International Journal for Scientific Research (IJSR)

المجلة الدولية للبحوث العلمية

Vol. (2), No. (12) December 2023 الإصدار (2)، العدد (12)

الجرائم المعلوماتية في المملكة العربية السعودية

إيناس الزهراني

أستاذ مساعد، كلية القانون (شطر البنات)، جامعة الأمير سلطان، المملكة العربية السعودية

xxncexx7@gmail.com

الملخص

في ظل رؤية المملكة 2030 نري أنه من الضروري تحليل نظام جريمة المعلوماتية، ونظام التعاملات الإلكترونية للوقوف على التكييف القانوني الصحيح للجريمة الرقمية والقانون الواجب التطبيق.

إن انتشار التكنولوجيا وتوسع دائرة الجرائم الرقمية وخروجها من نطاق التهديد الي مرحلة الواقع، الذي بات يؤرق الكثير، ويهدد الدول والمجتمعات من النواحي الاقتصادية والاجتماعية، وكذلك ظهور التطور التكنولوجي المتواتر والمتزايد في جميع الأوساط التي تحيط بنا، جعل منها أداة لارتكاب العديد من الجرائم ذات التقنية العالية التي تنتهك الحريات، وتسلب الكثير من الأموال وتزعزع الاستقرار والأمن الذي كان سائداً في العصور السابقة ما قبل انتشار التكنولوجيا وتطورها وتعاظم تأثيرها علي جميع المجالات في مجتمعنا العربي خاصة، وفي العالم أجمع.

وقد تصدي المنظم السعودي لتجريم ومعاقبة كافة الصور الإجرامية للجريمة الرقمية، موضحا أبعادها ونتائجها بموجب قانون خاص بالجرائم المعلوماتية، كما أفرد أيضا عقوبات للمساهمين، بل واعتبر المساهم في الجريمة الرقمية فاعلا أصليا. كما استنتجت الكثير من القواعد بالإضافة إلى القواعد الجزائية في القانون السعودي التي يجب أن تطال بكل حزم، الشخص الاعتباري في حال ارتكابه الجرائم الرقمية، بجانب معاقبة الشخص العادي الممثل للشخص الاعتباري وعدم الاكتفاء بتوقيع العقوبات على الشخص الاعتباري فقط.

كذلك من الضروري أن يوضع في عين الاعتبار خطورة الشخص المحرض على الجريمة الرقمية، باعتباره فاعل أصلي يستحق العقوبة الأصلية كاملة، علاوة على ذلك قد يكون المحرض من خارج الدولة محل الجريمة الرقمية.

الكلمات المفتاحية: الجريمة المعلوماتية، الجريمة الرقمية، القانون السعودي.

International Journal for Scientific Research (IJSR)

المجلة الدولية للبحوث العلمية

IJSR

Vol. (2), No. (12) December 2023 الإصدار (2)، العدد (12)

Information Crimes in the Kingdom of Saudi Arabia

Enas Al-Zahrani

Assistant Professor, College of Law (Girls Section), Prince Sultan University, Kingdom of Saudi Arabia

xxncexx7@gmail.com

Abstract

In light of the Kingdom's Vision 2030, we believe that it is necessary to analyze the information crime system and the electronic transactions system to determine the correct legal adaptation of digital crime and the applicable law.

The spread of technology and the expansion of the circle of digital crimes and their exit from the scope of the threat to the stage of reality, which has become a concern for many, and threatens countries and societies from the economic and social aspects, as well as the emergence of frequent and increasing technological development in all the circles that surround us, have made it a tool for committing many crimes with technology. High rates that violate freedoms, steal a lot of money, and destabilize the stability and security that prevailed in previous eras, before the spread and development of technology and its increasing impact on all areas of our Arab society in particular, and in the world as a whole.

The Saudi regulator has addressed the criminalization and punishment of all criminal forms of digital crime, explaining its dimensions and consequences under a special law on information crimes. It has also allocated penalties for contributors, and even considered the contributor to the digital crime to be an original perpetrator. It also concluded many rules, in addition to the penal rules in Saudi law, which must be strictly affected by the legal person in the event that he commits digital crimes, in addition to punishing the ordinary person representing the legal person and not being satisfied with imposing penalties on the legal person only.

It is also necessary to take into account the seriousness of the person instigating the digital crime, as he is an original perpetrator who deserves the full original punishment. Moreover, the instigator may be from outside the country that is the subject of the digital crime.

Keywords: Information Crime, Digital Crime, Saudi Law.

المقدمة

الحمد لله والصلاة والسلام على من لا نبي بعده وبعد، فإن من أبرز سمات التقدم الذي تشهده الذي عرفته البشرية في هذا العصر ارتباطه بالتقنية الإلكترونية والمعلوماتية واعتماده عليها في الكثير من نواحي الحياة، وأصبحت هذه التقنية تؤثر بشكل مباشر في الحياة الفردية والعامة، وارتبطت بها ووظفتها واعتمدت عليها الحكومات والشركات والأفراد، وتعلقت بها المصالح الخاصة والعامة، وأصبحت طرفا رئيسا في العلوم المختلفة والأنشطة المتنوعة[1].

كما أصبحت مجالات التجارة والثقافة والتعليم والصحة والإعلام والتواصل الاجتماعي والمراسلات وحفظ المعلومات، وغيرها كثيرا مرتبطة ارتباطا وثيقا بالتقنية المعلوماتية، بل تجاوز الأمر ذلك إلى ارتباطها بخصوصيات الأفراد وذكرياتهم.

ومثل هذا التوسع الهائل للتقنية المعلوماتية الالكترونية، والتطور الهائل في أساليبها وخدماتها، والأعداد الكبيرة جدا من المستخدمين لها، فإن هؤلاء المستخدمين في حاجة إلى حماية قانونية قوية وواضحة، تطفل للمتعاملين مع هذه التقنية حقوقهم وخصوصياتهم وأموالهم، وتضمن للمجتمعات أمنها ومصالحهم.

ومن أجل طبيعة جرائم تقنية المعلومات وخصوصية أساليبها، والمختلفة في جوانب كثيرة عن الجرائم التقليدية من الناحيتين الموضوعية والاجرائية، أصبحت الحاجة ملحة لإفراد جرائم المعلوماتية بأنظمة تخصها، وعقوبات تميزها، وتحدد بشكل دقيق تلك الجرائم وأركانها وعقوباتها[2].

لذلك أبين في هذا البحث جرائم المعلوماتية ومكافحتها وعقوباتها في المملكة العربية السعودية، سائلا الله التوفيق والسداد.

[1] محمد أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، 2005م، ص353.
[2] هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، ط1، 1994م، ص16.

منهج الدراسة

المنهج المتبع في هذا الدراسة هو المنهج الوصفي الذي يقوم على تحليل المضمون ومناقشته، والمنهج التأصيلي الذي يقوم بالتأصيل الفقهي الشرعي والقانون النظامي لما يحتاج إلى تأصيل شرعي أو نظامي، وذلك اعتمادا على النظام السعودي والاجتهادات الفقهية والقانونية من خلال آراء الفقهاء والشراح.

