المجلة الإلكترونية الشاملة متعددة التخصصات
العدد الرابع والعشرون شهر (٥) ٢٠٢٠

الجـرائـم السيبــرانيـة

روان بنت عطية الله الصحفي
المملكة العربية السعودية، جدة
E-mail: RaaWaaN555@hotmail.com

الملخص:

الجريمة السيبرانية هي إحدى الجرائم المعاصرة التي أصبحت تمثل خطرا على الفرد والمجتمع وعلى أمن الدولة ، إذ أنها تتقدم بوتيرة سريعة باستخدام المجرمون أحدث التقنيات في تنفيذ هجماتهم السيبرانية ، لذا كان علينا مواكبة الفضاء السيبراني والتعرف على طرق التصدي لهذه الجرائم المستحدثة بسن القوانين والأنظمة التي تختص بمكافحة الجرائم السيبرانية وفرض العقوبات على المجرمين .

ولهذا أحببت أن أقدم هذه الورقة البحثية لإعطاء نظرة حول الجرائم السيبرانية في التعدي على انتهاك المعلومات سواء أكانت على الفرد أو على الشركات أو الكيانات المنظمة ، حتى أيضا على الحكومات والدول ، ولوجود هذه الإشكالية تناولنا في هذا البحث مفهوم الجريمة السيبرانية والاطار القانوني للجريمة السيبرانية ودارسة الجوانب الموضوعية من أركان وعقوبات ، وكذلك الجوانب الإجرائية من الاستدلال والتحقيق والمحاكمة في الجريمة السيبرانية ، ووضع النتائج والتوصيات لما توصلت إليه الباحثة .

الكلمات المفتاحية: الجريمة السيبرانية،أمن الدولة، الفضاء السيبراني، الأنظمة.

Summary:

Cybercrime is one of the contemporary crimes that have become a threat to the individual, society and the security of the state, as it advances at a rapid pace using criminals with the latest technology in carrying out their cyber attacks, so we had to keep up with cyberspace and learn about ways to address these new crimes by enacting laws and regulations to combat Cybercrime and penalties for criminals.

That is why I liked to present this research paper to give a look at cybercrime in infringement of information violations, whether it is on the individual or on companies or organized entities, even also on governments and states, and for the existence of this problem we addressed in this research the concept of cyber crime and the legal framework of cyber crime and a study of aspects Objectivity of the pillars and penalties, as well as procedural aspects of reasoning, investigation and trial in cyber crime, and the development of the results and recommendations of what the researcher reached.

Keywords: Cybercrime, state security, cyberspace, regulations.

مقدمة

إننا نعيش في عصر التقنية والحاسبات والإنترنت في مختلف مجالات الحياة ، بل أصبح استخدامها ضرورة لا غنى عنها في جميع القطاعات الحكومية والخاص في تبادل المعلومات وتقديم الخدمات ، مواكبة للتطور الهائل في مجال الاتصالات وأنظمة المعلومات .

ولقد اجتمع قادة دول العالم في هذا الفضاء السيبراني في أول قمة استثنائية افتراضية لقادة دول مجموعة العشرين التي تضم أكبر اقتصادات العالم،

والذي ترأسها الملك سلمان بن عبد العزيز حفظه الله ملك المملكة العربية السعودية لمناقشة مكافحة جائحة كورونا والحدّ من تأثيرها الإنساني والاقتصادي.

ومع هذا الانفتاح ودخول العصر الرقمي وانتقال المجتمعات من الواقع الفعلي المادي إلى الواقع السيبراني أصبحنا نشاهد ظهور الجرائم السيبرانية وتعديها على الفرد والمجتمع ، بشكل ملحوظ ومتزايد ، ولهذا أحببت أن يكون مشروع بحثي عن الجرائم السيبرانية لأنها هي بالفعل جرائم العصر الحديث .

مشكلة الدراسة وتساؤلاتها :

كلما زاد تطور ثورة المعلومات والتكنولوجيا زاد معها التطور في هذه الجرائم ، ولذلك أصبحنا نرى صورا مستحدثة لتلك الجرائم ومنها الجرائم السيبرانية في التعدي على انتهاك المعلومات سواء أكانت على الفرد أو على الشركات أو حتى أيضا على الحكومات والدول ، فهي جرائم عابرة للحدود .

ولوجود هذه الإشكالية قررت أن أدرس الموضوع من حيث الجوانب الموضوعية والإجرائية للمسؤولية الجنائية في الجرائم السيبرانية .

هناك عدة تساؤلات منها :

١- ما هو تعريف الجريمة السيبرانية وماهي خصائصها ؟

٢- ماهو الإطار القانوني للجريمة السيبرانية ؟

٣- ماهي صور الجرائم السيبرانية ؟

٤- ماهو أركان وعقوبات الجرائم السيبرانية ؟

٥- كيف يكون الاستدلال والتحقيق والمحاكمة في الجريمة السيبرانية ؟

أهداف الدراسة :

تهدف الدراسة إلى معرفة مفهوم الجريمة السيبرانية والاطار القانوني للجريمة السيبرانية ودارسة الجوانب الموضوعية من أركان وعقوبات ، وكذلك الجوانب الإجرائية من الاستدلال والتحقيق والمحاكمة للمسؤولية ، ووضع النتائج والتوصيات لما توصلت إليه الباحثة .

أهمية الدراسة :

الجرائم السيبرانية من الجرائم المستحدثة التي تمثل خطرا وتهديدا كبيرا على الفرد والمجتمع وكذلك على الأجهزة الأمنية للدولة ، مما يجب علينا أن نتطرق لدراستها لمكافحة هذه الجرائم من وضع الأنظمة والعقوبات الرادعة، والتصدي لهجمات فايروسات المجرمين ومحاكمتهم أمام القضاء .

منهج الدراسة :

اعتمدنا منهج البحث على المنهج الاستنباطي (التحليلي) ببيان مفهوم الجريمة السيبرانية وخصائصها ، وتناول الجوانب الموضوعية والإجرائية للمسؤولية الجنائية .

المبحث الأول

مفهوم الجريمة السيبرانية

إن مصطلح الجرائم السيبرانية هو إحدى المصطلحات الحديثة والمستخدمة عن جرائم الإنترنت الذي تعددت مصطلحاته وذلك لنشأة وتطور ظاهرة الإجرام المرتبط والمتصل بتقنية المعلومات .

وفي الحقيقة لو تأملنا نجد بأن مصطلح الجرائم السيبرانية (cyber crime) هو مصطلح غير عربي ، لكنه هو المتداول والمستخدم حديثا في وقتنا الحالي في هيئة الاتصالات وتقنية المعلومات وكذلك في المؤتمرات والندوات (كملتقى الجرائم السيبرانية والأدلة الرقمية) الذي نظمته جامعة الأمير نايف العربية للعلوم الأمنية في مدينة الرياض عام ٢٠١٩ م .

وكذلك نجد كلمة سيبراني (cyber) قد ارتبط بالأمن الالكتروني فأصبحنا نعتمد مصطلح الأمن السيبراني وذلك انطلاقا من مسمى الهيئة الوطنية للأمن السيبراني ، وذلك وفق الأمر الملكي الكريم بالموافقة على تنظيمها بتاريخ ١٤٣٩/١٢/١١ هـ لتكون الهيئة هي الجهة المختصة في المملكة بالأمن السيبراني [١]، وليس ذلك فحسب بل اعتماد مصطلح الأمن السيبراني كتخصص جديد في جامعات المملكة مثل بكالوريوس الأمن السيبراني والتحدي الرقمي في جامعة الإمام عبد الرحمن بن فيصل في الدمام ، وكذلك بكالوريوس الأمن السيبراني في جامعة جدة ، وأيضا نجدها في تخصصات الدبلوم والماجستير في الأمن السيبراني كما في جامعة الملك عبد العزيز بجدة وغيرها .

[١] الهيئة الوطنية للأمن السيبراني - https://nca.gov.sa/pages/about.html .

لذلك فإن الباحثة ترى بأن مصطلح الجرائم السيبرانية في المجتمع العربي هو مصطلح عصري وحديث لجرائم الانترنت ، فكان من الضروري التطرق له في الأبحاث والرسائل الأكاديمية .

المطلب الأول

تعريف الجريمة السيبرانية

أولا : التعريف اللغوي للجريمة السيبرانية :

الجريمة السيبرانية تتكون من كلمتين هما الجريمة والسيبرانية ، لذا سنبدأ بتعريف الجريمة لغة أولا ، ويليها تعريف السيبرانية لغةً .

تعريف الجريمة في اللغة :

جاءت الجريمة في اللغة لمعنيين هما :

الأول : الذنب ، نقول جرم وأجرم ، وأجترم بمعنى واحد .

الثاني : الجناية ، كقولهم جرم إليهم وعليهم جريمة ، أجرم جني جناية وجرم إذا عظم جرمه أي أذنب .[٢]

[٢] د. خالد حسن أحمد لطفي ، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية ، دار الفكر الجامعي ، الإسكندرية ، الطبعة الأولى ،٢٠٢٠ م ، ص ١٣ .

تعريف السيبرانية في اللغة :

كما تطرقنا سابقا بأن (cyber) هي كلمة انجليزية ، "ولقد عرَّف قاموس أكسفورد كلمة سيبراني، أوCyber ، بأنها صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي ".[٣]

ثانيا : التعريف الشرعي للجريمة :

تعرف الجريمة بأنها " إتيان فعل محرم معاقب على فعله ، أو ترك فعل محرم معاقب على تركه ، أو هي فعل أو ترك نصت الشريعة على تحريمه والعقاب عليه .[٤]

ثالثا : التعريف القانوني للجريمة :

عُرِّف الجريمة من الناحية القانونية بعدة تعريفات منها : " هي إتيان فعل أو تركه عن إرادة جنائية إضرارا بمصلحة اجتماعية حماها المشرع بقواعد تجرمه وتعاقب عليه جزائيا "[٥]

ومن رأي الباحثة كان اختيارها على هذا التعريف لأنه لامس الجوانب الموضوعية والشكلية للجريمة ، إلا أنني أرى التعريف غير شامل لأنه في حدود والنطاق المحلي للجريمة المرتبكة .

