلت محاولات متعددة وتسعى إلى أبعاد تعريف مناسب لتلك الجرائم وإن كانت لا تخرج جميعها عن أحد اتجاهين، أولهما: مضيف لمفهوم الجرائم الالكترونية، والآخر موسه لهذا المفهوم على النحو الآتي:

أولا: الاتجاه الضيق لمفهوم الجريمة الالكترونية:

يذهب أنصار هذا الاتجاه إلى القول بأن الجرائم الالكترونية هي كل سلوك غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية وتملا دقته وتحقيقه من ناحية أخرى، وطبقا لهذا التعريف فإنه يجب أن تتوافر معرفة تكنولوجيا الحاسبات الآلية بدرجة كبيرة، ليس فقط من أجل ارتكاب الجريمة الالكترونية ولكن أيضا من أجل التمكن من ملاحقتها والتحقيق فيها على نحو صحيح، أي أن يكون مرتكب الجريمة الالكترونية والقائمون على ملاحقتها على درجة كبيرة من العلم بهذه التكنولوجيا، وقد أخذت وزارة

العدل الأمريكية بهذا التعريف في تقرير صادر عنها عام 1989 يتعلق بالجرائم الالكترونية.(**ابو بكر سلامة، 2006ص13**)

ويذهب أنصار هذا الاتجاه إلى أن الجرائم التي تفتقر إلى هذه الدرجة من المعرفة تعد جرائم عادية، تتكفل بها النصوص التقليدية للقوانين الجنائية فلا حاجة لنا في هذه الحالة إلى نصوص جديدة للتعامل مع هذه الأفعال، وذلك على خلاف الجرائم التي تتوافر لها هذه المعرفة فهي بحاجة إلى نصوص تتلائم مع طبيعتها التي تختلف عن غيرها من الجرائم التقليدية.

بل إن البعض من أنصار هذا الاتجاه قد ذهبوا لأبعد من هذا فالجريمة الالكترونية لديهم ليست هي التي يكون الحاسب الآلي أداة لارتكابها، وإنما هي التي تقع على الحاسب أو داخل نظامه فقط، فوفقا لهذا الفقه فإن الجريمة الالكترونية هي كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومة المخزنة داخل الحاسب الآلي أو تلك التي يتم تحويلها عن طريقه. (**أبو بكر سلامة، المرجع السابق، ص13**)

ثانيا: الاتجاه الموسع من مفهوم الجريمة الالكترونية

تباينت مواقف أنصار هذا الاتجاه في تعريفهم للجرائم الالكترونية، حسب نظرتهم التي يمكن أن يمتد إليها نطاق هذه الجرائم(**ابو بكر سلامة، المرجع السابق، ص14**).

فقد ذهب بعض الأنصار هذا الاتجاه إلى القول بأن الجريمة الالكترونية هي كل فعل غير مشروع يتم بمساعدة الحاسب الآلي، أو هي كل جريمة تتم في محيط الحاسبات الآلية.

وبما هذا التعريف أنها ما ذهبت إليه مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية سنة 1983، عند تناولهم موضوع الإجرام المرتبطة بالمعلوماتية حيث ذهبوا إلى القول بأن الجريمة الالكترونية هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به بتعلق بالمعالجة الآلية للبيانات أو بنقلها.

وقد أخذ على هذا الاتجاه أنه يوسع كثيرا من مفهوم الجريمة الالكترونية، حيث أن مجرد مشاركة الحاسب الآلي في النشاط الإجرامي يضفي على هذا النشاط وصف الجريمة الالكترونية وهذا ينطوي على مغالطة جسمية، فالحاسب الآلي قد لا يعدو وأن يكون محلا تقليديا في بعض الجرائم (كسرقة الحساب الآلي أو الأقراص أو الاسطوانات الممغنطة) وعلى ذلك لا يمكن إسباغ وصف الجريمة الالكترونية على سلوك الفاعل، لمجرد أن الحاسب أو أي من عناصره المادية كانوا محلا لفعل الاختلاس أحد عناصر الركن المادي لجريمة السرقة.

المطلب الثاني: التطور التاريخي للجريمة الالكترونية.

لقد ظهرت الانترنت في حقل جرائم التقنية العالية في نهاية الثمانينات وكان ذلك من خلال العدوان الفيروس وبالأخص جريمة " دودة موريس" المؤرخة واختتمتها في نوفمبر 1988.

ولقد أطلق مصطلح جرائم الانترنت في مؤتمر عقد في أستراليا في الفترة 16-1998/02/17، وتجدر الإشارة إلى أن الكثير من الباحثين يستخدمون مصطلحات غير دقيقة للتعبير عن جرائم الانترنت، إذ نجد البعض يستخدم مصطلح "الإجرام المعلوماتي" في حين أنه يجب استخدام المصطلح الدقيق والمتماشي مع طبيعة تلك الجرائم وهو " جرائم الانترنت" ذلك لأن الإجرام المعلوماتي وإن كان يقصد التعبيرعن الجرائم الواضعة عن طريق جهاز الكمبيوتر، إلا أن هذا لا يعني من جهة أخرى أن الاعتداء عن طريق جهاز الكمبيوتر إلا ان هذا لا يعني من جهة أخرى أن الاعتداء على المعلومة يتحقق دائما باستخدام الكمبيوتر وخصوصا استخدام الانترنت، ذلك لأن الوسائل التقليدية هي دائما ما تكون أداة لارتكاب تلك الجريمة وبالتالي فالجريمة الالكترونية قد تكون أشمل من جرائم الانترنت وذات الشأن بالنسبة للغش المعلوماتي وكذا جرائم التكنولوجيا المتقدمة

ولقد لاحظ مؤتمر القانون والانترنت المنعقد في لشبونة/ البرتغال في 2001/01/26 أنه يجب عدم الالتفات إلى مثل هذه المصطلحات غير الدقيقة، واعتماد مصطلح Cyber cum دون غيره للتعبير عن جرائم الانترنت مع الأخذ في الاعتبار التمييز بين تلك الجرائم التي يمكن ارتكابها عبر الانترنت (**بعرة، 2016، ص15**).

مرت جرائم الانترنت بتطور تاريخي تبعا لتطور التقنية واستخدامها ولهذا مرت بثلاث مراحل هي:

المرحلة الأولى: من شيوع استخدام الحواسيب من الستينات من القرن الماضي اقتضت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم شيء عابر أم ظاهرة إجرامية مستحدثة، إن الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة ومع تزايد استخدام الحواسيب الشخصية في السبعينات ظهرت عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر وعالجت

عددا من قضايا الجرائم الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة. (**أبو بكر سلامة، المرجع السابق، ص16-17**).

المرحلة الثانية: في الثمانينات حيث طفا على السطح مفهوم جديد لجرائم الكمبيوتر والانترنت وارتبطت بعمليات اقتحام نظام الكمبيوتر عن بعد وأنشطة نشر وزرع الفيروسات الالكترونية التي تقوم بعملية تدميرية للملفات أو البرامج(**عبد الفتاح ، ص43**).

شاع اصطلاح "الهاكرز" المعبر عن مقتحمي النظام لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل محظورا في رغبة المحترفين تجاوز أمن المعلومات وإظهار تفوقهم التقني، ولكن هؤلاء المغامرون أصبحوا أداة إجرام، وظهور المجرم المعلوماتي المتفوق المدفوع بأغراض إجرامية خطيرة القدرة على ارتكاب أفعال تستهدف الاستيلاء على أعمال أو التجسس على البيانات السرية والاقتصادية والاجتماعية والسياسية والعسكرية.

المرحلة الثالثة: شهدت التسعينات تناميا هائلا في حقل الجرائم الالكترونية وتغييرا في نطاقها ومفهومها وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات ظهرت أنماط تقوم على فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد وأكثر ما مورس ضد مواقع الانترنت التسويقية الهامة التي يتسبب انقطاعها عن الخدمة ساعات في خسائر مالية بالملايين، ونشطت جرائم نشر الفيروسات عبر المواقع الالكترونية لما تسهله من انتقالها إلى ملايين المستخدمين في ذات الوقت وظهرت الرسائل المنشورة على الانترنت أو المراسلة بالبريد الالكتروني المنطوية على الأحقاد أو المساس بكرامة واعتبار الأشخاص أو المروجة لمواد غير قانونية أو غير مشروعة

المطلب الثالث: أنواع الجرائم الالكترونية.

نظرا لانتشار الجريمة الالكترونية بشكل كبير فقد تعددت أنواع هذه الجرائم وأهمها ما يلي:

1. الجريمة المادية (Financial Crime)

وهي التي تسبب أضرارا مادية على الضحية أو المستهدف من عملية النصب، وتأخذ واحدة من الأشكال الثلاثة التالية:

– عملية السرقة الالكترونية كالاستيلاء على ماكينات الصرف الآلي، والبنوك كتلك المنتشرة الآن في الكثير من الدول وبها يتم نسخ البيانات الالكترونية لبطاقة الصراف الآلي ومن ثم استخدامها لصرف أموال حساب الضحية. (**هلال المزاهرة ، 2014، ص374**).

– إنشاء صفحة انترنت مماثلة جدا لموقع أحد البنوك الكبرى أو المؤسسات المالية الضخمة، لتطلب من العميل إدخال بياناته أوتحديث معلوماته بقصد الحصول على بياناته المصرفية وسرقتها.

– الرسائل البريدية الواردة من مصادر مجهولة بخصوص طلب المساهمة في تحرير الأموال من الخارج من الوعد بنسبة من المبلغ، أو تلك التي توهم صاحب البريد الالكتروني بفوزه بإحدى الجوائز أو اليانصيب، وتطالبه بموافاة الجهة برقم حسابه المصرفي. (**هلال المزاهرة ،المرجع السابق، ص375**).

2. الجريمة الثقافية: (Cultural Crime).

هي استيلاء المجرم على الحقوق الفكرية ونسبتها له من دون موافقة الضحية ومن الممكن أن تكون على إحدى الصور التالية:

– قرصنة البرمجيات وهي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية على أسطوانات وبيعها للناس بسعر أقل.

– التعدي على القنوات الفضائية المشفرة وإتاحتها عن طريق الأنترنت من خلال تقنية Soft Copy.

– جريمة لنسخ المؤلفات العلمية والأدبية بالطرق الالكترونية المستحدثة.

3. الجريمة السياسية والاقتصادية (Political And Economic Crime).

– تستخدم المجموعات الإرهابية حاليا تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية وهم لا يتوانون عن استخدام الوسائل المتقدمة مثل :الاتصالات والتنسيق وبث الأخبار المغلوطة وتوظيف بعض صغار السن وتمويل بعض الأموال في سبيل تحقيق أهدافهم(**هلال المزاهرة، نفس المرجع، ص375**).

ففي الولايات المتحدة الأمريكية يقوم الإرهابيون باستخدام الانترنت لاستغلال المؤيدين لأفكارهم وجمع الأموال لتمويل برامجهم الإرهابية.

