International Academic Journal for Law Studies

المجلة الأكاديمية العالمية للدراسات القانونية

Website: http://iajour.com/index.php/lr

ISSN: 2708-7840

جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها من حيث: أشكالها، خصائصها، أركانها والدافع من ارتكابها

أ. زياد بن محمد عادي العتيبي

مستشار قانوني،وزارة الدفاع، ماجستير في القانون،جدة

Zs.m.sa@hotmail.com

تاريخ استلام البحث: 2020/12/7 **تاريخ نشر البحث: 2021/1/12**

الملخص:

تناولت هذه الورقة مفهوم جرائم السيبرانية وبيان أشكالها،خصائصها،أركانها والدافع من ارتكابها، حيث أدى تطور تقنية المعلومات في القرن العشرين إلى ظهور أشكال جديدة ومستحدثة من الجرائم التي لم تعتاد عليها البشرية وأصبح الفضاء السيبراني مسرحاً لها، حيث يستطيع المجرم من خلال هذا الفضاء تمرير هجماته بشكل سريع وخفي ولا يترك في الغالب أثر لجريمته حتى أصبح من المصعب على المحققين والمختصين اكتشاف أو إثبات الجريمة؛ لأنها ارتكبت في فضاء سيبراني غير ملموس ولا حدود له ، وبالتالي يُصعب إدانة المتهم الأمر الذي أدى إلى ظهور تساؤل عن ماهية الجرائم السيبرانية، أشكالها ،خصائصها، أركانها، ودوافعها وحيث أن التحول الرقمي أحد الركائز الأساسية لتحقيق رؤية المملكة 2030 لتنمية البنية التحتية الرقمية ، ونظراً لأهميتها فقد ناقش البحث مفهوم الجرائم السيبرانية من حيث أشكالها ،خصائصها، أركانها، ودوافعها ، وقد توصلت الدراسة إلى العديد من النتائج والتوصيات أبرزها بأن المجرم السيبراني يستغل الأزمات وأن من أبرز أساليب التصيد الإلكتروني خلال هذه الفترة من الدراسة وما تشهده البلاد في مواجهة جائحة كورونا هي التصيد بإسم كورونا(COVID-19)،وكذلك ضرورة تدخل المشرع في اصدار نظام خاص ومستقل بالإجراءات الجزائية الرقمية بما يواكب التحول الرقمي الذي تشهده المملكة.

الكلمات المفتاحية: الجرائم المعلوماتية، الجرائم السيبرانية، دوافع، أشكال، خصائص.

1. المقدمة

في أواخر القرن المنصرم انطلقت الثورة المعلوماتية وانتشرت بين الدول والأفراد حتى طغت على حياة الناس وسهلت الاتصال الصوتي والمرئي على كافة الأصعدة، وأصبحت التقنية الرقمية تستخدم في كافة المجالات العلمية والتي لا يمكن الاستغناء عنها لفائدتها الاقتصادية والاجتماعية. وكانت النتيجة الرئيسة لهذه الثورة ولادة ما يسمى بالمجتمع المعلوماتي [1].

ومع ظهور هذه الثورة، ظهر الجانب السلبي، والمتمثل في ما يسمى بالجريمة السيبرانية من خلال استغلال المجرم للتقنية في تنفيذ أعمال جرمية سواءً كانت هذه الأعمال تستهدف أفراد أو منظمات أو حتى دول. ونتيجة لتطور تقنية المعلومات

1. رايز سالم الحقباني،مهارات البحث والتحقيق في الجرائم المعلوماتية،ط1(الرياض:كلية الملك فهد الأمنية، مركز الدراسات والبحوث،2014)،9-10.

انتشرت أشكال الجرائم السيبرانية حول العالم مع تطور التكنولوجيا وأصبح المجرم السيبراني بإمكانه السطو افتراضياً على البنوك، وكذلك استغلال التقنية في تنفيذه هجماته على أفراد أو حكومات إما لهدف مادي بقصد الحصول على مكاسب مالية كالاحتيال الرقمي أو سياسي أو انتقامي بهدف التخريب والعبث.

ونتيجة لظهور الجرائم السيبرانية ظهرت العديد من المصطلحات و المفاهيم المستحدثة كالجريمة المعلوماتية أو الجريمة السيبرانية والدليل الرقمي والفضاء السيبراني والتي لم تكن معروفة من قبل .وحيث أن التحول الرقمي هي أحد البرامج الأساسية لتحقيق رؤية المملكة العربية السعودية 2030، والذي يهدف إلى بناء مجتمع ووطن رقمي مبني على إنشاء منصات رقمية لإثراء التفاعل والمشاركة المجتمعية الفعالة بما يساهم في تحسين تجربة المواطن والمقيم والسائح والمستثمر ،أصبحت المملكة أمام تحدي تجاه الجرائم السيبرانية التي تستهدف أفرادها وكيانها والتي ظهرت بشكل أكبر مع التحول الرقمي الذي تشهده المملكة.

وانطلاقاً من حرص واهتمام خادم الحرمين الشريفين الملك سلمان بن عبد العزيز وسمو ولي العهد حفظهم الله في قيادة البلد لتكون نموذجًا في العالم على كافة الأصعدة، ولرؤية المملكة 2030 التي جعلت التحول الرقمي وتنمية بنيتها التحتية ضمن أهم أهدافها، واستشعاراً لأهمية البيانات ونظم المعلومات والبنى التحتية الحساسة ونظراً لارتباطها بالمصالح الوطنية، وأهمية حمايتها من أي تهديدات أو مخاطر يشهدها الفضاء السيبراني يأتي تأسيس الهيئة الوطنية للأمن السيبراني وارتباطها بالملك -حفظه الله- وذلك وفق الأمر الملكي الكريم رقم(6801) بتاريخ (1439/02/11هـ) بالموافقة على تنظيمها لتكون هذه الهيئة هي الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه[1] ؛حمايةً للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية.

تقدم هذه الورقة استعراض عن جرائم السيبرانية المرتكبة عبر الوسائط الرقمية من حيث بيان مفهومها ،أشكالها ،خصائصها، وكذلك استعراض أركان الجريمة السيبرانية ودوافع هذه الجريمة والفرق بينها وبين الجرائم الأخرى.

2. مفهوم الجرائم السيبرانية

بدأت الجريمة منذ بداية وجود الإنسان على سطح الأرض، فهي قديمة وتطورت أشكالها وأساليب ارتكابها واختلفت دوافعها والأدوات المستخدمة في ارتكابها مع مرور الزمن. ولا تزال الجريمة بشكل عام إحدى أكبر مشكلات المجتمع والملازمة له عبر العصور؛ولذلك فإن أهمية هذه المشكلة تكمن في زيادة انتشارها وتعدد صورها و أشكالها و دوافعها وتعدي أثرها على المجتمع.

وقد شهد العالم الحديث في عصرنا تقدماً هائلاً وسريعاً في مجال التكنولوجيا وظهرت وسائل اتصال متطورة حولت المجتمع إلى مجتمع رقمي وتلاشت معه الحدود الجغرافية بين الدول وكان من أهم وسائل الاتصال ظهوراً هي شبكة الإنترنت.

ومع ثورة المعلومات وزيادة الإقبال على استخدام شبكة الانترنت حول العالم وبدء الاعتماد عليها في جميع مناحي الحياة ودخول كافة فئات المجتمع إلى قائمة مستخدميها بدأ تظهر جرائم مستحدثة على هذه الشبكة وهي تزداد وتتنوع بزيادة تطور وتقدم التكنولوجيا، هذه الجرائم لها خصائص وأساليب جديدة لارتكابها وهي تختلف اختلافاً كبيراً عن الجرائم التقليدية، كما أن مرتكبيها لهم خصائص أو سمات تختلف عن خصائص مرتكبي الجرائم التقليدية.

ولهذه الأهمية من انتشار الجرائم السيبرانية أو المعلوماتية، يستعرض هذا الجزء تعريف الجريمة السيبرانية، أشكالها وخصائصها.

2.1 تعريف الجريمة السيبرانية

[1]. الموقع الإلكتروني للهيئة الوطنية للأمن السيبراني (2020م)، تاريخ الدخول(2020/03/20/)، متاح على https://nca.gov.sa/pages/about.html

تعتبر الجرائم السيبرانية من الجرائم المستحدثة، فلم يستقر الفقهاء على وضع تعريف محدد للجرائم الناشئة في بيئة الحاسب الآلي أو بيئة الشبكات ،وذلك بسبب نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات، فمنهم من يطلق عليها جرائم الإنترنت ، ومنهم من يطلق عليها الجريمة المرتبطة بالكمبيوتر ، أو جرائم التقنية العالية ،أو الجرائم المعلوماتية ،أو جرائم الشبكة العنكبوتية ،ومنهم من يطلق عليها أيضاً بجرائم الغش المعلوماتي حتى أصبح أخيراً يطلق عليها جرائم (السايبر كرايم) أو جرائم أصحاب الياقات البيضاء ، الأمر الذي يصعب عليه وضع تعريف ثابت ومحدد لهذه الجرائم نظراً لحداثتها[1].و للإجابة عن سؤال "ما هي الجرائم المعلوماتية؟" فلابد من توضيح أنّ المقصود في الغالب بالجرائم المعلوماتية أو السيبرانية هي الجرائم التي تتم باستخدام حاسب آلي متصل بالإنترنت؛لأنه يتم استخدام الحاسب الآلي كأداة لتحقيق الكثير من الغايات غير القانونية مثل ارتكاب عمليات الاحتيال أو سرقة الملكية الفكرية أو انتهاك الخصوصية أو لتدمير المواقع الإلكترونية الخاصة بالمنشآت الحكومية وجرائم الانترنت هي امتداد لما عُرف بجرائم الحاسوب[2].

قبل البدء في تعريف الجرائم المعلوماتية أو السيبرانية، فإنه من المهم البدء بتعريف الجريمة لغةً واصطلاحاً وكذلك تعريفها من الناحية الشرعية والقانونية.

أولاً: الجريمة في اللغة:

مشتقة من الجرم: وهي الذَّنْبُ[3]. وقد جاء ذكر الجريمة في قولُه تَعَالَى: (حَتَّى يَلِجَ الْجَمَلُ فِي سَمِّ الْخِياطِ وَكَذلِكَ نَجْزِي الْمُجْرِمِينَ)[4].

ثانياً: الجريمة اصطلاحاً:

أ. تعريف الجريمة في الشريعة الإسلامية:

ب. الجرائم في الشريعة الإسلامية هي "محظورات شرعية زجر الله عنها بحدٍ أو تعزير"(5).

ج. تعريف الجريمة في القانون:

عرفها فقهاء القانون بتعريفات عديدة ويرى الباحث بأن أشمل تعريف يتفق مع تعريفها الشرعي هو "كل فعل إيجابي نص القانون على منعه، أو امتناع سلبي عن أداء فعل أمر القانون به واعتبره جريمة وخصص له عقوبة معينه ذات ألم معين يوقع على الشخص المسؤول عنها جنائياً"[6].