---

[٣] د. وليد أحمد الروضان ، مالفرق بين أمن المعلومات والأمن السيبراني ، صحيفة الجزيرة الالكترونية ، مؤسسة الجزيرة للصحافة والطباعة والنشر ، ١٤٣٩ هـ ، العدد ١٦٦٣١ . https://www.al-jazirah.com/2018/20180411/rj3.htm

[٤] سامي علي حامد عياد ، الجريمة المعلوماتية وإجرام الانترنت ، دار الفكر الجامعي ، الإسكندرية ، بدون طبعة ، ٢٠٠٧ م ، ص١٢

[٥] د. عبد العزيز بن غرم الله آل جار الله ، جرائم الإنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية السعودي دراسة مقارنة (ويليه آثار العولمة على مستخدمي الإنترنت) ، دار الكتاب الجامعي ، الرياض ، الطبعة الأولى ، ٢٠١٧ م ، ص ٧٩ .

تعريف الجريمة السيبرانية:

إن الجرائم السيبرانية تعد من الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها ، فكانت بداية من مصطلح إساءة استخدام الكمبيوتر ، مرورا باصطلاح احتيال الكمبيوتر ، والجريمة المعلوماتية ، فاصطلاحات جرائم الكمبيوتر ، والجريمة المرتبطة بالكمبيوتر ، وجرائم التقنية العالية ، إلى جرائم الهاكرز ، فجرائم الإنترنت ، إلى آخر المصطلحات الجرائم السيبرانية .[٦]

ولهذا فإننا نجد في كل مرة مع ظهور مصطلح جديد لجرائم الإنترنت يظهر لنا تعريفا جديدا ، ففقهاء القانون لم يستقروا على تعريف واحد ، فنحن لا نستنكر ذلك أبدا لأنه من الطبيعي جدا أن يكون هذا الاختلاف وهذا التنوع في المفاهيم والآراء ، وذلك يرجع لحداثة الجرائم السيبرانية و لاختلافات الثقافات والقوانين بين الدول ، وأيضا خشية في أن يحصروا المصطلح في نطاق ضيق أو محدد .

فمنهم من عرف الجرائم السيبرانية : بأنها "هي التي تتم بواسطة الكمبيوتر أو أحد وسائل التقنية الحديثة على كمبيوتر آخر أو أحد وسائل أو أحد وسائل التقنية الحديثة ، مع ضرورة توفر شبكة اتصال فيما بينهما ".[٧]

والبعض الآخر عرفها : بأنها " نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود "[٨]

---

[٦] د. عبد العزيز بن غرم الله آل جار الله ، مرجع سابق ، ص ٧٠.
[٧] أسمامة مهمل ، الإجرام السيبراني ، رسالة ماجستير ، كلية الحقوق والعلوم السياسية ، جامعة محمد بوضياف ، ٢٠١٨/٢٠١٧ ، ص ٩ .
[٨] محمود أحمد القرعان ، الجرائم الإلكترونية ، دار وائل للنشر والتوزيع ، عمان ، الطبعة الأولى ، ٢٠١٧ ، ص ١٩ .

ومنهم من عرفها بأنها : " هي السلوك غير المشروع أو المنافي للأخلاق أو غير المسموح به المرتبط بالشبكات المعلوماتية العالمية فهي جرائم العصر الرقمي التي تطال بالمال والمعرفة والثقة والسمعة وهي كلها تنفذ عن طريق التقنية "[٩] .

وأما في النظام السعودي لمكافحة الجرائم المعلوماتية فلقد عرفها في المادة الأولى بأنها : أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام.

ومن خلال هذا التعريف لابد أن نوضح أكثر ما المقصود بالحاسب الآلي والشبكة المعلوماتية الذي قصده النظام السعودي .

فنجده عرف الحاسب الآلي أيضا في المادة الأولى من النظام بأنه : " أي جهاز إلكتروني ثابت أو منقول سلكي أو لا سلكي يحتوي على نظام معالجة البيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها ، يؤدي وظائف محددة بحسب البرامج ، والأوامر المعطاة له."

وعرف الشبكة المعلوماتية بأنها : ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية (الإنترنت) .

[٩] صالح علي عبد الرحمن الربيعة ، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت ، هيئة الاتصالات وتقنية المعلومات ، ص ٩ . http://myhistar1.blogspot.com/2019/01/pdf.html

وعرف أيضا برامج الحاسب الآلي بأنها : مجموعة من الأوامر، والبيانات التي تتضمن توجيهات أو تطبيقات حين تشغيلها في الحاسب الآلي ، أو شبكات الحاسب الآلي ، وتقوم بأداء الوظيفة المطلوبة.

وبناء على هذا التعاريف السابقة أصبح تعريف الجريمة السيبرانية في النظام السعودي أكثر توسعا فإنه يشمل دخول الأجهزة الالكترونية المعاصرة غير الكمبيوتر ضمن الحاسب الآلي ، وكذلك ارتباطها بالشبكات الخاصة والعامة والعالمية أيضا ، إلا أن هناك من مَيَّزَ جرائم الإنترنت عن الهواتف الخلوية من حيث العالم الافتراضي فجرائم الانترنت لا تقع إلا عن طريق الفضاء السيبراني بالاعتداء على البيانات أما الهواتف الخلوية فإن وقوع الجريمة قد يتعدى من عالم البيانات إلى العالم المادي الواقعي ، ويكون محل الجريمة أو المجني عليه هو كيان مادي ملموس[١٠] .

[١٠] د. محمود عمر محمود ، الجرائم المعلوماتية والإلكترونية ، خوارزم العلمية ، الطبعة الأولى ، ٢٠١٥ م ، ص٥٠ .

المطلب الثاني

خصائص الجريمة السيبرانية

إن الجريمة السيبرانية تتميز بعدة خصائص منها :

أولا : جرائم ترتكب بواسطة الأجهزة الالكترونية كالحاسب الالي والهواتف الخلوية :

وهما الأداتان التي تمكن المجرم من دخول الإنترنت لتنفيذ جريمته .

ثانيا : جرائم خفية :

فليس من السهولة اكتشافها لضعف القدرة الفنية للضحية وذلك مقارنة بالمجرم ، ولربما أيضا لمهارات المجرم الفنية والعلمية المتقدمة لقدرته على إخفائها ، أو لخوف الضحية من الإبلاغ عن الجريمة تجنبا للإساءة إلى السمعة [١١].

ثالثا : جرائم سريعة التنفيذ :

فسرعة ارتكاب الجريمة قد تكون خلال جزء من الثانية ، وقد لا تتطلب الإعداد قبل التنفيذ .[١٢]

رابعا : جرائم عن بعد :

فيمكن للجاني تنفيذ جريمته وهو في دولة بعيدة كل البعد عن المجني عليه .[١٣]

---

[١١] محمود أحمد القرعان ، مرجع سابق ، ص ٣٩ .
[١٢] تميم عبد الله سيف التميمي ، الجرائم المعلوماتية في الاعتداء على الأشخاص ، مكتبة القانون والاقتصاد ، الرياض ، الطبعة الأولى ٢٠١٦ ، ص ١٦ .
[١٣] تميم عبد الله سف التميمي ، مرجع سابق ، ص١٦ .

خامسا : جرائم عابرة للحدود :

فهي لا تعرف الحدود الجغرافية للدول ، لارتباط العالم بشبكة واحدة ، وهذا قد يسبب إشكاليات لدى الاختصاص القضائي من حيث التحقيق والمحاكمة ، وذلك تبعا لتعقيد الإجراءات التي تحكمها الاتفاقيات والمعاهدات والعلاقات الدولية ، والتنازع فيما بينهما على أي القانون الواجب التطبيق .

سادسا : جرائم صعبة الإثبات :

وتكمن " صعوبة إثباتها إلى أن متابعتها واكتشافها عن طريق الصدفة ، ومن الصعوبة حصرها في مكان معين ، حيث أنها لا تترك أثرا واضحا للعيان ، أو تشاهد بالعين المجردة ، فما هي إلا أرقام تدور في السجلات والمواقع الالكترونية ، كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها ، وتعود الصعوبة لعدة أسباب :

١- إنها كجريمة لا تترك أثرا بعد ارتكابها .

٢- صعوبة الاحتفاظ الفني بآثارها إن وجدت .

٣- تحتاج لخبرة فنية يصعب على المحقق التقليدي التعامل معها .

٤- تعتمد على الخداع في ارتكابها ، والتضبيب في التعريف على مرتكبيها .

٥- تعتمد على مستوى من الذكاء المرتفع في ارتكابها " [١٤]

[١٤] محمود أحمد القرعان ، مرجع سابق ، ص٤٠ .

سابعا : جرائم ناعمة :

فهي جرائم لا تمارس بالعنف ، ولا تحتاج إلى أدني مجهود عضلي ، بعكس بعض الجرائم التقليدية .[١٥]

ومن هنا نلاحظ بأن المجرم السيبراني يتميز بمهارات عالية ، فهو يعتمد على قدراته العقلية بالذكاء والدهاء ومعرفة الطرق السيبرانية لإتلاف البرامج واختراق الحواجز الأمنية ، ولعل الدافع للمجرمين السيبرانيين قد يكون بدافع المال بلجوئهم إلى الطرق الغير مشروعة وذلك بسبب ما يعانوه من البطالة ، وقد يكون بدوافع عقائدية وسياسية ، وقد يكون بدوافع شخصية كقيام الموظف بالانتقام من المؤسسة أو الشركة التي قامت بفصله ، أو للتجسس وانتهاك الخصوصية

المطلب الثالث

الاطار القانوني للجريمة السيبرانية

في هذا المطلب سنتعرف على أطراف الجريمة السيبرانية وهما المجرم السيبراني ، والمجني عليه في الجريمة السيبرانية .

أولا : المجرم السيبراني :

أ) خصائص المجرم السيبراني .