أسئلة الدراسة

1) ما هي الجرائم المعلوماتية؟
2) كيف يمكن الإبلاغ عن الجرائم المعلوماتية؟
3) كيف يمكن ضبط تلك النوع من الجرائم؟
4) كيف يمكن معالج آثار تلك الأنواع من الجرائم للحد من انتشارها؟

أهداف الدراسة

يهدف هذا البحث إلى معرفة الجرائم الإلكترونية، والجرائم تقنية المعلومات، كما يشجع على الإبلاغ عنها، كما سيساعد على سهولة ضبطها وسرعة معالجة آثارها والحد من انتشار تلك الآثار، كما سيوفر هذا البحث تصورا واقعيا عن كيفية تنفيذ الإجراءات المقترحة.

أهمية الدراسة

تتجلي أهمية الدراسة في تسليط الضوء على الجرائم الرقمية، والحد من انتشارها والوقوف على أسبابها، وتتمثل كذلك أهمية الدراسة في توضيح وشرح الجريمة الرقمية والمجرم الرقمي وأسباب الجريمة الرقمية وأهداف المجرم فيها ونتائج الجريمة الرقمية، والتي يقع ضحيتها الكثير من الأشخاص والفئات في المجتمعات المختلفة وكذلك تحليل القواعد القانونية الملائمة لمثل هذه الجرائم المستحدثة.

كذلك تتضح أهمية ذلك البحث في تثقيف الكثير من الفئات في مجتمعنا، وتوجيه الأنظار نحو هذا الشكل المستحدث من الجرائم حيث تشير الكثير من الاستفتاءات والأبحاث الميدانية إلي أن شريحة كبيرة من الأشخاص في مجتمعنا العربي يجهلون مثل هذه الجرائم الحديثة، أو لا يلقون لها بالا، كنوعية من عدم التصديق أو الجهل بها مما يسهل عملية وقوعهم فريسة لمثل هذه الجرائم بكل سهولة سواء كان ذلك جهلا منهم بنوعية الجرائم المستحدثة، أو حسن نية فكلاهما سواء، لذا تتجه هذه الدراسة نحو توعية مثل هذه الفئات نحو مثل هذه الجرائم وكيفية الوقاية منها، وماهي الإجراءات القانونية المتبعة في حال حدوث تلك الجرائم وبجانب التوعية يأتي دور الردع العام عن طريق شرح وتحليل

القواعد القانونية، والتي تكافح مثل هذه الجرائم الخطيرة والحد من انتشارها لما لها من تأثير سلبي يهدد المجتمعات ويزعزع أمنها ويهدر كل مبادئ الخصوصية وينتهك ممتلكات الغير بطريقة احترافية.

لذا نجد لهذه الدراسة أهمية مزدوجة، الأولي من جانب التوعية، والثانية من جانب الردع العام لمثل هذه الجرائم المستحدثة والخطيرة، والثالثة في تكييف الوقائع المادية وتحديد القانون الواجب التطبيق.

مشكلة الدراسة

يمكننا طرح إشكالية البحث في التساؤل الرئيسي الآتي:

ما هي سمات الجرائم المعلوماتية وما هي آليات مكافحتها في كل مجتمع المعلومات؟ كما يتفرع من هذا التساؤل الرئيسي التساؤلات الفرعية التالية:

- ما هو المقصود الجرائم المعلوماتية؟
- ما هي آليات مكافحة الجرائم المعلوماتية؟
- ما هو مفهوم مجتمع المعلوماتية؟
- ما هي طرق الحد من الجرائم المعلوماتية في ظل مجتمع المعلوماتية.

خطة الدراسة

المبحث الأول: الجريمة المعلوماتية في النظام السعودي وأنواعها.

- المطلب الأول: تعريف الجريمة المعلوماتية.
- المطلب الثاني: أركان وأنواع الجريمة المعلوماتية.

المبحث الثاني: الإجراءات القانونية للجرائم المعلوماتية في المملكة العربية السعودية وطرق إثباتها وعقوبتها.

- المطلب الأول: إثبات الجرائم ذات التقنية العالية.
- المطلب الثاني: العقوبات المقررة لارتكاب الجرائم ذات التقنية العالية.

المبحث الأول: الجريمة المعلوماتية في النظام السعودي وأنواعها

تعد الجريمة المعلوماتية الأكثر انتشارا وأصبح أمرا واقعا في ظل الثورة الرقمية، والتطورات الهائلة في وسائل الاتصال الحديثة، وتضم الجريمة المعلوماتية العديد من الأشكال والتي يصعب حصرها، وقد تشهد تطورا ملحوظا حول أساليب الجرائم الأخرى والتي تهدد جميع بلدان العالم.

وتعد الجرائم المعلوماتية من الجرائم المستحدثة، والتي انتشرت في عصرنا الحديث ويعود السبب إلى ارتباط مثل هذه الجرائم بالتقنيات الحديثة من الشبكة العالمية وأجهزة الحاسوب، والمواقع الإلكترونية.

وقد شكلت الجرائم المعلوماتية تهديدا كبيرا على المجتمع في المملكة العربية السعودية من النواحي الاجتماعية والاقتصادية والأمنية، مم جعل من الأهمية دراسة هذه الجرائم وتحليلها، وتوضيح أركانها، وسمات مرتكبيها والأثر المترتب عنها.

لذلك سوف نتطرق في المبحث إلى مطلبين:

المطلب الأول: تعريف الجريمة المعلوماتية وأركانها وأنواعها.

المطلب الثاني: أركان وأنواع الجريمة المعلوماتية

المطلب الأول: تعريف الجريمة المعلوماتية وأركانها وأنواعها.

توجد الجرائم بوجود الإنسان وتتطور بتطوره، وبما أن الإنسان دائما في تطور مستمر بفضل ثورة المعلومات والتكنولوجيا المتطورة، تطورت أيضا نوعية الجرائم من جرائم تقليدية تتميز بالعنف، إلى جرائم حديثة تتميز بالدقة واليسر وتعرف بالجرائم المعلوماتية، وحتى الوقت الحالي لا يوجد تعريف مانع جامع لهذا النوع من الجرائم.

مفهوم الجريمة في اللغة

هناك عدة تعريفات للجريمة ولكن تختلف من تشريعات إلى آخري، ومن علم إلى أخر، على الرغم من أن الجريمة لا يمكن أن تتغير في جوهرها ولكن يمكن طرحها في العديد من الأشكال كلا على حسب المصادر والنظم والأوامر.

وعطفا على ما سبق هناك العديد من التعريفات في الشريعة الإسلامية بأنها:" إتيان فعل محرم معاقب على فعله، أو ترك فعل واجب معاقب على تركه"[3].

[3] عبد القادر عودة، التشريع الجنائي الإسلامي مقارنة بالقانون الوضعي، مؤسسة الرسالة، مج1، بيروت، 1401هـ، ص40.

وتعرف الجريمة لغة بأنها:" الذنب والتعدي، يقال جرم فلان جرما أي ذنب، وهي مشتقة من الجرم بمعنى القطع والكسب واستعملت بمعنى التعدي والذنب والحمل على الفصل خملا آثما، فالجريمة مفرد وجمعها جرائم والجرم هو التعدي أو الذنب وقال تعالي (لا يجرمنكم شنئنا قوم)[4] أي لا يحملنكم على الخطأ.

أما من المنظور القانوني فقد تم تعريفها بأنها كل سلوك إيجابي أو سلبي يقع بالمخالفة لأحكام القانون"[5].