ثالثاً: تعريف الجريمة السيبرانية والفرق بينها وبين جرائم المعلوماتية أو الرقمية:

تعددت التعاريف الخاصة بالجرائم المعلوماتية أو السيبرانية حيث لا يوجد مصطلح موحد للدلالة عليها، وفي رأي الباحث خشية حصرها في مجال ضيق مما لا يؤدي إلى توسع مفهوم هذه الجرائم، يُعرف بعض الفقهاء هذه الجرائم في أن تكون البرامج المعلوماتية محلاً للجريمة ويُعرفها البعض من خلال كونها وسيلة أداة لارتكابها وما يهمنا في هذا البحث هو تعريف هذه الجرائم التي تُعبر عن الطابع التقني مما يعطي مفهوم أوسع. قبل تعريف الجريمة السيبرانية لابد من التطرق إلى مصدر كلمة سايبر(Cyber)،حيث تشير المراجع العلمية إلى أن عالم الرياضيات نوربرت وينر، هو أول من استخدم مصطلح السيبرانية في عام 1948م في أثناء دراسته لموضوع القيادة والسيطرة في حقل الهندسة الميكانيكية، أما مصدرها في المعاجم الأجنبية فهي يونانية الأصل وترجع إلى مصطلح(Kybernetes) والذي ورد في مؤلفات الخيال العلمي وتعني القيادة أو التحكم عن بعد، وبالرجوع إلى معاجم اللغة فلم تشر في الغالب إلى مصدر كلمة سايبر(Cyber) سوى في قاموس (المورد) والذي

---

1. عبد العزيز غرم الله آل جارالله، جرائم الإنترنت وعقوباتها وفق نظام مكافحة جرائم المعلوماتية السعودي: ويليه آثار العولمة على مستخدمي الإنترنت، ط1(الرياض: دار الكتاب الجامعي للنشر والتوزيع،2017م)،72.
2. عبدالعزيز غرم الله آل جارالله،المرجع السابق،76.
3. محمد ابن منظور،لسان العرب،ط3(بيروت: دار صادر،2003)مادة(ج ر م)جزء 3 ،129.
4. سورة الأعراف، الآية:40.
5. أبو الحسن الماوردي،الأحكام السلطانية،ط1(الكويت: دار ابن قتيبة،1989)،285.
6. طلال أبو عفيفه،أصول علمي الإجرام والعقاب وآخر الجهود الدولية والعربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية،ط1(القدس: دار الجندي للنشر والتوزيع،2013)،43.

عرفها بالقول:السيبرانية هي علم الضبط ومصدرها (Cybernetics) وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية، أي ضبط الأشياء عن بعد والسيطرة عليها[1].

يُعرف بعض الفقهاء مصطلح السيبرانية بأنها "هجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على مواقع الكترونية أو بنى تحتية محمية الكترونياً لتعطيلها أو تدميرها أو الإضرار بها"ويعرفه آخرون بأنها "هجوم عبر الإنترنت يقوم على التسلل إلى مواقع إلكترونية غير مرخص بالدخول إليها بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها"[2] كما تم تعريف مصطلح السبرانية في ورشة عمل بعنوان "الأمن الرقمي وحماية المستخدم من مخاطر الانترنت والذي نفذته هيئة الاتصالات وتقنية المعلومات المنعقد بتاريخ(2018/04/26م)" بأنها "مأخوذة من كلمة (سيبر) Cyber، وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي. فالسيبرانية تعني: (فضاء الانترنت)"[3].

ويُعرف أيضاً بأنه " المجال الجديد الخامس للحروب الحديثة بعد البر والبحر والجو والفضاء الحقيقي وهو يمثل جميع شبكات الحاسب الالي الموجودة حول العالم ويشمل ذلك الاجهزة الالكترونية المرتبطة من خلال شبكة الالياف البصرية والشبكات اللاسلكية الفضاء السيبراني ليس الإنترنت فقط وانما شبكات اخرى كثيرة متصلة مثل: / gps Acars / Swift / Gsm / pstn"[4]. أما تعريف مصطلح الجريمة السيبرانية "هو السلوك غير المشروع أو المنافي للأخلاق أو غير المسموح به المرتبط بالشبكات المعلوماتية العالمية"[5]

ويُعرف مايكل آرون دينس الجريمة السيبرانية بأنها" هي جرائم سيبرانية، والتي تسمى أيضًا جرائم الكمبيوتر، ويتم استخدام الحاسب الآلي والانترنت فيها كأداة لتحقيق أهداف غير قانونية، مثل ارتكاب الاحتيال، والاتجار في المواد الإباحية للأطفال والملكية الفكرية، وسرقة الهويات، أو انتهاك الخصوصية"[6].

2.2 تعريف الجريمة المعلوماتية:

عرف البعض جرائم المعلوماتية بأنها" كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"[7]،كما عرفتها منظمة التعاون الاقتصادي والتنمية بأنها "كل فعل أو امتناع عن فعل من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غيره مباشرة عن تدخل التقنية المعلوماتية"[8] أما تعريف الجريمة المعلوماتية في نظام مكافحة الجرائم المعلوماتية السعودي عرفها المنظم بأنها: "أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة العنكبوتية بالمخالفة لأحكام هذا النظام"[9]

يلاحظ مما سبق عدم وجود تعريف متفق عليه لهذه الجريمة سواء فيمن عرفوها كجرائم سيبرانية أو معلوماتية ولكن جميع هذه التعاريف تتفق بأن هذه الجرائم ترتكب بواسطة استخدام أجهزة الحاسب الآلي كأداة لتحقيق نتيجة غير مشروعة،وفقاً للتعاريف أعلاه، يُعرف الباحث الجرائم السيبرانية بأنها: كل فعل مادي يمثل اعتداء صريح على حق محمي بموجب النظام من قبل شخص لديه المعرفة باستخدام التقنية وذلك عن طريق دخول غير مصرح به إلى قاعدة بيانات رقمية متصلة بالفضاء السيبراني بهدف تحقيق مصلحة معينة غير مشروعه.

كما يتضح عدم وجود اصطلاح قانوني موحد يطلق على هذه الجرائم فمنهم من يطلق عليها جرائم الحاسب الآلي والانترنت ومنهم من يطلق عليها الجرائم الإلكترونية أو الرقمية، وسبب اختيارنا لمصطلح السيبرانية أو المعلوماتية في هذه الدراسة، فيعود ذلك للأسباب الآتية:

---

1. عبيس نعمة الفتلاوي،الهجمات السيبرانية:دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر،ط1(بيروت: منشورات زين الحقوقية،2018م)،11.
2. عبيس نعمة الفتلاوي،المرجع السابق،12.
3. ورشة عمل بتعليم جدة، (2018م) "الأمن الرقمي وحماية المستخدم من مخاطر الانترنت " تاريخ الدخول (2020/03/29م)، متاح على: https://www.spa.gov.sa/1757119
4. ورشة عمل بتعليم جدة، المرجع السابق.
5. ورشة عمل بتعليم جدة، المرجع السابق.
6. Michael Aaron Dennis,Cybercrime:Web article Selected by Britannica Academic, Encyclopedia Britannica,(2018):1. Available on: https://cutt.us/M4cZd
7. أيمن عبدالله فكري،الجرائم المعلوماتية:دراسة مقارنة في التشريعات العربية والأجنبية،ط1(الرياض،مكتبة القانون والإقتصاد،2014م)،97
8. خالد دوادي، الجريمة المعلوماتية، ط1(عمان: دار الأعصار العلمي للنشر والتوزيع،2018)،25.
9. المادة (8/1) من نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م / 17) وتاريخ (08 / 03 / 1428هـ).

1. أن موضوع هذا البحث يتناول حجية الأدلة الرقمية في إثبات الجرائم المعلوماتية بما يتفق مع نظام مكافحة جرائم المعلوماتية وتوجه الدولة في إنشاء الهيئة الوطنية للأمن السيبراني، إذن فإن المملكة قد اعتمدت المصطلحين (المعلوماتية والسيبرانية) لوصف الجرائم التي تقع على شبكات الإنترنت وملحقاتها.
2. يرى الباحث بأنه لا يمكن تسمية هذه الجرائم (بجرائم الحاسب الآلي) لأن هذه التسمية تجعلها قاصرة على الجرائم التي تقع على أجهزة الحاسب فقط دون أن يتعدى أثرها على شبكة الإنترنت أو الشبكات الأخرى.
3. يرى الباحث أن بعض المصطلحات مثل (الاختلاس المعلوماتي) أو (الغش المعلوماتي) تخص بالذكر أشكال محددة من جرائم الإنترنت والتي لا تشمل باقي الجرائم.
4. يرى الباحث بأن مصطلح الجريمة المعلوماتية والجريمة السيبرانية هي مصطلحات أصبحت رسمية بالمملكة العربية السعودية وذلك بعد صدور الآتي:
1. نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م / 17) وتاريخ (08/ 03 / 1428هـ).
2. الأمر الملكي الكريم بالموافقة على تنظيم وإنشاء الهيئة الوطنية للأمن السيبراني بتاريخ(1439/02/11هـ) وهو المرادف لمصطلح (معلوماتي).

لذا كان مصطلح (جرائم السيبرانية) أو (جرائم المعلوماتية) هو أنسب المصطلحات لأغراض هذا البحث وأُقربها لتوضيح وبيان هذا النوع من الجرائم.

3. أشكال وصور الجرائم السيبرانية

هناك العديد من الأشكال والصور لجرائم السيبرانية والتي من الصعب حصرها؛لأنها جرائم مرتبطة بالتقنية المعلوماتية والتي تتطور تبعاً لتطور هذه التقنية ووفقاً لنظام مكافحة جرائم المعلوماتية فقد تنبأ المنظم صور هذه الجرائم وأوردها بالمادة رقم(6) بفقرتها الأولى: فمنها ما هو واقع على النظام العام أو القيم الدينية ومنها ما هو واقع على الآداب العامة والحياة الخاصة كالسب والشتم و إفشاء الأسرار وكذلك نشر الوثائق المعلوماتية السرية وإفشائها[1]،عليه يستعرض الباحث في هذا المطلب أكثر أشكال وصور جرائم السيبرانية انتشاراً وشيوعاً، وذلك على النحو الآتي:

أولاً: جرائم ضد الحكومات وكيانها الاقتصادي

هذا النوع من الجرائم السيبرانية يتم من خلال نَشر الفيروسات بهدف تدمير ومَسح البرامج والملفّات وتعطيل أجهزة الكمبيوتر وكذلك محاولة تنفيذ هجمات منظمة على البنوك والمواقع الإلكترونية للأجهزة الحكومية لاستهداف اقتصادها، بالإضافة إلى اختراق وتعطيل المواقع الالكترونية الحكومية، وغير الحكومية، واختراق نُظُم حمايَة المعلومات والبوابات الإلكترونيَّة و تغيير محتوى صفحة المواقع الالكترونية، ويشمل التخريب إفساد البرامج والبيانات المخزنة في ذاكرة الجهاز من حيث تدميرها أو تعديل محتواها بهدف التزوير أو تغيير الحقائق[2] ،أو إنشاء مواقع إلكترونية لمنظمات إرهابية لتسهيل التواصل بين القيادات الإرهابية أو لغرض ترويج أفكارهم ،ونشير إلى التقرير الاقتصادي الذي تم نشره في جريدة مكة ما تتعرض له المملكة من هجمات الكترونية، حيث تعرضت إلى 54 ألف هجوم الكتروني خلال عام، مما وضعها في المرتبة الثالثة عالميا من حيث التعرض للهجمات، مبينا أنها تصل يوميا إلى نحو 150 هجوما، بمعدل 6.25 هجمات في الساعة. وأوضح التقرير الصادر عن غرفة الشرقية أن استهداف المملكة الكترونيا يجيء بسبب أن اقتصادها يعد واحدا من أقوى اقتصادات الشرق الأوسط، كما أنها من أقوى 20 اقتصادا في العالم، مما جعل الشركات والمؤسسات السعودية هدفا للهجمات التي يشنها قراصنة الانترنت[3].