[١٥] تميم التميمي ، مرجع سابق ، ص١٦ .

هو مجرم يتمتع بقدرة فائقة من الذكاء إذ يستغل مهاراته في اختراق الشبكات وكسر الشفرات وكلمات المرور ، موظفا مهاراته تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات ، كما أنهم في الغالب يتميزون بأنهم أفراد ذوي مكانة في المجتمع من أصحاب الوظائف الحيوية ، سواء في القطاع الخاص أو في القطاع العام ، وقد أطلق عليهم مصطلح ذوي الياقات البيضاء .

وقد ثبت من خلال الدراسات النفسية للمجرم السيبراني بأن ليس لديه أي شعور بعدم مشروعية الأفعال التي يمارسونها ، وعدم استحقاقهم للعقاب ، كما تغيب مشاعر الإحساس بالذنب ، وذلك لربما عدم احتكاك الجاني المجرم بالمجني عليه مما يسهل المرور إلى الفعل الغير مشروع ، وهم غالبا يخشون من اكتشافهم وافتضاح أمرهم .

ب) أصناف المجرم السيبراني :

١- **الهواة :** وهم من يرتكبون هذه الجرائم بغرض التسلية دون ضرر بالمجني عليه .

٢- **القراصنة :** ومنهم الهاكر : هم متطفلون على أمن النظم المعلوماتية والشبكات من خلال دخولهم إلى أنظمة الحاسبات وكسر الحواجز الأمنية وهدفهم الفضول أو اثبات الذات، ومنهم الكراكر : وهم من يقومون بالتسلل إلى أنظمة المعالجة للاطلاع على المعلومات المخزنة لإلحاق الضرر إما بالسرقة أو العبث بها .

٣- **المهووسون :** ويكون المجرم في حالة الجنون الذي يهدف إلى تحطيم كل الأنظمة .

٤- **الجريمة المنظمة :** فجهاز الحاسب أصبح أداة فعالة بأيدي عصابات المافيا .

٥ – **الحكومات الأجنبية** : وذلك باستعمال أجهزة الحاسب في مجال الجاسوسية .

٦ – **المتطرفون** : وهم من يستخدمون الشبكة المعلوماتية لنشر أفكارهم السياسية والدينية المتطرفة .[١٦]

ج) أساليب المجرم السيبراني لارتكاب الجريمة السيبرانية :

يستخدم المجرم السيبراني تقنية الاختراق لتنفيذ جريمته وذلك من خلال التحايل على الأنظمة المعلوماتية ، فيكون الاختراق بالقدرة على وصول هدف معين عن طريق ثغرات في نظام الحماية الخاصة ، و تتم عن طريق برنامجين الأول الخادم وهو بجاهز الضحية إذ ينفذ المهام الموكلة إليه ، والثاني يوجد بجهاز المخترق ويسمى بالبرنامج المستفيد .

كما أنهم يستخدمون عدة برامج منها :

١– حصان طراودة : وهو عبارة عن برنامج صغير مختبئ ببرنامج أكبر ، وتؤدي مهامها بشكل خفي في اطلاق الفيروسات والدودة التي تقوم بإرسال البيانات عن الثغرات الموجودة في النظام ، وارسال كلمات المرور السرية الخاصة بالهدف ، ومن أنواعه القنابل المنطقية التي يزرعها المبرمج داخل النظام الذي يطوره .

٢– فيروسات الكمبيوتر : وهي برامج صغيرة تستخدم لتعطيل شبكات الخدمات .

٣– الديدان : وهي تكاثر عن طريق نسخ نفسها عن طريق الشبكات وهدفها الشبكات المالية مثل البورصات .

[١٦] خالد حسن أحمد لطفي ، مرجع سابق ، ص ٣٨ .

٤- الأبواب الخلفية : وهي ثغرة تترك عن عمد من مصمم النظام للتسلل إليه وقت الحاجة .

٥- الاختناق المروري السيبراني : وهو سد وخنق الاتصالات لدى المستهدف بحيث لا يمكنه تبادل المعلومات .

٦- القصف السيبراني : وهو الهجوم على شبكة المعلومات بحيث يسبب ضغط كبير على الموقع فيفقد قدرة الموقع على استقبال الرسائل من العملاء ، وبالتالي يوقف عن العمل تماما .

ثانيا : المجني عليه في الجريمة السيبرانية :المجني عليه قد يكون شخصا طبيعيا عاديا وقد يكون شخصا طبيعيا لا كنه ذو منصب سياسي رفيع ، أو رجل أعمال ، أو صاحب شهرة عالمية ، وقد يكون شخصا اعتباريا كالشركات والبنوك والمؤسسات والقطاعات الحكومية والخاص والمؤسسات المالية إذا تعتبر من أكثر الأماكن استهدافا نظرا لما لها من أموال .[١٧]

[١٧] خالد حسن أحمد لطفي ، مرجع سابق ، ص ٤٣ .

المبحث الثاني

الجوانب الموضوعية للمسؤولية الجنائية

المطلب الأول

صور الجرائم السيبرانية

قبل البدء بالجوانب الموضوعية المتعلقة بأركان وعقوبات الجريمة السيبرانية ،يجب علينا أولا التعرف على صور الجرائم السيبرانية ، وهي كالآتي :

أولا : الاعتداء السيبراني على معطيات الحاسب الآلي :

كإتلاف البيانات والمعلومات والبرامج ، والتلاعب بالمعلومات المخزنة داخل الحاسب .

ثانيا : الاعتداء السيبراني على حرمة الحياة الخاصة :

١- يكون بالإفشاء العلني للوقائع الخاصة التي تمس الشخص كإفشاء واقعة إصابته بمرض مخزي ، أو عجز عن سداد ديونه أو نشر صورة لابنه .

٢- تشويه سمعة الشخص في نظر الجمهور ، والتشهير به .

٣- الاستيلاء على بعض العناصر الشخصية كالاسم والصورة والبيانات الشخصية المتصلة بالحياة الخاصة .[١٨]

[١٨] علي نعمة جواد الزرفي ، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة ، المكتب الجامعي الحديث ، بدون طبعة ،٢٠١٩م ، ص٣٨ .

ثالثا : الاعتداء السيبراني على حقوق الملكية الفكرية :

ويكون بالاعتداء على العلامات التجارية وبراءات الاختراع ، وكذلك نسخ وتقليد البرامج وإعادة إنتاجها وصنعها دون ترخيص فهو اعتداء على الحقوق المالية والحقوق الأدبية .[١٩]

رابعا : الاستيلاء والنصب والاحتيال السيبراني :

ويكون الاستيلاء إما لنفسه أو لغيره على مال منقول أو على سند ، أو توقيع هذا السند ، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة .[٢٠]

خامسا : الانتحال والتغرير السيبراني :

١- انتحال شخصية فردية : بسبب التنامي المتزايد لشبكة الإنترنت والذي أعطى للمجرمين قدرة أكبر على جمع المعلومات للشخصية المطلوبة والاستفادة منها في ارتكاب جرائمهم فتنتشر في شبكة الإنترنت الكثير من الإعلانات المشبوهة والتي تحاكي الطمع الإنساني في محاولة الاستيلاء على معلومات اختيارية من الضحية، فهناك إعلان عن جائزة فخمة يكسبها من يساهم بمبلغ رمزي لجهة خيرية، وهذا يتطلب الإفصاح عن معلومات سرية الأمر الذي يؤدي الى استيلاء على رصيده البنكي أو السحب من بطاقته الائتمانية أو الاساءة إلى سمعة الضحية

[١٩] غانم مرضي الشمري ، الجرائم المعلوماتية ، الدار العلمية الدولية ، عمان ، الطبعة الأولى ، ٢٠١٦ م ، ص٥٢ .
[٢٠] نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية ، مرجع سابق .

٢- انتحال شخصية المواقع : و يكون باختراق حاجز أمني وتتم عملية الانتحال بهجوم يشنه المجرم على الموقع للسيطرة عليه ومن ثم يقوم بتحويله كموقع بيني أو يحاول المجرم اختراق موقع لأحد مقدمي الخدمة المشهورين ثم يقوم بتركيب البرنامج الخاص به هناك مما يؤدي إلى توجه أي شخص إلى موقعه بمجرد كتابة اسم الموقع المشهور . .[٢١]

سادسا : الابتزاز والتهديد السيبراني :

كنشر صور أو معلومات صحيحة أو غير صحيحة عن المجني عليه بهدف الحصول على المال أو علاقة غير مشروعة .

سابعا : التنصت السيبراني :

استخدام برنامج في جهاز الشخص المعتدى عليه يمكن من خلاله الاطلاع والاستماع إلى جميع المحادثات والمراسلات الصادرة من الشخص المعتدى عليه ويتم إدخال هذا الملف إلى جهاز المعتدى عليه عن طريق البريد الالكتروني أو عن طريق مواقع مغرية يزورها المعتدى عليه فيقوم بتنزيل بعض البرامج ومنها برنامج التنصت ، استخدام برنامج المحادثة، فيقوم المجرم بإغراء الضحية بأن هذا البرنامج يحتوي على ألعاب مثيرة أو غير ذلك فيقوم الضحية باستقبال الملف .

[٢١] هيئة الاتصالات وتقنية المعلومات مرجع سابق ،
. https://www.citc.gov.sa/ar/mediacenter/awarenesscampaigns/Pages/awar_6.aspx

وجريمة التنصت إما أن تكون بالالتقاط وهو مشاهدة البيانات عبر الشبكة المعلوماتية أو أحد أجهزة الحاسب ، أو أن تكون بالاعتراض وهو اعتراض ماهو مرسل عبر الشبكة المعلوماتية أو أحد أجهزة الحاسب الالي بحيث يتم عمل إجرام كتحويل أموال .[٢٢]

ثامنا : السطو السيبراني على أموال البنوك :

عن طريق استخدام الجاني الحاسب الآلي للدخول إلى شبكة الإنترنت والوصول غير المشروع إلى البنوك والمصارف والمؤسسات المالية .وتحويل الأموال من تلك الحسابات الخاصة بالعملاء إلى حسابات أخرى وذلك بإدخال بيانات غير حقيقية أو تعديل أو مسح البيانات الموجودة بقصد اختلاس الأموال أو نقلها وإتلافها وتقوم هذه التقنية على الاستيلاء على الأموال بكميات صغيرة جدًا من الحسابات الكبيرة بحيث لا يلاحظ نقصان هذه الأموال .[٢٣]

تاسعا : الاعتداء السيبراني على الأخلاق والاتجار بالبشر وبالمخدرات :

١- إنشاء موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره لإتجار في الجنس البشري أو تسهيل التعامل به .