أما تعريف الجريمة في النظام السعودي، لم يتطرق النظام السعودي لتعريف الجريمة بصفة عامة، وإنما اكتفي بتعريفها على ما ورد في الفقه الإسلامي، بأنها:" إتيان فعل محرم معاقب على فعله، أو ترك فعل محرم"، أو هي " فعل أو ترك ما نصت الشريعة على تحريمه والعقاب عليه"[6].

وعطفاً على ما سبق يمكن القول أن الجريمة هي كل فعل إيجابي أو سلبي صادر عن إرادة إجرامية، يقرر له المنظم عقوبة أو تدبير احترازي، كما أننا لا نجد اختلاف في تعريف الجريمة في النظام السعودي عن تعريف الجريمة في الشريعة الإسلامية.

مفهوم الجريمة المعلوماتية:

تعرف الجريمة الرقمية بأنها "سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محله معطيات الحاسوب"[7].

كما عرفت بأنها "أنماط من الجريمة تستخدم فيها التقنية الحديثة من أجل تسهيل عملية الإجرام "[8].

كما عرفت الجريمة المعلوماتية أيضا بأنها "النشاط الإجرامي الذي تستخدم فيه التقنية الإلكترونية الرقمية بصورة مباشرة أو غير مباشرة، كوسيلة لتنفيذ الفعل الإجرامي المستهدف"[9].

وقد عرفت الجريمة المعلوماتية أيضا بأنها "أية جريمة يمكن ارتكابها بواسطة نظام حاسوب، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[10].

---

[4] سورة المائدة، الآية رقم (8).
[5] خالد بن مسعود البشر، مكافحة الجريمة في المملكة العربية السعودية، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 1424هـ، ص21.
[6] زكريا احمد عمار، الحلقة العلمية، الدليل الرقمي والتحقيق في الجرائم الإلكترونية، كلية علوم الأدلة الجنائية، جامعة نايف العربية للعلوم الأمنية، 1429هـ، ص15.
[7] أحمد خليفه الملط، الجرائم المعلوماتية، دار الفكر الجامعي الاسكندرية، ط2، 2006م، ص87.
[8] محمد حماد مرهج البيهتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، عمان، 2004م، ص165.
[9] خالد عباد الجلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، الأردن، ط1، 2001، ص30.
[10] أحمد أنور بدر، الجديد في الاتصال العلمي، دار الثقافة العلمية، مكتبة كلية الآداب، القاهرة، 2001م، ص17.

كما تعرف أيضا بأنها "الجريمة التي يتم ارتكابها إذا قام الشخص ما بطريقة مباشرة أو غير مباشرة في استغلال الحاسوب أو تطبيقاته بعمل غير مشروع وضار للمصلحة العامة، ومصلحة الأفراد الخاصة"[11].

كما عرفها نظام مكافحة جرائم المعلوماتية السعودي بأنها "أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام".

ونلاحظ من التعريفات السابقة، أن الجريمة المعلوماتية هي جريمة ناشئة من التطور التكنولوجي، وتزداد بمدي التطور الذي يطرأ عليه، ومرتبطة ارتباطا وثيقا بالتكنولوجيا التي تعتمد على الحواسيب وغيرها من الأجهزة التقنية المستحدثة والتي تتطور معها الجريمة الرقمية.

ونستخلص من خلال هذه التعريفات أن التعريف الأعم والأشمل للجريمة الرقمية هو أنها "الجريمة التي تتم باستخدام الحاسب الآلي، أو تلك التي تقع على الحاسب الآلي ذاته".

ويتضح من التعريف السابق أن الجريمة المعلوماتية لها ركنان أساسيان، مادي ومعنوي أي لكي يعد الفعل جريمة تستوجب العقاب لابد من توافر هذان الركنان، فالركن المادي يتعلق بإتيان الفعل الذي يشكل الجريمة، سواء كان إيجابيا كالفعل أو سلبيا كالامتناع عن فعل، وأما الركن المعنوي فهو يتعلق بمدي مسؤولية الجاني الجريمة، وهو ما يعرف بالقصد الجنائي وفيما يلي شرح كل من الركن المادي والمعنوي للجريمة المعلوماتية.

المطلب الثاني: أركان وأنواع الجريمة المعلوماتية

الركن المادي:

وهو النشاط أو السلوك أو الفعل الذي يشكل الجريمة، والذي يتطلب وجود بيئة رقمية واتصال بالشبكة العالمية، ولا يتصور قيام الجريمة الرقمية بغير الركن المادي، وهو يتكون من ثلاث عناصر أساسية؛ هي الفعل والنتيجة الإجرامية وعلاقة السببية بينهما، ويظهر الركن المادي في الجريمة عند تنفيذ الفعل المحظور سواء كان الفعل إيجابيا أم سلبيا، وقد ينهي المجرم الجريمة باكتمال أركانها وتعتبر جريمة تامة، وقد يضبط الجاني قبل الشروع في تنفيذ الجريمة، وهو ما يعرف بالشروع في الجريمة، وقد يرتكب الجريمة أكثر من جاني، وهو ما يسمي بالاشتراك في الجريمة ويتكون الركن المادي من ثلاث عناصر كما ذكرنا نوردها فيما يلي:

الفعل أو السلوك، كأن يقوم الجاني بإعداد البرامج والحاسوب وتحميله بملفات وبرامج اختراق، أو أن يقوم بإعداد برامج فيروسات تمهيدا لبثها[12].

[11] نهلا عبد القادر المومني، الجريمة المعلوماتية، ط2، 2010م، دار الثقافة، ص48.

ويدور التساؤل هنا أنه إذا افترضنا أن الركن المادي يتشكل أولا من الفعل أو السلوك فهل يشكل الفعل أو الأعمال التحضيرية في الجرائم الرقمية جريمة أم لا؟ وأجاب عن هذا التساؤل المنظم السعودي في المادة العاشرة من نظام جرائم المعلوماتية بأنه "يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة".

النتيجة الإجرامية:

وتعد من أهم عناصر الركن المادي لأي جريمة، وتعد هي الأثر المباشر للسلوك الإجرامي غير المشروع، وفي كثير من الأحيان لا يحدد النظام أوصاف السلوك علي وجه التفصيل، بل يكتفي بذكر النتيجة الإجرامية.

أما الجريمة الرقمية فهي مثل غيرها من الجرائم، والتي يتطلب وجود النتيجة الإجرامية بها كعنصر من عناصر الركن المادي للجريمة وكأساس له.

علاقة السببية:

تعتبر علاقة السببية عنصر هام من عناصر الركن المادي للجريمة وهي تعد حلقة الوصل بين النتيجة الإجرامية والسلوك الإجرامي، وذلك بثبوت أن السلوك الغير مشروع، هو سبب هذه النتيجة الإجرامية أي أنه بدون هذا السلوك لم تتحقق النتيجة الإجرامية، وأيضا فإن علاقة السببية هذه تساهم في تحديد نطاق المسؤولية الجزائية[13].

وتعد علاقة السببية أساسية لقيام كافة الجرائم الرقمية، وكذلك تعد عنصر أساسي من عناصر الركن المادي لأي جريمة رقمية.

الركن المعنوي

وهو عنصر أساسي لقيام المسئولية الجزائية، وبدون هذا الركن لا تقوم الجريمة فهو الوجه الباطني النفسي للسلوك الذي قام به الجاني، فلا يسأل شخص عن جريمة ما لم تقم علاقة بين ركنها المادي والإرادة الإجرامية للجاني، وهو ما يعرف بالقصد الجنائي، وعليه تتحدد صورة القصد للجريمة مقصودة أم اتخذ صورة الخطأ الذي به تتكون الجريمة غير مقصودة[14].