– الاستيلاء على المواقع الحساسة وسرقة المعلومات وامتلاك القدرة على نشر الفيروسات، وذلك يرجع إلى العدد المتزايد من برامج الكمبيوتر القوية والسهلة الاستخدام والتي يمكن تحميلها مجانا.

– نشر الأفكار الخاطئة بين الشباب كالإرهاب والإدمان والزنا لفساد الدولة لأسباب سياسية واقتصادية بالدرجة الأولى.

4. الجريمة الجنسية (Sexual Crime):

هذا النوع من الجريمة يمكن أن يتمثل بإحدى الصور التالية:

أ- **الابتزاز:** من أشهر حوادث الابتزاز عندما يقوم أحد الشباب باختراق جهاز إحدى الفتيات أو الاستيلاء عليه وبه مجموعة من صورها وإجبارها على الخروج معه وإلا سيفضحها بما يملكه من صور.

ب- **التغرير والاستدراج:** في العادة هذه الصورة عندما يتعرف أحد الشبان على إحدى الفتيات عبر الشات أو برامج المحادثة يكون على علاقة معها ثم يستدرجها بالكلام المعسول ويوهمها بالزواج لكي تثق به، ومن ثم يقوم بتهديدها وفضحها بما يملكه من صور أو تسجيلات لصوتها إن لم تستجب لطلباته.

المطلب الرابع: خصائص الجريمة الالكترونية.

1. **اعتبارها أقل عنفا في التنفيذ:** لا تتطلب جرائم الانترنت عنفا لتنفيذها أو مجهودا كبيرا فهي بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب أنواع من المجهود العضلي الذي قد يكون في صور ممارسة العنف والايذاء كما هو الحال في جريمة القتل أو الاختطاف أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة.

تتميز جرائم المعلوماتية بأنها جرائم هادئة بطبيعتها لا تحتاج إلى العنف بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة، وتحتاج كذلك إلى وجود شبكة المعلومات الدولية مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو التغرير بالقاصرين، فمن هذا المنطلق تعد الجريمة الالكترونية من الجرائم النظيفة فلا آثار فيها لأية عنف أو دماء وإنما مجرد أرقام وبيانات يتم تغييرها من السجلات المخزونة في ذاكرة الحاسبات الآلية وليس لها أثر خارجي مادي(**بن صغير، 2015، ص9**)

2. الحاسب الآلي هو أداة لارتكاب الجرائم الالكترونية: الحاسب الآلي هو دائما أداة الجريمة في الجرائم التي ترتكب على شبكة الانترنت خاصية متفردة عن أي جريمة أخرى، ذلك أن الحاسب الآلي هو الأداة الوحيدة التي يمكن الشخص من الدخول على شبكة الانترنت وقيامه بتنفيذ جريمته أي كان نوعها وعليه فالحاسب الآلي هو الأداة الوحيدة لارتكاب أي جريمة من الجرائم على شبكة الانترنت(**الجنيبهي، 2005، ص14**)

3. صعوبة اكتشاف الجرائم الالكترونية وثباتها: لا تحتاج الجرائم الالكترونية إلى أي عنف، أو سفك للدماء، أو آثار اقتحام لسرقة الأموال وإنما هي أرقام وبيانات تتغير أو تمحى تمام من السجلات المخزونة في ذاكرة الحاسبات الآلية، ولأن هذه الجرائم في أغلب الأحيان لا تترك أي أثر خارجي مرئي لها، فإنها تكون صعبة في الإثبات ومما يزيد من صعوبة إثبات هذه الجرائم أيضا ارتكابها عادة في الخفاء وعدم وجود أي أثر كتابي لما يجري خلال تنفيذها من عمليات أو أعمال إجرامية، حيث يتم بالنبضات الالكترونية نقل المعلومات، كما أن هذه الجرائم ترتكب غالبا وبصورة منظمة على صعيد أكثر من دولة باستخدام شبكات الاتصالات والمعلومات ودون تحمل عناء الانتقال، أضف إلى ذلك إحجام مجتمع الأعمال عن الإبلاغ عنها تجنبا للإساءة إلى السمعة وهذا الثقة في كفاءة المنظمات والمؤسسات المجنى عليها، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الزمنية(**عبابنة، 2009، ص34**).

وهناك صعوبات أخرى أيضا في إثبات الجرائم التي تكمن في الجناة مرتكبي تلك الجرائم الذين يتسمون بالذكاء والدهاء والخبرة التقنية أثناء ارتكابها إضافة إلى عدم ملائمة الأدلة التقليدية في القانون الجنائي في إثباتها وحيث ثم يلزم البحث عن أدلة جديدة نابحة من ذات الحاسب، ومن هنا تبدأ صعوبات البحث عن الدليل، وجمع هذا الدليل وتبدأ مشكلات قبوله إن وجد ومدى موثوقيتهأو مصداقيته على إثبات وقائع الجريمة.

4. الجريمة الالكترونية جريمة عابرة للحدود: أخذت تكنولوجيا الحاسب الآلي تلعب دورا بالغ الأهمية في العالم المعاصر، وغزت الأسواق سواء الخاصة بالدول المتقدمة صناعيا أو دول العالم الثالث، فالدول المتقدمة صناعيا تقوم بتصنيع أجهزة الحاسب الآلي وابتكار برامج ومنصفات لتحقيق الربح المادي، وتقوم دول العالم الثالث باستقبال هذه المبتكرات وتستخدمها على نطاق واسع نظرا لصغر حجمها وقلة كلفتها وتزايد الحاجة إليها.

هذا التطور التكنولوجي في مجال الحاسبات وبرامجها وشبكات الاتصال، وخاصة شبكة الانترنت جعل الإنتاج الذهني يتصف بالعالمية universal لأنه لا يقتصر على دولة دون أخرى، فالبشرية كلها شريكة في الاستفادة من هذا الإنتاج الأدبي والفني.

إلى جانب هذا فإن الاستخدام غير الشرعي الناجم عن الاتصال بالحاسوب أيضا اتصف بالعالمية أو بالعابر للحدود، فالجرائم لم تعد تقتصر على إقليم ولا تتعداه بل أصبح بالإمكان ارتكاب الجرائم عن طريق الحاسب الآلي باختراقه لحواسب في بلد آخر أو إتلاف معطياتها، فالتعدي في بلد وأثره في بلد آخر وهكذا.

ولهذا فإن جرائم الحاسوب تشترك مع غيرها من الجرائم أنها تتخطى حدود الدول كتجارة المخدرات وغسيل الأموال(**عبابنة ، 2009، ص33**).

المبحث الثاني: تصنيف الجريمة الالكترونية.

سنتطرق في هذا المبحث إلى تصنيف الجريمة الالكترونية من أطرافها وخصائص وسمات الجرائم الإلكترونية ثم أسباب ودوافع ارتكاب الجريمة الالكترونية.

المطلب الأول: أطراف الجريمة الالكترونية.

يمكن تصنيف أطراف الجريمة الالكترونية إلى :

1. أصناف المجرم المعلوماتي:

إن التسارع الرهيب في مجال تقنيات الرقمية الحديثة ساهم بدوره في التطور السريع لأنماط جريمة تقنية بصفة عامة مما أصبح عائقا أمام دراسات علم الإجرام الحديثة التي تسعى إلى وضع تصنيف ثابت لمجرمي المعلوماتية ويمكن تصنيف مرتكبي الجرائم الالكترونية إلى مجموعة الطوائف، ولا يعني بطبيعة الحال أن كل مجرم يندرج ضمن طائفة محددة دون غيرها بل يمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة أو فئة ويمكن تصنيف المجرم المعلوماتي إلى الفئات التالية(**سعيداني ، 2013، ص53**)

أ- فئة صغار مجرمي المعلوماتية: أو كما يسميهم البعض صغار نوابغ المعلوماتية وتضم هذه الطائفة الأشخاص الذين يرتبكون جرائم المعلوماتية بغرض التسلية والمزاح دون أن تكون لديهم نية إحداث أي ضرر

بالمعنى عليهم، وذلك بمدارسهم ومن بينهم فئة لم تبلغ بعد سن الأهلية مفتونين كثيرا بالتقنيات الرقمية (**حامد عياد، 2007، ص52**).

وهم غالبا ما يكونون في مرحلة المراهقة وعلى الرغم من صغر سنهم إلا أنهمن قادرون على اقتحام كافة أنواع الأنظمة المعلوماتية وقد أثارت هذه الفئة جدلا واسعا في الوسط الفقهي، ففي حين كثر الحديث عن مخاطر هذه الفئة التي يمكن أن تتحول إلى فئة القراصنة عندما يصبحون على درجة عالية من الخبرة والمهارة فيتم استئجارهم واستغلالهم في أعمال ذات أهداف إجرامية، ذهب جانب من الفقه أنه من الأحسن عدم تصنيف هؤلاء ضمن دائرة الإجرام بما لديهم من ميل للمغامرة في البحث والاستكشاف.

2. **فئة القراصنة أو المخترقون:**

– **الهواة الهاكرز (Le HAckers)**:وهم المتطفلون الذين يتحدون أمن النظم المعلوماتيةوالشبكات من خلال الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها وكسرالحواجز الأمنية الموضوعة لهذا الغرض، وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية وإنماينطلقون من هدف اكتساب الخبرة أو بدافع الفضول أوبمجرد التحدي وإثبات الذات.(**الشناوي، 2008، ص45**)

– **المحترفون Les Cracheres**: وهذا النوع أخطر من الهواة، ويحدث أضرار بالغة وقد يؤلف المجرمون في إطار هذا النوع أندية لتبادل المعلومات فيما بينهم ويفضل القراصنة العمل في جماعات عن العمل الفردي، وغالبا ما يكون دافعهم لارتكاب الجريمة إما الحصول على المال، أو بغرض الشهرة أو إثبات تفوقهم العلمي ومدى ما يتمتعون به من الذكاء(**الشناوي، 2008، ص46**).

3. **المخادعون swindlers**:وهؤلاء يتمتعون بقدرات فنية عالية باعتبارهم عادة من الأخصائيين في المعلوماتية ومن أًحاب الكفاءات وتنصب معظم جرائمهم على شبكات تحويل الأموال، ويمكنهم التلاعب على حسابات المصارف أو فواتير الكهرباء والهاتف أو بطاقات الائتمان أو ما شابه ذلك.

4. **أفراد يحلون مشكلة (Personnel Problem Solvers):** فهم الطائفة الأكثر شيوعا بين مجرمي المعلوماتية فهم يقومون بارتكاب جرائم المعلوماتية التي تلحق بالمجني عليهم خسائر ويكون الهدف من ورائها إيجاد حلول لمشكلات مادية تواجههم، ولا يستطيع حلها بالوسائل الأخرى بما فيها اللجوء الى الجريمة التقليدية وغالبا ما يكون المجني عليه مؤسسة مالية(**سوير ، 2011، ص30**).