٢- إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها.

[٢٢] هيئة الاتصالات وتقنية المعلومات مرجع سابق ، https://www.citc.gov.sa/ar/mediacenter/awarenesscampaigns/Pages/awar_6.aspx .

[٢٣] هيئة الاتصالات وتقنية المعلومات مرجع سابق ، https://www.citc.gov.sa/ar/mediacenter/awarenesscampaigns/Pages/awar_6.aspx .

٣- إنشاء موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره للإتجار بالمخدرات أو المؤثرات العقلية أو ترويجها أو طرائق تعاطيها أو تسهيل التعامل بها .

عاشرا : الاعتداء السيبراني على الأمن :

كإنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات ، أو أي من أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرات أو أي أداة تستخدم في الأعمال الإرهابية ، والدخول غير المشروع إلى موقع إلكتروني أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني.[٢٤]

المطلب الثاني

أركان الجريمة السيبرانية

لاتختلف أركان الجريمة السيبرانية عن أركان أي جريمة أخرى فلابد من توافر الركن المادي والركن المعنوي .

أولا : الركن المادي :

[٢٤]

ويُعَرّف بأنه : " النشاط المادي الذي يصدر عن الجاني متخذا مظهرا خارجيا يتدخل من أجله القانون بتقرير العقاب " .[٢٥]

ويتمثل الركن المادي للجريمة في سلوك إرادي يترتب عليه نتيجة إجرامية تربطها بالسلوك الإجرامي رابطة سببية مادية ، بمعنى أن الركن المادي يتكون من ثلاث عناصر :

العنصر الأول : السلوك الإجرامي :

وصوره متعددة كالسلوك الإجرامي الإيجابي وذلك بمخالفته نصا ينهي عن الإتيان بهذا الفعل كسرقة بيت أو جهاز معين ، سواء كان التحرك الإيجابي بحركة واحدة كالقتل بالرصاص ، أو بحركات متعددة كالمشاجرة التي تنتهي بالوفاة .

وقد يكون سلبيا بمخالفة نص يأمر بإتيان فعل معين ، كامتناع ممرضة عن إعطاء جرعة الدواء لمريضها العاجر بما يؤدي لوفاته .

وقد يكون السلوك الإجرامي بصورة بسيطة كما في جريمة القذف ، وقد تكون بصورة معقدة كما في جريمة الإرهاب أو السطو المسلح .

فالقانون الجنائي لا يعوّل كثيرا على الوسيلة التي ارتكبت بها الجريمة أو وقع بها السلوك الإجرامي ولا يعتد بزمان أو مكان وقوع الجريمة إلا عند تقديره للظروف المشددة أو المخففة ، فيستوي القتل أن يكون بمسدس أو بالسكين ، أو حتى عن طريق الريموت كنترول أو بواسطة أجهزة الحاسوب .

[٢٥] عبد العزيز غرم الله آل جار الله ، مرجع سابق ، ص ٨٥ .

فأهمية هذه الصور المجرمة والظروف المصاحبة لها تظهر مدى توافر القصد الجنائي ، كما تفيد تحديد الاختصاص القضائي ، والقانون واجب التطبيق ، وبدء سريان مدة التقادم في الأنظمة المقارنة .

كما يمكن تقسيم وتكييف الجرائم بنفس تقسيم الجرائم التقليدية ، وذلك حين تتشابه معها في ذات السلوك الإجرامي .[٢٦]

العنصر الثاني : النتيجة الإجرامية :

وتثير مسألة النتيجة الإجرامية في الجرائم السيبرانية جدلا كبيرا بين أنصار المذهب المادي وأنصار المذهب القانوني حول تحديد الجريمة السيبرانية هل هي جرائم مرتكبة سلوكا أو كنتيجة في العالم الافتراضي ، أم أن هناك امتدادا للنتيجة لتحقيق وجودها المادي .[٢٧]

وتنقسم النتيجة الإجرامية إلى قسمين :

١- جرائم الضرر : هي التي يطلب القانون في ركنها المادي حصول ضرر معين ، وذلك مثل حصول الضرر في الجرائم السلبية والإيجابية .

٢- جرائم الخطر : فهر جرائم السلوك المجرد حتى لو لم تقع النتيجة الإجرامية وكذلك كما في جرائم المشروع والتي تعاقب عليها الأنظمة في حالة كونها جناية ، وذلك لما يمثله السلوك الإجرامي من خطر دون النظر في نتيجة ذلك الفعل،

[٢٦] عبد العزيز غرم الله آل جار الله ، مرجع سابق ، ص ٨٨ .

[٢٧] محمود أحمد القرعان ، مرجع سابق ، ص ٣٤ .

بينما يختلف الأمر في الجنح والمخالفات فلا يعاقب عليها القانون بصفة عامة نظرا لقلة خطورة الدافع الإجرامي في نفس الفاعل .

العنصر الثالث : علاقة السببية :

لم يحدد القانون الجنائي معيارا لتحديد الرابطة السببية ، فناقش علماء القانون واستقر رأيهم على ثلاث نظريات :

١- نظرية تعادل الأسباب : وهي تساوي جميع العوامل التي تساهم في إحداث النتيجة الإجرامية ، فهي متعادلة من حيث قوة أثرها في حصول النتيجة .

٢- نظرية السبب الأقوى أو السبب المباشر : فهي لا تساوي بين الأسباب المساهمة في حصول الجريمة ، بل تنظر إلى السبب الأقوى سواء كان هو سلوك الجاني أو غيره ، وهذه النظرية حصرت النتيجة في عامل واحد هو أقوى الأسباب ، وهذا يؤدي بالجاني إلى الإفلات من العقاب .

٣- نظرية السببية الملائمة : ومضمونها أن الجاني يسأل عن النتائج المحتملة أو المتوقعة لفعله وذلك حسب المجرى العادي للأمور ، مالم يتدخل لقطع تلك العلاقة سبب شاذ أو غير مألوف ، وقد تكون هذه النظرية هي أنسب النظريات ظن فلو أر[٢٨]سل الجاني فيروسا إلى بريد المجني عليه الالكتروني مما تسبب في تلف الجهاز بالكامل لدى فتح المجني عليه بريده الالكتروني ، فهذا سبب مباشر يسأل الجاني عنه،

[٢٨] عبد العزيز غرم الله آل جار الله ، مرجع سابق ، ص ٩٣ .

بينما لو كان المجني عليه قد أُرسلت له عدة فيروسات من عدة أشخاص وتسببت بمجموعها بتلف الجهاز ، فإن القضاء حينئذ يعمل إحدى النظريات السابقة .

ثانيا : الركن المعنوي

وهو مايعرف بأنه العلم بعناصر الجريمة وإرادة ارتكابها وبالتالي يتكون هذا الركن من عنصرين هما العلم والإرادة [٢٩].

فالركن المادي والركن المعنوي يرتبطان ببعض ارتباطا قويا ، وذلك أن الركن المعنوي انعكاس لما في نفسية المجرم من قصد الجريمة وتوجه إرادته نحو تحقيق ذلك الركن المادي للجريمة ، ولايتحقق إلا بوجود هذه العنصرين عنصر الإرادة وعنصر العلم .

عنصر العلم :

ويشمل على عدة عناصر :

- العلم بالوقائع .
- العلم بموضوع الجريمة .
- العلم بحقيقة الفعل وخطورته وأنه يلحق ضررا بالحق المعتدى عليه .

ولايشترط شرط العلم في القانون الجنائي أن يكون الجاني عالما بأن الفعل الذي يقدم عليه هو فعل مجرم يعاقب عليه القانون .[٣٠]

[٢٩] محمود أحمد القرعان ، مرجع سابق ، ص٣٥ .
[٣٠] عبد العزيز غرم الله آل جار الله ، مرجع سابق ، ص ٩٥ .

عنصر الإرادة :

هي " قوة نفسية ونشاط نفسي يوجه لتحقيق هدف معين بوسيلة معينة ، فهي ظاهرة نفسية يصدر عن وعي وإدراك "[٣١]

وتقوم الإرادة على عنصرين :

- إرادة الفعل : وهي إثبات بأن الجاني قد اتجه إلى عمل يمثل فعله خطرا على الحق الذي يحميه القانون .
- إرادة النتيجة : فلايكتفى بإرادة الفعل بل لابد من إرادة النتيجة ، ليكتمل القصد الإجرامي بالركن المعنوي .

والقصد الجنائي يتأخذ عدة صور منها القصد العام والقصد الخاص وهي كالآتي :

القصد الجنائي العام : هو الهدف الفوري والمباشر للسلوك الإجرامي ويتحصر في حدود تحقيق الغرض من الجريمة أي لا يمتد لما بعدها .[٣٢]

القصد الجنائي الخاص : هو ما يتطلب توافره في بعض الجرائم فلا يكفي بمجرد تحقيق الغرض من الجريمة ، بل هو أبعد من ذلك ، أي أنه يبحث في نوايا المجرم .[٣٣]

إن المجرم السيبراني يتوجه من أجل ارتكاب فعل غير مشروع أو غير مسموح مع علم هذا المجرم بأركان الجريمة،

---

[٣١] خالد حسن أحمد لطفي ، مرجع سابق ، ص٥٠ .
[٣٢] محود أحمد القرعان ، مرجع سابق ، ص ٣٥ .
[٣٣] محود أحمد القرعان ، مرجع سابق ، ص ٣٦ .

