مجلة مستقبل العلوم الإجتماعية
Future of Social Sciences Journal
FSSJ

الاختصاص القضائي في الجرائم الإلكترونية وفقاً النظام السعودي

The relationship between neuroticism and future anxiety among children of unknown parentage in residential institutions

أ / خالد عايض آل حمدان الغامدي

جامعة الملك عبدالعزيز – المملكة العربية السعودية

DOI: 10.21608/fjssj.2023.215987.1158 **Url**:https://fjssj.journals.ekb.eg/article_307388.html
تاريخ إستلام البحث: ٢٠٢٣/٥/٢م **تاريخ القبول:** ٢٠٢٣/٦/٦م **تاريخ النشر:** ٢٠٢٣/٧/١٠م
توثيق البحث: الغامدي، خالد عايض آل حمدان. (٢٠٢٣). الاختصاص القضائي في الجرائم الإلكترونية وفقاً النظام السعودي. مجلة مستقبل العلوم الإجتماعية،ع. ١٤،ج.(٢)،ص-ص:٣-٢٦.

٢٠٢٣م

المجلد: الرابع عشر. **العدد**: الثاني. يوليو ٢٠٢٣م.

الاختصاص القضائي في الجرائم الإلكترونية وفقاً النظام السعودي

مستخلص:

تلقي الدراسة الضوء على موضوع الاختصاص القضائي في الجرائم الالكترونية من خلال استعراض النظرة القانونية لنظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية وما رتبة من عقوبات على تلك الجرائم كما تبين لنا ذات الدراسة مدى كفاية هذا القانون للحد من هذه الجرائم في المملكة العربية السعودية وتكمن أهمية هذه الدراسة من أهمية موضوعها حيث تتعرض للأنظمة السعودية في إبراز الجوانب القانونية التي تحكم الجرائم ذات التقنية العالية مع بيان خصائصها ومفاهيمها. ومن التوصيات يقترح الباحث على المنظم السعودي وهو في بداية تطبيق القضاء المتخصص في المملكة أن يبادر إلى إنشاء نيابات متخصصة (جهات تحقيق)، وكذلك إنشاء دوائر قضائية متخصصة بنظر الجرائم والمخالفات الناشئة عن عقود الجرائم الالكترونية بوجه عام، وأن يتم اختيار أعضاء النيابة العامة والقضاة المتخصصين في هذه الدوائر، ويقترح الباحث على الجهات ذات الاختصاص القضائي في المملكة بضرورة الاهتمام بتدريب رجال الضبط الجزائي والأشخاص المنوط بهم عملية الضبط في الجرائم والمخالفات المتعلقة بأنظمة الجرائم الالكترونية.

الكلمات المفتاحية: الاختصاص القضائي، الجرائم الإلكترونية، النظام السعودي.

Jurisdiction in cybercrime according to the Saudi system

Abstract:

The study sheds light on the subject of jurisdiction in cybercrimes by reviewing the legal view of the system for combating cybercrimes in the kingdom of Saudi Arabia and the rank of penalties for those crimes.the same study also shows us the adequacy of this law to reduce these crimes in the kingdom of Saudi Arabia. the importance of this study lies in the importance of its subject as it is exposed to the Saudi regulations in highlighting the legal aspects governing high-tech crimes with an indication of their characteristics and concepts. Among the recommendations, the researcher suggests to the Saudi regulator, which is at the beginning of the application of specialized judiciary in the kingdom, to initiate the establishment of specialized prosecution (investigation bodies), as well as the establishment of judicial departments specialized in the consideration of crimes and violations arising from contracts of cybercrimes in general, and to select members of the public prosecution and judges specialized in these departments,

and the researcher suggests to the competent authorities in the kingdom the need to pay attention to the training of criminal officers and persons entrusted with the seizure process in crimes and violations related to cybercrime regulations.

Keywords: Jurisdiction, cybercrime, the Saudi system.

المقدمة:

تتميز حياة الإنسان بممارسة أنشطة عديدة ترتبط بتكنولوجيا المعلومات والاتصالات، التي تتسم بالسرعة ووفرة المعلومات ومن بين ما أفرزه هذا التطور هو ظهور مصطلحات جديدة تعدت الحدود المادية والجغرافية وألغت جميع القيود التي تحد من حرية الإنسان في ممارسته لمعاملاته، ومن بين هذه المصطلحات الجديدة مصطلح (الجرائم الإلكترونية) الذي أصبح يتداول في الاستخدام العادي للأفراد.

مع زيادة انتشار شبكة الإنترنت وتوسع استخدامها في كل مجالات الحياة ودخول جميع فئات المجتمع إلى قائمة المستخدمين بدأت تظهر جرائم ذات طبيعة خاصة على هذه الشبكة وازداد عددها وتعددت صورها وأشكالها وتسمى هذه الجرائم بالجرائم الإلكترونية أو الجرائم المعلوماتية.

ولعل التطور المستمر للأنترنت وما تتميز به من سرعة في إعداد ونقل وتخزين المعلومات وما تتوفر عليه من السرية التامة جعلها بيئة ملائمة للإجرام بعيد عن أعين الجهات الأمنية، وما زاد الأمر سهولة وجود فراغ تشريعي على المستوى الداخلي والدولي.

وعلى هذا الأساس أفرزت الجريمة الالكترونية تحديات واضحة للقوانين الوضعية التي وضعت لمكافحة، ذلك أنها غيرت من صورتها التقليدية المتمثلة في صورتها المادية إلى أخرى معنوية وما ينتج عن ذلك من مشكلة في تفسير النصوص القانونية وحضر القياس في المواد الجنائية واصطدامها بمبدأ الشرعية الجنائية وهذه القيود من شأنها أن تساهم في إفلات الكثير من المجرمين من العقاب. (العابدين، ٢٠٢١، ص.٣٢)

- أهمية الموضوع:

١. بيان الاختصاص القضائي في أنظمة الجرائم الإلكترونية وأنواعها وتطورها في الفقه الإسلامي والأنظمة السعودية وهو موضوع ينطوي على جملة من الأحكام الفقهية والقانونية والقضائية المهمة.

٢. يعتبر موضوع الدراسة من الموضوعات الحديثة التي لم تنل حظها من البحث، حيث ينطوي هذا الموضوع على جملة من الأحكام الفقهية والنظامية والقضائية المهمة في الفقه الإسلامي وفي أنظمة الجرائم الإلكترونية السعودية.