5.دعاة متطرفون (Extreme Advocates): فتدخل في عدادها الجماعات الإرهابية أو المتطرفة والتي تتكون بدورها من مجموعة أشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي، ويركز نشاطهم بصفة عامة في استخدام العنف ضد الأشخاص أو الممتلكات من أجل لفت الأنظار إلى ما يدعون إليه وإن اعتماد المؤسسات المختلفة داخل الدول على أنظمة الحاسبات الآلية في انجاز أعمالها والأهمية القصوى للمعلومات التي تحتويها في أغلب الحالات قد جعل من هذه الأنظمة هدفا حذا بهذه الجماعات، ومن الأمثلة الشهيرة في هذا الخصوص قيام إحدى الجماعات الإرهابي المعروفة باسم الأولوية الحمراء "***The red Brigades***" بتدمير ما يزيد عن 60 مركز للحاسبات الآلية خلال الثمانينات لتلفت النظر إلى أفكارها ومعتقداتها (**سعيداني، 2013، ص55**).

المطلب الثاني: سمات مرتكبي الجرائم الالكترونية.

يتميز المجرم المعلوماتي عن غيره من المجرمين بصفات وسمات معينة جعلت منه محل العديد من الأبحاث والدراسات، واختلف الباحثون في تحديد هذه الخصائص كما اختلفوا في مدى انطباق وصف جرائم ذوي الياقات البيضاء على مجرمي المعلوماتية ذلك أن كلا من هؤلاء المجرمين قد يكون من ذوي الكفاءات ولهم القدرة على التكيف الاجتماعي ومن أهم هذه السمات ما يلي:

1. **المهارة:** يتمتع مجرمي المعلوماتية بقدر لايستهان به من المهارة بتقنيات الحاسوب والانترنت، بل إن مرتكبي الجرائم الالكترونية هم من المتخصصين في مجال معالجة المعلومات آليا، فتنفيذ الجريمة الالكترونية يتطلب قدرا من المهارة لدى الفاعل التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات(**صغير ، 2013، ص33**).

2. **الذكاء:** يعتبر الذكاء من أهم صفات مرتكب الجرائم المعلوماتية، لأن ذلك يتطلبمنه المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي والقدرة على التعديل والتغيير في البرامجلذلك عادة ما يذكر أن الإجرام المعلوماتي هو إجرام الأذكياء وذلك بالمقارنةبالإجرام التقليديالذي يميل إلى العنف،فهذا المجرم لا يمكن أن ينتميإلى طائفة المجرمين الأغبياء، فمن يستعينبجهاز الحاسوب للاستيلاء على أسرار بنك أو شركة مخزنة به لابد أن يتميز بالمستوى الرفيع منالذكاء حتى يمكنه أن يتغلب على كثير من العقبات التي تواجهه في ارتكاب جريمته.

وتتجلى أهمية صفة الذكاء بالنسبة لمرتكب الجريمة المعلوماتية في عدم استخدامه للعنف في ارتكابهللجريمة، فالسلوك الإجرامي ينشأ من تقنيات التدمير الناعمة Sabotage softفيكفي أن يقوم المجرم المعلوماتي بالتلاعب ببيانات وبرامج الحاسبالآلي لكي يمحو أو يدمر هذهالبيانات أو يعطل استخدام هذه البرامج(**سعيداني، 2013، ص51**).

3. **مجرم متكيف اجتماعيا:** لأن المجرم المعلوماتي يرتكب جرائمه من خلال وسائط التكنولوجيا فإنه لا يكون ظاهرا في الغالب ولذا فهو ينأى بنفسه عن حالة العداء السافر للمجتمع الذي يعيش فيه، بل إنه إنسان متكيف، ولا يعني ذلك التقليل من شأن المجرم المعلوماتي بل إن خطورته الإجرامية قد تزيد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه.

4. **مجرم عائد إلى الإجرام:** يعود كثير من مجرمي المعلومات إلى ارتكاب الجرائم أخرى في مجال الكمبيوتر انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وتقدمهم إلى المحكمة في المرة السابقة، ويؤدي ذلك إلى الإجرام، وقد ينتهي بهم مع ذلك في المرة التالية إلى تقديمهم إلى المحاكمة(**الشناوي، 2008، ص47**)

الضحيةفيالجريمةالمعلوماتية

لقدحددالإعلان العالمي الخاصبالمبادئ الأساسية لتوفير العدالة لضحايا الجريمة وإساءةاستعمال السلطة الذي اعتمدته الجمعية العامة للأمم المتحدة بقرارها رقم 401434الصادر بتاريخ85/11/29مصطلح الضحية والذي جاء شاملا لكل من المجني عليه والمتضرر من الجريمةفوفقا لهذا الإعلان المشار إليه يقصد بالضحية الأشخاص الذين أصيبوا بضرر فردي أوجماعي بما في ذلك الضرر البدني أو العقلي أو المعاناة النفسية أو الخسارة الاقتصادية أو الحرمانبدرجة كبيرة من التمتع بحقوقهم الأساسية، عن طريق أفعال أو حالات إهمال تشكل انتهاكاللقوانين الجنائية النافذة في الدول بما فيها القوانين التي تحرم الإساءة لاستعمال السلطة، كما يشملالمصطلح أيضا حسب الاقتضاء العائلة المباشرة للضحية الأصلية أو فاعليها المباشرين والأشخاصالذين أصيبوا بضرر من جراء التدخل لمساعدة الضحايا في محنتهم أو لمنع الإيذاء .

وعليه فإن الضحية في الجريمة بصفة عامة كل شخص طبيعي أو معنوي أصيببخسارة أو ضرر أو بعدوان نتيجة ارتكاب جريمة سواء بفعل أو بالامتناع عن فعل، أما المقصودبالضحية في الجريمة المعلوماتية هو كل شخص أصابه ضرر مادي أو معنوي نتيجة الاستخدام غيرالمشروع لتقنية المعلومات، وقد يكون شخصا عاما ممثلا في مؤسسات الدولة وهيآكلها وقد يكونخاصا ممثلا في الأشخاص الطبيعية أو المعنوية.

فنظرا لطبيعة استخدام تقنية المعلومات في جميع المعاملات الاقتصادية والمالية الوطنية والدوليةوالاعتماد عليها في تسيير شؤون الحياة اليومية بالنسبة للأفراد والشؤون العامة بالنسبة للحكوماتكان من شأن ذلك أن يضفي أبعادا غير مسبوقة في توسع دائرة المتضررين من الجرائم المعلوماتيةوتعدد فئاتهم (**سعيداني، مرجع سابق، ص63-64**)

المطلب الثالث: دوافع ارتكاب الجريمة الالكترونية.

تسبق الحاجات عادة الدوافع فالحاجة تنشأ من الشعور بالنقص أو الرمان من شيء ما لدى الفرد مما يؤدي إلى التأثير في القوى الداخلي لديه (الدوافع) بغرض إشباع هذه الحاجات التي تواجدها حالة من الرضا

النفسي، وتتنوع دوافع الإقدام على الجريمة الالكترونية باختلاف منفذها، تبعا لطبيعة ودرجة خبرته في مجال المعلوماتية ويمكن تصنيف هذه الدوافع إلى صنفين دوافع شخصية ودوافع خارجية.

1. **الدوافع الشخصية:** يكمن رد الدوافع الشخصية لدى مرتكب الجرائم الالكترونية إلى دوافع مالية ودوافع ذهنية نمطية(**سعيداني نعيم ، نفس المرجع، ص60**)

2. **الدوافع المادية (تحقيق الربح وكسب المال):** يعد الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة الالكترونية وذلك أن الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم المعلوماتي إلى تطوير نفسه حتى يواكب كل حديث يطرأ على التقنية المعلوماتية ويقتنص الفرص ويسعى إلى الاحتراف حتى يحقق أعلى المكاسب وبأقل جهد دون أن يترك أثرا وراءه (**الحمود ، المجالي ، 2005، ص30**)

فيعتمد الجاني رغبة منه في تحقيق الثراء والكسب المادي إلى التلاعب بأنظمة المعالجة الآلية للبنوك والمؤسسات المالية وإن كان أحد موظفيها، أو اختراق نظم المعالجة الآلية لها من خلال اكتسابه لفجواتها الأمنية على استغلالها وبرمجتها لتحويل مبالغ مالية لحسابه أو لحساب شركائه أو لحساب من يعمل لحسابهم إن كان من خارج المؤسسة كما يمكن الحصول على المكاسب المادية من خلال المساومة على البرامج أو المعلمات المتحصل عليها بطريق الاختلاس من جهاز الحاسوب ولقد أشارت في هذا الإطار مجلة (Securiteinformatique) وهي مجلة متخصصة في الأمن المعلوماتي أن 43% من حالات الغش المعلن عنها قد تمت من اجل اختلاس أموال 23 % من أجل سرقة معلمات و 19% أفعال اتلاف و15% الاستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية.

3. **الدوافع الذهنية (المتعة والتحدي والرغبة في فهم النظام المعلوماتي واثبات الذات).**

فالدافع في هذا الغرض لا ينبئ عن خطورة كامنة في نفس مقترف هذه الأفعال، إذ أنهم عادة لا يكونون من معتادي الإجرام بل يتمثل في رغبة هؤلاء بتحدي النظام التكنولوجي المعقد للحاسب الآلي بل مكوناته ومعطياته ومحاولاته اختراقه عن طريق الوصول إلى المعلومات (**عبابنة، ص2009، ص25**)

ففي الوقت الذي يزداد فيه الاهتمام بأمن الحاسب، عن طريق تطوير طرق جديدة وصعبة الاختراق كبرمجيات التشفير التي تمكن مستقبلها وحده من فهمها، ومن الأمثلة على ذلك وزارة الدفاع الأمريكية (البنتاغون) التي تقوم بتغيير أنظمة الزمن للبيانات المستخدمة يوميا، حتى أن بعض المعلومات الحساسة تغير

كل ساعة أنظمة ترميزها وهذا مما لاشك فيه يدل على قدر عال من التقنية والنظام المتطور فإن الجانب الآخر الذي يقف على الضفة الأخرى، أصحاب الشغف الالكتروني يتسابقون لخرق هذه الأنظمة وإظهار تفوقهم عليها، والدليل على ذلك قيام أحد الهواة في أوربا بحل شفرة أحد مراكز المعلومات في البنتاغون وتمكنه من العبث في البيانات هذا المركز(**عبد الباقي، 1992، ص17**).

4. الدوافع الخارجية: لارتكاب بعض الجرائم المعلوماتية قد يتأثر بمؤثرات ودوافع خارجية لوجوده في بيئة المعالجة الآلية للمعلومات وتعد المؤثرات التي تدفع الإنسان إلى اقتراف هذا السلوك سواء بدافع الانتقام أو بدافع الرغبة في التفوق.

- **الانتقام من رب العمل وإلحاق الضرر به:** الدافع إلى ارتكاب الجريمة الالكترونية قد يكون الرغبة في الانتقام من شخص أو مؤسسة أو حتى من بعض الأنشطة السياسية في بعض الدول أو من رب العمل (**المومني، 2010، ص48**).