وبالرغم من أن بعض المخترقين يبرّرون أفعالهم بأنهم مجرد فضوليون ، وأنهم قد تسللوا صدفة ، فلا انتفاء العلم كركن للقصد الجنائي ، كان يجب عليهم أن يتراجعوا بمجرد دخولهم ، ولا يستمروا في الاطلاع على أسرار الأفراد والمؤسسات ، لأن جميع المجرمين والأشخاص الذين يرتكبون هذه الأفعال يتمتعون بمهارات عقلية ومعرفية كبيرة تصل في كثير من الأحيان إلى حد العبقرية .

فالقصد الجنائي متوافر في جميع الجرائم السيبرانية دون أي استثناء ، ولكن هذا لايمنع أن هناك بعض الجرائم السيبرانية تتطلب أن تتوافر فيها القصد الجنائي الخاص مثل جرائم تشويه السمعة عن طريق الإنترنت ، وفي كلا الحالات فإن المنظم هم من يختص بتحديد الحالات التي يشترط فيها توافر القصد الجنائي الخاص .

المطلب الثالث

عقوبة الجريمة السيبرانية

تعريف العقوبة لغة :

" مصدرها عاقب ، وهو جزاء فعل السوء " [٣٤]

تعريف العقوبة في الاصطلاح :

هي " زواجر وضعها الله تعالى للردع عن ارتكاب ماحظر وترك ماأمر به " [٣٥].

[٣٤] د. أحمد مختار عبد الحميد عمر ، معجم اللغة العربية المعاصرة ، عالم الكتب ، الطبعة الأولى ، ٢٠٠٨ م .
[٣٥] تميم عبد الله سيف التميمي ، مرجع سابق ، ص ٢٣٤ .

وقد عرفها بعض المعاصرين من أهل العلم بأنها " الجزاء المقرر لمصحلة الجماعة على عصيان أمر الشارع "[٣٦]

تعريف العقوبة في القانون :

وهو " الجزاء الذي يقرره القانون ويوقعه القاضي من أجل الجريمة ويتناسب معها "[٣٧]

فالعقوبة لا تكون إلا بحكم قضائي ، فهو " لا يجوز توقيع عقوبة جزائية على أي شخص إلا بعد ثبوت إدانته بأمر محظور شرعا أو نظاما بعد محاكمة تجرى وفقا للمقتضى الشرعي " [٣٨] .

وتنقسم العقوبات إلى عدة تقسيمات :

أولا : عقوبات أصلية :

وهي العقوبات المقررة أصلا للجريمة ، ومنها الجلد للجاني المحصن ، والجلد للقاذف ، والقطع للسارق ، والسجن للمشهر به .

ثانيا : عقوبات بديلة :

وهي العقوبات التي تحل محل العقوبة الأصلية إذا امتنع عن تطبيق هذه لسبب شرعي ، كما أنها العقوبة الذي يفرضها القضاء على المحكوم عليه عوضا عن العقوبة الأصلية ومنها الدية إذا دُرء القصاص عن القاتل عمدا ، والتعزيز إذا دُرء الحد أو القصاص .

[٣٦] تميم عبد الله سيف التميمي ، مرجع سابق ، ص ٢٣٤ .
[٣٧] فوزية عبد الستار ، شرح قانون العقوبات ، دار النهضة ، القاهرة ، ١٩٨٢م ، ص ٦٦٦ .
[٣٨] نظام الإجراءات الجزائية في النظام السعودي ، المادة الثالثة .

ثالثا : عقوبات تبعية :

وهي العقوبة التي تتبع العقوبة الأصلية بقوة العقوبة دون الحاجة للحكم بها ، ومنها حرمان القاتل من الميراث .

رابعا : عقوبات تكميلية :

وهي العقوبة التي تتبع العقوبة الأصلية ولا تصيب الجاني إلا إذا حكم عليه ، وأيضا العقوبات التي تنطق بها المحكمة بالإضافة إلى عقوبة أخرى أصلية ، وقد تكون تكميلية وجوبية ، وقد تكون تكميلية جوازية .

أهداف العقوبات :

- المساعدة على تحقيق الأمن السيبراني .
- حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات السيبرانية .
- حماية المصلحة العامة ، والأخلاق، والآداب العامة.
- حماية الاقتصاد الوطني.[٣٩]

العقوبات المقررة ضد مرتكبي الجرائم السيبرانية وفقا لنظام مكافحة الجرائم السيبرانية في النظام السعودي نستعرض أهمها :

أولا : عقوبة التنصت ، والتهديد والابتزاز ، والدخول الغير مشروع لموقع الكتروني ، والتشهير بالآخرين والحاق الضرر بهم :

[٣٩] نظام مكافحة جرائم المعلوماتية في النظام السعودي ، المادة الثانية .

يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين ، وفقا للمادة الثالثة من النظام .

ثانيا : عقوبة الاستيلاء لنفسه أو لغيره ، والسطو على أموال البنوك :

يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين ، وفقا للمادة الرابعة من النظام .

ثالثا : عقوبة الاعتداء على معطيات الحاسب الآلي :

يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين ، وفقا للمادة الخامسة من النظام .

رابعا : عقوبة المساس بالنظام العام أو القيم الدينية أو حرمة الحياة الخاصة ، وكذلك الاتجار بالبشر والاتجار بالمخدرات :

يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال ، وفقا للمادة السادسة من النظام .

خامسا : عقوبة إنشاء المنظمات الإرهابية على الشبكات السيبرانية ، وكذلك المساس بالأمن الداخلي والخارجي للدولة أو اقتصادها الوطني :

يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال ، وفقا للمادة السابعة من النظام .

سادسا : عقوبة التحريض على الجرائم السيبرانية :

يعاقب كل من حرَّض غيره، أو ساعده، أو اتفق معه على ارتكاب أيٍّ من الجرائم المنصوص عليها في هذا النظام ؛ إذا وقعت الجريمة بناء على هذا التحريض، أو المساعدة، أو الاتفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها ، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية ، وفقا للمادة التاسعة من النظام .

كما أن هناك عقوبات تبعية أيضا للجرائم السيبرانية ومنها :

مع عدم الإخلال بحقوق حسني النية ، يجوز الحكم بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها . كما يجوز الحكم بإغلاق الموقع الإلكتروني ، أو مكان تقديم الخدمة إغلاقًا نهائيًّا أو مؤقتًا متى كان مصدرًا لارتكاب أي من هذه الجرائم ، وكانت الجريمة قد ارتكبت بعلم مالكه ، وفقا للمادة الثالثة عشر من النظام .

المبحث الثالث

الجوانب الإجرائية للمسئولية الجنائية

المطلب الأول

الاستدلال في الجريمة السيبرانية

إن جمع الاستدلالات من الإجراءات التي تسبق التحقيق ورفع الدعوى الجنائية والتي يختص بها مأموري الضبط الجنائي والتي يكون النائب العام مشرف ومسؤول عن أعمالهم ، وإجراءات جمع الاستدلال ينطوي فيها عملية البحث والتحري حول الجريمة والتمهيد للتحقيق فيها والتي تختص بها النيابة العامة دون غيرها .

فالاستدلال هو : " مجموعة الإجراءات الأولية السابقة على تحريك الدعوى الجنائية والتس تستهدف التحري عن الجرائم والتثبت من وقوعها وجمع معلومات كافية بشأنها ، وإثبات الآثار التي تولدت عنها على وجه يتيح لسلطة التحقيق التصرف في التهمة ، سواء بتحريك الدعوى الجنائية الناشئة عنها ، أو بحفظ أوراقها وصرف النظر عنها ، فهو إجمالا بمثابة إعداد العناصر الازمة للتحقيق في الجريمة "[٤٠]

وعلى رجال الضبط الجنائي بحسب المهمات الموكلة إليهم وحسب اختصاصاتهم بأن يستقبلوا جميع البلاغات والشكاوى التي تردهم في الجرائم،

[٤٠] د. محمد حميد المزمومي ، الوسيط في شرح نظام الإجراءات الجزائية السعودي ، مركز النشر العلمي بجامعة الملك عبد العزيز ، جدة ، الطبعة الثانية ، ٢٠١٩ ، ص ٩٨ .

ولقد حدد نظام الإجراءات الجزائية السعودي في المادة السادسة والعشرون رجال الضبط الذين خولهم النظام بالقيام بأعمال الضبط وهم:

١- أعضاء هيئة النيابة العامة في مجال اختصاصاتهم .

٢- مدير الشرطة ومعاونيهم في المدن والمحافظات والمراكز ؟

٣- الضباط في جميع القطاعات العسكرية بحسب المهمات الموكلة إليهم في الجرائم التي تقع ضمن اختصاص كل منهم .

٤- محافظي المحافظات ورؤساء المراكز .

٥- رؤساء المراكب السعودية البحرية والجوية في الجرائم التي ترتكب على متنها .

٦- رؤساء مراكز الأمر بالمعروف والنهي عن المنكر في حدود اختصاصاتهم .

٧- الموظفين والأشخاص الذين خولوا صلاحيات الضبط الجنائي بموجب أنظمة خاصة .

٨- الجهات واللجان والأشخاص الذين يكلفون بالتحقيق ، بحسب ما تقضي به الأنظمة .

الواجبات المحددة لرجال الضبط الجنائي :

أولا : تلقي البلاغات والشكاوي والتحري عنها :

عادة تبقى الجريمة مستترة حتى يصل خبرها إلى السلطات المختصة ، و أي إخبار أو بلاغ عن الجريمة لابد وأن يتضمن على الأقل معلومات أولية عن الجريمة مثل محل الجريمة ومكان وقوعها ونوعها ، ويتم الكشف عن الجرائم السيبرانية بوضع برمجيات حاسوبية معينة خصوصا فيما يخص جرائم القرصنة أو نشر المواد الإباحية.

وللحصول على البيانات المتعلقة بارتكاب الجريمة من نظام الحاسب الآلي لإن هناك وسيلتان تستندان إلى معايير تقنية وقانونية وتتمثل في الآتي :

١- يتم الحصول على الملعومات من الموقع نفسه الذي تم من خلاله ارتكاب الجريمة بعد أن يتم اكتشافه ، باستخدام البرمجيات الحديثة .