٣. عدم وجود دراسات علمية تناولت موضوع البحث من الناحية الفقهية التحليلية التطبيقية حيث يأتي هذا البحث ليسد الفراغ البحثي في هذا الموضوع، وليكون معيناً للمتعاملين بأنظمة الجرائم الإلكترونية والأكاديميين والعاملين في المجال العدلي والحقوقي باعتبار سبقه.

٤. الاهتمام بالجرائم الإلكترونية وتعاملاتها أصبح أمراً واقعاً عملياً، لا يمكن تجاهله في الوقت الحالي، ومن المتوقع أن تحظى الجرائم الإلكترونية بتوسع وزيادة مستقبلية كبيرة في المملكة.

٥. التوسع الكبير في استخدام شبكة الانترنت وتعاملاتها سينتج عنه العديد من المنازعات في كافة المجالات، وخاصة فيما يتعلق بتطبيق الجزاءات القضائية بأنواعها المختلفة.

- أهداف الدراسة:

تهدف الدراسة الحالية إلى:

١. بيان المقصود الإختصاص القضائي النظام السعودي وبيان مفهوم الجزاء القضائي في مخالفة أنظمة الجرائم الإلكترونية.

٢. الوقوف على مفهوم الاختصاص القضائي في الجرائم الإلكترونية النظام السعودي.

٣. توضيح الاختصاص القضائي في الجرائم الإلكترونية النظام السعودي.

- مشكلة البحث:

تظهر إشكالية البحث في الاختصاص القضائي للجرائم المعلوماتية الواقعة، يستدعي دراسة تأثيراتها ومن ثم وضع استراتيجية واضحة المعالم للحد من الآثار والمخاطر الناجمة عن هذا النوع من الجرائم المعلوماتية.

- منهج الدراسة:

اتبعت الدراسة المنهج الوصفي التحليلي الذي يسعى للتعريف بالاختصاص القضائي للجرائم الالكترونية في النظام السعودي، وتحليل وتشخيص موضوع الدراسة من مُختلف جوانبها وأبعادها، بهدف التوصل إلى نظرة واضحة عن الآليات المُلائمة لمُكافحة هذه الظاهرة المُستحدثة، بالنظر لنتائج التجربة السعودية.

سيكون منهج الباحث قائم على الاستقراء والتحليل ومن ثم المقارنة والتطبيق وذلك بتتبع المسائل محل الدراسة وعرضها في النظام السعودي وأنظمة الجرائم الإلكترونية السعودية وذلك للوصول إلى حلول لمشكلة البحث وتساؤلاته، وذلك ببيان بيان موقف النظام السعودي من مسائل البحث.

تمهيد وتقسيم:

أورد المنظم السعودي النص في أنظمة الجرائم الإلكترونية على عدداً من الجزاءات يتم تطبيقها على المخاطبين بأحكام هذه الأنظمة، وذلك في حال مخالفتهم للضوابط والأحكام الواردة فيها، وتتنوع هذه الجزاءات ما بين الجزاء الجنائي في حال توافر أركان المسؤولية الجنائية في حق الشخص مرتكب هذه المخالفات، والتي تؤدي إلى إصابة الفرد بأضرار مع توافر القصد الجنائي، وهو ما يرتبه الشارع على مخالفة نظام المعاملات أو الجزاء الذي يترتب في حالة الاعتداء على حق خاص أو إنكاره.

وفي سبيل تطبيق هذه الجزاءات المقررة في أنظمة الجرائم الإلكترونية فإن المنظم السعودي منح الاختصاص بنظر كل نوع منها لجهة قضائية متخصصة، تتولى النظر في منازعاته وتطبيق أحكامه، وعليه فإننا نجد أن هناك اختصاص قضائي جنائي تختص به المحاكم الجزائية بتوقيع الجزاءات الجنائية الواردة في هذه الأنظمة، وكذلك هناك اختصاص قضائي مدني وتجاري بنظر الجزاءات المدنية والتجارية الواردة في تلك الانظمة، وكذلك اختصاص قضائي إداري بتوقيع الجزاءات الإدارية الواردة في تلك الأنظمة.

المبحث الأول

الاختصاص القضائي الجنائي في النظام السعودي

إن الهدف من وضع قواعد الاختصاص القضائي بوجه عام تتمثل في تحقيق المصلحة العامة، ويظهر ذلك من ناحية أولى في تنظيم وظيفة من وظائف الدولة وهي وظيفة السلطة القضائية، وتظهر من ناحية ثانية في رعاية مصالح كافة الأفراد بدون تمييز، حتى لو كان المستفيد منها خصماً بعينه في خصومة معينه بالذات.

ومما لا شك فيه أن المنظم يهدف الى تحقيق العدالة فيما يطرح على القضاء من وقائع جزائية، وهو في هذا السبيل يخول المحاكم الجزائية سلطة الفصل في القضايا التي تدخل في اختصاصاها النظامي، واضعاً نصب عينه مصلحة الجماعة لذا فإن توزيع الاختصاص بين مختلف المحاكم الجزائية من ورائه حكمة قصدها المنظم فيجب ان تكون المحكمة مختصة بالفصل في الجريمة المطروحة عليها واختصاصها يتحدد بأمور ثلاثة للشخص والنوع والمكان، فينبغي ان يدخل في اختصاصها سلطة محاكمة المتهم في الدعوى وان تختص بالفصل في الجريمة المطروحة عليها، وأخيراً يتعين أن تكون مختصة مكانياً بنظر هذه الدعوى.

ويقتضي بيان الاختصاص القضائي الجنائي في أنظمة التجارة الإلكترونية أن يتناوله الباحث في مطالب ثلاث على النحو التالي:

المطلب الأول: التعريف بالاختصاص الجنائي في النظام السعودي.

المطلب الثاني: الجريمة الالكترونية في النظام السعودي.