والانتقام موجود داخل النفس البشرية، فكثير من الأفراد يفضلون تعسفيا أو بغير وجه حث من الشركة أو منظمة حكومية، أو حتى مصرف وهم يملكون المعلومات والتدريب اللازم والمعرفة الكافية بخفايا هذه الجهة لذا يرتكب الجاني الجريمة رغبة منه في الانتقام ليجعل الشركة أو المؤسسة تتكبد الخسائر المالية الكبيرة من جراء ما يسببه لها من ضرر يحتاج إصلاحه إلى وقت كبير.

- **دوافع التعاون والتواطؤ:** هذا النوع كثير التكرار في الجرائم الالكترونية وغالبا ما يحدث من متخصص في الأنظمة المعلوماتية أين يقوم بالجانب الفني من المشروع الإجرامي وآخر من المحيط أو خارج المؤسسة المجني عليها يقوم بتغطية عمليات التلاعب تحويل المكاسب المالية وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منتظمة حول أنشطتهم.

المبحث الثالث: استراتيجية الدور الوطني في محاربة الجريمة الالكترونية.

تناولنا في هذا المبحث استراتيجية الدور الوطني في محاربة الجريمة الالكترونية من خلال التعريف بمهام المركز الوطني في محاربة الجريمة الالكترونية وكذا أساليب المركز، وأخيرا إجراءات البحث والتحري في الجريمة الالكترونية.

المطلب الأول: مهام المركز الوطني في محاربة الجريمة الالكترونية

1. التعريف بالمركز الوطني لمحاربة الجريمة الالكترونية:

ضمت اجراءات وشروط شراكة بين الجزائر والاتحاد الأوربي وكذا المنظمة العالمية للتجارة (OMC) مشروطة بمدى تحكم البلاد في الأخطار المعلوماتية والتكنولوجية، من هذا المنطلق أصبح من الضروري وضع تهيئة المناخ المناسب الكفيلة لمحاربة الجريمة الالكترونية، وبما أن الدرك الوطني أحد الأجهزة الأمنية المكلفة بردع وحصر الجريمة، ارتقت قيادة الدرك الوطني لتسطير برنامج مشروع فريد من نوعه والمتمثل في المركز الوطني لمحاربة الجريمة الالكترونية المتواجد في عاصمة البلاد.(**مغالط، 2014، ص28**)

جاء نتيجة استراتيجية مؤسسة الدرك في تعقب أطوار الجريمة والاسراع في صدها إيمانا منها بأن المعلوماتية أصبحت وسيلة استراتيجية في التنمية الاقتصادية والتكنولوجية، ولا سيما الاعلام الآلي الذي اجتاح كل الخدمات العامة والخاصة بصورة يومية، وأصبح ما يسمى بالمجتمع المعلوماتي.

2. مهام المركز الوطني في محاربة الجريمة الالكترونية.

أ) **المراقبة العامة:** هي من مهام وحدة الحماية والتحليل(unité de veille et analyse) تسهر على تحليل المخزون المعلوماتي على مدار 24سا/24سا الخاصة بالاستعلامات على شبكة الأنترنت.

- حماية بنك المعلومات المفتوحة على الأنترنت.

ب) الوقاية: هي من مهام خلية المساعدة ومعالجة الحوادث المعلوماتية cellule d'assistance et de réponse aux incidents informatique تسهر على حماية وتقديم المساعدة في تخطي الجرائم الالكترونية على مستوى المؤسسات والمرافق الدستورية للدولة.

ج) المحاربة: هي من مهام الوحدة المركزية للتنسيق والتعاون unité centrale de coordination et de lutte contre la cybercriminalité وتتفرع منها وحدات فرعية على مستوى المجموعات الولائية والمتمثلة في الوحدات المحلية لمحاربة الجريمة الالكترونية. (**مغالط، المرجع نفسه، ص28**)

المطلب الثاني: طرق الحصول على أدلة الجرائم الالكترونية.

إن التعامل في الجريمة الالكترونية يتطلب اجراءات روتينية متفق عليها وذلك من أجل حماية الدليل غير أن وسائل حفظ الأدلة واستنتاجها تختلف من الجريمة التقليدية إلى الجريمة الالكترونية، ذلك لأن البرامج والبيانات عنصران أساسيان يتحتم على أجهزة تنفيذ القانون وخبراء الأدلة الجناحية جمعها واستخلاصها، وتعد المعاينة والتفتيش من بين الاجراءات التي تباشرها سلطات التحقيق والتي تؤدي للوصول إلى الدليل المستهدف من الواقعة الاجرامية، عن طريق التنقيب عن الحقيقة من حيث ثبوت التهمة ونسبتها إلى المتهم من عدمه، وكل هذا يتعلق بالمجرم المعلوماتي ما دام أن اجراءات الحصول على الدليل نفسها، ومن بين هذه الطرق: المعاينة والتفتيش.

1) المعاينة:

ويقصد بها الانتقال إلى الأماكن التي وقعت فيها الجريمة لإثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة عن الجريمة ومرتكبها، وبالتالي يجب على السلطات المختصة بإجراء المعاينة والانتقال إلى أماكن وقوع الجريمة فور ارتكابها، حتى لا يكون هناك فارق زمني طويل بين وقوع الجريمة واجراء المعاينة التي تسمح للجاني بتغيير أو إزالة بعض الآثار المادية للجريمة التي تساعد في التنقيب عن الحقيقة، وحتى لا يقع الشك في الدليل المستنبط منه وهذا ما تتضمنه نص المادة 42 من قانون الاجراءات الجزائية الجزائري.

أ) **طبيعة المعاينة وأهميتها في الجرائم الالكترونية**:قد تكون المعاينة اجراء تحقيق أو استدلال يستهدف إلى اظهار الحقيقة في واقعة يبلغ أمرها إلى السلطات المختصة، بحيث لا تتوقف طبيعتها على صدفة من يجريها بل على ما يقتضيه اجرائها من مساس بحقوق الأشخاص، فإذا تم اجراء المعاينة في مكان عام كانت اجراء استدلال أما إذا ما اقتضت دخول حرمة مسكن خاص كانت إجراء تحقيق (**ممدوح ابراهيم، 2009، ص150**).

وتظهر أهمية المعاينة في كونها تقوم بإحاطة صورة شاملة لموقع الجريمة لجهة التحقيق والمحاكمة، وبكل ما يحتويه من تفصيلات سواء تعلقت بمكانه أو وصفه من الداخل أو الآثار الموجودة به، وهذا حتى يتسنى لضباط الشرطة القضائية والقضاة وضع تصور لكيفية وقوع الجريمة واستخلاص بعض الأدلة التي تم جمعها (**حجازي، 2007، ص18**).

ب) شروط صحة معاينة مسرح الجريمة الالكترونية: حتى تحقق المعاينة الغرض المرجو منها في كشف غموض الحادث ومعرفة الفاعل يجب التنفيذ بعدة شروط كالتالي:

- **سرعة الانتقال إلى مكان وقوع الجريمة الالكترونية:** على السلطة المختصة بالتحقيق الانتقال فور وصول خبر وقوع الجريمة إلى علمها مكان الواقعة.
- **السيطرة والتحكم على مكان وقوع الجريمة الالكترونية:** عند وصول سلطة التحقيق لمكان الحادث لمعاينته وجب أن تقوم بالسيطرة عليه وذلك:
  - بمنع أي شخص من مبارحة مكان الواقعة ريثما تنتهي الضبطية القضائية من تحرياتها.
  - حماية كل ما له علاقة بالحادث من وسائل وأشياء وأشخاص.
  - قيام الخبراء كل حسب اختصاصه برفع لآثار بمسرح الجريمة.
- **الترتيب في المعاينة:** ولضمان اجراء معاينة بصورة مرتبطة ومتسلسلة ينبغي على السلطة المختصة الالتزام بالطرق التالية:
  - تحديد نقاط البدء في المعاينة.
  - عدم الانتقال من مكان لآخر إلا بعد التأكد من معاينته تماما.
- **الدقة والعناية الفائقة في معاينة مسرح الجريمة الالكترونية:** وذلك بوصف المنطقة التي ارتكبت فيها الجريمة، وإذا كانت هذه الأخيرة داخل مبنى فيجب معاينة كل منافذ الدخول والخروج، وكذا وصف المحتويات فيما هو مرتبط بالجريمة، كأجهزة الكمبيوتر والماسح الضوئي (السكانير) والطابعة والأسطوانات المدمجة، وغير ذلك من الوسائل المستخدمة في اقتراف الجريمة.
- **التحفظ على مسرح الجرائم الالكترونية بعد المعاينة:** لأن الهدف من الحفاظ على آثار الجريمة بعد انتهاء المعاينة هو من أجل امكانية العودة إليه كلما أراد المحقق أو القاضي كشف الغموض أو التأكد من آثار معينة.

2) التفتيش:

يقع التفتيش على محل منح له القانون حرمة خاصة باعتباره مستودع السر، وقد يكون المحل شخص أو مسكن أو محل ألحقه القانون في حكم المسكن، ويباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أدلة أو أشياء يكون كشفها مفيد لإظهار الحقيقة.

أ) **تعريف التفتيش:**لا يختلف معنى التفتيش في الجريمة التقليدية عن الجريمة الالكترونية، وبالتالي يقصد به اجراء من اجراءات التحقيق الذي يهدف الوصول إلى أدلة تفيد اظهار الحقيقة واسنادها إلى المتهم المنسوب إليه التهمة، حيث تباشر السلطة المختصة بالدخول إلى نظم المعالجة الآلية للمعطيات بما تحتويه من مدخلات وتخزين ومخرجات، وذلك من أجل البحث عن الأفعال والسلوكات المرتكبة وغير المشروعة والتي تشكل جناية أو جنحة.

ب) **خصائص التفتيش:**يتميز التفتيش بناءً على التعريف السالف ذكره بعدة خصائص منها:

– **اجراء من اجراءات التحقيق:** يعتبر التفتيش من أوامر التحقيق الابتدائي والذي يدخل ضمن الاختصاصات العادية لقاضي التحقيق، وهذا ما قضت به نص المادة 68-1 واستثناءً يجوز لضابط الشرطة القضائية القيام بهذا الاجراء بناءً على شروط وهذا ما بينته نص المادة 17-1 من خلال ما يلي: يباشر ضباط الشرطة القضائية...، اجراء التحقيقات الابتدائية.

– **أنه يهدف إلى البحث عن أدلة مادية:** إن الهدف من التفتيش هو الوصول إلى الأدلة المادية للجريمة والتي تؤثر في اقتناع القاضي لأنه في الغالب ما يترك الجاني في مسرح الجريمة بعض الوسائل والأدوات التي يكون قد استخدمها في ارتكاب الجريمة، أو بصمات الاصبع غير ذلك من الأدلة الت يستعين بها القاضي في الاثبات.