٢- يتم الحصول على المعلومات عن طريق اعتراض أو رصد البيانات المنقولة من الموقع أو إليه أو في إطاره .[٤١]

ولقد حددت المملكة العربية السعودية أدوات البلاغ عن الجرائم السيبرانية وهي كالآتي :

- عن طريق الشرطة حسب الاختصاص المكاني .
- الاتصال على الرقم ٩٨٩ .
- التطبيق الالكتروني (كلنا أمن) على الأجهزة الذكية .
- البوابة الإلكترونية لوزارة الداخلية (أبشر) .
- هيئة الأمر بالمعروف أو النهي عن المنكر عن طريق الهاتف ١٩٠٩ أو الموقع الإلكتروني https://www.pv.gov.sa/Pages/PVHome.aspx
- عن طريق ارسال بريد الكتروني لهيئة الاتصالات وتقنية المعلومات info.cybercrime@moisp.gov.sa
- عن طريق البلاغ عن حادثة سيبرانية في موقع الالكتروني للهيئة الوطنية لأمن السيبراني https://www.my.gov.sa/wps/portal/snp/main

[٤١] خالد حسن أحمد لطفي ، مرجع سابق ، ص ٩٩ .

ثانيا : معاينة مسرح الجريمة :

والمقصود به هي تلك الآثار التي يتركها مستخدم الشبكة السيبرانية المشتملة على الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الحاسب الآلي والشبكة ، فالمعاينة في الجرائم التقليدية قد تحتوي على آثار مادية فعلية ، ولكن في الجرائم السيبرانية قد تطول الفترة الزمنية بين وقوع الجريمة واكتشافها مما يعرض الاثار الناجمة عنها إلى المحو أو التلف أو العبث بها ، كما يستطيع مأمور الضبط الجنائي الاستعانة بأهل الخبرة عند إجراء المعاينة إذا لزم الأمر ، وذلك لإعطاء رأيهم الفني في ذلك ، وإذا تمت المعاينة بعد وقوع الجريمة في المجال السيبراني فيجب مراعاة الآتي :

١- تصوير الحاسب والأجهزة الطرفية المتصلة به على ان يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة ،

٢- العناية بملاحظة الطريقة التي تم بها إعداد النظام .

٣- ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على المحكمة .

٤- عدم نقل أي مادة سيبرانية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة .

٥- التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة وفحصها ، ويرفع من عليها البصمات ذات الصلة بالجريمة .

٦- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة ، لرفع ومضاهاة ما قد يوجد عليها من بصمات .

٧- قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر لهم الكفاءة العلمية والخبرة في مجال الحاسبات .[٤٢]

ثالثا: سماع أقوال الشهود والمشتبه بهم:

وفي الواقع نادرا ما نجد شاهدا على وقائع الجريمة السيبرانية ، وذلك لعدة أسباب أهمها أن الجرائم السيبرانية تتطلب دراية كافية بالجوانب الفنية والتقنية للحاسب الآلي ، كما أن الجرائم السيبرانية ترتكب في هدوء أي أن الجاني يرتكبها وحده دون وجود أحد معه ، وكما انها لاتترك أي آثار خارجية يشهد بها أحد كما هو المعتاد في الجرائم التقليدية .

وليس لمأمور الضبط الجنائي أن يأمر بإحضار متهم او شاهد ، بل له استدعاء من يشاء لسماع أقواله ، وإذا رفض الحضور فليس له إكراه في ذلك ، أو احضاره بمذكرة قبض ، لأن هذا من اختصاص النيابة العامة .[٤٣]

[٤٢] خالد حسن أحمد لطفي ، مرجع سابق ، ص ١٠٢ .
[٤٣] خالد حسن أحمد لطفي ، مرجع سابق ، ص ١٠٢ .

رابعا: الاستعانة بالخبراء

تستعين الشرطة وسلطات التحقيق أو المحاكمة بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي ، وذلك بغرض كشف غموض الجريمة أو تجميع أدلتها والتحفظ عليها ، وبناء عليه فإن الاستعانة بخبير فني في المسائل الفنية البحتة أمر واجب على جهة التحقيق والقاضي ، فهو أوجب في مجال الجرائم السيبرانية ، حيث تتعلق بمسائل فنية آية في التعقيد ومحل الجريمة فيها غير مادي ، والتطور في أساليب ارتكابها سريع ومتلاحق ، و لا يكشف غموضها إلا متخصص وعلى درجة كبيرة من التميز في مجال تخصصه .

خامسا : التحفظ على أدوات الجريمة

يقوم رجل الضبط الجنائي بضبط الكيانات المادية السيبرانية في مسرح الجريمة مثل أجهزة الربط بالشبكات والطابعات وغيرها .

وتقوم النيابة العامة من ضبط الكيانات المعنوية السيبرانية باكتشافها من بعد ضبط الكيان المنطقي للحاسب الآلي مثل البرامج والفيروسات والبيانات والمعلومات المسروقة وكل المواد المعنوية التي تتعلق بالجريمة وتم ارتباطها بالحاسب الالي .

سادسا : تحرير محضر الواقعة

يجب أن تثبت جميع الإجراءات في محاضر موقع عليها منهم ، مبينا بها وقت اتخاذ الإجراءات ومكان حصوله،

وتوقيع الشهود والخبراء وترسل المحاضر للنيابة العامة مع الأوراق المضبوطة .

حالة التلبس في الجريمة السيبرانية :

وتعد حالة التلبس من الحالات التي يباح فيها مأمور الضبط الجنائي أن يتخذ إجراءات لم يكن باستطاعته مباشرتها في الظروف العادية وذلك مراعاة لظروف الاستعجال التي تتطلب كشف الحقيقة وجمع الأدلة .

ويتحقق ذلك في الجريمة السيبرانية في حالة القيام بالإمساك بالجاني عند قيامه بنشر مواد إباحية عبر الانترنت ، أو هو يخترق إحدى أنظمة البنوك لسرقة أموال منها ، وقد يضبط الجاني في حالة تلبس في مكان عام كما لو استخدم حاسب في إحدى مقاهي الانترنت ، أو قد يضبط الجاني في مكان خاص كمنزله .

وكون حالة التلبس حالة استثنائية فقد مُنح لرجل الضبط الجنائي مجموعة من الإجراءات التي يجب عليه اتخاذها إذا توافرت حالة التلبس .[٤٤]

[٤٤] خالد حسن أحمد لطفي ، مرجع سابق ، ص ١٠٨ .

المطلب الثاني

التحقيق في الجريمة السيبرانية

يعتبر التحقيق هو المرحلة الأولى للدعوى الجنائية التي تسبق المحاكمة ، وتقوم به النيابة العامة بعد البلاغ عن القضية وإحالتها لها ، إذا توجد بها دوائر متخصصة في التحقيق في الجرائم السيبرانية ، تسمى بدوائر المال ، تقوم هذه الدوائر باستجواب المتهم والتحقيق معه في الجريمة المنسوبة إليه .

وتتميز بأنها ذات طبيعة قضائية ويمكن مباشرتها بطريقة القهر والإجبار بخلاف إجراءات الاستدلال التي تتميز بطبيعة إدارية ، كما تتميز إجراءات التحقيق أيضا بأن ما ينتج عنها من أدلة يمكن أن يعتمد عليها في إصدار أحكام القضاء الجنائي بعكس إجراءات الاستدلال التي تكون مكملة لأدلة أخرى.

من إجراءات التحقيق :

وتكون بجمع الأدلة من المعاينة وندب الخبراء والتفتيش وضبط الأشياء ومراقبة المحادثات وتسجيلها وسماع الشهود والاستجواب والمواجهة ، ولا يلزم المحقق ترتيب معين عند مباشرة هذه الإجراءات .

أولا : المعاينة .

على المحقق ضبط كل ماله علاقة بالجريمة ، وإثبات حالة الأشخاص والأماكن والأشياء ذات الصلة بالجريمة ، وقد يكون إثبات المعاينة مع الجرائم السيبرانية أمرا صعبا للفترة الزمنية التي قد تطول ما بين وقوعها واكتشافها مما يؤدي بها إلى تلف البيانات أو نقلها أو إخفائها .

وهنا نلاحظ بان المعاينة قد تكون إجراء تحقيق أو استدلال ، و لا تتوقف طبيعتها على صفة من يجريها ، بل على مدى ما يقتضيه إجراؤها من مساس بحقوق الأفراد وحرياتهم ، فإذا جرت المعاينة في مكان عام كانت إجراء استدلال ، وإذا اقتضت دخول مسكن أو مكان له حرمة خاصة كانت إجراء تحقيق .[٤٥]

ثانيا : ندب الخبير

وللمحقق أن يستعين بالخبراء المختصين لاستكمال إجراءات التحقيق ، وهذا بالفعل ماتتطلبه طبيعة الجرائم السيبرانية الذي تقتضي معرفة تامة بنظم الحاسبات و مهارة وتقنية فنية عالية تمكنهم من مباشرة التحقيق في مجال الجرائم السيبرانية .

وقد تعددت النصوص المذكورة في اللائحة التنفيذية لنظام الإجراءات الجزائية السعودي في ندب الخبراء ما يلي:

نصت المادة الخمسون :

[٤٥] د. محمد حميد المزمومي ، مرجع سابق ، ص ١٦٥ .

١- يكون ندب المحقق للخبير لإبداء رأيه في مسألة متعلقة بالتحقيق – وفقا لما ورد في المادة السادسة والسبعين من النظام – مكتوبا ، ويحدد في الندب المهمة المطلوبة والمدة المحددة لإنجازها ، ويخضع الخبير أثناء مباشرته مهمته لرقابة التحقيق .

٢- للمحقق تمكين الخبير من الإطلاع على الأوراق والمستندات المتعلقة بطلب الخبرة .

٣- يلتزم الخبير المنتدب بالمهمة المكلف بها .