المطلب الأول

التعريف بالاختصاص الجنائي في النظام السعودي

أولاً: تعريف الاختصاص في اللغة:

الاختصاص مصدر من اختص يختص اختصاصاً إذا انفرد بالشيء ولم يشاركه فيه أحد، ولم يكن مشاعاً بينه وبين غيره، فيقال خاصة بالشيء خصاً وخصوصاً وخصوصية وخصوصي فضله وخصه بالود كذلك، والخاص والخاصة ضد العامة والتخصيص ضد التعميم واختص بالشيء خصه به.(لسان العرب،٢٠١٠،ص.١٨٣) التخصيص، والاختصاص والتخصص: تفرد بعض الشيء بما لا يشاركه فيه الجملة، وذلك خلاف العموم والتعميم والخاصة ضد

العامة(الأصفهاني،٢٨٤) قال الله تعالى: {وَاتَّقُوا فِتْنَةً لا تُصِيبَنَّ الَّذِينَ ظَلَمُوا مِنكُمْ خَاصَّةً وَاعْلَمُوا أَنَّ اللَّهَ شَدِيدُ الْعِقَابِ} (القرءان الكريم)

ثانياً: مفهوم الاختصاص في الاصطلاح

لا يخرج المعنى الاصطلاحي للاختصاص في عبارات الفقهاء القدامى عن المعنى اللغوي، فقد عرف علماء الأصول التخصيص والاختصاص بأنه: «قصر العام على بعض مسمياته أو أفراده.(الأصفهاني،٢٣٥) وهذا المعنى بنفسه يستعمله الفقهاء، فليس عندهم للفظ الاختصاص معنى آخر يختص بهم، وقد أفرد العلماء في علم الأصول باباً أسموه باب الخاص والعام بحثوا فيه قواعد التخصص والتخصيص.

ثالثاً: مفهوم الاختصاص الجنائي في النظام:

عرف البعض من شراح النظام الجنائي الاختصاص الجنائي "بأنه مباشرة ولاية القضاء الجنائي في نظر الدعوى الجنائية في الحدود التي رسمها القانون فإذا ما وقعت جريمة في مكان ما فلا بد من تحديد المحكمة المختصة بالنظر فيها وفقاً لقواعد الاختصاص المحددة قانوناً" (سلامة، ٢٠٠٦)

في حين عرف البعض الآخر من الشراح الاختصاص الجنائي بأنه " :منح سلطه لجهة معينه للفصل فيما قد يطرح عليها من قضايا.(الغامدي، ٢٠٠٤)

ومن خلال ما سبق يعرف الباحث الاختصاص القضائي الجنائي في أنظمة التجارة الإلكترونية بأنه: السلطة المخولة للقاضي أو للمحكمة الجزائية بالفصل في القضايا التي تعرض عليها، وفقاً لما رود النص عليه في نظام التجارة الإلكترونية والأنظمة ذات الصلة بالتجارة الإلكترونية ووفقاً للحدود والضوابط التي وضعها المنظم للجرائم التي تدخل في اختصاص تلك المحكمة والوارد النص عليها في هذه الأنظمة.

المطلب الثاني

الجريمة الإلكترونية في النظام السعودي

المطلب الأول: مفهوم الجريمة الالكترونية في النظام السعودي:

مفهوم الجريمة:

الجريمة هي كل فعل أو ترك ضار، له مظهر خارجي، ليس استعمالا لحق ولا قياما بواجب، يحرمه القانون ويفرض له عقابا، يؤديه إنسان أهل لتحمل المسئولية الجنائية(العتيبي،١٤١٣)

تنوعت تعريفات الجرائم الالكترونية فعند بعض الكتاب تعرف بأنها مجموع الجرائم التي تتصل بالحاسب او النظام المعلوماتي سواء كان ذلك النظام أو احد مكوناته المادية الاجهزة والمعدات–او غير المعنوية غير المادية البرامج او البيانات سواء المختزنة في الحاسب او المنقولة عن طريق شبكات الاتصال هو موضوع الاعتداء في الجرائم المعلوماتية أو الالكترونية أو كان نظام المعلوماتي بوجه عام او احد مكوناته المادية او غير المادية هو الاداة في ارتكاب هذه الجرائم(عباس،٢٠١٠) وهناك فريق اخر اعتمد معايير مختلفة منها الموضوع، او وسيلة ارتكاب الجريمة او سمات شخصية لدى الفاعل (العبيدي،١٤١٣) لتعريف الجرائم المعلوماتية. ومنهم من يرى انها (كل فعل او امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف الى الاعتداء على الاموال المادية او المعنوية)(العمري،٢٠١٠)

يلاحظ مما سبق ان شراح القانون لم يعتمدوا تعريفا موحدا يجمع شمل شتات الجرائم الإلكترونية، لذا نجد بعض الانظمة القانونية لم تورد تعريفا لمصطلح الجرائم المعلوماتية ومنها القانون السوداني في قانون جرائم المعلوماتية لسنة ٢٠٠٧ والقانون الإماراتي (قانون اتحادي رقم ٢ لسنة ٢٠٠٦ والخاص بمكافحة جرائم تقنية المعلومات وهو ذات ما انتهجه في قانون رقم ٥ لسنة ٢٠١٢)

عرف النظام السعودي الجريمة الالكترونية أي فعل يرتكب متضمنا استخدام الحاسب الألى او الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام(نظام مكافحة جرائم المعلوماتية لسنة ١٤٢٨هـ)

وهو ما يعد في تقديري خطوة حسنة تحسب للمنظم السعودي لان النص على تعريف الجريمة الإلكترونية بشكل محدد وواضح بهذا الشكل يساعد بدرجة كبيرة على المحاسبة والعقاب عليها.

فقد نصت المادة الأولى من نظام مكافحة جرائم المعلوماتية بأن الجريمة المعلوماتية هي " أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا كما عرفت نفس المادة التقنية النظام" كما تعرف بأنها "مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال، أو التفسير أو التأويل، أو للمعالجة، سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة

ونحن نرى أن المشرع السعودي جانبه الصواب بوضعه تعريف جامع مانع للجريمة المعلوماتية، حيث كان من الأجدى به أن يترك ذلك للفقه والقضاء من جهة، ومن جهة ثانية بقيت عدم حصر الجريمة المعلوماتية في إطار أفعال محددة تحسباً للتطور التكنولوجي والتقني في المستقبل الذي من الممكن أن يفرز أخرى قد لا يشملها التعريف الذي وضعه القانون، ومن المعلوم أن الفقه والقضاء عادةً يتفادى التسرع في وضع تعاريف للمفاهيم والظاهرة القانونية الجديدة لكونها متطورة وقابلة للتغير فيكون التعريف والحال هكذا بمثابة مجازفة لا تسلم من المخاطر.