---

[12] أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الآلي، ط1، دار النهضة العربية للنشر والتوزيع، القاهرة، 2000م، ص125.

[13] ماجد عمار، المسؤولية القانونية الناشئة عن استخدام فيروس الكمبيوتر ووسائل حمايتها، دار النهضة العربية، القاهرة، 1989م، ص122.

[14] أحمد خليفة الملط، الجرائم المعلوماتية، ط2، دار الفكر الجامعي، القاهرة، 2006م، ص187.

فالقصد الجنائي هو اتجاه الإرادة على نحو معين تحت سيطرة الركن المادي، وذلك تعبير عن خطورة الجاني، وهو النتيجة المؤكدة والحتمية على الإدانة للجاني أمام المحكمة متي تبين للمحكمة صدق إرادة الجاني.

ويعد الركن المعنوي للجرائم الرقمية كغيره من أهم أركان الجريمة، وبغيره لا تتحقق المسؤولية الجزائية لجريمة الرقمية، وتعد الجرائم الرقمية كغيرها من الجرائم والتي تفترض أساسا وجود القصد العام (العلم، والإرادة) وذلك لتحديد المسؤولية الجنائية، ولا يمكننا التصور بوجود القصد الخاص في الجرائم الرقمية دون أن يسبقه القصد العام، فأما عن وجود القصد في الجرائم الرقمية فهو يرجع إلي طبيعة الجريمة المرتكبة والنية الخاصة لدي المجرم من وراء قيامه بالفعل الغير مشروع أو ارتكاب الجريمة، فكل جريمة رقمية تختلف عن غيرها من الجرائم الرقمية الأخرى من حيث أركانها وماهيتها، وطبيعتها[15].

ففي بعض الجرائم الرقمية وبحكم طبيعتها لا يتطلب لقيامها، وقيام الركن المعنوي فيها وجود قصد خاص، فمثلا في جريمة التعدي على برامج الحاسب الآلي نجدها من الجرائم العمدية التي لا تقوم إلا بتوافر القصد الجنائي العام (العلم، والإرادة) لدي الجاني فيشترط في الجاني فقط علمه التام بأن ما يقوم به من نشاط هو غير مشروع.

ونري أن القصد العام والخاص في الجرائم الرقمية هو أساس تحديد المسؤولية الجزائية، والذي يحدد وجود قصد خاص في بعض الجرائم الرقمية، وكذلك نية الإضرار، والتي نستشفها من مكونات كل جريمة على حدة، وبشكل مستقل وعليه فإن الجرائم الرقمية باعتبارها جرائم مستحدثة هي كغيرها من الجرائم التقليدية والتي تشترط وجود الركن المعنوي لقيام الجريمة[16].

وتتولي هيئة التحقيق والادعاء العام التحقيق والادعاء عبء إثبات مدي توافر الركن المعنوي.

أنواع الجرائم المعلوماتية:

1- جرائم التخريب المعلوماتي لمكونات نظم المعلومات الرقمية مثل:

- التخريب المنطقي وتستهدف تلك الصور من الجرائم أنظمة التشغيل والبرامج وكذلك قواعد البيانات كاستعمال برامج خبيثة تصيب مكونات النظام الرقمي.
- التخريب المادي وتتم مثل هذه الجرائم من خلال الاختراق أو الإغراق بالمياه وما يرتبه من أضرار بالأجهزة والمعدات أو تعطيلها أو إتلافها.

[15] مروان مرزوق الروقي، القد الجنائي في الجرائم المعلوماتية، مكتبة القانون والاقتصاد، الرياض، 1434هـ، ص64.
[16] محمد بن عبد الله بن علي المنشاوي، جرائم الإنترنت في المجتمع السعودي، أكاديمية نايف للعلوم الأمنية، الرياض، 1434هـ، ص119.

ومن أمثلة هذه الجرائم في نظام مكافحة جرائم المعلوماتية السعودي:

- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها[17].
- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، وإتلافها، أو تعديلها.

2- جرائم النصب والتلاعب الرقمي وتعتمد على الأساليب التالية:

- التلاعب أثناء إدخال البيانات حيث يتعمد مرتكبي الجريمة الرقمية إدخال بيانات مزورة وغير صحيحة أو منع إدخال بيانات صحيحة أو وثائق معينة.
- التلاعب في أنظمة المعالجة الرقمية للبيانات عن بعد.
- التلاعب أثناء إعداد وتطوير البرامج فهنا يمكن لمرتكبي الجريمة الرقمية إدخال بعض التعديلات الغير شرعية مما يحقق أهداف غير مشروعة.

ومن أمثلة جرائم التلاعب الرقمي في النظام السعودي:

- الاستيلاء لنفسه أو للغير على مال منقول أو علي سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.
- 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 تتيح من خدمات[18].

3- جرائم التجسس والقرصنة الرقمية وتعتمد على الأساليب الأتية:

- أساليب فنية وهي التي تعتمد على الفكر التكنولوجي والتقنيات الرقمية الحديثة والبرامج والمعدة خصيصا للتجسس والتنصت.
- القرصنة الرقمية (الإلكترونية) كالنسخ الغير قانوني للبرامج.

4- الجرائم الرقمية المتعلقة بخصوصه وسلامة الأفراد والجرائم المنافية للآداب العامة، كما أوردتها المادة السادسة في نظام مكافحة جرائم المعلوماتية.

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

[17] مصطفي محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مطابع الشرطة، القاهرة، ط1، 2008م، ص196.
[18] ميسون خلف حمد الحمدان، مشروعية الأدلة الالكترونية في الإثبات الجنائي، كلية الحقوق، جامعة النهرين، 2016م، ص55.

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

5- الجرائم الرقمية السياسية كإنشاء مواقع إلكترونية ذات اتجاهات متطرفة، وقد أوضحت المادة السابعة من نظام مكافحة جرائم المعلوماتية السعودي هذه الجرائم على النحو التالي:

- إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره؛ لتسهيل الإيصال 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.
- الدخول 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.

الجريمة الرقمية في النظام السعودي

تبذل المملكة العربية السعودية جهودا كبيرة في عملية تنظيم تقنية المعلومات وحمايتها من الجرائم التي تقع ضدها، ويوضح النظام السعودي أن الجرائم الرقمية هي عبارة عن جرائم تقع عن طريق الحاسب أو الشبكة العالمية، وتعتبر هذه الجرائم من الموضوعات الهامة التي تثير العديد من الجوانب الجديدة، والتي يرجع اتصالها اتصالا مباشرا بتطور وسائل التعاملات، وذلك بسبب انتشار استخدام الحاسب الآلي والشبكة العالمية فقد أصبحت هذه الشبكة ذات طابع دولي يتاح لجميع الأفراد في العالم التعامل من خلالها، وذلك بإبرام الصفقات المختلفة وتبادل المعلومات والمراسلات الخاصة[19].

(1) جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، القاهرة 2002، دار النهضة العربية، صفحة 6.