المادة الحادية والخمسون :

١- يقدم الخبير عند إنجاز مهمته المطلوبة منه – وفقا لما ورد في المادة السابعة والسبعين من النظام – تقريرا مؤرخا وموقعا منه يتضمن ملخصا للمهمة وإجراءات الكشف والفحص والتحاليل الفنية التي باشرها ومشاهدته والنتائج التي خلص إليها بشكل دقيق ومسبب .

٢- عند تعداد الخبراء واختلافهم في الرأي فعليهم أن يقدموا تقريرا واحدا يتضمن رأي كل واحد منهم وأسانيده .

٣- تضم تقارير الخبرة وجميع مرفقاتها إلى ملف الدعوى .[٤٦]

ثالثا : التفتيش

وهو إجراء من إجراءات التحقيق التي تؤدي إلى ضبط أدلة الجريمة بعد اكتشافها ، وللتفتيش شروط موضوعية تتعلق بسببه وقوع الجريمة بالفعل وأن يوجه اتهام إلى الشخص المراد تفتيشه والغاية منه من ضبط أشياء تفيد في كشف الحقيقة،

[٤٦] د. محمد حميد المزمومي ، مرجع سابق ، ص ١٦٨ .

وهناك شروط شكلية وهو أن يكون المر بالتفتيش مسببا وحضور المتهم أو ينيبه أو الغير أو من ينيبه التفتيش، وأن يتم تحرير محضر بالتفتيش ، ومحل التفتيش في الجرائم السيبرانية هو المكونات المادية للحاسب الآلي وكذلك البرامج أو الكيانات المنطقية وهي المكونات الغير مادية وتشمل على :

- البيانات المسجلة في ذاكرة الحاسب أو في مخرجاته .
- السجلات المثبتة لاستخدام نظام المعالجة الآلية للبيانات .
- دفتر يومية التشغيل وسجل المعاملات .
- السجلات الخاصة بعمليات الدخول إلى نظام المعالجة الآلية للبيانات ومايتعلق بعا من سجلات كلمات السر ، ومفاتيح الدخول ، ومفاتيح فك الشفرة .[٤٧]

رابعا : ضبط الرسائل ومراقبة المحادثات .

جاء في نص نظام الأساسي للحكم في المملكة العربية السعودية بأن المراسلات البرقية والبريدية والمخابرات الهاتفية وغيرها من وسائل الاتصال مصونة ولايجوز مصادرتها أو تأخيرها أو الاطلاع عليها أو الاستماع إليها إلا في الحالات التي يبينها النظام .

ومن الأهمية القصوى ضرورة وضع الضوابط القانونية التي تنظم الإجراءات المتبعة من قبل سلطة التحقيق أثناء ممارسة أعمالهم في سبيل الكشف الوصول إلى الأدلة الثبوتية في جريمة ارتكبت،

[٤٧] خالد حسن أحمد لطفي ، مرجع سابق ، ص ١١٣ .

وفي هذا الشأن فقد نصت المادة السادسة والخمسون من النظام بانه للرسائل البريدية والرقمية والمحادثات وغيرها من وسائل الاتصال حرمة فلايجوز الاطلاع عليها أو مراقبتها إلا بأمر مسبب ولمدة محدودة وفقا لما ينص عليه هذا النظام ، وتقضي المادة السابعة والخمسون بأنه لرئيس هيئة التحقيق والادعاء العام أن يأمر بضبط الرسائل والخطابات والموضوعات والطرود ، وله أن يأذن بمراقبة المحادثات الهاتفية وتسجليها متى كان لذلك فائدة من ظهور الحقيقة من جريمة وقعت على أن يكون الأمر أو الإذن مسببا أو محددا بمدة لاتزيد عن عشرة أيام قابلة للتجديد وفقا للتحقيق ، وفي ذات الشأن تقضي المادة الثامنة والخمسون بأنه للمحقق وحده الاطلاع على الخطابات والرسائل والأوراق والأشياء الأخرى المضبوطة وله أن يستمع إلى التسجيلات وله بحسب مقتضيات التحقيق أن يأمر بضبطها أو نسخ منها إلى ملف القضية ، أو أن يأمر بردها إلى من كان حائز لها أو مرسله اليه ، وعلى المحقق أن يحافظ على سرية المعلومات من خلال التفتيش وألا ينتفع بها بأي طريقة كانت أو يفضي بها إلى غيره إلا في الأحوال التي يقضي النظام بها ، فإذا أفضي بها دون مسوغ نظامي أو انتفع بها بأي طريقة كانت تعينت مساءلته .[٤٨]

خامسا : الشهادة

والشهادة هي إجراء من إجراءات التحقيق ، كما أنها إجراء من إجراءات المحاكمة ، فيجل أن تؤدى أمام سلطة التحقيق أو أمام المحكمة ، إما أن تسمع أقواله أمام الخبير فلا تعد شهادة بالمعنى النظامي الذي أراده المنظم ، بل جزء من عمل الخبير،

[٤٨] د. محمد حميد المزمومي ، مرجع سابق ، ص ١٨٢ .

ولكنه يستطيع القاضي أن يتخذ قرينة إلى جانب قرائن أخرى في الدعوى ، وهناك ما يسمى بالشهادة السماعية : كمن يشهد بأنه سمع من آخر أنه شاهد ارتكاب المتهم للجريمة ، وهذه تكون قوتها في الإثبات أقل ، وهناك الشاهد بالتسامع وهي كأن تكون ترديد لشائعة متناولة بين الناس قد تكون محل صدق أو قد لا تكون ، فهذه شهادة لا ترد على الواقعة .[٤٩]وقد جاء نظام الإجراءات الجزائية واللائحة التنفيذية منظما للشهادة أمام سلطة التحقيق وذلك حيث نصت المادة السادسة والستون : على المحقق أن يثبت في المحضر البيانات الكاملة عن كل شاهد ، وتدون تلك البيانات وشهادة الشهود وإجراءات سماعها في المحضر من غير تعديل أو شطب أو كشط أو إضافة ، ولا يعتمد شي من ذلك إلا إذا صدق عليه المحقق والكاتب والشاهد .

سادسا : الاستجواب

وهو إحدى الإجراءات المهمة من إجراءات التحقيق بهدف الوقوف على حقيقة التهمة من المتهم ، والوصول إما إلى اعتراف منه يؤيدها ، أو إلى دفاع منه ينفيها .

وهناك نوعان من الاستجواب :

- الاستجواب الحقيقي : وهو توجيه التهمة إلى المتهم ومناقشته تفصيليا عنها ومواجهة بالأدلة القائمة ضده .
- الاستجواب الحكمي : هو مواجهة المتهم بغيره من الشهود أو المتهمين في حكم الاستجواب ، فهذه المواجهة تنطوي على إحراجه ومواجهته بما هو قائم ضده .

[٤٩] د. محمد حميد المزمومي ، مرجع سابق ، ص ١٨٤ .

ضمانات الاستجواب :

- لا يجوز أن يجري الاستجواب غير السلطة المختصة بالتحقيق .
- دعوة محامي المتهم إلى الحضور أثناء استجوابه .
- يتعين إحاطة المتهم علما بالتهمة المنسوبة إليه .
- يتعين كفالة حرية كاملة للمتهم أثناء استجوابه .
- لا يجوز استجواب المتهم خراج مقر جهة التحقيق إلا لضرورة يقدمها المحقق .

هذه جميعها هي إجراءات التحقيق التي تكون من اختصاص هيئة التحقيق والادعاء العام (النيابة العامة) وبعد أن ينتهي المحقق من التحقيق في القضية المعروضة عليه ، فإنه إما أن يأمر بتقديم المتهم إلى المحاكمة الجنائية ، وإما أن يصدر فيها أمرا بألا وجه لإقامة الدعوى الجنائية ، والمقصود بها قرار المحقق بعدم إحالة الدعوى إلى المحكمة المختصة .

المطلب الثالث

المحاكمة في الجريمة السيبرانية

المحاكمة :

وهي تمثل المرحلة الأخيرة من مراحل الدعوى الجزائية ، وتعرف بأنها مجموعة من الإجراءات التي تتم أمام قضاة المحاكم تستهدف تمحيص أدلة الدعوى جميعها ما كان منها ضد مصلحة المتهم وما كان في مصلحته،

وبذلك تهدف إلى تقصي الحقيقة الواقعية والقانونية في شأنها ثم الفصل في موضوعها ، كما تكمن أهميتها في الحماية الفردية للإنسان ، وتحقيق الاستقرار والعدالة بين أفراد المجتمع ، وتحقيق الردع العام والخاص في المجتمع ، ومراقبة الإجراءات السابقة على المحاكمة ، وتطبيق النظام بين أفراد المجتمع .[٥٠]

المحكمة الجزائية :

تتنوع المحاكم لدينا في المملكة العربية السعودية ، فأول المحاكم هي المحكمة العليا ، ويليها محاكم الدرجة الثانية (الاستئناف) ، ثم يليها محاكم الدرجة الأولى والمكونة من (المحكمة العامة ، والمحكمة التجارية ، والمحكمة العمالية ، ومحكمة الأحوال الشخصية ، والمحكمة الجزائية) .

وما يهمنا هو المحكمة الجزائية إذا تعتبر هي المحكمة المختصة في الجرائم الجنائية والسيبرانية ، وتتألف من ثلاث دوائر متخصصة :

- دوائر قضايا القصاص والحدود .
- دوائر القضايا التعزيرية .
- دوائر قضايا الأحداث .

كما أنها تختص بالفصل في جميع القضايا الجزائية .

[٥٠] د. محمد حميد المزمومي ، مرجع سابق ، ص ٢٣٣ .

فالمحاكمة في الجريمة السيبرانية بعد أن يتم الإبلاغ عن الجريمة وإحالتها للنيابة العامة للتحقيق ، تحال الدعوى بعد استكمال مرحلة التحقيق بدعوى عامة تقوم النيابة العامة بالترافع فيها أمام المحكمة الجزائية مطالبة بتطبيق المواد الواردة في نظم مكافحة الجرائم السيبرانية .