المطلب الثاني: أركان الجريمة الالكترونية في النظام السعودي وخصائصها وتصنيفها:

أركان الجريمة الإلكترونية

أولاً: الركن المادي:

ويمثل هذا الركن كيان الجريمة، وهو وجود بيئة رقمية واتصال بالإنترنت ومن خلالها يقوم المجرم المعلوماتي بتحميل الحاسب الآلي ببرامج الاختراق أو إعداده لهذه البرامج المخترقة بصورة يمكن إثباتها كجريمة، وبه يتحقق الاعتداء على المصلحة المراد حمايتها وهذا الفعل يمثل النشاط الذي يصدر عن الجاني مرتكب الجريمة.

ثانيا – الركن المعنوي:

يعبر عن إرادة المجرم المعلوماتي (القصد الجنائي) والعلاقة التي تربطه بماديات الجريمة وشخصيته فلابد أن يرتكب هذا الفعل المجرّم بعلم وإرادته الفعلية طواعية ورغبة وعن إدراك لأهداف التخريبية.(مكاوي،٢٠٢١)

ثالثاً- خصائص الجرائم ذات التقنية العالية وتصنيفاتها:

الفرع الثاني خصائص الجرائم الالكترونية

تتميز الجرائم ذات التقنية العالية بعدة خصائص بحيث أنها تختلف عن الجريمة التقليدية وذلك لارتباطها بتقنية وتكنولوجيا المعلومات، ويمكن توضيح هذه الخصائص كما يلي:

١. أنها من الجرائم الناعمة أي التي لا تتطلب عنفاً كالجريمة التقليدية مثل جرائم السرقة أو الجرائم التي تتطلب احتكاكا مع رجال الشرطة ونعومتها تتمثل في أنها عبارة عن سطو إلكتروني، حيث أن نقل البيانات من حاسب لأخر أو قرصنة حاسوب يتم دون عنف يصعب إثباتها، نسبة لافتقاد الأدلة التي تدل على الجاني وغياب البصمات أو الشواهد التي تتوافر لدى الجرائم التقليدية.

٢. تعتبر من الجرائم العابرة للحدود الدولية (Transnational) فالطفرة في الاتصالات حولت العالم إلى قرية كونية صغيرة، وربطت بين الشعوب المتباعدة، فأصبحت عملية تبادل المعلومات والمعارف سهلة وميسورة فالعالم كله أصبح مربوط بشبكة من الاتصالات عن طريق الأقمار الصناعية والإنترنت مما سهل الجريمة التقنية وانتشارها فهي لا تعرف الحدود بين الدول ولا تعرف مكاناً أو زماناً.

٣. **السرعة في التنفيذ:** أي السهولة في تنفيذ الجريمة ذات التقنية العالية بضغطة زر واحدة يمكن نقل ملايين العملات من مكان لآخر بعد الإعداد لتنفيذها واستخدام البرامج المعينة والمعدات للسرقة الإلكترونية والديمومة المعدات والبرامج المسروقة التي يمكن أن تستخدم لفترة طويلة.

٤. **القيمة:** معلومات بطاقات الائتمان والحسابات المصرفية والتصاميم ذات القيمة.

٥. **الإزالة:** الجريمة الإلكترونية لا تتطلب الإزالة فيمكن نسخها وحذفها فقط.(مكاوي،٢٠٢١)

الفرع الثالث: تصنيف الجرائم ذات التقنية العالية

تختلف الجرائم ذات التقنية العالية عن بعضها البعض باختلاف كيفية التنفيذ، والهدف من الجريمة لذا يمكن تصنيفها حسب التالي:

أولاً: تصنف الجرائم وفقاً لنوع الجريمة ومحلها:

وهذا النوع من الجرائم يشمل نوعين منها ما هو متعلق بالحاسوب أو معلوماته كتشويه البيانات أو إتلافها وذلك عن طريق الفيروسات أو جرائم تقع على ما تمثله المعلومات من

أموال وأصول وتلاعب في المعلومات المخزنة داخل الحاسب الآلي. كذلك الجرائم التي تكون متعلقة بالمتعلقات الشخصية أو الحياة الخاصة بالإنسان كبياناته ومعلوماته مثال الصور والفيديوهات. والجرائم التي تمس الشخص بحقوقه سواء المملوكة له أو الفكرية المتعلقة ببرامج الكمبيوتر وأنظمته أي جملة بمعني قرصنة البرمجيات.

ثانياً: تصنيف حسب المهمة التي قام بها الحاسوب ودوره في الجريمة

وتضم العناصر السرية والنظم كالدخول غير المصرح به وغير القانوني مثل أن يخترق شخص شبكة حواسيب مرتبطة بالأنترنت واختراق نظام الأمن والدخول للمحتويات والكشف عنها. وكذلك العمل على تدمير كل محتويات الجهاز الذي تم الدخول عليه ويقوم الشخص المخترق بدحض البيانات ومسحها أو يعمل على تعطيلها أو تشويشها وتعطيل برامجها لكي يجعلها غير قابلة للاستخدام. والعمل على اعتراض أنظمة الحاسب وعدم معرفة استخدام جهاز الكمبيوتر واستخدامه بسوء أو الإساءة إليه. (الحربي،٢٠٢٠)

ثالثاً – تصنيف حسب الهدف الذي كان من أجله الجريمة أو دوافعه لذلك:

ويكون من هذه الأهداف المعلومات والوصول لهذه المعلومات بطريقة غير شرعية، كذلك بالنسبة للبنوك أو الشركات الكبيرة والحكومات يكون الهدف سرقة المعلومات السرية سواء لهدف سياسي أو من أجل الهدف المادي. كذلك يكون الغرض من أجل تعطيل خادم الذي يوفر المعلومات عن طريق شبكة الأنترنت والتلاعب بها. أيضاً الكسب غير المشروع سواء كان مادي أو معنوي أو سياسي، وذلك إما بالعمل على تزوير البطاقات الائتمانية لسرقة الحسابات البنكية. المطلب الثالث: صور لبعض الجرائم ذات التقنية العالية في المملكة العربية السعودية تتعدد صور الجرائم التقنية وتتفرع كما ذكرنا سابقا في أنواعها، ونحدد في هذا المطلب الجرائم ذات التقنية العالية الأكثر انتشاراً في المملكة العربية السعودية كما يلي:

١. **الجرائم الجنسية والممارسات غير الأخلاقية:** تؤكد عدد من الدراسات أن الجرائم الجنسية والتردد على المواقع الإباحية بصورة متواصلة تتصدر القائمة في المملكة العربية السعودية وهذا يؤدي إلى انحرافات أخلاقية غير مرغوبة وسلوكيات شاذة تضر بالمجتمع، مما يترتب عليه انتشار الجريمة وأن تشيع الفاحشة.