فالتعاملات التي تتم عن طريق الوسائل الرقمية أصبحت تشكل قمة في التطور المتبادل بين الأفراد والشركات والجهات المختلفة، فقد كان على المشتري أن يتقابل مع البائع فيما يعرف بمجلس العقد، والذي يلتقي فيه الإيجاب والقبول، ثم تطور ذلك وأصبح مجلس العقد أكثر اتساعا بتطور وسائل الاتصالات، ومنها الاتصالات الهاتفية والفاكس.

وبناء على التطور في الوسائل والتعاملات الرقمية فقد وافق مجلس الوزراء في 1428/3/7هـ والموافق 2007/3/26م على نظامي مكافحة جرائم المعلوماتية ونظام التعاملات الإلكترونية، وكان ذلك للحد من وقوع الجرائم الرقمية وتحديد الجرائم المستهدفة بالنظام والعقوبات المقررة لكل جريمة.

[19] محمد مروان نظام الأثبات فب المواد الجنائية في القانون الوضعي الجزائري، دوان المطبوعات الجامعية، الجزائر، 1999م، ج2، ص327.

المبحث الثاني: الإجراءات القانونية للجرائم المعلوماتية في المملكة العربية السعودية وطرق إثباتها وعقوبتها

أدى انتشار المعلومات السريعة عبر وسائل الاتصال المختلفة إلى تدفق هائل في المعلومات والأخبار والمعارف والأبحاث والرسائل الثقافية، يعجز الإنسان بقدراته العادية عن متابعتها والإلمام بها في عمر القصير.

كما أن حدوث طفرة في تقنية المعلومات تمثلت في اختراع الحاسب الآلي الذي أضاف للإنسان قدرات هائلة على الاحتفاظ بالمعلومات ومعالجتها بسرعة خيالة لم تكن تخطر على باله من قبل، وهكذا تتضح إيجابيات الثورة المعلوماتية والتكنولوجية التي جاء بها الحاسب الآلي وقدراتها على تغيير أوجه الحياة إلى الأفضل، بالإضافة إلى أن الثورة المعلوماتية ذاتها تحمل في طياتها بذور الشر المتمثلة في الاستخدام غير المشروع لنظام الحاسب الآلي والوسائط التكنولوجيا الأخرى[20].

فترتب علة ذلك ظهور أنواع جديدة من الجرائم المعلوماتية، التي تتم من خلال الحاسوب، والتي أصبحت ظاهر إجرامية جديدة ومستحدثة تقرع أجراس الخطر وتنبه المجتمعات الحديثة لحجم المخاطر والخسائر التي قد تنجم عن جرائم الحاسوب (الجرائم المعلوماتية)، حيث أن هذا النوع من الجرائم هي تقنية ناتجة عن استخدام التكنولوجيا الرقمية كأداة لتحقيق غايات غير قانونية تنشأ في الخفاء ويقترفها أناس أذكياء، يمتلكون أدوات المعرفة التقنية الحديثة، وبالمقابل لابد من تطوير وسائل إثبات بما يواكب هذه الطفرة التي حدثت في طرق ارتكابها، ومن هذه الجرائم انتهاك الخصوصية، وانتحال الشخصية، والعمل على سرقة الملكية الفكرية، وكذلك سرقة الهويات والاتجار بالمواد الإباحية، وتسريب المعلومات والمواد الإلكترونية المملوكة للمؤسسات والشركات سواء الحكومية أو الخاصة وتدميرها عن طريق فيروس، وغيرها من الجرائم التي تكون فيها الأجهزة والشبكات المحوسبة مسرحا أو وسيلة لتنفيذها[21].

كما وضح أن جرائم الاختراق هي الأولي في المملكة العربية السعودية من بين تلك الجرائم، ونتيجة لظهور هذا النوع من الجرائم الذي تسبب في أضرار لكثير من الافراد والمجتمع والبيئة التكنولوجيا، أصدر المنظم السعودي نظام مكافحة الجرائم المعلوماتية رقم (م/17) بتاريخ 1428/3/8هـ والمعدل بتاريخ 1436هـ.

[20] أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الآلي، ط1، دار النهضة العربية للنشر والتوزيع، القاهرة، 2000م، ص125.
[21] هلالي عبد اللاه أحمد حجية المخرجات الكمبيوترية في المواد الجنائية (دراسة مقارنة)، 2006م، ص89.

المطلب الأول: إثبات الجرائم ذات التقنية العالية

تتجلى طبيعة الجرائم المعلوماتية في قدرتها على نقل وتبادل المعلومات، حيث أن هذه المعلومات أما أن تكون معلومات ذات طابع شخصي ويكون الاعتداء فيها على الخصوصية، أو معلومات ذات طابع عام[22].

لذلك من الضروري التعرف على كيفية إثبات هذه الجرائم، والنظام القانوني الواجب تطبيقه على من يحاول استخدام هذه التقنية لغرض غير مشروع ويحاول التعدي على الآخرين إلكترونيا، فالدول المتقدمة تكنولوجيا مثل المملكة العربية السعودية وضعت قواعد موضوعية لمواجهة الاستخدام غير المشروع للحساب الآلي والانترنت، كما أجرت المملكة تعديلات على قوانينها الإجرائية تكفل مكافحة هذه الجرائم في إطار الشرعية الجنائية، ولأن المملكة أدركت أن هذه الجرائم ترتكب بتقنيات حديثة في عالم يختلف عن العالم المادي الذي عادة ما ترتكب فيه الجرائم بالطرق التقليدية وإجراءاتها، التي ترتكب بواسطة المجابهة بين الأشخاص كالقتل والايذاء والسرقة، فالقانون الجنائي التقليدي بشقية "الإجرائي والموضوعي" تم وضعه لمكافحة الاعتداءات المادية والمواجهة بين الأشخاص وجها لوجه، وإثبات الإدانة بإقامة الأدلة التي تثبت وقوع الجريمة[23].

بيد أن الجريمة التقنية أو المعلوماتية مختلفة عن هذه الجرائم التقليدية، فهي ترتكب في عالم افتراضي وعلى مسافات بعيدة، ويتطلب وجود بيئة رقمية واتصال بالإنترنت ومعرفة النشاط وما ينطوي عنه، ونتيجة، لذلك يعد الإثبات من أهم التحديات التي تواجهه الأجهزة الأمنية، فالإثبات هو تأكيد حق متنازع فيه له أثر قانوني بالدليل الذي أباحه القانون لإثبات ذل الحق.

كما عرفه الدكتور عبد الرازق السنهوري بقوله: "هو إقامة الدليل أمام القضاء بالطرق التي حددها القانون على وجود واقعة قانونية ترتب عليها آثارها".

أما بالنسبة لوسائل الإثبات فهي كثيرة ومتنوعة منها على سبيل المثال لا الحصر، البينة والإقرار والقرائن والكتابة واليمين، والخبرة والمحررات أو الدليل الكتابي، غير أن للخبرة دورا بارزا في مجال الجرائم ذات التقنية العالية، وهي إجراء يتعلق بموضوع يتطلب إلماما بعلم معين لإمكان استخلاص الدليل منه، فإنه الخبرة تفترض وجود شيء مادي أو واقعة يستظهر منها الخبير رأيه.

---

[22] زهير الكرمي، العلم ومشكلات الإنسان المعاصر، ط5، سلسة عالم المعرفة، الكويت، 1978م، ص21.
[23] وليد طه، التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابست، عضو قطاع التشريع بوزارة العدل جمهورية مصر العربية، ورقة بحثية.