– **أن تكون الأدلة ناشئة عن جناية أو جنحة تحقق وقوعها:** باعتبار التفتيش عمل من أعمال التحقيق فلا يجوز اجراءه إلا اذا وقعت الجريمة بالفعل، وكانت مما يصفها القانون بجناية أو جنحة، بالتالي لا يجوز التفتيش في المخالفات نظرا لضآلتها وعدم خطورتها.

– **أن يتم التفتيش وفقا للإجراءات القانونية المقررة:** يتم القيام بإجراء التفتيش وفقا للشروط القانونية، بحيث يجب مباشرته طبقا لإجراءات صحيحة فإذا شاب التفتيش الواقع على نظام الحاسوب فإنه باطل، لأن

التفتيش الذي يقوم به المحقق بغير الشروط المنصوص عليها في القانون يعتبر باطل بطلان مطلق، وبالتالي لا يجوز التمسك بما ورد في محضر التفتيش وكما لا يجوز للمحكمة الاعتماد عليه في اصدار حكمها .

ج) القواعد الاجرائية للتفتيش:

- **القواعد الموضعية لتفتيش أجهزة الحاسوب:** وتخلص هذه القواعد كالآتي (حجازي، 2006، ص385، 386)
  - وقوع جريمة الكترونية.
  - ارتكاب شخص أو أشخاص معينين لإحدى الجرائم الالكترونية أو الاشتراك فيها.
  - توافر أدلة قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية أو الكترونية تفيد كشف الحقيقة.
  - أن يكون محل التفتيش هو الحاسوب بكل مكوناته المادية والمعنوية وشبكات الاتصال الخاصة به.
- **القواعد الشكلية لتفتيش نظام الحاسوب:** يتضمن عدة قواعد نذكر منها:
  - أن يكون أمر التفتيش مسببا.
  - أن يتم بأسلوب آلي الكتروني من قبل الأجهزة القائمة بالتفتيش وبصورة سريعة.
  - تكوين فريق تفتيش يتضمن خبراء وفنيين متخصصين بالحاسوب والأنظمة الالكترونية.

المطلب الثالث: اجراءات البحث والتحري في محاربة الجريمة الالكترونية.

1) مراقبة الاتصالات الالكترونية:

استحدث المشرع الجزائري اجراءات المراقبة الالكترونية بموجب المادة 03 من القانون 09-04 المصادر بتاريخ 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها حينما أجاز تبعا لمستلزمات التحريات والتحقيقات القضائية الجارية في اظهار هذا النوع من الجرائم اللجوء إلى وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها (المادة 03 من القانون 09-04 مع مراعاة الأحكام القانونية التي تتضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الاجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية، وتجميع وتسجيل

محتواها في حينها والقيام بإجراءات التفتيش داخل منظومة معلوماتية)، في حينها والقيان بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

الحالات التي تسمح باللجوء إلى المراقبة الالكترونية:

اعتبر المشرع الجزائري المراقبة التقنية للاتصالات وسيلة اجرائية للحصول على الدليل في مجال الجريمة الالكترونية بمجموعة من الشروط أهمها (**سعيداني، نفس المرجع، ص185**).

- أن يتم تنفيذ هذه الاجراءات تحت سلطة القضاء وبإذنه، وهو ما أكدته المادة 04 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها بنصها: "على أنه لا يجوز اجراء عملية المراقبة إلا بإذن من السلطة القضائية المختصة".
- أن تكون هناك ضرورة تتطلب هذا الاجراء، وتتحقق هذه الضرورة عندما يكون من الصعب الوصول إلى نتيجة تهم مجريات التحري والتحقيق دون اللجوء إلى المراقبة الالكترونية.

2) تفتيش المنظومات المعلوماتية:

يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الاجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 من القانون 09-04، الدخول بغرض التفتيش ولو عن بعد إلى كل منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها أو في أي منظومة تخزين معلوماتية.

3) حجز المعطيات المعلوماتية:

عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وإنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات في محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في احراز وفقا للقواعد المقررة في قانون الاجراءات الجزائية(**سعيداني ، نفس المرجع، ص186**)

خلاصة الفصل:

إن ظاهرة الجرائم الالكترونية أو جرائم التقنية العالية، ظاهرة اجرامية حديثة نوعا ما ذات مخاطر لا يستهان بها، كونها موجهة للاعتداء على المعطيات بدلالتها التقنية الواسعة المعبرة عن الواقع الخاص بكل ميدان، فهي تقترف في الخفاء من مجرمين أذكياء لهم دراية واسعة في هذا المجال، فهي تطال الحق في المعلومات وتمس الحياة الخاصة للأفراد وتهدد الأمن القومي وابداع العقل البشري، ولمجابهتها وضعت المصالح الأمنية استراتيجيات ووحدات وهياكل مختلفة مهمتها رفع الجرائم التي من شانها المساس بأمن الدولة.

الفصل الثالث

الإطار التطبيقي للدراسة

الدراسة التحليلية:

تم اجراء المقابلة مع ضابطين بالمجموعة الاقليمية للدرك الوطني بالمسيلة، تتراوح أعمارهم ما بين 35 و45 سنة، رتبهم، رائد ونقيب، يعملان في القسم الخاص بالإعلام والاتصال للمجموعة، وهما المكلفين بالإعلام والاتصال داخل خلية الدرك الوطني والمتخصصون في مجال محاربة الجريمة الالكترونية.

المقابلة الأولى: مقابلة مع الرائد المكلف بالإعلام والاتصال.

المحور الأول: المبادئ الأساسية للتحقيق في الجرائم الالكترونية:

من خلال هذا المحور سنتم بمعرفة أهم الأسباب والطرق التي يعتمد عليها الدرك الوطني في اثبات الجريمة الالكترونية والتحقيق فيها، وأهم الاجراءات الأمنية الني يضعها للحد منها.

السؤال الأول: ما هو مفهومك للجريمة الالكترونية، وما أهم ما يميزها عن الجرائم الأخرى؟

ج1: هي أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية، ومن أهم ما يميزها عن غيرها أنها لا تترك أثرا بعد ارتكابها وتحتاج إلى خبراء للتحقيق فيها.

تعليق: من خلال اجابة المبحوث نستطيع القول أن ارتباط الجريمة الالكترونية وارتكابها بجهاز الحاسوب والشبكة العنكبوتية أضف عليها مجموعة من الخصائص والسمات.

السؤال الثاني: ماهي الأساليب وطرق التحري التي يقوم بها المحقق لإثبات وقوع الجريمة الالكترونية وشخصية مرتكبها؟

ج2: توجد الطرق المعتادة تتمثل في التحقيق الابتدائي، وضمت التحقيق الابتدائي الأساليب وهي: المعاينات والتفتيش، المعاينات تعني القيام بجمع الدلائل التي نستدل بها عن الجريمة ومعاينة الجرائم وضبط الأولى وكل ما يتعلق بالجريمة والبحث عن المجرمين، أما التفتيش يكون في الأماكن التي جرت فيهم الجريمة وهدفه الوصول إلى أدلة تفيد إظهار الحقيق وتخدم التحقيق.

التعليق: من خلال اجابة المبحوث نرى بأن المحقق المخول له التحقيق في الجريمة الالكترونية يقوم بمعاينة الجرائم أثناء وقوعها وضبط الأدلة وكل ما يتعلق بالجريمة والبحث عن المجرمين والقيام بإجراءات التفتيش للوصول إلى دليل يفيد التحقيق.

السؤال الثالث: ماهي الأساليب الخاصة للبحث والتحري عن الجريمة الالكترونية؟

ج3: إن مراقبة الاتصالات الالكترونية حسب ما نصت عليه المادة من القانون 04-09 المؤرخ في 2009/08/02، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها واعتراض المراسلات في تسجيل الأصوات والتقاط الصور.

التعليق: حسب اجابة المبحوث أنه هناك قانون نص على امكانية استعمال الأساليب الخاصة للبحث والتحري عن الجرائم المتصلة بتكنولوجيا الاعلام والاتصال لمكافحتها وكشف النقاب عنها.

السؤال الرابع: ما هي أهم الاجراءات التي تتخذها فرقتكم في القيام بالمعاينات وجمع الدلائل للاستدلال عن الجريمة الالكترونية؟

ج4: بعد تلقي الشكوى أو البلاغ أو البحث والتحري، يتم فتح تحقيق قضائي بعد اخطار السلطة القضائية وجمع أكبر عدد من المعلومات، واستدعاء المشكوك فيهم أو الشهود أو تسخير الأشخاص المؤهلين وتحرير محضر وتقديم الجناة أمام السيد وكيل الجمهورية حسب نص المواد 16، 17، 18 و49 من قانون الاجراءات الجزائية.

تعليق: من خلال اجابة المبحوث نستطيع القول بأن فرقة الدرك الوطني تقوم باتباع الاجراءات المخولة لها في إطار البحث والتحري عن الجرائم والأدلة والمعلومات حول الأشخاص المشتبه فيهم بارتكابهم الجرائم أو مشاركتهم فيها.

السؤال الخامس: ماهي الأدوات التقنية التي يتم وضعها في معاينة مسرح الجريمة الالكترونية؟

ج5: لمعاينة مسرح الجريمة يجب أن يتوفر تقنيين أو خبراء متخصصين في محاربة الجريمة الالكترونية مع استعمال أجهزة الكمبيوتر والتطبيقات المختلفة.

تعليق: حسب اجابة المبحوث أنه يشترط في معاينة مسرح الجريمة الالكترونية توفر تقنيين وخبراء في استعمال أجهزة الكترونية كالحاسوب وملحقاته والبرمجيات.

السؤال السادس: إلى ماذا تحتاج اجراءات التفتيش في الجرائم الالكترونية؟

ج6: طبقا للمواد 44 و45 من قانون الاجراءات الجزائية تحتاج اجراءات التفتيش في الجريمة الالكترونية إلى طلب تفتيش موجه إلى السيد وكيل الجمهورية المختص اقليميا وبعدها يسلمنا إذن بالتفتيش.

التعليق: من خلال اجابة المبحوث نرى بأن عملية اجراءات التفتيش تجرى بموجب إذن من وكيل الجمهورية بعد تلقيه للطب وتباشر تحت مراقبته.

السؤال السابع: كيف يتم اجراء التفتيش وما هو الأسلوب الذي يتم به؟

ج7: يتم التفتيش بعد الحصول على الإذن الكتابي من السيد وكيل الجمهورية، مراعاة وقت التفتيش، حضور صاحب المنزل أو ما ينوب عنه وإن تعذر ذلك يتم تسخير شخصين وحجز أي شيء يفيد التحقيق وتحرير محضر تفتيش مع اخطار السيد وكيل الجمهورية عن مستجدات التفتيش.

التعليق: حسب اجابة المبحوث أنه اجراء التفتيش يتم بضوابط لازمة أهمها الحصول على إذن مكتوب صادر من الجمهورية وتحديد الميقات الزمني للعملية.