٢. **جرائم الاختراقات أو الدخول غير المصرح به:** (unauthorized access) لموقع إلكتروني أو إلى نظام معلوماتي أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو

لتعديلها، أو يكون الاختراق إما للابتزاز (extortion أو لتهديد شخص، أو لحمله على القيام بفعل أو الامتناع عن فعل ويقع هذا الفعل ضمن التصرفات غير القانونية

٣. **التنصت والتسجيل سواء المرئي أو الصوت:** (wiretapping) زراعة برامج في جهاز المعتدى عليه للاطلاع على محادثاته ومراسلاته.

٤. **الابتزاز:** وهو الحصول على مكاسب مادية أو معنوية عن طريق الإكراه أو التهديد، وتعد خطورة الابتزاز في أن توفر الإنترنت يساعد المبتزين بعدة أوجه (١١)، لأنه يمكنهم من تحديد الهدف نسبة لأن الإنترنت ملئ بالمعلومات التي تساعد على ذلك، كما أنه وسيلة لتهديد الضحية بتهديده بنشر ما لديه من صور أو مستندات أو بيانات سرية أو تسجيلات صوتية وفيديوهات على الشبكة لابتزاز الضحية مقابل طلب تحويل مبالغ مالية أو لحمله على القيام بأفعال مخلة بالآداب العامة وذلك دون معرفة حساب أو هوية المبتز(فريجه،٢٠١١)

المطلب الثالث

إثبات الجرائم الالكترونية في النظام السعودي

يعيش عالمنا المعاصر ثورة علمية ومعرفية هائلة ويشهد تغيرات تكنولوجية واجتماعية متسارعة، مهدت لظهور مجتمع المعرفة الذي تتسابق فيه الدول وتتصارع حول تملك وحيازة أكبر قدر من المعارف والمعلومات، وقد أدى انتشار المعلومات السريع عبر وسائل الاتصال المختلفة إلى تدفق هائل في المعلومات والأخبار والمعارف والأبحاث والرسائل الثقافية، يعجز الإنسان بقدراته العادية عن متابعتها والإلمام بها في عمره القصير

كذلك حدثت طفرة في تقنية المعلومات تمثلت في اختراع الحاسب الآلي الذي أضاف للإنسان قدرات هائلة على الاحتفاظ بالمعلومات ومعالجتها بسرعة خيالية لم تكم تخطر على باله من قبل، وهكذا تتضح إيجابيات الثورة المعلوماتية والتكنولوجية التي جاء بها الحاسب الآلي وقدرتها على تغيير أوجه الحياة إلى الأفضل. غير أن هذه الثورة المعلوماتية ذاتها (per se) تحمل في طياتها بذور الشر المتمثلة في الاستخدام غير المشروع لنظام الحاسب الآلي والوسائط التكنولوجية الأخرى.

حيث ترتب على ذلك أن ظهرت أنواع جديدة من الجرائم الحديثة عالية التقنية تتم من خلال الحاسوب، والتي أصبحت ظاهرة إجرامية جديدة ومستحدثة تقرع أجراس الخطر وتنبه المجتمعات الحديثة لحجم المخاطر والخسائر التي قد تنجم عن جرائم الحاسوب (الجرائم المعلوماتية Cyber Crime)، وهذه الجرائم هي تقنية ناتجة عن استخدام التكنولوجيا الرقمية

كأداة لتحقيق غايات غير قانونية تنشأ في الخفاء ويقترفها أناس أذكياء (hackers) 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 (invasion of privacy) وانتحال الشخصية، والعمل على سرقة الملكية الفكرية، وكذلك سرقة الهويات (identity theft) والإتجار بالمواد الإباحية (pornography) وتسريب المعلومات والمواد الإلكترونية المملوكة للمؤسسات والشركات سواء الحكومية أو الخاصة وتدميرها عن طريق فيروس (virus) وغيرها من الجرائم التي تكون فيها الأجهزة والشبكات المحوسبة مسرحاً أو وسيلة لتنفيذها. حيث اتضح أن جرائم الاختراقات هي الأولى في المملكة العربية السعودية من بين تلك الجرائم والتي أخذت ما نسبته ٥,٦ % لاختراقات مواقع حكومية، و ٣,٥ اختراقات لمواقع تجارية ونتيجة طبيعية لظهور مثل هذه الجرائم التي تسبب ضرراً على الأفراد والمجتمع والبيئة التكنولوجية، أصدر المنظم السعودي نظام مكافحة الجرائم المعلوماتية رقم (م/١٧) بتاريخ ٨/٣/١٤٢٨هـ والمعدل بتاريخ ١٤٣٦هـ.(داوود،٢٠٠٩)

إن إثبات الجرائم ذات التقنية العالية يصعب اكتشافها وإثباتها، وذلك يرجع لخصائص هذه التقنية ذاتها وخاصة السرعة الفائقة التي ترتكب بها، والسمات التي يتصف بها المجرم من حيل وغش عند استخدامه لتقنيات معلوماتية ذات كفاءة عالية، ومحو آثارها وطمسها قبل أن يتم اكتشافها، فالمجرم التقني لا يترك أثراً ملموساً لأنها تتم بتقنيات عالية، والجنات يكونون على مستوى عالي من الذكاء، كما يمكنهم 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 مسألة الإثبات تبقى جد صعبة.

لذا يصعب إثبات 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 حتى يتم الوصول إلى 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 الإثبات 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 غالباً ما يتم الإثبات بتقنية تصوير الشاشة أو الاعتماد على أمر قضائي بمعاينة الصفحة الإلكترونية ومعاينة موضوع القذف أو التشهير وما شابه ذلك.

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 جمعها وتحليلها باستخدام برامج تكنولوجية 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 تحركاته وبعض الأمور الشخصية والعمل على تحليلها في ذات الوقت.(العبيدي،٢٠٠٨)

فنرى أن رؤية المسرح الحقيقي المادي للجريمة والمسرح المعلوماتي الرقمي واستخلاص وسائل الاستدلال يمكن أن تكون ثرية جداً بما تحتويه من معلومات للكشف عن المجرم، لابد أن يتحرى القاضي جيداً عن الأدلة الجرمية الرقمية وان يكون ملماً بالعمليات الإلكترونية.