ويلاحظ بأن المجرم السيبراني يستغل تطور الأجهزة الحكومية التي تعتمد على التحول الرقمي وذلك بتنفيذ هجماته على الشبكات الحكومية بهدف سرقة بيانات معينة أو التأثير على اقتصاد الدولة من خلال تدمير الأجهزة بالفيروسات أو اختراق أنظمة البيانات والعبث في بيانات العملاء وتحويل الأموال أو استغلال التقنية في ترويج ونشر الأفكار الإرهابية وتسهيل

---

1. المادة رقم (1/6) من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م / 17) وتاريخ (08 / 03 / 1428هـ).
2. إبراهيم جابر وأحمد شوقي، الجرائم الإلكترونية والمعلوماتية: بطاقات الإئتمان -الكمبيوتر والإنترنت، ط1(الإسكندرية: مؤسسة شباب الجامعة،2018م)،162-163.
3. علي شهاب(2017م) المملكة الثالثة عالميا في التعرض للهجمات الالكترونية،متاح على: https://cutt.us/I1jll تاريخ الدخول:(2020/03/29م).

التواصل بين الإرهابيين، كما يهدف المجرم السيبراني إلى تعطيل الخدمات الحكومية الإلكترونية عن العمل وهو يُعد من أخطر أنواع الجرائم السيبرانية وقد جرم المنظم السعودي جرائم الإرهاب الإلكتروني وجرائم استهداف كيانها الاقتصادي حيث نصت المادة رقم(7) من نظام مكافح جرائم المعلوماتية بأنه "يعاقب بالسجن مدة لا تزيد على عشرة سنوات وبغرامة لا تزيد على خمسة ملايين ريال أو إحدى هاتين العقوبتين ؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتي[1]:

1. إنشاء موقع لمنظمات إرهابية على الشبكة العنكبوتية أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات الأجهزة الحارقة أو المتفجرات أو أي أداة تستخدم في الأعمال الإرهابية.
2. الدخول غير الشروع 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".

نجد أن الفقرة الأولى من النظام يجرم إنشاء مواقع إلكترونية لمنظمات إرهابية حيث أصبح الإرهاب في الوقت الحالي ظاهرة عالمية ترتبط بعوامل اجتماعية وثقافية و سياسية والتكنولوجيا أفرزت هذه الجرائم في العصر الحديث وقد شهدت العقود الأخيرة بروز العديد من التنظيمات و العمليات الإرهابية المسلحة عبر الإنترنت عن طريق تأسيس مواقع افتراضية لترويج أفكارهم وخططهم الإرهابية وتعلن عن حاجتهم لتجنيد عناصر جديدة تساعدهم في تنفيذ أعمالهم الإجرامية وهم في ذلك يعتمدون على فئة صغار السن من الشباب لاستغلالهم في تنفيذ عمليات انتحارية كما لو كانت تعلن عن وظائف شاغرة للشباب مستخدمة في ذلك الجانب الديني.

ثانياً: جرائم الاعتداء على حرمة الحياة الخاصة

الخصوصية الشخصية مكفول للإنسان وبالتالي يحق له حجب معلوماته وبيانات الشخصية عن الآخرين. ويعتبر التطفل عل مكتب شخص آخر أو منزله أو على جهاز حاسبه الشخصي انتهاك لهذه الخصوصية وبالتالي لا نعني في هذه الحالة تدمير المعلومات او التعديل عليها بل إن مجرد فتح الحاسب الآلي او اختراق اجهزة الآخرين من خلال شبكة الانترنت تعُد جريمة وانتهاك لخصوصية الآخرين[2] ومثال هذا النوع من الجرائم هو التعدي على حياة الآخرين بالتنصت كاستخدام الجاني برنامج خاص وزرعه في جهاز الشخص المعتدى عليه يمكن من خلاله الاطلاع والاستماع إلى جميع المحادثات والمراسلات الصادرة من المجني عليه ويتم إدخال هذه الملف إلى جهاز المعتدى عليه عن طريق البريد الإلكتروني أو عن طريق مواقع مغرية يزورها المعتدى عليه فيقوم بتنزيل بعض البرامج الضارة ومنها برنامج التنصت أو يقوم الجاني بإغراء الضحية من خلال الحديث معه في تطبيق محادث(الواتساب مثالاً) ويقنعه بأن الرابط المرسل له يحتوى على ألعاب مثيره أو غير ذلك فيقوم الضحية بفتح الرابط أو استقبال الملف. ونظراً لحرمة الحياة الخاصة ولما يترتب عليه العديد من الآثار الاجتماعية والنفسية على مستوى الأفراد ونظراً لما في نفوس الآخرين من وقوع في الوقوع كضحايا لهذه الجرائم المرتكبة نتيجة للاستخدام السيئ للهاتف الجوال كمثال، فقد نصت المادة الفقرة (4) من المادة رقم (3) على أنه يعاقب بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال أو بإحدى هاتين العقوبتين أياً من يرتكب الجرائم المعلوماتية التالية: المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بكاميرا أو ما في حكمها[3].

وهذا كله لحماية حرمة الحياة الخاصة خصوصاً ما يتعلق بالنشر والتصوير والتهديد أياً كان نوعه سواء بالتصوير أو النشر، وقول المنظم أو ما في حكمها ليدخل تسجيل الأصوات أو غيرها مما يطرأ من مستجدات تقنية مستقبلاً.

ثالثاً: جرائم الاعتداء على الأموال

---

1. المادة رقم (7) من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م / 17) وتاريخ (08 / 03 / 1428هـ).
2. حسن طاهر داود، جرائم نظم المعلومات، ط1(الرياض: جامعة نايف العربية للعلوم الأمنية،2000م)،50.
3. المادة رقم (4/3) من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م / 17) وتاريخ (08 / 03 / 1428هـ).

في هذا النوع من الجرائم يقوم المجرم السيبراني باستهداف الأموال عن طريق الاستيلاء أو الاحتيال، وتُعد من أكثر الجرائم انتشاراً وأخطرها؛ لأنها تمس الحقوق المالية للأفراد وتشمل هذه الجرائم اختراق المواقع التجارية التي تقدم خدمة عرض السلع عن طريق الانترنت ، ثم الحصول على قواعد البيانات والمعلومات الخاصة بالزبائن المتعاملين مع هذه المواقع بالحصول على معلومات دقيقة من بطاقاتهم الائتمانية واستخدامها في عمليات شراء غير قانونية ، وهذا بالطبع يؤدي إلى خسارة سمعة الموقع، وما يحدث في هذ المواقع هو قيام المستخدم بتخزين معلومات بطاقته الائتمانية بحيث يستطيع الشراء في كل مرة من نفس الموقع دون الحاجة إلى ادخال بيانات بطاقته مرة أخرى فيقوم المجرم السيبراني باستغلال هذه الفرصة واختراق جهاز الضحية والحصول على بيانات البطاقة واستخدامها في الشراء دون علم الضحية في حينه. عليه قامت شركة أمازون الشهيرة بتغيير استراتيجيتها في البيع وطالبت المستخدمين بإدخال أرقام بطاقاتهم الائتمانية في كل مرة يقومون بعملية الشراء[1]ومن ضمن جرائم التعدي على الأموال جريمة الاعتراض على الحوالات المالية وجريمة الاختلاس بوسيلة إلكترونية[2].

وقد جُرمت هذه الأفعال في نظام مكافحة جرائم المعلوماتية سواء كانت عن طريق الاستيلاء أو الاحتيال كما نصت عليها المادة رقم (4) بفقرتها الثانية على " يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية[3]:

1. الاستيلاء 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.
2. الوصول-دون مسوغ نظامي صحيح- إلى بيانات بنكية أو ائتمانية أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات أو أموال أو ما تتيحه من خدمات"

وبناءً على مما سبق يلاحظ بأن جريمة السطو على أموال البنوك إلكترونياً تتم عن طريق استخدام المجرم أحد أجهزة الحاسب الآلي للدخول عبر شبكة الإنترنت والوصول غير المشروع إلى البنوك والمؤسسات المالية وتحويل الأموال من تلك الحسابات الخاصة بالعملاء إلى حسابات أخرى من خلال تحويل مبالغ صغيرة جداً بحيث لا يلاحظ الضحية نقصان أمواله، ويرتبط مفهوم عدم مشروعية الدخول بمعرفة من له الحق في الدخول إلى نظام الحاسب الآلي ومن ليس له هذا الحق ويدخل في عدم المشروعية حالة دخول العاملين في الجهة التي يوجد بها نظام الحاسب الآلي متجاوزاً الصلاحيات المحددة له.

رابعاً: الجرائم الواقعة على حقوق الملكية الفكرية

إن الجرائم المعلوماتية الواقعة على الحقوق الفكرية في الانترنت تتباين درجاتها وأهميتها بشكل كبير فهناك فرق بين سرقة الطالب لمقال في الانترنت وتسليمه في المدرسة على انه هو الكاتب الاصلي وبين سرقة البرامج الأصلية ونسخها وتوزيعها بشكل غير قانوني في المواقع المختلفة وفي مؤتمر المنظمة العالمية للملكية الفكرية حذر روبرت هليمان الرئيس والمدير التنفيذي لاتحاد منتجي برامج الكمبيوتر التجاري في الكلمة التي ألقاها في المؤتمر من أن سرقة المطبوعات والمنشورات مباشرة من شبكة الانترنت تتصاعد إلى ابعاد خطيره الأمر الذي يهدد الصناعات الابداعية إلى جانب عرقلة مسيرة تطوير التجارية الإلكترونية، وعلى الرغم من الجهود المبذولة في حماية الملكية الفكرية إلا ان المقلدون تطوروا من قدراتهم ووسعوا جهودهم بالطرق التي تمكنهم من استخدام ادوات لإلحاق الضرر بأصحاب الملكية الفكرية[4] ومثال هذا النوع من الجرائم هي الجرائم الواقعة على حقوق الملكية الفكرية من جريمة تقليد التواقيع وأختام المؤلف ، وجريمة وضع اسم المختلس منسوب إلى شخص آخر[5].