السؤال الثامن : ماهي أهم التقنيات التي يلجأ إليها الخبراء للتحقيق في الجريمة الالكترونية؟

ج8: اعتراض المراسلات التي تتم عبر الوسائل السلكية واللاسلكية –تحديد عناوين البريد الالكتروني المستعملة في ارتكاب الجريمة– استخدام تقنيات التخفي عن طريق نظام البروكسي.

التعليق: من خلال اجابة المبحوث نستطيع القول بأن خبراء التحقيق في الجرائم الالكترونية يستعينون بالوسائل التقنية العالية الدقة والذكية لضبط الأدلة.

السؤال التاسع: ماهي طبيعة الأجهزة والبرامج التي يحتاجها خبراء الأدلة في معالجة الأدلة للجرائم الالكترونية؟

ج9: برامج نسخ الأقراص المدمجة والمحمولة، برامج حماية من الاختراق، كما أضاف يوجد بالمعهد الوطني العام للإجرام والأدلة الجنائية ببوشاوي (دائرة الاعلام الآلي والإلكترونيك) مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي وتماثلي من شأنه فك لغز الجريمة والتوصل إلى الجناة وهذا عن طريق تقارير الخبرة المقدمة للجهات المعنية، كما يوجد مصلحة أخرى تسمى المصلحة المركزية لمكافحة الاجرام السيبرياني للدرك الوطني ببئر مراد رايس، تقوم بمساعدة وحدات الدرك الوطني في انجازات التحقيقات.

التعليق: حسب اجابة المبحوث نرى بأن خبراء الأدلة الجنائية يحتاجون إلى أجهزة وبرامج تقنية متنوعة تساعدهم في اكتشاف المعلومات التي يحتويها كل دليل.

السؤال العاشر: ماهي أبرز الصعوبات التي تواجهكم أثناء التحقيق في الجريمة الالكترونية؟

ج10: عدم كفاية القوانين التشريعية، عدم التبليغ عن الجريمة من طرف الضحية، وذلك حسب عادات وتقاليد المنطقة وخشية على السمعة والمكانة، صعوبة متابعة الجريمة واكتشافها حيث لا تترك أثر فهي مجرد أرقام تتغير في سجلات فمعظم الجرائم الالكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها.

التعليق: من خلال اجابة المبحوث نستطيع القول أن المحققون في الجرائم الالكترونية يتعرضون إلى صعوبات عديدة تعرقل مجال البحث واثبات الجريمة خاصة بعد مرور طويل من الزمن من ارتكابها.

المقابلة الثانية: مقابلة مع النقيب في القسم الخاص بالإعلام والاتصال.

المحور الثاني: دور مختلف مصالح الدرك الوطني في مجال الوقاية من الجريمة الالكترونية ومحاربتها.

السؤال الأول: ما هو دور مختلف مستويات الشرطة القضائية للدرك الوطني في مجال محاربة الجريمة الالكترونية؟

ج1: إن مؤسسة الدرك الوطني مسايرة لهذا التطور الرهيب في التكنولوجيا والجرائم بمختلف أنواعها قامت بتطوير تقنيات التحقيق واستحداث التكنولوجيا والجرائم بمختلف أنوعها قامت بتطوير تقنيات التحقيق واستحداث وحدات خاصة ونذكر منها: المصلحة المركزية لمكافحة الجرائم السيبرانية للدرك الوطني بالجزائر العاصمة، المعهد الوطني لعلم الاجرام والأدلة الجنائية للدرك الوطني بالجزائر العاصمة.

التعليق: حسب اجابة المبحوث أن مهمة الشرطة القضائية للدرك الوطني في مجال الوقاية من الجريمة الالكترونية تتمثل في تقييم وتوجيه نشاط الوحدات في مجال الوقاية من الجريمة ودراسة مدى انتشار هذا النوع من الاجرام في إقليم المجموعة وتوفير واقتراح الوسائل الناجحة في ردعها؟

السؤال الثاني: ما هو دور مختلف هياكل اسناد التحقيق القضائي للدرك الوطني في مجال الجريمة الالكترونية؟

ج2: التنقل إلى مسرح الجريمة وجمع الأدلة –جمع أكبر قدر ممكن من المعلومات حول المشكوك فيهم– المشاركة في مختلف الملتقيات والقاء المحاضرات على مستوى المدارس.

التعليق: من خلال اجابة المبحوث نرى أن مهمة هياكل اسناد التحقيق القضائي جمع المعلومات والأدلة والتحقيق، وأيضا المشاركة في مختلف الملتقيات لتحسيس المجتمع بخطورة انتشار هذه الظاهرة على المجتمع.

السؤال الثالث: ما أهم النشاطات التي قام بها المركز الوطني في ميدان الوقاية من الجريمة ومحاربتها (التحسيس، الأيام الاعلامية)؟

ج3: القيام بالحملات التحسيسية لفائدة المؤسسات التعليمية والتكوينية بمختلف أطوارها مع اجراء تدخلات عبر وسائل الاعلام للتذكير بخطورة الجريمة الالكترونية.

التعليق: حسب اجابة المبحوث نرى أن المركز الوطني لمحاربة الجريمة يساهم بشكل كبير في ردع الجريمة الالكترونية والحد منها وذلك من خلال القيام بالحمالات التحسيسية وتوعية الأفراد حول المخاطر والتهديدات المعلوماتية لأمن أنظمة الاعلام واستعمال تكنولوجيات الاتصال.

السؤال الرابع: ماهي الاجراءات الأمنية المتخذة لحماية المنظومة المعلوماتية للدرك الوطني؟

ج4: اجراءات تقنية لعتاد متخصص واجراءات انضباطية وتحسيسية في كيفية التعامل مع الأجهزة الالكترونية ومختلف التطبيقات.

التعليق: من خلال اجابة المبحوث نستطيع القول بأن قيادة الدرك الوطني قامت بوضع استراتيجيات لحماية المنظومات المعلوماتية الخاصة بها، وذلك باتخاذ العديد من الاجراءات التنظيمية لحماية هذه المنظومات.

السؤال الخامس: فيما يتمثل الدور الذي تقوم به الفرقة الاقليمية لردع الجريمة الالكترونية؟

ج5: القيام بحملات تحسيسية لفائدة المؤسسات التعليمية والتكوينية بمختلف أطوارها وعامة الجمهور مع اجراء تدخلات عبر وسائل الاعلام للتذكير بخطورة الجريمة الالكترونية، ويتم التركيز على اعطاء نصائح وارشادات لتفادي الوقوع ضحية لجريمة الكترونية، نذكر منها عدم بيع جهاز الهاتف أو الكمبيوتر، عدم الاحتفاظ بصور أو فيديوهات شخصية على الهاتف أو جهاز الكمبيوتر، عدم فتح ملفات مرسلة من طرف أشخاص مجهولين.

التعليق: من خلال اجابة المبحوث نرى بأن الدرك الوطني إلى جانب اجراءات البحث والتحري عن الجريمة يقوم بدوره بإعطاء نصائح وارشادات مهمة حول خطر الجرائم الالكترونية لتفادي وقوعها، والقيام ببرمجة حملات تحسيس لفائدة المؤسسات التربوية والمدارس التعليمية للتعريف بخطر الاجرام المستحدث.

عرض وتحليل النتائج:

من خلال المقابلات التي أجريناها توصلنا إلى النتائج التالية:

- تشير نتائج الدراسة أن التطور التكنولوجي وما صاحبه من تطورات، أدى إلى ظهور جرائم متعددة ومنها ظاهرة الجريمة الالكترونية وتفاقمها، وهذا ما جعل الجهات المختصة للدرك الوطني اللجوء إلى اتخاذ اجراءات وأساليب متنوعة لمحاربة هذه الظاهرة.
- أظهرت نتائج الدراسة أن ادراك ماهية الجرائم الالكترونية باستظهار موضوعها وخصائصها وسندها القانوني، يتخذ أهمية سلامة التعامل مع هذه الظاهرة مما يسهل عملية التحقيق في حالة وقوع الجريمة.
- أوضحت دراستنا أن اثبات الجريمة الالكترونية من العقبات التي يعمل الخبراء على كسرها من أجل ايجاد الوسائل المناسبة، وبالتالي فهي تتطلب تقنيات عالية وأجهزة متنوعة ومهارات استثنائية في التحقيق.
- أكدت النتائج بشكل عام أن قلة الخبرة في مجال التحقيق والتحري عن جرائم العالم الافتراضي، عامل من شأنه أن يضعف دور الأجهزة المختصة بالتحقيق في مجال الجرائم الالكترونية.
- أثبتت اجابات المبحوثين أنه يتوفر جهات وكوادر وأجهزة متخصصة تعنى بعملية البحث والتحري عن الجرائم الالكترونية واثباتها والوصول إلى الحقائق والأهداف المرجوة.
- تلعب الأجهزة الأمنية دورا أساسيا في صيانة أمن المجتمع من خلال القيام بدور وقائي وقضائي يهدف إلى منع ارتكاب الجرائم الالكترونية وضبط مرتكبيها بعد حدوثها.
- تواجه طرق التحقيق في الجريمة الالكترونية عراقيل وصعوبات متعددة يتعرض لها المحققون خاصة وأنها ترتكب في العالم الافتراضي ولا تترك أي أثر باعتبارها جريمة عالمية يرتكبها أشخاص خارج التراب الوطني والضحية داخل التراب الوطني مما يصعب توقيفه.
- أظهرت نتائج الدراسة بأن تأطير وتجهيز الهياكل المعدودة لمحاربة الجرائم الالكترونية والمتمثلة خاصة في مؤسسة الدرك الوطني واحاطتها لكل المستلزمات يؤهلها بأن تكون الراعي الحريص على سلامة البلاد.
- أوضحت النتائج أن التحقيق في الجرائم يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته، وأن يحاول بكل جهد أن يقوم بالتحقيق في الجريمة ومتابعتها والبحث فيها وفي الأدلة والتنقيب عنها وصولا لإظهار الحقيقة.

- أشارت النتائج أن الدرك الوطني بدوره يقوم بتوعية المجتمع ويخلق له ثقافة اجتماعية جديدة عن هذه الجرائم بأنها أعمال غير مشروعة ويتعرض صاحبها لعقوبات جزائية، وتحسيس الأفراد بالمظاهر والآثار المترتبة عن الجريمة الالكترونية.

- تبين النتائج أنه نتيجة للتطور المستم لتكنولوجيات الاعلام والاتصال، تم الاعتماد على أساليب واجراءات مخصصة للتحقيق في الجرائم المعقدة والحديثة الجرائم الالكترونية التي تتطلب امكانات مادية وتقنيات خاصة تساير الأنماط والوسائل المستعملة من طرف المجرمين والمنظمات الاجرامية والتي تتمثل في اعتراض المراسلات السلكية واللاسلكية، تسجيل الأصوات والتقاط الصور أما الاجراءات فتتمثل في مراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية.