أن للجرائم ذات التقنية العالية طبيعة خاصة تكمن في أن لشبكة المعلومات قدرة على نقل وتبادل المعلومات، وهذه المعلومات إما أن تكون معلومات ذات طابع شخصي ويكون الاعتداء فيها على الخصوصية، أو معلومات ذات طابع عام. لذا لابد من معرفة كيفية إثبات هذه الجرائم، والنظام القانوني الواجب تطبيقه على كل من يحاول استخدام هذه التقنية لغرض غير مشروع ويحاول التعدي على الآخرين إلكترونياً، فالدول المتقدمة تكنولوجياً مثل المملكة العربية السعودية وضعت قواعد موضوعية لمواجهة الاستخدام غير المشروع للحاسب الآلي والإنترنت، وأجرت 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 تُرتكب فيه الجرائم بالطرق التقليدية وإجراءاتها، والتي ترتكب عن طريق المجابهة بين الأشخاص كالقتل والإيذاء والسرقة، فالقانون الجنائي التقليدي بشقيه الإجرائي والموضوعي) تم وضعه لمكافحة الاعتداءات المادية والمواجهة بين الأشخاص وجهاً لوجه (٢٣) وإثبات الإدانة بإقامة الأدلة التي تثبت وقوع الجريمة.

بيد أن الجرائم التقنية مختلفة عن هذه الجرائم التقليدية، فهي ترتكب في عالم افتراضي (virtual) وعلى مسافات بعيدة؛ ويتطلب وجود بيئة رقمية واتصال بالإنترنت ومعرفة النشاط وما ينطوي عنه، ونتيجته، لذلك يعد الأثبات من أهم التحديات التي تواجه الأجهزة الأمنية فالأثبات هو تأكيد حق متنازع فيه له اثر قانوني بالدليل الذي أباحه القانون لإثبات ذلك الحق وعرفه الدكتور عبد الرزاق السنهوري بقوله (هو إقامة الدليل أمام القضاء بالطرق التي حددها القانون على وجود واقعة قانونية ترتب عليها آثارها وسائل الإثبات فهي كثيرة ومتنوعة منها على سبيل المثال لا الحصر، البيئة 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 إلماماً يعلم معين لإمكان استخلاص الدليل منه، فإن الخبرة تفترض وجود شيء مادي أو واقعة يستظهر منها الخبير، ويعد تقرير الخبير من الأدلة، إما إجراء ندبه فهو إجراءات جمع الأدلة من شأن المعاينة والتفتيش وضبط الأشياء والخبرة تشمل معاينة القاضي وخبرة المتخصصين والمتمرسين في استخدام الحاسب الآلي والإنترنت وغيرها مما يحتاج إلى مزيد من علم ومعرفة وخبرة وتجربة في كثير من المجالات خصوصاً في مجال الإلكترونيات مما لا يستطيع القاضي أو الإنسان العادي معرفتها بمجرد معلوماته العامة.(عبدالحليم،٢٠١١)

المبحث الثاني

الاختصاص القضائي في الجرائم الإلكترونية والعقوبات المقررة في النظام السعودي

المطلب الأول: الاختصاص القضائي في أنظمة الجرائم الإلكترونية في النظام السعودي

نظام الجريمة المعلوماتية: فإننا نجد أن المنظم السعودي قد أناط الاختصاص بنظر الجرائم والمخالفات الوارد النص عليها في هذه الأنظمة إلى المحكمة الجزائية المختصة، وذلك باعتبارها هي المحكمة صاحبة الاختصاص القضائي الأصيل في نظر مثل هذا النوع من الجرائم، وذلك لأن هذه الجرائم تستوجب توقيع عقوبة السجن والغرامة على مرتكبيها. وهو ما يدخل في الاختصاص النوعي للمحكمة الجزائية.[١]

[١] يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية ١- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه. ٢- الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا .٣-الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو

وبنا على ما سبق يرى الباحث أن أول الشروط الواجب توافرها هو اختصاص القضاء الجزائي في التصدي للجرائم والمخالفات الوارد النص عليها في أنظمة الجرائم الإلكترونية، كونه هو المختص ولائياً بنظر هذا النوع من الدعاوى وفقاً لما أورده المنظم بالنص على إحالة الدعاوى والمخالفات الناشئة عن تطبيق أنظمة الجرائم الالكترونية إلى المحكمة الجزائية، بوصفها هي المحكمة صاحبة الاختصاص القضائي الأصيل في نظر مثل هذا النوع من الجرائم.(المنشاوي،١٤٣٤)

وقوع فعل يشكل جريمة وارد النص عليها في أنظمة الجرائم الإلكترونية:

وقوع فعل يشكل جريمة وارد النص عليها في أنظمة الجرائم الإلكترونية من المسلم به أن العقوبة شخصية لا يقضي بها إلا على من تقررت مسؤوليته الجنائية عن الجريمة التي ارتكبها، ومن المسلم به أيضا في التشريعات الجنائية الحديثة أن المسؤولية الجنائية شخصية لا يتحملها إلا من ارتكب الجريمة أو ساهم فيها بوصفه فاعلاً أو شريكاً.

عقد المجلس الأعلى للقضاء الاختصاص للمحاكم الجزائية في نظر الحق الخاص في قضايا القذف والسب والشتم عبر وسائل التواصل الاجتماعي حسماً لتنازع الاختصاص القائم ما بين المحاكم الجزائية واللجنة الابتدائية لنظر مخالفات النشر الإلكتروني السمعي والبصري بوزارة الثقافة والإعلام، والعمل جار في هيئة التحقيق والادعاء العام على إحالة من تثبت إدانته للمحكمة الجزائية لتعزيره وفقاً لما نصت عليه الفقرة (٥) من المادة الثالثة من نظام مكافحة جرائم المعلوماتية، وهذه القضايا غير مشمولة بأنظمة النشر الإلكتروني، إذ نصت الفقرة (٩) من المادة (١٨) من اللائحة التنفيذية لنشاط النشر الإلكتروني على: (مخالفات النشر الإلكتروني مما يوصف بكونه جريمة، وورد بنصه في نظام "مكافحة الجرائم المعلوماتية " تقدم الشكوى فيه لدى الجهات المختصة بنظر تطبيق هذا النظام). ويشهد العمل في المحاكم الجزائية تبايناً بين أصحاب الفضيلة القضاة فمنهم من يقبل نظر الدعاوى والقضايا المتعلقة بالجرائم المعلوماتية ويبت فيها وبعد رفع الأحكام لمحكمة الاستئناف يتم المصادقة عليها، ومنهم من يحكم بصرف النظر عن دعوى المدعي العام والمدعي بالحق الخاص لعدم الاختصاص الولائي ويتم المصادقة على مثل هذا الأحكام من محكمة الاستئناف ايضاً! وأمام هذا التباين في وجهات النظر اضحى نظر "قضايا الجرائم المعلوماتية" خاضعاً للسلطة

إتلافه، أو تعديله، أو شغل عنوانه. ٤- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها.٥- التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة.