ويعد تقرير الخبير من الأدلة، إما إجراء ندبه فهو إجراءات جمع الأدلة من شأنه المعاينة والتفتيش وضبط الأشياء، والخبرة تشمل معاينة القاضي وخبرة المتخصص والمتمرسين في استعمال الحاسوب والإنترنت وغيرها مما يحتاج إلى مزيد من علم ومعرفة وخبرة وتجربة في كثير من المجالات خصوصا في مجال الإلكترونيات مما لا يستطيع القاضي أو الإنسان العادي معرفتها بمجرد معلوماته العامة.

كما أن الجرائم المعلوماتية يصعب اكتشافها وإثباتها، وذلك يرجع إلى سمات هذا النوع من الجرائم وخاصة السرعة الفائقة التي ترتكب بها، وكذلك صفات المجرم الذي يقوم بارتكاب هذا النوع من الجرائم من حيل وغش عند استخدامه لتقنيات معلوماتية ذات كفاءة عالية، ومحور آثارها وطمسها قبل أن يتم اكتشافها[24].

حيث أن المجرم التقني لا يترك أثراً ملموساً لأنها تتم بتقنيات عالية، والجنات يكونوا على مستوى عالي من الذكاء، ما يمكنهم من العمل على تدمير وسائل الإثبات بعد ارتكابهم للجريمة، لأنه حتى الضحايا من الممكن ألا يكون في مصلحتهم إثبات أو القيام بشكوى للسلطات المعنية حتى يحفظوا ربما حياتهم الخاصة وخوفهم من أن تنتشر ويشهر بهم داخل الرأي العام، لذلك فإن مسألة الإثبات تكون شديدة الصعوبة.

ولكن على الرغم من ذلك توجد عدة طرق لجمع الأدلة عن الجرائم ذات التقنية العالية نسبة لطبيعتها الفنية المعقدة، ولكن توجد عدة طرق لجمع الأدلة عن الجرائم ذات التقنية العالية وفي نفس الوقت تعد من طرق الإثبات حتي يتم التوصل إلي الحقيقة، وهي المعاينة ومشاهدة الآثار المادية إن وجدت وعلى الرغم من أهمية المعاينة في إثبات حالة الجريمة لكن ربما لا تكون فعالة للضبط، كذلك التفتيش وهو البحث والاستقصاء والهدف منه ضبط أدلة الجريمة وكل ما يفيد في كشف الحقيقة، والشهادة والخبرة كما أسلفنا، والإثبات بجميع وسائل الأثبات إذا الأمر يتعلق بواقعة مادية للبيئة التقنية فإن الأمر لا يثير أي صعوبة، أي أن الضبط يرد بالأساس على الأشياء المادية محل الجريمة مثل الأثبات بالشهود ولكن في الأغلب على حسب ما يتم العمل به في جرائم الصحافة وجرائم أخرى متعلقة بجرائم القذف أو التشهير غالبا ما يتم الإثبات بتقنية تصوير الشاشة أو الاعتماد على أمر قضائي بمعاينة الصفحة الإلكترونية ومعاينة موضوع القذف أو التشهير وما شابه ذلك[25].

كما يمكن الإثبات عن طريق الدليل الرقمي ويكون هذا الدليل في شكل مجالات ونبضات مغناطيسية أو كهربائية، والذي يتم أخذها من أجهزة الحاسوب والعمل على جميعها وتحليلها باستخدام برامج

[24] طالب محمد جواد، جرائم تقنية المعلومات وإثباتها، مجلة الرافدين الجامعة للعلوم، العراق، 2011م، ص53-69.
[25] محمد مصطفي الزحيلي، وسائل الإثبات في الشريعة الإسلامية في المعاملات المدنية والأحوال الشخصية، ط1، دار البيان، دمشق، 1982م، ص22.

تكنولوجيا خاصة وتطبيقات، وهي مكون رقمي لتقديم معلومات إما أن تكون في شكل صور ورسومات أو أصوات أو نصوص كتابية، فالدليل الرقمي يمتاز عن الدليل المادي، فالبرامج والتطبيقات الصحيحة التي سيتم استخدامها ستحدد العبث أو التعديل الذي تم مقارنته بالأصل.

كذلك يمكن رصد معلومات عن الجاني من خلال الدليل الرقمي الذي يسجل تحركات وبعض الأمور الشخصية والعمل على تحليلها في ذات الوقت.

لذلك نري أن المسرح الحقيقي المادي للجريمة والمسرح المعلوماتي الرقمي واستخلاص وسائل الاستدلال يمكن أن يكون ثرية جدا بما تحتويه من معلومات للكشف عن المجرم، لابد أن يتحرى القاضي جيدا عن الأدلة الجريمة الرقمية وإن يكون ملما بالعمليات الإلكترونية وكل ما يتعلق بالجرائم التقنية وأن يستعين بأصحاب الخبرة والاختصاص التي تمكنه من اكتشاف الأدلة، لأن الأدلة التي يتحصل عليها من الوسائل الإلكترونية وما قد يصاحب الحصول عليها من خطوات معقدة فإن قبولها في الإثبات قد يثير الكثير من المشكلات والتلاعب والتغيير فيها[26].

وعطفا على ما سبق يتبن لنا أن الدليل الإلكتروني مثله مثل الدليل التقليدي، وسيلة من وسائل الأثبات حيث لا تقوم الجريمة الإلكترونية إلا في وجود دليل إلكتروني، غير أن الدليل الإلكتروني يختلف بعض الشيء عن الدليل التقليدي، حيث أنه دليل فنيا بحتا وقد يكون في شكل رسالة أو أرقام أو شفرات أو معلومات أو بيانات مشفرة أو حتى صور، كما أنه دليلا وهميا غير ملموس يسهل طمسه وإزالته واختراقه حتى بعد أن يتم العثور عليه، لذلك لابد من التعامل معه بشكل تقني عالي جداً[27].

المطلب الثاني: العقوبات المقررة لارتكاب الجرائم ذات التقنية العالية

ألزمت أنظمة مكافحة الجريمة المعلوماتية السعودية جملة من العقوبات تتناسب مع جسامة كل جريمة للحد من حدوثها، ولتكون رادعا لكل من تسول له نفسه الاعتداء على الناس والانتقاص من حقوقهم وزرع الخوف والقلق في نفوسهم، وذلك بالسجن لفترات وغرامات مختلفة بحسب الجريمة ونوعها ومقدار ما تسببه من ضرر، سواء اجتمعت الغرامتان معا، أو تم توقيع أي منها بشكل منفرد بقوله (أو بإحدى هاتين العقوبتين)[28]، وذلك وفق التوصيف التالي: نص المادة رقم (2) من قانون مكافحة الجرائم المعلوماتية على أنه يعاقب بالسجن مدة أقصاها عام واحد، بالإضافة إلى غرامة مالية

[26] مأمون محمد سلامة، الإجراءات الجنائية في التشريع الليبي، كلية الحقوق الجامعة الليبية بنغازي، ط1، ليبيا الجامعة اللبيبة، 1971م، ص306.
[27] فيصل بن معيض، هيئة التحقيق والادعاء العام ودورها في نظام العدالة الجنائية في المملكة العربية السعودية، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية،1999م، ص24.
[28] عبد الفتاح مصطفي الصيفي، تأصيل الإجراءات الجنائية، دار المعارف الجامعية، الإسكندرية 2002م، ص119.