- أكدت النتائج بشكل عام أنه لمكافحة هذا النوع من الجرائم (الجرائم الالكترونية)، قامت قيادة الدرك الوطني بإعادة تنظيم سلسلة الشرطة القضائية وتدعيمها بمحققين مختصين في هذا النوع من الجرائم، وكذا انشاء هياكل اسناد التحقيق القضائي.

- وبينت الدراسة أن عدم كفاية القوانين التشريعية وقصور وسائل الرقابة صعوبات تؤدي إلى زيادة فرص ارتكاب الجرائم الالكترونية وانتشارها وارتفاع نسبة ضحاياها.

نستخلص في الأخير أن الجرائم الالكترونية وعلى اختلاف أساليبها وصورها أصبحت تشكل أولى اهتمامات وانشغالات الأجهزة والمنظمات الأمنية الوطنية، وقيادة الدرك الوطني واحد من المصالح الأمنية التي أولت للجريمة الالكترونية أهمية بالغة، وذلك بوضع هياكل ووحدات مهمتها رفع الجرائم التي من شأنها المساس بأمن الدولة والأشخاص وتقديم مرتكبيها إلى العدالة.

خاتمة

خاتمة:

من خلال هذه الدراسة المتواضعة وكخلاصة لما جاء فيها، يمكن القول أن الجريمة الإلكترونية أخذت منحى تصاعدي نتيجة البيئة الخصبة التي وفرتها تكنولوجيات الإعلام والاتصال، تتمثل هذه البيئة في الشبكة العالمية أو ما تسمى بالأنترنت التي أصبحت تشكل العمود الفقري للحياة اليومية للأشخاص والمؤسسات العامة والخاصة ما صعب من تحديد مفهوم موحد ودقيق لهذا النوع من الجرائم ، فالتباين والاختلاف في المفاهيم من شأنه أن يعرقل سبل وآليات مكافحته .

ومن خلال دراستنا للجريمة الإلكترونية ودور الدرك الوطني في محاربتها ومجابهتها توصلنا في ختام هذه الدراسة إلى عدة جوانب يمكن بلورتها في عدة نتائج وتوصيات اتضحت من خلال تحليل وتفسير البيانات التي تم الحصول عليها من خلال هذه الدراسة، وفي هذا سيتم عرض أهم النتائج والتوصيات التي توصلنا إليها وهي كالآتي:

- الجريمة الإلكترونية من بين أهم الجرائم المستحدثة والناتجة عن التطورات الحاصلة في مجال تكنولوجيا الإعلام والاتصال، والتي يمكن حصر مفهومها الأساسي فيما يلي:
- كل اعتداء على النظام المعلوماتي.
- كل استخدام لنظام معلوماتي للاعتداء على نظام آخر.
- كل استعمال لنظام معلوماتي من أجل ارتكاب سلوك مجرم قانونا.
- تتميز الجريمة الإلكترونية بعدة خصائص تجعلها مختلفة عن الجرائم الأخرى، تتمثل في طابعها العابر للحدود وصعوبة متابعتها واكتشافها وارتكابها في العالم الافتراضي، مما يصعب كشفها وحاجتها لخبراء في مجال المعلوماتية للتحري عنها.
- مجرمي المعلومات يتميزون بالمهارة لمعرفة والذكاء، الشيء الذي يجعلهم يرتكبون جرائمهم ويحققون أهدافهم في هدوء دون لفت الانتباه إليهم.
- التطور الذي شهده الإجرام المعلوماتي حتم على المجتمع الدولي والمحلي على مسايرته بتعديل القوانين السارية وإصدار عدة قوانين خاصة من أجل مكافحته.
- الدرك الوطني لم يغفل على المخاطر التي قد تتعرض لها منظومة المعلومات الداخلية، فقام بأخذ الإجراءات اللازمة لحمايتها من كل تهديد.

- الدرك الوطني بدوره رافق التطور الحاصل في المجتمع بإنشاء هياكل ووحدات متخصصة، تم تزويدها بالأفراد المؤهلين والوسائل اللازمة لضمان المكافحة الناجعة لمثل هذه الجرائم المتمثلة في تسجيل الأصوات والتقاط الصور واعتراض المراسلات السلكية واللاسلكية.

الاقتراحات

- ضرورة نشر الوعي في أوساط المجتمع بالمخاطر الاقتصادية والاجتماعية والنفسية وغيرها، الناجمة عن الاستخدامات غير المشروعة وغير الآمنة للأنترنت، وما يترتب من انعكاسات سلبية على حياة الفرد.
- وضع برامج للحملات التحسيسية الموجهة خاصة للتلاميذ في سن المراهقة لحمايتهم من مختلف الانحرافات والإغراءات المقدمة على شبكة الانترنت ، خاصة التي تشمل المواضيع الإباحية والمخدرات.
- إعداد الدراسات والبحوث ذات العلاقة بالجرائم الناشئة عن استخدام الانترنت وتنظيم المؤتمرات والندوات، بالمشاركة مع الباحثين على مستوى وزارة التعليم العالي والبحث العلمي .
- عقد اتفاقيات عربية ودولية مشتركة لمواجهة ظاهرة الإجرام الالكتروني، وتبادل المعلومات عن الأشخاص المشبوهين بالقرصنة كون الجريمة لا تعترف بالحدود الجغرافية للدولة .
- معرفة فرقة الدرك الوطني ميول المستعملين لشبكة الانترنت، خاصة بمقاهي الانترنت، وذلك بالتقرب من أصحاب هذه المقاهي والاستعلام على أنواع المواقع التي يتصفحها المواطنين بكثرة.
- إتاحة الفرصة للمواطنين للمشاركة في مكافحة الجرائم الالكترونية من خلال إنشاء خطوط ومواقع اتصال تسمح لأي كان بالإبلاغ عن بعد بوقوع جريمة إلكترونية دون قيد أو شرط .

قائمة المراجع

قائمة المراجع

المراجع باللغة العربية:

1. أبو بكر سلامة، محمد عبد الله.(2006) .**جرائم الكمبيوتر والانترنت**.
2. بن مرسلي، أحمد .(2005) .**منهاج البحث العلمي في علوم الاعلام والاتصال**.ط2. ديوان المطبوعات الجامعية. الجزائر.
3. الجبوري، عبودي نعمة .(2016) .**إدارة العلاقات العامة: بين الابتكار والتطبيق**. ط1. دار الرياحين للنشر والتوزيع. عمان.
4. جميل، عبد الباقي .(1992). القانون الجنائي والتكنولوجيا الحديثة الجرائم الناشئة عن استدام الحاسب الآلي. ط1. دار النهضة العربية. مصر.
5. الجنيهي، منير محمد. (2005) .**جرائم الانترنت والحاسب الآلي ووسائل مكافحتها**. دار الفكر الجامعي. الإسكندرية
6. الجهيني، منير محمد . الجهنين. محمد ممدوح (2005) .أمن المعلومات الالكترونية. دار الفكر الجامعي. الإسكندرية.
7. حامد عياد، سامي علي .(2007) .الجريمة المعلوماتية واجرام الانترنت. دار الفكر الجامعي. الإسكندرية.
8. حامد قشقوش .هدى .(1992) .جرائم الحاسب الآلي. دار النهضة العربي. مصر.
9. الحلبي، خالد عباد. (2011) .**إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت**.دط. دار الثقافة للنشر والتوزيع. الأردن.
10. الحمود، وضاح محمود . المجالي، نشأت مفضي .(2005) .**جرائم الأنترنت**. دار المنار للنشر. عمان.
11. دليو، فضيل . عباسي، بصلي فضة . (2011) . تكنولوجيا الاتصال والاعلام الحديثة الاستخدام والتأثير. ط1. مؤسسة كنوز الحكمة للنشر والتوزيع. الجزائر.
12. ربحي، مصطفى وآخرون .(2008) .**أساليب البحث العلمي وتطبيقاته في التخطيط والإدارة**. ط1 . دار صفاء. عمان.
13. زيدان، محمد .(1980) .**الاستقراء والمنهج العلمي وطرق اعداد البحث العلمي**. د ط. ديوان المطبوعات الجامعية. الجزائر.

14. الشناوي، محمد .(2008) .**جرائم النصب المستحدثة**. دار الكتب القانونية. مصر.

15. طه تمام، أحمد حسام .(2000) .الجرائم الناشئة عن استخدام الحاسب الآلي. القاهرة.

16. عبابنة، محمود أحمد .(2009) .**جرائم الحاسوب وأبعادها الدولية**. دار الثقافة للنشر والتوزيع. عمان. الأردن.

17. عبد الفتاح، مراد .**دور الكمبيوتر في مجال ارتكاب الجرائم الالكترونية**. شرح شرائح الكمبيوتر والاترنت. دار الكتب والوثائق المصرية. مصر.

18. عبد الله، عبد الكريم عبد الله (2007) .**جرائم المعلوماتية والانترنت –الجرائم الالكترونية–**. ط1. منشورات الحلبي الحقوقية. بيروت.

19. عبيدات، محمد وآخرون (1989) .**منهجية البحث العلمي القواعد والمراحل والتطبيقات**. ط3. دار وائل. عمان.

20. العكش، عبد الله(1986) .**البحث العلمي ومناهج الإجراءات**. مطبعة عين الحديثة .الإمارت العربية.

21. غربي، علي .(2006) .**أبجديات المنهجية في كتابة الرسائل الجامعية**.دط. مطبعة سيرتا كولي. الجزائر.

22. لازم كماش، يوسف.(2016).**البحث العلمي مناهجه، أساليبه الإحصائية**.دار دجلة. عمان.

23. محجوب، وجيه .(2014). **البحث العلمي ومناهجه**. دار المناهج للنشر والتوزيع. عمان.

24. محمد حسين، إحسان .(1982) .**الأسس العلمية لمناهج البحث العلمي**. د ط. دار الطليعة للطباعة والنشر. بيروت.

25. المراغي، أحمد عبدالله .(2017) .**الجريمة الالكترونية ودور القانون الجنائي في الحد منها**. ط1. القاهرة.

26. مصطفى، محمد موسى .**التحقيق في الجرائم الالكترونية**. ط1. مطابع الشرطة.

27. ممدوح، إبراهيم خالد .(2008) .أمن الجريمة المعلوماتية. الدار الجامعية .الاسكندرية.

28. نهلا، المومني عبد القادر .(2016) .**الجريمة المعلوماتية**. ط2. دار الثقافة للنشر والتوزيع. الأردن.

قائمة المراجع

المذكرات والأطروحات:

29. بعرة، سعيدة . (2016/2015) .**الجريمة الالكترونية في التشريع الجزائري**. مذكرة مكملة لنيل شهادة الماستر في الحقوق. تخصص قانون جنائي. كلية الحقوق. جامعة محمد خيضر. بسكرة.

30. سعيداني، نعيم .(2013/2012) .**آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**. مذكرة لنيل شهادة الماجستير في العلوم القانونية. تخصص علوم جنائية.

31. سوير، سفيان .(2011). **جرائم المعلوماتية**.رسالة ماجستير. كلية الحقوق والعلوم السياسية. جامعة مولود معمري. تيزي وزو.