التقديرية لناظر القضية ابتداءً وبالتالي فإن الأمر يحتم ضرورة حسم مسألة الاختصاص الولائي في قضايا الجرائم المعلوماتية بشكل واضح وصريح وتوحيد اجراءات نظر قضايا الجرائم المعلوماتية لدى كافة الدوائر الجزائية بالمحاكم الشرعية ومحاكم الاستئناف بالمملكة تحقيقاً للعدالة وإرساءً لقواعد قضائية غير قابلة للتأويل والاجتهاد فالأمل معقود على المحكمة العليا بتقرير مبدأ قضائي واضح وصريح يحسم الاضطراب القائم ويكون ملزماً للمحاكم الجزائية ومحاكم الاستئناف في نظر قضايا الجرائم المعلوماتية ويحسم مادة الخلاف القائم في شأن الاختصاص.(بن هدوب،٢٠١٧)

وضع النظام السعودي قانون وقواعد للحد من الجريمة المعلوماتية **وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، وبما يؤدي إلى ما يأتي:**

١. المساعدة على تحقيق الأمن المعلوماتي.
٢. حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.
٣. حماية المصلحة العامة، والأخلاق، والآداب العامة.
٤. حماية الاقتصاد الوطني.(المادة الثانية من نظام الجرائم المعلوماتية)

المطب الثاني

العقوبات المقررة للجرائم الالكترونية في النظام السعودي

فرض نظام مكافحة الجرائم المعلوماتية السعودي 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 معاً، أو تم توقيع أي منهما بشكل منفرد بقوله أو بإحدى هاتين العقوبتين)، وذلك وفق التوصيف التالي : نصت المادة الثالثة من قانون مكافحة الجرائم المعلوماتية على أنه يعاقب بالسجن مدة أقصاها عام واحد، بالإضافة إلى غرامة مالية لا تتجاوز خمسمائة ألف ريال سعودي، أو بأي من هاتين العقوبتين كل من يرتكب أيا من الجرائم المعلوماتية الآتية : التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوغ نظامي صحيح أو التقاطه أو اعتراضه. الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا. الدخول غير

المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو تشغيل عنوانه. (المنشاوي،١٤٣٤)

تنص المادة الربعة، على أن يعاقب بالسجن مدة لا تتجاوز ثلاث سنوات، وبغرامة مالية حدها الأقصى مليونين ريال سعودي، أو بإحدى هاتين العقوبتين كل من يرتكب أيا من الجرائم المعلوماتية الآتية:

- الاستيلاء للنفس أو للغير على الأموال المنقولة أو تلك التي تكون على سند من جراء الاحتيال أو انتحال أي من الملفات غير الصحيحة أو اتخاذ اسم كاذب.
- التوصل إلى أي من البيانات البنكية أو الائتمانية من دون مسوغ نظامي، أو تلك البيانات التي تتعلق بملكية الأوراق المالية من أجل الحصول على المعلومات أو الأموال أو ما تتضمنه من خدمات.

تنص المادة الخامسة على أن يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد عن ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية الآتية:

- الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.
- إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها أو تعديلها.
- إعاقة الوصول إلى الخدمة، أو تشويشها أو تعديلها، أو تعطيلها بأي وسيلة. تنص المادة السادسة على أن يعاقب بالسجن مدة لا تتجاوز الخمس سنوات، إضافة إلى غرامة مالية حدها الأقصى ثلاثة ملايين ريال سعودي، 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 حرمة 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 من البينات والمعلومات التي 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 سنوات، إضافة 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 وقياداتها أو أعضائها أو العمل على الترويج إليها ولأفكارها أو تمويلها إضافة إلى نشر طريقة إعداد المتفجرات أو أي من الأجهزة أو مختلف الأدوات التي يتم استخدامها في العديد من العمليات الإرهابية.
- الدخول غير المشروع إلى موقع 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 ألا تقل عقوبة السجن أو الغرامة عن نصف حده الأعلى أذا 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 غيره 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 يعاقب كل من يشرع في القيام بأي من الجرائن المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة.

المادة الحادية عشر تنص على أن للمحكمة المختصة أن تعفي من هذه العقوبات كل من يبادر من الجناة بإبلاغ السلطة المختصة بالجريمة قبل العلم بها وقبل وقوع الضرر، وان كان الإبلاغ بعد العلم بالجريمة وتعين للإعفاء أن يكون من شأن الإبلاغ ضبط باقي الجناة في حال تعددهم، أو الأدوات المستخدمة في الجريمة.

– الخاتمة:

بعد دراستنا لموضوع الاختصاص القضائي للجرائم الالكترونية وفقاً للنظام السعودي وذلك بالوقوف على الاختصاص القضائي في المملكة العربية السعودية والجرائم الالكترونية وفقاً للنظام السعودي وذلك حماية للمجتمع من هذه الهجمات وما ورد في النظام بهذا الخصوص فقد توصلنا للعديد من النتائج ولكن قبل عرضها لابد من توضيح أن ما تم التوصل إليه من نتائج متعلقة من إثبات الجرائم الالكترونية تشكل صعوبة لأنها متغيرة ومتطورة لان التقنية دائما تتشكل بشكل كبير في هذا العالم الافتراضي وبصورة مهولة.

أولاً: النتائج:

١. أن المنظم السعودي قد أناط الاختصاص بنظر الجرائم والمخالفات الوارد النص عليها في هذه الأنظمة إلى المحكمة الجزائية المختصة.
٢. لكي تستقيم الحياة لابد من توفر الوعي الكافي للبعض والتعرف على جميع أنواع تلك الجرائم ومواكبة تطورات العصر وخاصة ما يحدث من تطورات مرتكبي الجرائم ذات التقنية العالية.
٣. يجب العمل والاشتغال على معالجة أي خلل قد يحدث ثغرة قد تؤدي بتلك الجرائم أو خللاً بالمجتمع، لذا لابد من العمل على توعيته بصورة دائمة وتثقيفية بالوسائل والطرق التي يستخدمها مجرمي التقنية.
٤. يعد إثبات الجرائم الالكترونية من أهم التحديات التي تواجه الأجهزة الأمنية فإثبات هذه الجرائم أمر يستلزم الكثير من الجهد والخبرات الفنية المتدربة على أعلى المستويات والطرق التي يستخدمها مجرمي التقنية
٥. أن المنظم السعودي حدد الاختصاص المكاني الذي يطبق فيه نظام الجريمة الالكترونية على الجرائم التي تقع من موفر الخدمة داخل المملكة.