خامساً: جرائم الاستغلال الجنسي للقاصرين

---

1. عبدالقادر عبدالله الفنتوخ،الجريمة في الإنترنت وطرق الحماية منها،ط1(الرياض: العبيكان للنشر،2012م)،50.
2. محمد قاسم الردفاني، تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية،المجلة العربية للدراسات الأمنية والتدريب،السنة(30)،العدد(61)،المجلد(31)،(2014)،169-170.
3. المادة رقم (4) من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م / 17) وتاريخ (08 / 03 / 1428هـ).
4. عبدالقادر عبدالله الفنتوخ،مرجع سابق،53-55
5. محمد قاسم الردفاني، مرجع سابق،169.

في هذا النوع من الجرائم يقوم المجرم بالاستغلال الجنسي عبر استخدام منصات التواصل الاجتماعي المتاحة على الشبكة من خلال ارسال الكتابات والصور والرسومات والأفلام والإشارات التي يشارك بها القاصرين وينطبق هذا الحال على جرائم التهديد والابتزاز الإلكتروني للقاصرين والفتيات لاستدراجهم لهدف جنسي، و أدى انتشار هذا النوع من الجرائم على شبكة الانترنت إلى دعوة أعضاء المجتمع الدولي إلى مؤتمر عقد عام(1999م) بباريس ومؤتمر آخر في ذات العام عقد في النمسا وكانت أهداف هذي المؤتمرين كفالة التعاون الدولي في مجال مكافحة عرض وتوزيع الصور الجنسية للأطفال عبر الأنترنت[1].

في جرائم التهديد والابتزاز المعلوماتي يقوم الجاني بتهديد المجني عليه إما بنشر أخباره أو صوره أو معلومات غير صحيحه وفي هذه الحالة لا يرغب المجني عليه لسبب ما ظهورها للآخرين، وإما يهدده بنشر صور أو أخبار أو معلومات غير صحيحه ويقوم الجاني بطلب مقابل حتى لا ينشرها سواء كان هذا المقابل مادي أو علاقة غير مشروعه، وقد جرم المنظم السعودي هذا التهديد والابتزاز المعلوماتي حيث نصت المادة رقم(3) بفقرتها الثانية والرابعة والخامسة من نظام مكافحة جرائم المعلوماتية بأنه "يعاقب بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتي العقوبتين؛كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية[2]:

1. التنصت على ما هو مرسل عن طريق شبكة المعلوماتية أو أحد أجهزة الحاسب الآلي -دون مسوغ نظامي صحيح- أو التقاطه أو اعتراضه.
2. الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً.
3. الدخول غير المشروع إلى موقع إلكتروني، والدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع أو إتلافه أو تعديله أو شغل عنوانه.
4. المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها.
5. التشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة".

فيتضح من النص أن مجرد التهديد أو الابتزاز عبر الإنترنت كاف لقيام هذه الجريمة.

سادساً: جرائم المعلوماتية الأخلاقية والإتجار بالبشر والإتجار بالمخدرات وترويجها عبر استخدام منصات التواصل الاجتماعي

أكد مختصون أن الإنترنت من الوسائل الحديثة التي يستخدمها مروجو المخدرات على مستوى العالم، إذ من السهل التغرير بصغار السن واستدراجهم للوقوع في المخدرات من خلال مواقع التواصل الاجتماعي، موضحين أن المروجين يستخدمون بعض المسميات الجذابة سواء التي تجذبهم لإدخال السعادة ونسيان همومهم ومن هذه المسميات ما يرتبط بتصور القوة والنشاط ومنها ما يرتبط بالإغراءات[3].

يرى الباحث بأن أخطر الجرائم المعلوماتية التي تستهدف فئة المراهقين هي جريمة ترويج المخدرات بشكل منظم ومحاولة إغواء أكبر عدد ممكن من شباب وشابات الوطن وإيقاعهم في وحل المخدرات، إذ يحاول المجرمون الوصول لضحاياهم عبر طرق متعددة وعصرية، ويجد كثير من مروجي المخدرات ضالتهم عبر مواقع التواصل الاجتماعي باستخدام ألغاز وشفرات وصور خاصة عبر حسابات مشبوهة بغرض بيع سمومهم والإيقاع بضحاياهم.

وقد نصت المادة رقم (6) من نظام مكافحة جرائم المعلوماتية على "يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد عن ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية[4]:

1. إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية أو الآداب العامة أو حرمة الحياة الخاصة أو إعداده أو إرساله أو تخزينه عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي.
2. إنشاء موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره للاتجار في الجنس البشري أو تسهيل التعامل به.
3. إنشاء المواد والبيانات المتعلقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة أو نشرها أو ترويجها.

---

[1]. محمد أمين الرومي،جرائم الكمبيوتر والإنترنت،ط1(الإسكندرية: المكتبة القانونية لدار المطبوعات الجامعية،2003)،130.

[2]. المادة رقم (3) من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م / 17) وتاريخ (08 / 03 / 1428هـ).

[3]. موقع وزارة الإتصالات وتقنية المعلومات،المركز الإعلامي (2020م)، مواقع التواصل الاجتماعي تستخدم في بيع المخدرات، متاح على : https://cutt.us/O0r6h تاريخ الدخول على الموقع(2020/03/20م).

[4]. المادة رقم (6) من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م / 17) وتاريخ (08 / 03 / 1428هـ).

4. إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشرة للاتجار بالمخدرات أو المؤثرات العقلية أو ترويجها أو طرق تعاطيها أو تسهيل التعامل بها".

كما أن هناك العديد من صور الجرائم السيبرانية كالاصطياد الإلكتروني من خلال استغلال وسائل تقنية المعلومات لمحاولة خداع الضحية للكشف عن معلوماته السرية مثل كلمات السر الخاصة به أو معلومات حسابه المصرفي[1] أو انتحال الشخصية كأن يتقمص شخصية أحد المشاهير أو الأقارب للحصول على معلومات خاصة للضحية أما للابتزاز أو الاستيلاء.
سابعاً: التصيد بإسم كورونا (COVID-19)

وفي ظل الظروف التي تشهدها البلاد والعالم في مواجهة جائحة كورونا، قد يستغل البعض فرصة التصيد وسرقة المعلومات الشخصية للضحية من خلال إرسال رسائل من حسابات وهمية تحت مسمى وزارة الصحة وتطلب من الضحية الدخول إلى رابط غيري معروف تستهدف البيانات الشخصية و قد نبهت وزارة الصحة وكذلك المركز الوطني الإرشادي للأمن السيبراني على من هذه الرسائل المشبوه وعدم فتح الروابط الإلكترونية مجهولة المصدر[2]، ودعى المركز الوطني الإرشادي للأمن السيبراني جميع المواطنين والمقيمين على أرض هذه البلاد بمكافحة هذه الأساليب بالإجراءات الوقائية الآتيه:

1. المتابع بشكل مستمر الأخبار الموثوقة من الحسابات الرسمية لوزارة الصحة.
2. التأكد من أن الرسالة الواردة هي من الحسابات الرسمية والأرقام الموحدة لوزارة الصحية.
3. التأكد من المُرسل قبل فتح الروابط مجهولة المصدر[3].

ويرى الباحث من خلال ما ورد أعلاه بأن المجرم السيبراني يستغل الأزمات للإيقاع بالضحايا. وترى سوزان برينير، بأن أغلب الجرائم السيبرانية التي نراها الآن ببساطة هي تمثل الجرائم التقليدية التي ترتكب في الحياة الواقعية ولكن على فضاء سيبراني، فالفضاء السيبراني أصبحت الأداة لارتكاب جريمة قديمة ولكن بطريقة حديثة[4]، ولتقريب هذا الرأي نعيد طرح المثال كما أسلفنا كمن يقوم بالسب والشتم بصورة تقليدية أو ارتكاب جريمة السطو التقليدية على بنك أصبح بوسع المجرم السيبراني بإستخدام التقنية الحديثة أن يقوم بارتكاب نفس الجريمة ولكن على فضاء سيبراني.

4. خصائص الجريمة السيبرانية والمجرم السيبراني

تتميز الجريمة السيبرانية بالعديد من الخصائص التي تميزها عن غيرها من الجرائم التقليدية، وكذلك المجرم السيبراني يختص بالعديد من السمات التي تميزه عن المجرم التقليدي، وفي هذا المطلب يستعرض الباحث أبرز الخصائص التي تتميز بها الجريمة السيبراني والمجرم السيبراني عن غيرهم، وذلك على النحو الآتي:

أولا: خصائص الجريمة السيبرانية:

تعتبر الجرائم السيبرانية من الجرائم المستحدثة وسريعة التطور لأنها تتطور تبعاً لتطور تقنية المعلومات وهي تتميز عن غيرها من الجرائم التقليدية بالعديد من الخصائص يستعرض الباحث أبرزها على النحو الآتي:

1. **الحاسب الآلي هي الأداة الرئيسية في ارتكاب الجرائم السيبرانية:**

---

[1]. خالد سليمان الغثبر و سليمان عبدالعزيز بن هيشة،الإصطياد الإلكتروني: الأساليب والإجراءات المضادة له،ط1(الرياض: جامعة الملك سعود،2009م)،65.

[2]. المركز الوطني الإرشادي للأمن السيبراني(2020م)، التصيد بإسم كورونا (COVID-19)، متاح على: https://cert.gov.sa/en/awareness/-covid-19/ تاريخ الدخول:2020/04/07م.

[3]. المركز الوطني الإرشادي للأمن السيبراني، المرجع السابق.

[4] Sausan W Brenner,Criminal Threats from Cyberspace, (Santa Barbra: greenwood publishing group,2010),10.

لا يستطيع المجرم السيبراني بتنفيذ هجماته في بيئة سيبرانية إلا باستخدام أجهزة الحاسب الآلي المتصلة بشبكة الإنترنت، فارتكاب هذه الجريمة تتطلب توفر وسائل التقنية الحديثة التي لا بد أن يكون لدى المجرم المعرفة والدراية في كيفية التعامل معها[1]. وتُعد أجهزة الكمبيوتر العادية والمحمولة وكذلك الأجهزة الذكية، وهي الأداة الرئيسية لارتكاب هذه الجرائم.

2. الجريمة السيبرانية جريمة خفية يُصعب اكتشافها:

تختص الجريمة السيبرانية بالخفاء؛لأنها تقع في بيئة رقمية أو فضاء سيبراني لا حدود له وفي الغالب لا يشعر بها المجني عليه كسرقة البيانات أو إرسال الفايروسات إلى الجهاز المضيف، فمن ناحية تقنية يتم نقل المعلومات بواسطة النبضات الإلكترونية في صيغة أوامر رقمية[2].