لا تتجاوز خمسمائة ألف ريال سعودي، أو بأي من هاتين العقوبتين كل من يرتكب أيا من الجرائم المعلوماتية الآتية:

- الدخول غير المشروع لإلغاء البيانات الخاصة، أو حذفها أو تدميرها وإعادة إنشائها.
- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرنامج، أو البيانات الموجودة، أو المستخدمة فيها، أو تسريبها أو تعديلها.

كما تنص المادة السادسة على أن يعاقب بالسجن مدة لا تتجاوز الخمس سنوات، إضاقة إلى غرامة مالية حدها الأقصى ثلاثة ملايين ريال سعود، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

- إنتاج ما من شأنه المساس بالنظام العام أو القيم الدينية أو الآداب العامة، أو جرمة الحياة الخاصة أو إعداده أو إرساله أو تخزينه عن طريق الشبكة المعلوماتية، أو أجهزة الحاسب الآلي.
- يؤسس أو ينشر أي موقع على أجهزة الحاسوب أو شبكة الإنترنت المعلوماتية وذلك للإتجار أو تسهيل الإتجار بالجنس البشري.
- تأسيس أو نشر أي من المواقع على الشبكة المعلوماتية الإلكترونية أو على أي من أجهزة الحاسوب وذلك للإتجار أو الترويج أو نشر طرق التعاطي أو تيسير التعامل من خلالها بالنسبة إلى أنواع المخدرات، فضلا عن المؤثرات العقلية المختلفة.
- نشر أو إنشاء أو ترويج أي بيانات أو معلومات تتعلق بالشبكة الإباحية أو أي من أنشطة الميسر التي من شأنها الاختلال بالآداب العامة.

تنص المادة السابعة على أن يعاقب بالسجن مدة لا تزيد على عشر سنوا ت، بالإضافة إلى غرامة مالية لا تتجاوز خمسة ملايين ريال سعودي أو بأي منهما، لأي من مرتكبي الجرائم التالية:

- العمل على تأسيس أو نشر أي من المواقع للمنظمات الإرهابية والتي من شأنها تسهيل الوصول إلى المنظمات الإرهابية وقيادتها أو أعضائها أو العمل على الترويج إليها ولأفكارها أو تمويلها.

إضافة إلي نشر طريقة إعداد المتفجرات أو أي من الأجهزة أو مختلف الأدوات التي يتم استخدامها في العديد من العمليات الإرهابية.

- الدخول غير المشروع إلى مواقع إلكتروني، أو نظام معلوماتي مباشر، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني.

المادة الثامنة تنص على:" أن لا تقل عقوبة السحن أو الغرامة عن نصف حده الأعلى إذا اقترنت الجريمة بأي من الحالات الموضحة التالية:

- إذا شغل الجاني أي من الوظائف العامة أو الاتصال بين وظيفته والجريمة التي ارتكبها أو في حال ارتكابه الجريمة مستغلا سلطته أو نفوذه.
- إذا ارتكب الجاني أي من الجرائم من خلال العصابات المنظمة.
- صدور أحكام أجنبية أو محلية سابقة بالإدانة بحق الجاني في جرائم مماثلة.
- العمل على التغرير بالقصر، أو من في حكمهم والعمل على استغلالهم.

تنص المادة التاسعة على:" أن يعاقب كل من حرض غيرة أو ساعده أو اتفق معه ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، إذا وقعت الجريمة بناء على هذا أو الاتفاق أو التحريض أو المساعدة، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها، ويعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية".

المادة العاشرة تنص على أن المحكمة المختصة أن تعفي من هذه العقوبات كل من يبادر من الجناة بإبلاغ بعد العلم بالجريمة وتعين للإعفاء أن يكون من شأن الإبلاغ ضبط باقي الجناة في حال تعددهم، أو الأدوات المستخدمة في الجريمة

آلية التبليغ عن الجرائم ذات التقنية العالية

- يتم التبليغ عن الجرائم ذات التقنية العالمية في المملكة العربية السعودية من خلال الدخول لمنصة أبشر الإلكترونية، ثم الدخول إلى خدمات الأمن العام، ومن بعد ذلك إلي خدمة بلاغ الجريمة الإلكترونية ومن ثم تحديد أنوع البلاغات والقيام باستيفاء كافة الحقوق المطلوبة، يتم بعد ذلك النقر على حقل إرسال، وأخيرا وبعد إرسال البلاغ يتم تزويد المستخدم بالرقم المرجعي الخاص بالبلاغ.
- أتاحت المملكة رقما موحدا يتم من خلاله تلقي مختلف بلاغات الجرائم الإلكترونية، إضافة إلى توفير خدمة التوعية والتوجيه من خلال الاتصال على الرقم (1909).

الخاتمة

بعد دراستنا لموضوع الجرائم المعلوماتية، وفقا للنظام السعودي ذلك بالوقوف على أوجه الحماية التي من الهجمات الإلكترونية وفقا للنظام السعودي ذلك بالوقوف على أوجه الحماية التي وفرها النظام السعودي لحماية المجتمع من تل الهجمات وما ورد في هذا النظام بهذا الخصوص، فقد توصلنا من خلال البحث للعديد من النتائج ولكن قبل عرضها لابد من توضيح أن ما تم التوصل إليه من نتائج متعلقة بإثبات الجرائم المعلوماتية ذات التقنية العالية تشكل صعوبة لأنها متغيره ومتطورة، ولأن التقنية دائما تتطور بشكل كبير في هذا العالم الافتراضي وبسرعة مهولة.

النتائج

- من الضروري العمل والإشغال على معالجة أي خلل قد يحدث ثغرة قد تؤدي بتلك الجرائم أو خللا بالمجتمع، لذا لابد من العمل على توعيته بصورة دائمة وتثقيفية بالوسائل والطرق التي يستخدمها مجرمي التقنية.
- بعد إثبات الجريمة ذات التقنية العالية من أهم الصعوبات التي تعترض الأجهزة الأمنية، فإثبات هذه الجرائم أمر يستلزم الكثير من الجهد والخبرات الفنية المتدربة على أعلى المستويات والتأهيل، فنقص الخبرة يشكل عائقا أمام الإثبات.
- العمل بشكل دوري على حماية حواسبنا الشخصية بعمل برامج الحماية القوية.
- عدم حفظ أي شيء مهم سواء صورة شخصية أو ملفات مهمة قد تؤدي إلى مشارف الهلاك.
- إن معرفة الأسباب التي تجعل وجودا لي أي خلل في حواسيبنا بكل أشكاله تسهل وتوفر على المختص بسرعة الحماية وتكثيف الجهود والتواصل بسرعة لمرتكب الجريمة ومعرفة الهدف.
- عدم قدرة النصوص التقليدية في القانون الجزائي السعودي على مسايرة هذا النوع الجديد من الجرائم.
- الجرائم الرقية اقل عنفاً من الجرائم التقليدية أي أنها تحتاج إلى مجهود عضلي وبسيط، وتعتمد اعتماد كلياً على التفكير الذهني والعقلي المدروس القائم على معرفة بالتقنيات الحديثة للحاسب الآلي.
- اغلب الجرائم الرقمية تحتاج لتوافر القصد العام، والبعض منها يتطلب توافر القصد الخاص الذي يعد عنصراً من عناصر الركن المعنوي
- أبدع المنظم السعودي بمواكبة حجم التطور التقني في شتي المجالات الاقتصادية منها والاجتماعية، وقد أحسن صنعاً بإصدار نظام مكافحة الجرائم المعلوماتية ونظام التجارة الإلكترونية السعودي ونظام التعاملات الإلكترونية تأييداً منه على قدرة المملكة على المواكبة القانونية لحجم التطور القني ورؤية المملكة نحو2030.ءي