٦. أنه يشترط لاختصاص القضاء الجنائي بنظر الجرائم والمخالفات في الجرائم الالكترونية أن تكون هذه الجرائم والمخالفات قد ورد النص عليها صراحة في هذه الأنظمة، واعتبر المشرع كل من يرتكب أي منها مستحقاً لعقاب معين ورد النص عليه كذلك في نصوص التجريم الواردة في هذه الأنظمة، وذلك تطبيقاً لمبدأ الشرعية الجنائية الذي يقضي بأنه " لا جريمة بغير بنص".

ثانياً: التوصيات:

يقترح الباحث على المنظم السعودي وهو في بداية تطبيق القضاء المتخصص في المملكة أن يبادر إلى إنشاء نيابات متخصصة (جهات تحقيق)، وكذلك إنشاء دوائر قضائية متخصصة بنظر الجرائم والمخالفات الناشئة عن عقود الجرائم الالكترونية بوجه عام، وأن يتم اختيار أعضاء النيابة العامة والقضاة المتخصصين في هذه الدوائر.

يقترح الباحث على الجهات ذات الاختصاص القضائي في المملكة بضرورة الاهتمام بتدريب رجال الضبط الجزائي والأشخاص المنوط بهم عملية الضبط في الجرائم والمخالفات المتعلقة بأنظمة الجرائم الالكترونية

المراجع:

أحمد، جمال زين العابدين أمين (٢٠٢١م)، الاختصاص القضائي وإجراءات التحقيق في الجرائم الالكترونية: دراسة مقارنة، مجلة مستقبل العلوم الاجتماعية، المجلد (٤)، العدد (١).

ينظر لسان العرب، لابن منظور (١٨٣/٢)

ينظر مفردات ألفاظ القرآن للأصفهاني، ص٢٨٤.

سورة الأنفال الآية (٢٥).

ينظر شرح مختصر ابن الحاجب، للأصفهاني (٢٣٥/٢).

سلامة ، مأمون محمد: ينظر الإجراءات الجنائية في التشريع المصري.

الغامدي، ناصر بن محمد: ينظر الاختصاص القضائي في الفقه الإسلامي، مع بيان التطبيق الجاري في المملكة العربية السعودية.

العتيبي، معجب بن معدي الحويقل (١٤١٣ هـ). حقوق الجاني بعد صدور الحكم في الشريعة، الرياض، مطبعة سفير.

عباس، عمرو حسين (٢٠١٠)، ادلة الاثبات الجنائي والجرائم الالكترونية (المعلوماتية)، مجلة الحق التي يصدرها اتحاد المحامين العرب مجلة فصلية، العدد الاول، السنة ٣٧، القاهرة،٢٤/٢٦ابريل – نيسان.

العبيدي، اسامة بن غانم (٢٠٠٨)، جرائم الحاسب الآلي والانترنت: الصعوبات التي تعترض المكافحة، دورية الادارة العامة التي يصدرها معهد الادارة العامة، مجلد ٤٨، العدد الأول، الرياض، محرم ١٤٢٩هـ/يناير.

العمري، عادل عبد الله خميس (٢٠١٣)، التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، مجلد٢٢، العدد٣.

نظام مكافحة جرائم المعلوماتية لسنة ١٤٢٨هـ، المادة الاولى فقرة (٨)

مكاوي، محمد محمد (٢٠٢١)، الجرائم ذات التقنية العالية والحماية من الجهات الإلكترونية في النظام السعودي، مجلة الاجتهاد القضائي، المجلد (١٣)، العدد (١)

الحربي، مبارك بن عبيد (٢٠٢٠م)، جرائم المعلوماتية والقيم الواقعة منها في النظام السعودي: دراسة استقرائية وصفية، مجلة العلوم الشرعية واللغة العربية، العدد (٩)، جامعة الامير سطام بن عبد العزيز

حسين، فريجه (٢٠١١) الجرائم الالكترونية والانترنت، مجلة المعلوماتية، العدد٣٦، اكتوبر.

داود ، حسن طاهر (٢٠٠٩)، جرائم نظم المعلومات ،مركز الدراسات والبحوث بأكاديمية نايف العربية للعلوم الامنية ،الرياض.

العبيدي ، اسامة بن غانم(٢٠٠٨)، جرائم الحاسب الآلي والانترنت: الصعوبات التي تعترض المكافحة، دورية الادارة العامة التي يصدرها معهد الادارة العامة، مجلد ٤٨، العدد الاول، الرياض، محرم ١٤٢٩هـ/يناير.

عبدالحليم، عواطف محمد عثمان (٢٠١٠)، جرائم المعلوماتية (تعريفها، صورها، جهود مكافحتها)، مجلة العدل التي تصدرها وزارة العدل السودانية، العدد٢٤، السنة ١٠، الخرطوم

حسين، فريجه (٢٠١١) الجرائم الالكترونية والانترنت، مجلة المعلوماتية، العدد٣٦، اكتوبر.

المنشاوي ، محمد بن عبدالله بن علي (١٤٣٤)، جرائم الانترنت في المجتمع السعودي، أطروحة ماجستير، قسم العلوم الشرعية، أكاديمية نايف للعلوم الأمنية، الرياض، ١٤٣٤هـ

بن هدوب، خالد (٢٠١٧م)، تنازع اختصاص نظر قضايا الجرائم المعلوماتية، جريدة الرياض، https://www.alriyadh.com/

– المادة الثانية من نظام الجرائم المعلوماتية الصادر بتاريخ ١٤٢٨/٣/٨هـ الموافق ٢٠٠٧/٣/٢٧م من المرسوم الملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨، قرار مجلس الوزراء رقم ٧٩ بتاريخ ٧ / ٣ / ١٤٢٨.

المنشاوي، محمد بن عبدالله بن علي (١٤٣٤) جرائم الانترنت في المجتمع السعودي، أطروحة ماجستير، قسم العلوم الشرعية، أكاديمية نايف للعلوم الأمنية.