يلاحظ بأنها جرائم تفتقد إلى الآثار التقليدية، كما أن التخلص من تلك الأوامر الرقمية أمر في غاية البساطة خصوصاً عندما تكون الجريمة واقعة بسلوك جرمي واحد يمثل الضغط على أحد أزرار لوحة التحكم في الحاسب الآلي إلا أنها تقود إلى مشكلة أخرى أعقد وأخطر وهي صعوبة تحديد الفاعل وكشفه مما يجعل الصدفة المحضة الوسيلة لذلك كما يُلاحظ بأن الأدلة التقليدية لا تنجح في إثبات هذه الجريمة؛لأن الجرائم السيبرانية لا يمكن إثباتها إلا بدليل ذو طبيعة خاصة تنتمي إلى نفس الفضاء السيبراني التي تقع علي الجريمة ،و يحرص على عدم الظهور في مسرح الجريمة ومواجهة المجني عليه أو الجهة المستهدفة لخوفه من اكتشاف هويته.

3. جريمة عابرة للحدود الوطنية والقارات:

وهذه هي إحدى الخصائص الهامة التي تتميز بها الجرائم السيبرانية، حيث أن المسرح الجنائي الخاص بها لا ينحصر في مكان معين أو دولة معينة؛لأنها تتم في بيئة افتراضية لا حدود لها، وبالتالي يُعد الفضاء السيبراني حول العالم كله مسرحاً لها ،وبإمكان المجرم السيبراني تنفيذ هجماته في أي مكان وزمان بالعالم، وهذا الأمر يُعد بحد ذاته تحدي كبير في حقل الاختصاص القضائي والقانوني الواجب التطبيق من حيث الملاحقة والتحقيق و الضبط والتفتيش، عليه فإن الوصول إلى الحقيقة يستوجب الاستعانة بخبرة فنية ذات مهارة عالية وتكافل بين الدول عن طريق عقد الاتفاقيات المنظمة لهذا الشأن[3].

فلا يتواجد الفاعل في مسرح الجريمة، حيث تتباعد المسافات بين الفاعل والنتيجة، وهذه المسافات لا تقف كما أسلفنا عند حدود دولية معنية بل تمتد إلى النطاق الإقليمي لدول أخرى مما يضعف صعوبة اكتشافها أو ملاحقتها.

4. الجريمة السيبرانية جريمة ناعمة:

جرى تسمية الجرائم السيبرانية أو المعلوماتية بالجرائم الناعمة؛ لأنها لا تتطلب استخدام الأساليب التقليدية في ارتكاب الجريمة وأيضاً لا تحتاج إلى مجهود بدني في ارتكابها كما هو حال الجرائم التقليدية فلا يوجد دماء أو أسلحة مادية نتيجة لإرتكابها،بل تعتمد على تخطيط منظم ومعرفة باستخدام الأجهزة الذكية[4].

ويلاحظ بأن هذه الجرائم تتميز بأنها تُرتكب بسرعة فائقة وفي وقت قصير وبأسلوب هادئ فهي لا تحتاج إلى العنف كالجرائم التقليدية؛لذلك لا يتم اكتشافها إلا بعد مدة زمنية، فهي تنصب على البيانات والمعلومات المخزنة في نظام المعلومات مما ينفي وجود أي أثر مادي أو تقليدي يمكن الاستعانة به في إثباتها فالجرائم المعلوماتية ينتفي فيها العنف ولا توجد فيها آثاراً كما ذكرنا أعلاه وإنما هي أوامر وأرقام ودلالات تتغير أو تمسح من السجلات أو تستولى على البيانات وغيرها من الصور التي لا يمكن حصرها.

5. صعوبة إثبات الجريمة:

تختص الجرائم المرتكبة عبر استخدام شبكات الإنترنت بالغموض وصعوبة اكتشافها[5]؛وفي رأي الباحث تكمن الصعوبة لأنها لا تترك أثراً تقليدياً كالبصمات فمعظم هذه الجرائم يتم اكتشافها على محض الصدفة وبعد وقت طويل من ارتكابها مما يشكل صعوبة في اكتشافها ومما يزيد صعوبة إثبات هذه الجرائم أنها تقع في فضاء سيبراني غير ملموس ولا تترك أثراً، والتي تحتاج إلى معرفة وإلمام ومهارة كافية في تقنية وعلوم الحاسب الآلي حتى يمكن اكتشافها وتتبعها.

---

1. محمد قاسم الردفاني،المرجع السابق،171.
2. محمد عبيد الكعبي،الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت،ط2(القاهرة: دار النهضة العربية،2009)،38.
3. محمد قاسم الردفاني،مرجع سابق،164
4. غادة نصار، الإرهاب والجريمة الالكترونية، ط1(القاهرة: العربي للنشر والتوزيع،2017)،38.
5. عبدالمحسن بدوي محمد،الجرائم المعلوماتية،مجلة الأمن والحياة: جامعة نايف العربية للعلوم الأمنية،المجلد(29)،العدد(335) ،(2010م) ،67.

ثانياً: خصائص المجرم السيبراني:

أثبتت الدراسات بأن المتورطين في الجرائم السيبرانية يتميزون بسمات تميزهم عن غيرهم من المتورطين في الجرائم التقليدية[1] يوضح الباحث في هذا الجانب أبرز الخصائص المميزة للمجرم السيبراني على النحو الآتي:

1. مهارة المجرم السيبراني في استخدام التقنية الحديثة لأنظمة المعلومات:

وهي من أهم الخصائص التي تتميز بها المجرم السيبراني والتي تتمثل في إلمام المجرم السيبراني باستخدام الحاسب الآلي والمهارات الفنية بتقنية المعلومات، وقد يكون المجرم السيبراني من المتخصصين في معالجة البيانات الرقمية حيث أن آلية ارتكاب هذه الجريمة تشترط أن يتمتع المجرم بالصفات الفنية الخاصة في استخدام التقنية الذكية[2]. ويرى الباحث بأنه لا يشترط فعلاً بأن يكون المجرم السيبراني من المتخصصين في مجال الحاسب الآلي وتقنية المعلومات؛لأن كثير من فئة الهاكرز اكتسبوا هذه المهارة الفنية كهواية من الآخرين أو من خلال الاطلاع والقراءة في الشبكة العنكبوتية مثل بدر الغامدي والذي يُعد أصغر هاكر سعودي في سن الحادي عشرة[3].

2. المجرم السيبراني على قدر عالي من الذكاء والابتكار:

وهي من أهم خصائص المجرم السيبراني؛لأنه مجرم محترف لديه المعرفة الواسعة في استخدام الأجهزة الذكية وتسخير التقنية الرقمية لصالحه وتحقيق أهدافه واختراقه الشبكات وكسر كلمات المرور والتعمق في الفضاء السيبراني من خلال القدرة على التعامل مع أحدث وسائل التقنية ، ولا يشترط في المجرم السيبراني ان يكون ذو مهارة عالية جداً و إنما يكفي أن يكون لديه الإلمام الكافِ في علوم تقنية الحاسب الآلي وكيفية اختراق الشبكات المحمية والقدرة على إخفاء جريمته[4].

3. صعوبة الإمساك بالمجرم السيبراني:

تعود صعوبة الإمساك بالمجرم السيبراني إلى ذكائه؛ لأنه يحرص على إخفاء هويته وتدمير أي دليل يحتمل أن يستدل من خلاله رجال الضبط الجنائي، لذلك يسعى المجرم السيبراني دائماً إلى تحقيق أهدافه بكل هدوء، بالإضافة إلى أن مسرح الجريمة تتم في بيئة رقمية الأمر الذي يزيد من صعوبة اكتشاف الجريمة. ويطلق على المجرم السيبراني بذوي الياقات البيضاء؛ لأنهم ينتمون إلى مناصب رفيعة المستوى ويكونوا أحياناً من ذوي التخصصات والكفاءات العالية بل أن بعضهم يتمتع بثقة الأشخاص المحيطين به[5]. ويكونوا أحياناً من فئات صغار السن وهذه الفئة يكون لديها الشغف والميل للمغامرة والتحدي والرغبة في الاستكشاف ونادراً ما يكون أهدافهم محظورة فهم لا يدركون النتائج التي قد تترتب من ارتكابهم الجريمة المعلوماتية[6].

4. خوف المجرم السيبراني من كشف الجريمة:

يختص المجرم السيبراني بالخوف من اكتشاف هويته لما يترتب على ذلك من فقدان وظيفتهم ومكانتهم الاجتماعية وسمعتهم في الوسط العائلي لذلك فإن المجرم السيبراني يحافظ كثيراً على سرية أفعاله ولا يخبر بها أحد وهي أهم الأسباب التي تساعده في عدم اكتشاف جريمته. عليه يتضح بأن المجرم السيبراني يخشى من اكتشاف جريمته مردها إلى انتمائه في الغالب إلى وسط اجتماعي متميز سواء من حيث التعليم أو الثقافة أو المستوى المهني[7].

---

1. طاهر محمود أبوالقاسم،الجرائم المعلوماتية: صعوبات التحقيق فيها وكيفية مواجهتها،ط1(الشارقة: منشورات المنظمة العربية للتنمية الإدارية بجامعة الدول العربية،2019)،53.
2. عفيفي كامل عفيفي وفتوح عبدالله الشاذلي،جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية،ط1(بيروت: منشورات الحلبي الحقوقية،2003م)،43.
3. قناة الإخبارية (2017م)، صوت المواطن-أصغر هكر سعودي، متاح على: https://www.youtube.com/watch?v=oEok6lp-TQY تاريخ الدخول:(2020/03/29م).
4. ناصر محمد البقمي،أهمية الأدلة الرقمية في الإثبات الجنائي: دراسة وفق الأنظمة السعودية،مجلة الفكر الشرطي،المجلد(21)،العدد(80) ،(2012م) 45،
5. نهلا عبدالقادر المومني،الجرائم المعلوماتية،ط1(عَمان: دار الثقافة للنشر والتوزيع،2008)،76.
6. عبدالعال الديربي و محمد صادق إسماعيل،الجرائم الإلكترونية،دراسة قانونية قضائية مقارنه مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت،ط1(القاهرة: المركز القومي للإصدارات القانونية،2012)،58.
7. نهلا عبدالقادر المومني،المرجع السابق،80.

5. المجرم السيبراني إنسان اجتماعي:

المجرم السيبراني إنسان اجتماعي فهو قادر على التكيف في بيئته الاجتماعية بل أن الكثير منهم يتمتع بثقة كبيرة في مجال العمل والأصدقاء والأسرة، فالمجرم السيبراني دائماً لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به؛لأنه إنسان قادر على التكيف والتصالح مع مجتمعه، وقد تزداد خطورته الإجرامي إذا زاد تكيفه الاجتماعي[1].

ويرى الباحث بأن شعور المجرم السيبراني بأنه محل ثقة في المجتمع المحيط به وأنه خارج إطار الشبهات قد يدفعه إلى التمادي في ارتكاب جرائمه والتي قد يصعب اكتشافها لعدم الشك به.