التوصيات

في ضواء النتائج التي تم التوصل إليها، يمكن حصر عدد من التوصيات التي قد تساهم في تفعيل إثبات الجرائم ذات التقنية العالية وذلك كما يلي:

- الاهتمام بتطور الخبراء الفنين لما لهم من دور أساسي وفعال في إثبات الجرائم ذات التقنية العالية، أو الجرائم المعلوماتية، وإتقانهم لهذا المجال والتمكن من نقل الأدلة دون تدميرهم أو إتلافهم وكل ما هو مسجل على دعامة ممغنطة.
- التوعية ونشر العلوم الشرعية المستنبطة من الكتاب والسنه والبعد بقدر المستطاع وتوضيح العقوبات الإسلامية للسرقة أو التشهير أو التجسس.

- كما أصبح الإرهاب عبر وسائل الاتصال من أكثر صور الجرائم ذات التقنية العالية، فأصبح الاختراق سهلا لهم فلابد لنا أن لا نفتح أي ثغرة لهذا الاستغلال وأن نحمي مجتمعنا من أي فكر دخيل أو مصدر منحرف لمنع الفساد ومحاربة كل مصدر فيه إجرام.
- العمل على التنسيق الدائم والمستمر ما بين الجهات القضائية والجهات الأمنية والجهات التي لها علاقة بالتكنولوجيا لمعرفة كل ما هو مستجد من تقنيات.
- الدورات المستمرة للقضاء وتعريفهم بكل ما هو جديد في مجال التقنية الحديثة من أساليب وأنواع.
- مشاركة المملكة في العديد من الاتفاقيات الدولية والمؤتمرات التي تجعل للمملكة السيطرة على المجرمين الذين يرتكبون أعمال إجرامية عبر السوائل الرقمية خارج حدود الدول نظرا لمبدأ إقليمية القوانين.
- إجراء التعديل التنظيمي بنظام مكافحة الجرائم المعلوماتية ليوضح مدي مسؤولية مزودي الخدمات عما بيثونه عبر الشبكة العالمية.
- تعزيز دور هيئة الاتصالات وتقنية المعلومات في أداء دورها في مكافحة الجرائم الرقمية لكي يتسنى لها تقديم لدعم الفني والمساندة للجهات الأمنية المختصة خلال مرحلة الضبط والتحقيق أثناء المحاكمة.
- إعطاء التراخيص اللازمة لأكثر من شركة لكي تعمل على تقديم التقارير الفنية والتقنية التي تفيد بوقوع الجريمة الرقمية، واعتبار هه التقارير أدلة جزائية رقمية وإحكام السيطرة على مثل هذه الشركات عبر هيئة تنظيم الاتصالات وتقنية المعلومات ووزارة الداخلية، ضرورة التنسيق بينها وبين الجهات القضائية والأمنية.

قائمة المراجع

1) عبد الفتاح مصطفي الصيفي، تأصيل الإجراءات الجنائية، دار المعارف الجامعية، الإسكندرية 2002م.
2) محمد مصطفي الزحيلي، وسائل الإثبات في الشريعة الإسلامية في المعاملات المدنية والأحوال الشخصية، ط1، دار البيان، دمشق، 1982م.
3) مأمون محمد سلامة، الإجراءات الجنائية في التشريع الليبي، كلية الحقوق الجامعة الليبية بنغازي، ط1، ليبيا الجامعة الليبية، 1971م.
4) فيصل بن معيض، هيئة التحقيق والادعاء العام ودورها في نظام العدالة الجنائية في المملكة العربية السعودية، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية،1999م.

5) وليد طه، التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابست، عضو قطاع التشريع بوزارة العدل جمهورية مصر العربية، ورقة بحثية.
6) طالب محمد جواد، جرائم تقنية المعلومات وإثباتها، مجلة الرافدين الجامعة للعلوم، العراق، 2011م.
7) أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الآلي، ط1، دار النهضة العربية للنشر والتوزيع، القاهرة، 2000م.
8) هلالي عبد اللاه أحمد حجية المخرجات الكمبيوترية في المواد الجنائية (دراسة مقارنة)، 2006م.
9) زهير الكرمي، العلم ومشكلات الإنسان المعاصر، ط5، سلسة عالم المعرفة، الكويت، 1978م.
10) أحمد خليفة الملط، الجرائم المعلوماتية، ط2، دار الفكر الجامعي، القاهرة، 2006م.
11) مروان مرزوق الروقي، القد الجنائي في الجرائم المعلوماتية، مكتبة القانون والاقتصاد، الرياض، 1434هـ.
12) محمد بن عبد الله بن علي المنشاوي، جرائم الإنترنت في المجتمع السعودي، أكاديمية نايف للعلوم الأمنية، الرياض، 1434هـ.
13) أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الآلي، ط1، دار النهضة العربية للنشر والتوزيع، القاهرة، 2000م.
14) ماجد عمار، المسؤولية القانونية الناشئة عن استخدام فيروس الكمبيوتر ووسائل حمايتها، دار النهضة العربية، القاهرة، 1989م.
15) عبد القادر عودة، التشريع الجنائي الإسلامي مقارنة بالقانون الوضعي، مؤسسة الرسالة، مج1، بيروت، 1401هـ.
16) خالد بن مسعود البشر، مكافحة الجريمة في المملكة العربية السعودية، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 1424هـ.
17) زكريا احمد عمار، الحلقة العلمية، الدليل الرقمي والتحقيق في الجرائم الإلكترونية، كلية علوم الأدلة الجنائية، جامعة نايف العربية للعلوم الأمنية، 1429هـ.
18) أحمد خلبفه الملط، الجرائم المعلوماتية، دار الفكر الجامعي الاسكندرية، ط2، 2006م.
19) محمد حماد مرهج البيهتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، عمان، 2004م.
20) خالد عباد الجلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة، الأردن، ط1، 2001.
21) أحمد أنور بدر، الجديد في الاتصال العلمي، دار الثقافة العلمية، مكتبة كلية الآداب، القاهرة، 2001م.

22) نهلا عبد القادر المومني، الجريمة المعلوماتية، ط2، 2010م، دار الثقافة.
23) محمد أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، 2005م.
24) خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، ط1، 2009م.
25) هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، ط1، 1994م.
26) كمال محمد عواد، الضوابط الشرعية والقانونية للأدلة الجنائية، دار الفكر الجامعي، الإسكندرية، مصر، ط1، 2011.
27) محمد مروان نظام الأثبات فب المواد الجنائية في القانون الوضعي الجزائري، دوان المطبوعات الجامعية، الجزائر، 1999م، ج2.
28) مصطفي محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، ط1، 2008م، ص196.
29) ميسون خلف حمد الحمدان، مشروعية الأدلة الإلكترونية في الإثبات الجنائي، كلية الحقوق، جامعة النهرين، 2016م، ص55.