الإثبات الجنائي في محاكمة الجريمة السيبرانية :

وهي تلك الأدلة الجنائية الرقمية التي تضاف إلى وسائل الإثبات ، لإثباتها في المحاكمة الجنائية السيبرانية ، فالدليل الرقمي هو " الدليل المأخوذ من أي جهاز يعتمد في تشغيله على التقنية الرقمية ، وهو يكون في شكل مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتخليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية "[٥١].

كما يجب أن تكون العلاقة واضحة في القانون بين الدليل الرقمي وطبيعة الواقعة سواء كانت واقعة افتراضية بانها تبدأ وتنتهي في إطار العلم الافتراضي فهي تشكل البناء الحقيقي للجريمة الافتراضية ، أو واقعة مادية كأن تتم واقعة مادية (جريمة) ويتم الاستعانة بالحوسبة الرقمية من أجل الكشف عنها ، وكذلك الواقعة المزدوجة وهي التي يكشف عنها الدليل الرقمي في مدى قدرة الاستعانة بالحواسيب للارتكاب جرائم مادية ممزوجة بطابع رقمي ، وهنا سوف يكون الدليل شراكة بين المادية والرقمية .

[٥١] خالد حسن أحمد لطفي ، مرجع سابق ، ص ١٢٨ .

وقد قضت المحاكم بإمكانية اعتماد الأدلة الجنائية الرقمية وهي تلك الأدلة الغير ملموسة وذلك للأسباب التالية:

١- الثقة التي اكتسبها الحاسوب والكفاءة التي حققتها النظم الحديثة للمعلوماتية في مختلف مجالات الحياة .

٢- ارتباط الأدلة الجنائية الرقمية وآثارها بالجريمة موضوع المحاكمة .

٣- وضوح الأدلة الرقمية ودقتها في إثبات العلاقة بين الجاني والمجني عليه أو بين الجاني والسلوك الإجرامي .

٤- إمكانية تعقب آثار الأدلة الرقمية والوصول إلى مصادرها بدقة .

٥- قيام الأدلة الرقمية على نظريات حسابية مؤكدة لا يتطرق إليها الشك ممن قوى يقينية الأدلة الرقمية .

٦- انتهاء العلم برأي قاطع إلى صحة النتائج التي توصل إليها علوم الحاسب .

٧- الأدلة الجنائية الرقمية يدعمها عادة رأي الخبير ، وللخبرة في المواد الجنائية دورها في الكشف عن الأدلة وفحصها وتقييمها وعرضها أمام المحاكم .[٥٢]

كما تتميز الأدلة الجنائية الرقمية بعدة مميزات لتكون حجة قوية في الإثبات أمام القضاء :

١- يمكن استخراج نسخ منها مماثلة ومطابقة للأصل ولها ذات الحجية .

٢- يمكن بالأساليب العلمية الملائمة تحديد وتأكيد ماإذا كانت الأدلة الرقمية قد تعرضت لتعديل أو تحريف .

[٥٢] د. محمد الأمين البشري ، الأدلة الجنائية الرقمية ، المجلة العربية للدراسات الأمنية والتدريب ، مجلد ١٧ ، العدد ٣٣ ، ص ١٢٨ .

٣- من الصعب إتلاف الأدلة الجنائية الرقمية ، وفي حالة محوها أو إتلافها يمكن استرجاعها من ذاكرة الحاسوب .

٤- إذا حاول المتهمون إتلاف الأدلة الرقمية يمكن الاحتفاظ بنسخ منها في أماكن عامة ، علما بان للنسخ قيمة الأصل .[٥٣]

وكما رأينا فإن الأدلة الجنائية الرقمية من أكثر أنواع الأدلة المادية وفرة وثباتا ، وهي مخزنة في الأجهزة الرقمية المختلفة أو المنقولة عبر شبكات الاتصال ، وتشكل ثورة للعدالة الجنائية متى أحسن استغلالها .

الخاتمة

الحمد الله الذي بنعمته التي تتم الصالحات ، والصلاة والسلام على رسوله وبعد ،،

فإن هذه الخاتمة تتضمن أهم النتائج والتوصيات :

النتائج :

١- مصطلح الجرائم السيبرانية هو أحدث مصطلحات جرائم الإنترنت والحاسب وهو المستخدم حاليا في العالم العربي .

٢- العصر الحديث للجرائم هو التحول من الواقع المادي إلى الواقع الافتراضي والرقمي .

٣- الجرائم السيبرانية هي جرائم عابرة للحدود .

[٥٣] د. محمد الأمين البشري ، مرجع سابق ، ص ٩٩ .

٤- الجرائم السيبرانية هي جرائم تتطور بسرعة هائلة من خلال استحداث برمجيات وفايروسات خبيثة .

٥- الجرائم السيبرانية هي انتهاك وتعدي قد يكون على الفرد وقد يكون على المجتمع وقد يكون على الأمن وكذلك الاقتصاد .

٦- نظام مكافحة الجرائم السيبرانية السعودي لم يعاقب مرتكبي الجرائم السيبرانية وحسب بل وضع عقوبة من يحرض غيره أو يساعده أو يتفق معه في ارتكاب هذه الجريمة وفقا للمادة التاسعة من النظام .

٧- تختص النيابة العامة بالتحقيق في الجرائم السيبرانية وذلك بتخصيص دوائر مختصة بالتحقيق في الجرائم السيبرانية والتي تسمى بدوائر المال .

٨- إثبات الدليل الجنائي الرقمي في المحاكمة.

التوصيات:

توصي الباحثة بإنشاء هيئة وطنية مختصة بالجرائم السيرانية تشمل على :

- مركز استقبال جميع البلاغات المتعلقة بالجرائم السيبرانية .
- كوادر من الفنيين والتقنيين يمتلكون الخبرة والمهارة العالية في المجال السيبراني .
- خبراء معنيين في مجال الاستدلال والتحقيق السيبراني .
- اعتماد المحاضر والضبوط والموثقة من الهيئة الناتجة من التحقيق كأوراق رسمية تقدم لدى المحكمة المختصة .
- اعتماد نظام ولائحة تنفيذية للهيئة .

- انضمام الهيئة كقطاع رسمي تحت وزارة العدل .
- لجنة رقابية على الهيئة .
- لجنة الجودة والتطوير.

المراجع والمصادر

أولا : الكتب .

١- د. أحمد مختار عبد الحميد عمر ، معجم اللغة العربية المعاصرة ، عالم الكتب ، الطبعة الأولى ، ٢٠٠٨ م .

٢- أسامة مهمل ، الإجرام السيبراني ، رسالة ماجستير ، كلية الحقوق والعلوم السياسية ، جامعة محمد بوضياف ، ٢٠١٨/٢٠١٧ .

٣- تميم عبد الله سيف التميمي ، الجرائم المعلوماتية في الاعتداء على الأشخاص ، مكتبة القانون والاقتصاد ، الرياض ، الطبعة الأولى ٢٠١٦ .

٤- خالد حسن أحمد لطفي ، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية ، دار الفكر الجامعي ، الإسكندرية ، الطبعة الأولى ،٢٠٢٠ م .

٥- سامي علي حامد عياد ، الجريمة المعلوماتية وإجرام الانترنت ، دار الفكر الجامعي ، الإسكندرية ، بدون طبعة ، ٢٠٠٧ م .

٦- عبد العزيز بن غرم الله آل جار الله ، جرائم الإنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية السعودي دراسة مقارنة (ويليه آثار العولمة على مستخدمي الإنترنت) ، دار الكتاب الجامعي ، الرياض ، الطبعة الأولى ، ٢٠١٧ م

٧- علي نعمة جواد الزرفي ، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة ، المكتب الجامعي الحديث ، بدون طبعة ،٢٠١٩م .

٨- غانم مرضي الشمري ، الجرائم المعلوماتية ، الدار العلمية الدولية ، عمان ، الطبعة الأولى ، ٢٠١٦ م

٩- فوزية عبد الستار ، شرح قانون العقوبات ، دار النهضة ، القاهرة ، ١٩٨٢م .

١٠- د. محمد الأمين البشري ، الأدلة الجنائية الرقمية ، المجلة العربية للدراسات الأمنية والتدريب ، مجلد ١٧ ، العدد ٣٣ .

١١- د. محمد حميد المزمومي ، الوسيط في شرح نظام الإجراءات الجزائية السعودي ، مركز النشر العلمي بجامعة الملك عبد العزيز ، جدة ، الطبعة الثانية ، ٢٠١٩ .

١٢- محمود أحمد القرعان ، الجرائم الإلكترونية ، دار وائل للنشر والتوزيع ، عمان ، الطبعة الأولى ، ٢٠١٧ .

١٣- د. محمود عمر محمود ، الجرائم المعلوماتية والإلكترونية ، خوارزم العلمية ، الطبعة الأولى ، ٢٠١٥ م .

ثانيا المواقع الإلكترونية:

أ) أنظمة المملكة العربية السعودية من موقع هيئة الخبراء بمجلس الوزارء

: https://www.boe.gov.sa/ar/Pages/default.aspx

١ نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية ، مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨ ، ساري .

٢ نظام الإجراءات الجزائية في المملكة العربية السعودية ، مرسوم ملكي رقم (م/٢) بتاريخ ٢٢ / ١ / ١٤٣٥ ، ساري ،

ب) الهيئة الوطنية للأمن السيبراني – https://nca.gov.sa/pages/about.html .

د) صالح علي عبد الرحمن الربيعة ، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت ، هيئة الاتصالات وتقنية المعلومات ، ص ٩ .

http://myhistar1.blogspot.com/2019/01/pdf.html

ج) د. وليد أحمد الروضان ، مالفرق بين أمن المعلومات والأمن السيبراني ، صحيفة الجزيرة الالكترونية ، مؤسسة الجزيرة للصحافة والطباعة والنشر ، ١٤٣٩ هـ ، العدد ١٦٦٣١ .

https://www.al-jazirah.com/2018/20180411/rj3.htm