6. المجرم السيبراني عائد للإجرام:

يتميز المجرم السيبراني عن المجرم العادي بأنه عائد للإجرام؛ لأنه يعود بارتكاب الجريمة مرة أخرى وبنفس الطريقة، فهو يكيف مهاراته الجرمية في كيفية التعامل مع أجهزة الحاسب الآلي وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات واختراقها عدة مرات، وقد تتعدد الدوافع لارتكابها في كل مرة يعود فيها[2].

7. المجرم السيبراني يستغل الأزمات للإيقاع بالضحايا:

يرى الباحث وتطبيقاً لهذه الخاصية في ظل الظروف التي تشهدها البلاد والعالم في مواجهة جائحة كورونا، أن المجرم السيبراني استغل فرصة التصيد الإلكتروني وسرقة المعلومات الشخصية للضحية من خلال إرسال رسائل من حسابات وهمية تحت مسمى وزارة الصحة وتطلب من الضحية الدخول إلى رابط غيري معروف تستهدف البيانات الشخصية وقد نبهت وزارة الصحة وكذلك المركز الوطني الإرشادي للأمن السيبراني على من هذه الرسائل المشبوه وعدم فتح الروابط الإلكترونية مجهولة المصدر[3].

5. أركان الجريمة السيبرانية

تُعد الجريمة السيبرانية على الرغم من حداثة جرمها إلا أنها كغيرها من الجرائم لابد لها من أركان حتى تصبح جريمة معاقب عليها وفقاً للأنظمة بحيث إذا أنتفى أي ركن من الأركان انتفى عنها شق التجريم .في الأنظمة الجنائية تتشابه الجرائم السيبرانية مع غيرها من الجرائم التقليدية في الأركان العامة للجريمة وهو توفر الركن الشرعي أو النظامي(نص التجريم والعقاب) والركن المادي والمعنوي،[4].وفي هذا المطلب يتناول الباحث الأركان العامة للجرائم الواقعة على شبكات الأنترنت وذلك باستعراض الركن المادي وعناصره في الفرع الأول ، ثم استعراض الركن المعنوي في الفرع الثاني ،وفي الفرع الثالث سيتم التطرق إلى الركن القانوني وذلك على النحو الآتي:

الفرع الأول: الركن المادي

يعرف الركن المادي بأنه: " سلوك إجرامي بارتكاب فعل جرمه القانون أو الامتناع عن فعل أمر به القانون"[5]ويعتبر توفر الركن المادي أمراً هاماً ؛لأنه لا جريمة في حال عدم تحقق هذا الركن و لا تكون الجريمة إلا من خلال ارتكاب فعل مادي يعاقب عليه النظام، وبناء عليه فلا تتحقق هذه الجريمة في ما يدور في الأذهان والنيات أو الرغبة في القيام بها من دون الإقدام على الفعل المادي، إذا لابد من هذه النية أن تتجسد في سلوك مادي محسوس وهذا السلوك المادي المتجسد هو ما يُعرف بالركن المادي للجريمة والذي يُعتبر شرطاً في للبدء في عملية البحث والتحري عن توافر الجريمة من عدمها[6].

ويرى الباحث بأنه يمكن القول بأن الركن المادي يمثل كيان الجريمة والذي وعبارة عن فعل الفاعل بصورة يمكن إثباتها كجريمة وبه يتحقق الاعتداء على المصلحة المراد حمايتها وعن طريق هذا الفعل تقع الأعمال التنفيذية للجريمة فهو يمثل النشاط الذي يصدر عن الجاني ليتدخل من أجل هذا الفعل النظام ويقوم بتوقيع الجزاء على المجرم والركن المادي في الجرائم

---

1. محمد أمين الرومي،مرجع سابق،23.
2. سحر فؤاد مجيد،الجرائم المستحدثة: دراسة معمقة ومقارنة في عدة جرائم،ط1(القاهرة:المركز العربي للنشر والتوزيع،2019)،53.
3. المركز الوطني الإرشادي للأمن السيبراني(2020م)، التصيد بإسم كورونا (COVID-19)، متاح على: https://cert.gov.sa/en/awareness/-covid-19/ تاريخ الدخول:2020/04/07م.
4. داليا قدري عبدالعزيز،الوجيز في بعرض جرائم التعزيز المنظمة في المملكة العربية السعودية،ط1(الرياض: دار الرشد،2017)،56.
5. ضرغام جابر عطوش،جريمة التجسس المعلوماتي:دراسة مقارنه،ط1(القاهرة: المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع ،2017م) ،171.
6. عبدالعزيز غرم الله آل جارالله،المرجع السابق،86.

المعلوماتية أو السيبرانية كغيرها من الجرائم تتكون من ثلاثة عناصر رئيسية كما أقرها الفقهاء متى ما توافرت نكون أمام ركن مادي متكامل يستعرضها الباحث على النحو الآتي:

1. **السلوك الإجرامي:** ويقصد به " النشاط الخارجي الذي يقوم به الجاني، ويبرز في العالم الخارجي مكوناً لماديات الجريمة ومسبباً لما قد يترتب عليها من ضرر أو خطر"[1]، فالسلوك الإجرامي له صوره متعددة وتختلف باختلاف نوع الجريمة المرتكبة ففي الجرائم المعلوماتية، لابد من قيام الجاني بممارسة نشاط تقني والشروع فيه باستخدام جاهز الحاسب الآلي متصل بشبكة الإنترنت في بيئة رقمية، فمثلاً في جريمة الوصول إلى معلومات بنكية يقوم المجرم بإعداد جهاز ذكي وتحميل برامج اختراق وإرساله إلى الجهاز المضيف للحصول على بيانات المرور البنكية بهدف الاستيلاء على أموال الضحية، أو قيام الجاني بإرسال ملف تجسس إلى جهاز المجني عليه ويسمى هذا الملف بحصان طروادة وذلك من خلال عدة طرق، إما عن طريق برامج المحادثة كتطبيق واتساب أو عن طريق ارسال ملف يحمل برنامج اختراق إلى عنوان البريد الإلكتروني للضحية و طريقة أخرى مثل أن يقوم الضحية بتصفح بعض المواقع التي تتدعي احتواءها على برامج وتطبيقات مجانية فيقوم المجني عليه بتحميل هذا البرنامج وهو لا يعلم بأنه يحوي على ملف تجسس[2].

والسلوك الإجرامي في أركان الجريمة العامة يأتي في شكلين: ما يُعرف بالنشاط الإيجابي وكذلك ما يسمى بالنشاط السلبي وهي صورة ثانية من صور السلوك الإجرامي والذي يُعرف بأنه: "امتناع الفرد عن تأدية واجب يقع على عاتقه"[3] أما فيما يخص الجرائم المرتكبة عبر استخدام أجهزة الحاسوب المتصلة بالإنترنت فإنها لا تتحقق إلا بالدخول غير المشروع والذي يتطلب من الجاني مباشرة نشاط إيجابي تقني عبر استخدامه اجهزة حديثه متصلة بالإنترنت، فالنشاط في هذا النوع من الجرائم هو نشاط إيجابي ولا يمكن أن تتحقق بنشاط سلبي[4]. فمثلاً جريمة الدخول غير المشروع إلى موقع إلكتروني لتغيير تصاميمه أو تدميره أو تعديله، فهذا النوع من الجرائم لا يتحقق إلا إذا قام الجاني بالدخول غير المشروع من دون مسوغ نظامي إلى الموقع الإلكتروني للضحية سواء كانت عائدة ملكيته لشخص أو مؤسسة أو شركة خاصة أو حكومية وقيامه بعملية التعديل أو التدمير أو التشهير إلكترونياً، فقد نصت المادة رقم (3) من نظام مكافحة جرائم المعلوماتية بأنه "يعاقب بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتي العقوبتين؛كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية[5]:

1. التنصت على ما هو مرسل عن طريق شبكة المعلوماتية أو أحد أجهزة الحاسب الآلي -دون مسوغ نظامي صحيح- أو التقاطه أو اعتراضه.
2. الدخول غير المشروع لتهديد شخص أو ابتزازه؛لحمله على القيام بفعل أو الامتناع عنه ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً.
3. الدخول غير المشروع إلى موقع إلكتروني، والدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع أو إتلافه أو تعديله أو شغل عنوانه.
4. المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها.
5. التشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة".

في الدخول غير المشروع كمثال الذي أشرناه إليه يلاحظ من خلال الفقرة رقم (3) من المادة السابقة بأن المنظم السعودي قد حدد السلوك الإجرامي المادي في ارتكاب هذا النوع من الجرائم.

2. **النتيجة الإجرامية:** وهي العنصر الثاني من عناصر تكوين الركن المادي، وهي تختلف بطبيعة الحال عن السلوك الإجرامي. وتُعرف النتيجة الإجرامية بأنها "الأثر المادي أو القانوني المترتب على حصول جريمة يعاقب عليها القانون"[6] وهي تتمثل في النتيجة التي توصل إليها الجاني بالدخول الغير مشروع تقنياً باستخدام جهاز حاسب آلي إلى بيانات الضحية بهدف الاستيلاء على معلومات بنكيه أو تدمير مواقع الكترونية وذلك باستخدام برامج اختراق التي تمكنه من الدخول غير المصرح به وتحقيق نتيجة ضاره.

---

1. عبدالعزيز غرم الله آل جارالله،المرجع السابق،87.
2. محمد أمين الرومي،المرجع السابق،102.
3. محمد حميد المزمومي،النظام الجزائي(نظرية الجريمة-نظرية الجزاء):دراسة مقارنة،ط1(جدة: جامعة الملك عبدالعزيز،2018م)،110.
4. محمد حماد الهيتي،جرائم الحاسوب،ط1 (عمان: دار المناهج للنشر والتوزيع،2006)، 182.
5. المادة رقم (3) من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م / 17) وتاريخ (08 / 03 / 1428هـ).
6. عبد العزيز غرم الله آل جارالله، المرجع السابق،89.

3. **علاقة سببيه:** لابد للركن المادي حتى تكتمل كافة عناصره من وجود علاقة سببية تربط بين السلوك الإجرامي وما تحقق من نتيجة إجراميه، بحيث يمكن القول بأنه لولا وقوع هذا السلوك الإجرامي لما تحققت هذه النتيجة الجرمية، وهي تتمثل في العلاقة المباشرة بين السلوك الإجرامي المتمثلة في اختراق بيانات الضحية بطريقة غير مشروعه وما تحقق من نتيجة ضارة وهي الحصول على البيانات البنكية[1]. مع مراعاة بأن الركن المادي في الجرائم المعلوماتية تتخذ عدة صورة بحسب كل جريمة[2].

ويلاحظ أنه إذا انتفت العلاقة السببية التي تربط بين السلوك الإجرامي والنتيجة فلن تكون هناك مساءلة جنائية للمتهم، كما أن المنظم السعودي لم يضع معياراً تحكم العلاقة السببية وإنما ترك المجال مفتوحاً للمحققين والقاضي الجنائي حسب ظروف وملابسات القضية.