32. صغير، يوسف .(2013) .**الجريمة المعلوماتية**. رسالة ماجستير . كلية الحقوق والعلوم السياسية. جامعة أبو بكر بلقايد .تلمسان.

33. لورنس، سعيدة الحوامد .(2010) .**الجرائم المعلوماتية أركانها ومكافحتها** . دراسة تحليلية .جامعة طيبة. كلية الحقوق. المملكة العربية السعودية.

المجلات والملتقيات:

34. دليو، فضيل .(2003) . مدخل الى الاتصال الجماهيري. مخبر علم الاجتماع والاتصال. جامعة منتوري قسنطينة.

35. عادل يوسف عبد النبي، السكري .الجريمة المعلوماتية وأزمة الشرعية الجزائرية. العدد السابع. جامعة الكوفة. كلية الحقوق.

36. مغالط، الطاهر .(أوت 2014). الجريمة المعلوماتية. مجلة المدرسة العدد 14 .

37. البداينة دياب موسى. (سبتمبر 2014).الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية .ملتقى علمي بالمملكة الأردنية.

38. طالبي المل ،سرور. (مارس 2017) .ملتقى وطني آليات مكافحة الجرائم الالكترونية في التشريع الجزائري. الجزائر العاصمة .

المواقع الالكترونية:

39. Https://ar.wikipedia.org.wiki.

الملاحق

أسئلة المقابلة:

المحور الأول: المبادئ الأساسية للتحقيق في الجرائم الالكترونية:

السؤال الأول: ما هو مفهومك للجريمة الالكترونية، وما أهم ما يميزها عن الجرائم الأخرى؟

ج1 .....

.....

السؤال الثاني: ماهي الأساليب وطرق التحري التي يقوم بها المحقق لإثبات وقوع الجريمة الالكترونية وشخصية مرتكبها؟

ج2 .....

.....

السؤال الثالث: ماهي الأساليب الخاصة للبحث والتحري عن الجريمة الالكترونية؟

ج3 .....

.....

السؤال الرابع: ما هي أهم الاجراءات التي تتخذها فرقتكم في القيام بالمعاينات وجمع الدلائل للاستدلال عن الجريمة الالكترونية؟

ج4 .....

.....

السؤال الخامس: ماهي الأدوات التقنية التي يتم وضعها في معاينة مسرح الجريمة الالكترونية؟

ج5 .....

.....

السؤال السادس: إلى ماذا تحتاج اجراءات التفتيش في الجرائم الالكترونية؟

ج6 .....

.....

السؤال السابع: كيف يتم اجراء التفتيش وما هو الأسلوب الذي يتم به؟

ج7 .....

.....

السؤال الثامن : ماهي أهم التقنيات التي يلجأ إليها الخبراء للتحقيق في الجريمة الالكترونية؟

ج8 .....

.....

السؤال التاسع: ماهي طبيعة الأجهزة والبرامج التي يحتاجها خبراء الأدلة في معالجة الأدلة للجرائم الالكترونية؟

ج9 .....

.....

السؤال العاشر: ماهي أبرز الصعوبات التي تواجهكم أثناء التحقيق في الجريمة الالكترونية؟

ج10.....

.....

المحور الثاني: دور مختلف مصالح الدرك الوطني في مجال الوقاية من الجريمة الالكترونية ومحاربتها.

السؤال الأول: ما هو دور مختلف مستويات الشرطة القضائية للدرك الوطني في مجال محاربة الجريمة الالكترونية؟

ج1 .....

.....

السؤال الثاني: ما هو دور مختلف هياكل اسناد التحقيق القضائي للدرك الوطني في مجال الجريمة الالكترونية؟

ج2 .....

.....

السؤال الثالث: ما أهم النشاطات التي قام بها المركز الوطني في ميدان الوقاية من الجريمة ومحاربتها (التحسيس، الأيام الاعلامية)؟

ج3 .....

.....

السؤال الرابع: ماهي الاجراءات الأمنية المتخذة لحماية المنظومة المعلوماتية للدرك الوطني؟

ج4 .....

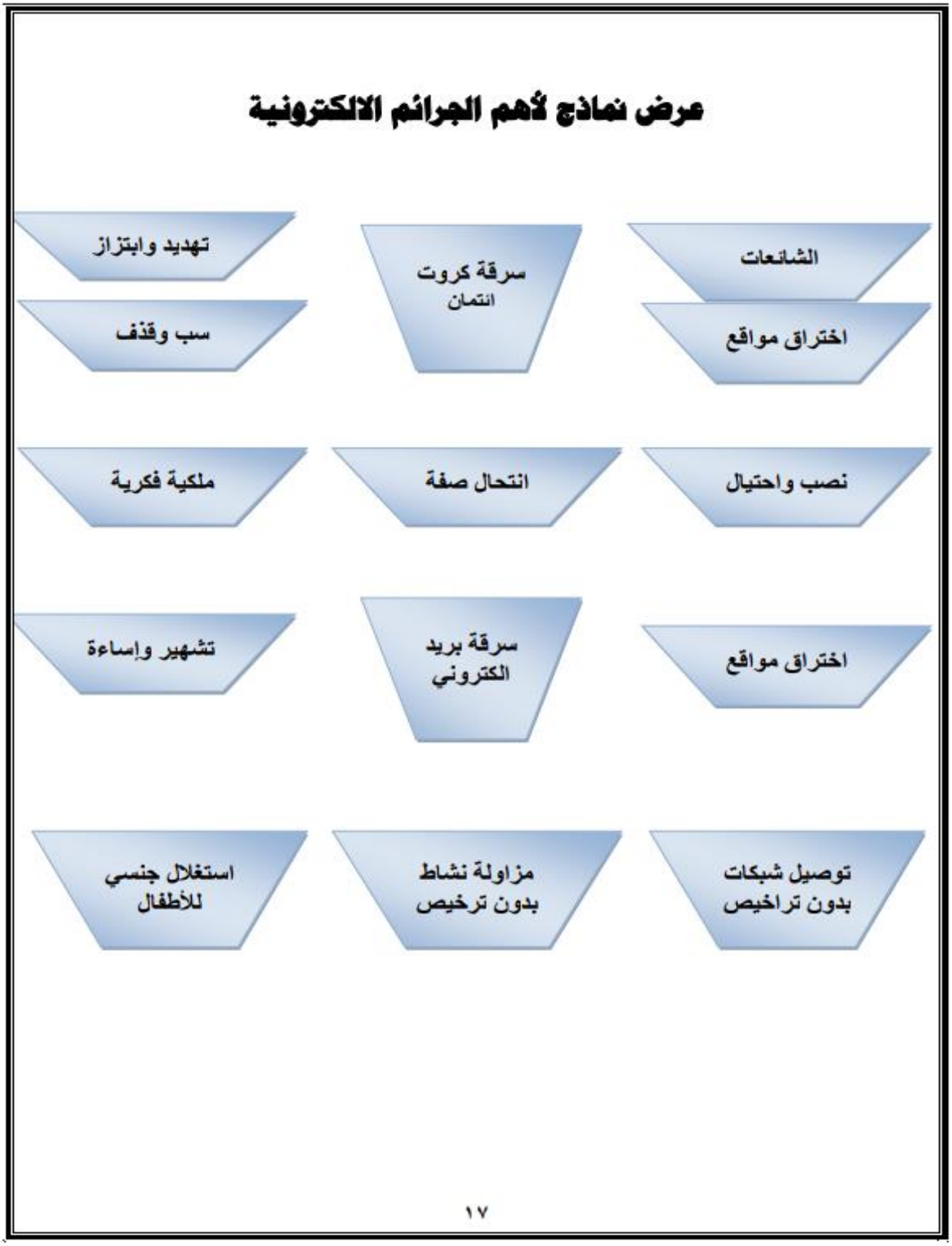
.....

السؤال الخامس: فيما يتمثل الدور الذي تقوم به الفرقة الاقليمية لردع الجريمة الالكترونية؟

ج5 .....

.....

الملحق 01: أهم نماذج الجرائم الالكترونية.



الملحق 02: تجسس المجرم المعلوماتي (القراصنة) على البيانات السرية والخاصة بالأشخاص والمؤسسات في كل أنحاء العالم

الملحق 03: تحصين الخصوصية لقصي والتقليل من الجرائم الالكترونية

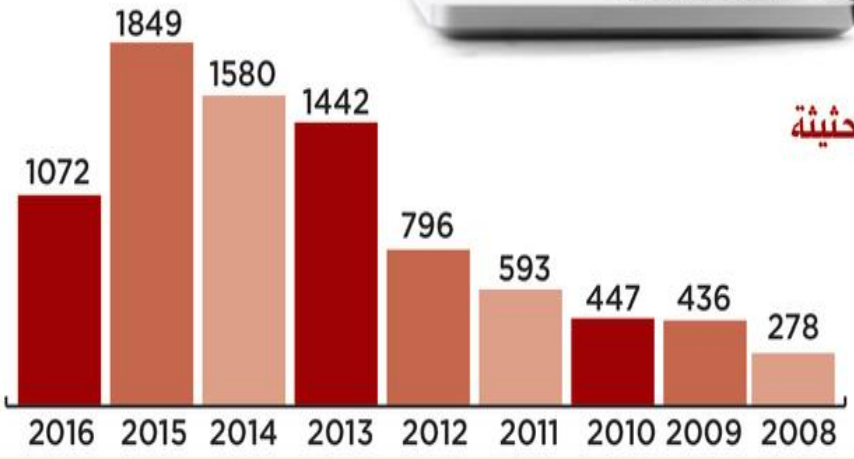
تحصين الخصوصية ورصد الجرائم

منذ 2008 وإدارة المباحث الجنائية في شرطة دبي تعمل جاهدة لرصد وتقصي الجرائم الإلكترونية التي باتت مصدر مضايقة تصل إلى حدّ التهديد إلى الأشخاص والشركات من خلال اختراق المواقع الإلكترونية ناهيك عن الابتزاز والاحتيال الذي بات نمطاً يتخذه المجرمون سبيلاً لقضاء مآربهم الخبيثة. وفي المقابل دعاوى إلى تحصين البيانات الشخصية للحيلولة دون وقوع اختراقات للخصوصية تتخذ أوجهاً كثيرة على شاكلة الابتزاز والتهديد.

آليات تحصينية

- الحذر من رسائل الاصطياد التي ترد عبر الهاتف المتحرك
- تجنّب استخدام كلمات السر الأكثر شيوعا.
- عدم استخدام كلمة المرور ذاتها لكافّة الحسابات
- تجنّب استخدام شبكات الانترنت اللاسلكيّة العامة
- تجنب فتح أي رسالة بريد إلكتروني قبل التأكد من مصدرها

متابعة حثيثة



البيان

غرافيك: حسام الحوراني

الملحق 04: حماية العالم من مخاطر المعلومات والحاسوب

فهرس المحتويات

فهرس المحتويات