الفرع الثاني: الركن المعنوي

الجريمة السيبرانية كغيرها من الجرائم، لابد من توافر القصد الجنائي للمجرم والذي يتكون من عنصري العلم والإرادة، فمن حيث العلم لابد أن يكون الجاني على علم بأن الدخول إلكترونياً على بيانات خاصة غير مصرح للاطلاع أو الحصول عليها هو أمر غير مشروع، أما فيما يخص الإرادة فلابد أن تتجه إرادة الجاني إلى ارتكاب الفعل المجرَم[3]. فالركن المعنوي يسميه بعض الفقهاء بالركن الأدبي والتي تمثل الإرادة الآثمة التي تقترن بالفعل المادي وأيضاً يُعرف بالقصد الجنائي[4]. لكن الدخول إلى قاعدة البيانات الرقمية عن طريق الخطأ ينفي المسؤولية الجنائية لانتفاء القصد الجنائي[5].

ويلاحظ بأن العلاقة بين الركن المادي والركن المعنوي متصلان ببعض اتصالاً قوياً؛ لأنها تعكس ما في نفسية المجرم من قصد جنائي وتوجه إرادته إلى ارتكاب الجريمة، عليه يتحقق الركن المعنوي بتوفر عنصرين جوهريين هما العلم، والإرادة، ونلخص القول بأن الركن المعنوي يعبر إرادة المجرم المعلوماتي (القصد الجنائي) بحيث يُرتكب الفعل المجرم من شخص مريد إرادة فعلية وبطواعية دون إكراه من أحد وعن رغبة وإدراك.

الفرع الثالث:الركن القانوني

بمعنى أن ينص في النظام على تجريم هذا الفعل غير المشروع والمقصود من المجرم، فالقاعدة القانونية تنص على أنه لا جريمة ولا عقوبة إلا بنص، ولقد تم تجريم هذه السلوكيات الجريمة في نظام مكافحة جرائم المعلوماتية وتم وصف الجريمة وصفاً دقيقاً مع بيان العقوبات.

6.دوافع الجريمة السيبرانية

الدافع هو الباعث ويُعرف بأنه: "العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام"[6]فالجرائم السيبرانية تقع بسبب عدة دوافع فبعضها يرجع إلى دافع سياسي ومنها ما يرجع إلى دافع مالي ومنها ما هو دافع شخصي، يستعرض الباحث في هذا المطلب أهم البواعث التي تدفع المجرم السيبراني إلى ارتكاب جريمته وهذه البواعث عديدة ومتنوعة لذلك سيتم استعراض أهمها على النحو الآتي:

1. **دافع مادي:** وهي التي يكون سببها الهدف إلى تحقيق مكاسب مادية مثال على ذلك تحويل حساب مالي إلى حسابه.
2. دافع شخصي: وهي التي يكون سببها الرغبة في تعلم كيفية اختراق المواقع الممنوعة وتخريب المواقع الخاصة والحكومية.
3. **دافع ذهني:** وهي التي يكون سببها دافع المجرم السيبراني إلى تحقيق الرغبة في الانتصار على النظام المعلوماتي وهزيمتها عبر اختراقها والتحكم فيها.

---

[1]. عبدالصبور عبدالقوي المصري، نظام مكافحة الجرائم المعلوماتية في ميزان التحليل الفقهي، ط1(جدة: دار حافظ للنشر والتوزيع،2012)،69-72.
[2]. أيمن العباد، المسؤولية الجنائية لمستخدمي شبكات التواصل الإجتماعي، ط1(الرياض: مكتبة القانون والاقتصاد،2015)،77.
[3]. المصري، المرجع السابق،72.
[4]. عيسى صالح العمري و محمد شلال العاني، فقه العقوبات في الشريعة الإسلامية: دراسة مقارنة،ط 1(إربد: دار الكتاب الثقافي للطباعة والنشر والتوزيع،2010م)،18.
[5]. محمد حماد الهيتي، المرجع السابق، 193.
[6]. نهلا عبد القادر مومني ،المرجع السابق،89.

4. **دافع للانتقام:** وهي من أخطر الدوافع التي يقوم بها المجرم المعلوماتي، وذلك من خلال الثأر من أشخاص لأسباب شخصية أو انتقام الموظف الذي تم فصله من المنشأة التي كان يعمل بها فيقوم بإختراق نظامها.
5. **دافع سياسي وعقائدي:** يتم من خلال المجرمين المعادين للحكومة، وذلك عبر تخريب المواقع الحكومية أو اختراق الحسابات الحكومية عبر منصات التوصيات الاجتماعي مثل تويتر وفيس بوك لكتابة أخبار ومعلومات غير صحيحة بغرض إثارة الفتنه والرأي العام بين المواطنين(1). وأيضاً نتيجة للهزات السياسية التي تعرض لها العالم بعد احداث 11 سبتمبر وما تلاه من غزو العراق وافغانستان والتوترات والنشاطات الارهابية التي حدث حول العالم(2)

ويلاحظ بأن دوافع ارتكاب الجريمة السيبرانية متعددة ولا يمكن حصرها فمنها ما هو لتحقيق كسب مادي غير مشروع، أو بدافع شخصي تتمثل في تعلّم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية لأنظمة الشبكات. أو بدافع نفسي لإثبات ذاته وتحقيق الانتصار على تقنية الأنظمة الرقمية، أو بدافع الانتقام عند امتلاك شخص ما معلومات كبيرة عن المؤسسة أو الشركة التي يعمل فيها، أو بدافع التسلية، والتي في الغالب لا يقصد من ورائها إحداث ضرر للمجني عليه وإنما بقصد التطفل والفضول.

7.الفرق بين الجرائم السيبرانية والجرائم الأخرى

في هذا المطلب يستعرض الباحث أوجه الشبه والاختلاف بين الجرائم السيبرانية والجرائم المشابهة لها مثل الجرائم التي تقع على أجهزة الحاسب الآلي غير المتصلة بالشبكة وذلك في الفرع الأول ثم يستعرض أوجه الاختلاف بين الجريمة السيبرانية وغيرها من الجرائم التقليدية في الفرع الثاني، وذلك على النحو الآتي:

الفرع الأول: أوجه الشبه والاختلاف بين الجرائم السيبرانية والجرائم المشابهة لها (الجرائم التي تقع على جهاز الحاسب الآلي)

أ. أوجه الشبه بين الجريمتين:

كلاهما من الجرائم المعلوماتية الحديثة والغير مشروعة[3] والتي قد تستهدف كيانات سياسية وأفراد ومنظمات باستخدام جهاز محوسب والذي يتميز فيه المجرم بالذكاء والتخطيط وبذلك يُصعب اكتشاف الجريمة ويَسهل إخفاءها[4].

ب. أوجه الاختلاف بين الجريمتين:

يتطلب ارتكاب الجريمة السيبرانية توفر جهاز متصل بالشبكة وفضاء سيبراني، أما جريمة الحاسب الآلي فإنها تتم دون اتصالها بالأنترنت كجرائم سرقة معلومات مهمة من ذاكرة التخزين أو تدميرها[5].

الفرع الثاني: الفرق بين الجرائم السيبرانية وغيرها من الجرائم التقليدية

تختلف الجرائم المستحدثة عن الجرائم التقليدية اختلافاً جوهرياً، فمن حيث مسرح الجريمة فإن الجريمة السيبرانية لا تتم إلا في بيئة رقمية وهو ما يُعرف بالمسرح الافتراضي فالجاني والمجني عليه لا يشترط أن يكونا في مكان واحد على خلاف الجرائم التقليدية أو العادية، كالقتل أو السرقة التي لها مسرح جريمة واقعي، ومن ثم يكون لها محل معاينة[6].

ويستدل من خلال أوجه الشبه والاختلاف بين الجرائم السيبرانيه والجرائم التي تقع على الحاسب الآلي بأن كلاهما من الجرائم المستحدثة؛لأنها تقع على قاعدة بيانات رقمية ويختلفون في أن الجريمة السيبرانية تتطلب لارتكابها الاتصال بشبكة الانترنت ، أما جرائم الحاسب الآلي فلا يشترط في ارتكابها الاتصال بالشبكة بل يكفي توفر جهاز كالحاسب الآلي وسرقة بياناتها ذاكرة تخزينها أو العبث بها أو تدميرها كلياً. كما يلاحظ بأن الجريمة التقليدية ظاهرة اجتماعية قديمة يعاقب عليها القانون والشرائع أما الجريمة السيبرانية فهي ظاهرة مستحدثه ظهرت بعد ثورة المعلومات الرقمية في القرن العشرين ويلاحظ أيضاً بأن مرتكبو الجرائم السيبرانية يختلفون عن المجرمين التقليديين؛ لأن المجرم السيبراني مجرم على مستوى من الذكاء

---

1. لينا جمال محمد، الجرائم الإلكترونية، ط1(مكة المكرمة: دار خالد اللحياني للنشروالتوزيع،2016)،99-101.
2. محمود أحمد القرعان،الجرائم الالكترونية،ط1(عَمان: دار وائل للنشر والتوزيع،2017)،49.
3. عبدالعزيز بن غرم الله آل جارالله،مرجع سابق،76.
4. محمد علي سكيكر،الجرائم المعلوماتية وكيفية التصدي لها،ط1(القاهرة :دار الجمهورية للصحافة،2010)،39.
5. محمد علي سكيكر،المرجع السابق،39.
6. محمد قاسم الردفاني،المرجع السابق،167.

والعلم والمعرفة في استخدام تقنية المعلومات بينما المجرم التقليدي يكون في الغالب في مستوى عادي من الذكاء والعلم ولا يشترط في ارتكاب جريمته مهاره معينة.

8.الخاتمة

استعرضت الورقة تعريف الجريمة السيبرانية وتعدد مصطلح الجريمة المعلوماتية (رقمية الكترونية، سيبرانية). كما أوضحت الورقة بأن الجرائم السيبرانية أقل عنفاً من الجرائم التقليدية؛ لأنها لا تتطلب إلى مجهود بدني حتى يتم ارتكابها، بل تعتمد على التخطيط المنظم والتفكير الذهني المبني على أسس علمية بمعرفة تقنية الحاسب الآلي. بالإضافة إلى ذلك، أوضحت الورقة بأن الجرائم السيبرانية لها أشكال متنوعة ومتعددة وتتطور تبعاً لتطور تقنية المعلومات، وعليه لابد من تطور أساليب مكافحة هذه الجريمة باستمرار وتطوير الكادر المختص بالتحقيق فيها تبعاً لتطور التقنية. علاوة على ذلك، أوضح الورقة بأن الفضاء السيبراني منفلت أمنياً وأصبحت مسرحاً افتراضياً لارتكاب الجرائم وذلك بسبب زيادة عدد مستخدمي الحاسب الآلي، و أنه تختلف دوافع ارتكاب الجريمة السيبرانية من شخص لآخر، فقد تكون دوافع سياسية يكون هدفها تدمير البنية السيبرانية للمواقع الحكومية، أو دوافع شخصيه لغرض الانتقام من الغير.

9.المراجع والتوثيقات

1. ابن منظور، محمد ،لسان العرب،ط3(بيروت: دار صادر،2003)
2. أبو عفيفه، طلال ،أصول علمي الإجرام والعقاب وآخر الجهود الدولية والعربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية،ط1(القدس: دار الجندي للنشر والتوزيع،2013)
3. أبوالقاسم،طاهر محمود ،الجرائم المعلوماتية: صعوبات التحقيق فيها وكيفية مواجهتها،ط1(الشارقة: منشورات المنظمة العربية للتنمية الإدارية بجامعة الدول العربية،2019)
4. آل جارالله ،عبد العزيز غرم الله ، جرائم الإنترنت وعقوباتها وفق نظام مكافحة جرائم المعلوماتية السعودي: ويليه آثار العولمة على مستخدمي الإنترنت، ط1(الرياض: دار الكتاب الجامعي للنشر والتوزيع،2017م)
5. البقمي ،ناصر محمد ،أهمية الأدلة الرقمية في الإثبات الجنائي: دراسة وفق الأنظمة السعودية،مجلة الفكر الشرطي،المجلد(21)،العدد(80) ،(2012م)
6. البقمي، ناصر محمد ،أهمية الأدلة الرقمية في الإثبات الجنائي:دراسة وفق الأنظمة السعودية،مجلة الفكر الشرطي،المجلد(21)،العدد(80) ،(2012م).
7. جابر، إبراهيم وشوقي ،أحمد ، الجرائم الإلكترونية والمعلوماتية: بطاقات الإئتمان -الكمبيوتر والإنترنت، ط1(الإسكندرية: مؤسسة شباب الجامعة،2018م)
8. الحقباني،رايز سالم ،مهارات البحث والتحقيق في الجرائم المعلوماتية،ط1(الرياض:كلية الملك فهد الأمنية، مركز الدراسات والبحوث،2014)
9. داود ،حسن طاهر ، جرائم نظم المعلومات، ط1(الرياض: جامعة نايف العربية للعلوم الأمنية،2000م)
10. دوادي، خالد ، الجريمة المعلوماتية، ط1(عمان: دار الأعصار العلمي للنشر والتوزيع،2018)
11. الديربي ،عبدالعال و إسماعيل ،محمد صادق ،الجرائم الإلكترونية،دراسة قانونية قضائية مقارنه مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت،ط1(القاهرة: المركز القومي للإصدارات القانونية،2012)
12. الردفاني، محمد قاسم ، تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية،المجلة العربية للدراسات الأمنية والتدريب،السنة(30)،العدد(61)،المجلد(31)،(2014)
13. الرومي ،محمد أمين ،جرائم الكمبيوتر والإنترنت،ط1(الإسكندرية: المكتبة القانونية لدار المطبوعات الجامعية،2003)،130.
14. سكيكر ،محمد علي ،الجرائم المعلوماتية وكيفية التصدي لها،ط1(القاهرة :دار الجمهورية للصحافة،2010)
15. سورة الأعراف، الآية:40.
16. شهاب ،علي (2017م) المملكة الثالثة عالميا في التعرض للهجمات الالكترونية،متاح على: https://cutt.us/I1jll تاريخ الدخول:(2020/03/29م).

17. العباد ،أيمن ، المسؤولية الجنائية لمستخدمي شبكات التواصل الإجتماعي، ط1(الرياض: مكتبة القانون والاقتصاد،2015)
18. عبدالعزيز، داليا قدري ،الوجيز في بعرض جرائم التعزيز المنظمة في المملكة العربية السعودية،ط1(الرياض: دار الرشد،2017)
19. عطوش، ضرغام جابر ،جريمة التجسس المعلوماتي:دراسة مقارنه،ط1(القاهرة: المركز العربي للدراسات والبحوث العلمية للنشر والتوزيع ،2017م)
20. عفيفي، كامل عفيفي والشاذلي ،فتوح عبدالله ،جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية،ط1(بيروت: منشورات الحلبي الحقوقية،2003م)
21. العمري ،عيسى صالح و العاني، محمد شلال ، فقه العقوبات في الشريعة الإسلامية: دراسة مقارنة،ط 1(إربد: دار الكتاب الثقافي للطباعة والنشر والتوزيع،2010م)
22. الغثبر ،خالد سليمان و بن هيشة، سليمان عبدالعزيز ،الإصطياد الإلكتروني: الأساليب والإجراءات المضادة له،ط1(الرياض: جامعة الملك سعود،2009م)
23. الفتلاوي،عبيس نعمة ،الهجمات السيبرانية:دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر،ط1(بيروت: منشورات زين الحقوقية،2018م)
24. فكري، أيمن عبدالله ،الجرائم المعلوماتية:دراسة مقارنة في التشريعات العربية والأجنبية،ط1(الرياض،مكتبة القانون والإقتصاد،2014م)
25. الفنتوخ، عبدالقادر عبدالله ،الجريمة في الإنترنت وطرق الحماية منها،ط1(الرياض: العبيكان للنشر،2012م)
26. القرعان ،محمود أحمد ،الجرائم الالكترونية،ط1(عَمان: دار وائل للنشر والتوزيع،2017)
27. قناة الإخبارية (2017م)، صوت المواطن-أصغر هكر سعودي، متاح على: https://www.youtube.com/watch?v=oEok6lp-TQY تاريخ الدخول:(2020/03/29م).
28. الكعبي، محمد عبيد ،الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت،ط2(القاهرة: دار النهضة العربية،2009)
29. المادة (8/1) من نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م / 17) وتاريخ (08 / 03 / 1428هـ).
30. المادة رقم (3) من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م / 17) وتاريخ (08 / 03 / 1428هـ).
31. المادة رقم (3) من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م / 17) وتاريخ (08 / 03 / 1428هـ).
32. المادة رقم (4/3) من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م / 17) وتاريخ (08 / 03 / 1428هـ).
33. المادة رقم (4) من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م / 17) وتاريخ (08 / 03 / 1428هـ).
34. المادة رقم (6) من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م / 17) وتاريخ (08 / 03 / 1428هـ).
35. المادة رقم (1/6) من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م / 17) وتاريخ (08 / 03 / 1428هـ).
36. المادة رقم (7) من نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م / 17) وتاريخ (08 / 03 / 1428هـ).
37. الماوردي، أبو الحسن ،الأحكام السلطانية،ط1(الكويت: دار ابن قتيبة،1989)
38. مجيد ،سحر فؤاد ،الجرائم المستحدثة: دراسة معمقة ومقارنة في عدة جرائم،ط1(القاهرة:المركز العربي للنشر والتوزيع،2019)

39. محمد ،عبدالمحسن بدوي ،الجرائم المعلوماتية،مجلة الأمن والحياة: جامعة نايف العربية للعلوم الأمنية،المجلد(29)،العدد(335) ،(2010م)
40. محمد ،لينا جمال ، الجرائم الإلكترونية، ط1(مكة المكرمة: دار خالد اللحياني للنشروالتوزيع،2016)
41. المركز الوطني الإرشادي للأمن السيبراني(2020م)، التصيد بإسم كورونا (COVID-19)، متاح على: https://cert.gov.sa/en/awareness/-covid-19/ تاريخ الدخول:2020/04/07م.
42. المزمومي، محمد حميد ،النظام الجزائي(نظرية الجريمة-نظرية الجزاء):دراسة مقارنة،ط1(جدة: جامعة الملك عبدالعزيز،2018م)
43. المصري ،عبدالصبور عبدالقوي ، نظام مكافحة الجرائم المعلوماتية في ميزان التحليل الفقهي، ط1(جدة: دار حافظ للنشر والتوزيع،2012)
44. الموقع الإلكتروني للهيئة الوطنية للأمن السيبراني (2020م)، تاريخ الدخول(2020/03/20/)، متاح على https://nca.gov.sa/pages/about.html
45. موقع وزارة الإتصالات وتقنية المعلومات،المركز الإعلامي (2020م)، مواقع التواصل الاجتماعي تستخدم في بيع المخدرات، متاح على : https://cutt.us/O0r6h تاريخ الدخول على الموقع(2020/03/20م).
46. المومني، نهلا عبدالقادر ،الجرائم المعلوماتية،ط1(عَمان: دار الثقافة للنشر والتوزيع،2008)
47. نصار ،غادة ، الإرهاب والجريمة الالكترونية، ط1(القاهرة: العربي للنشر والتوزيع،2017)
48. الهيتي ،محمد حماد ،جرائم الحاسوب،ط1 (عمان: دار المناهج للنشر والتوزيع،2006)
49. ورشة عمل بتعليم جدة، (2018م) "الأمن الرقمي وحماية المستخدم من مخاطر الانترنت " تاريخ الدخول (2020/03/29م)، متاح على: https://www.spa.gov.sa/1757119
50. Michael Aaron Dennis,Cybercrime:Web article Selected by Britannica Academic, Encyclopedia Britannica,(2018):1. Available on: https://cutt.us/M4cZd
51. Sausan W Brenner,Criminal Threats from Cyberspace, (Santa Barbra: greenwood publishing group,2010),10.

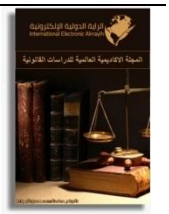
الرايه الدولية الالكترونية
INTERNATIONAL ELECTRONIC ALRRAYIH

International Academic Journal for Law Studies

المجلة الأكاديمية العالمية للدراسات القانونية

Website: http://iajour.com/index.php/lr

ISSN: 2708-7840



Cyber Crimes Committed via Digital Media Demonstrate Their Concept In Terms of: its Forms, Characteristics, Elements and Motive of Committing it

Ziyad Mohammed A. Alotaibi

Legal Adviser,Ministry of defince. Master of Laws, Jeddah
Zs.m.sa@hotmail.com

Submission date: 7/12/2020 **Accepted date:12/1/2021**

Abstract:

This paper dealt with the concept of cybercrime and its forms, characteristics, pillars, and motive for committing them, as the development of information technology in the twentieth century led to the emergence of new and new forms of crimes that mankind is not used to and the cyberspace has become a scene for them, where the criminal can pass through this space. His attacks are fast and hidden, and often do not leave a trace of his crime, so that it becomes difficult for investigators and specialists to discover or prove the crime; Because it was committed in an intangible and borderless cyber space, and therefore it is difficult to convict the accused, which led to the emergence of a question about what cybercrime is, its forms, characteristics, pillars, and motives, as digital transformation is one of the main pillars of achieving the Kingdom's vision 2030 for the development of digital infrastructure. Because of its importance, this research discussed the concept of cybercrime in terms of its forms, characteristics, pillars, and motives, and this study reached many results and recommendations, most notably that the cyber criminal exploits crises and that one of the most prominent methods of phishing during this period of study and what the country is witnessing in the face of the Corona pandemic is phishing in the name of Corona (COVID-19), as well as the need for the legislator to intervene in issuing a special and independent system for digital penal procedures in line with the digital transformation taking place in the Kingdom**.**

Key words: *information crimes, cybercrime, motives, forms, characteristics.*